Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 1–39

Michio Suzuki

Koichiro Harada

§1. Biographical Sketch

1926, October 2. Born in Chiba, Japan.

1942, April. Entered the Third High School of Japan located at Kyoto (Noboru Ito, Katsumi Nomizu, Hidehiko Yamabe were his seniors by one year and Singo Murakami was in the same class).

1945, April. Entered the University of Tokyo. Majored in mathematics. (Gaishi Takeuchi, Nagayoshi Iwahori, Tsuneo Tamagawa were friends of this period.)

1948, April. Entered the Graduate School of Tokyo University. Suzuki's supervisor was Shokichi Iyanaga. Kenkichi Iwasawa had a profound influence on Suzuki.

1948-'51. Received a special graduate fellowship from the Government of Japan.

1951, April to '52, January. Held a lecturership at Tokyo University of Education

1952, January to '52, May. Held a graduate fellowship at University of Illinois at Urbana-Champaign.

Received April 27, 1999.
Revised May 17, 1999.

1952, May. Received the Doctor of Science Degree from the University of Tokyoin absentia.

1952. Spent two months in the summer at University of Michigan. R. Brauer was a professor of Mathematics at Michigan. J. Walter, W. Feit were graduate students there.

1952, September to '53, May. Held a post-doctoral fellowship at University of Illinois at Urbana-Champaign.

1952, November. Married to a daughter Naoko of Yasuo Akizuki (then Professor at Kyoto University).

1953, September to '55, May. Held a research associateship at University of Illinois.

1955, September. Promoted to an assistant professor at University of Illinois.

1956, September to '57, May. Held a research associateship at Harvard University.

1958, September. Promoted to an associate professor at University of Illinois.

1959, September. Promoted to a full professor at University of Illinois.

1960. Discovered a new series of finite simple groups $Sz(q)$.

1960-'61. Held a visiting appointment at the University of Chicago.

1962. Invited to speak at the International Congress of Mathematicians in Stockholm.

1962-'63. Held a Guggenheim Fellowship.

1962, September to '63, May. Held a membership at the Institute for Advanced Study, Princeton.

1967. Discovered a sporadic simple group *Suzuki* of order 448,345,497,600.

1968-'69. Held a visiting appointment at the Institute for Advanced Study, Princeton, NJ.

1970. Invited to speak at the International Congress of Mathematicians in Nice, France.

1974. Received the Academy Prize from the Japan Academy.

1987. The conference of group theory and combinatorics for the occasion of Suzuki's 60th birthday was held in Kyoto, Japan.

1991. Awarded an honorary doctoral degree from the University of Kiel, Germany.

1997. The conference of group theory and combinatorics for the occasion of Suzuki's 70th birthday was held in Tokyo, Japan.

1998, May 31. Died at the age of 71. (Evariste Galois died on May 31, 1832.)

(A cancer was discovered in his liver early in February, 1998. Left for Japan. Received the same diagnosis. Stayed in the hospital (February 12 - March 13), at a Guest House of the International Christian University (March 14 - April 17). Back to hospital on April 18.)

June 7: Funeral Service at the International Christian University, Mitaka, Japan.

September 18: Memorial Service at the University of Illinois, Urbana, Illinois.

§2. The early work of Michio Suzuki

Among Suzuki's earliest research papers are:

[2] On the finite group with a complete partition, 1950.

[5] A characterization of simple groups $LF(2,p)$, 1951.

[6] On finite groups with cyclic Sylow subgroups for all odd primes, 1955.

In [2], Suzuki investigates the structure of a finite group G having a partition by its subgroups $H_i, i = 1, \dots, n$:

$$G = \bigcup_{i=1}^{n} H_i, H_i \cap H_j = 1 \text{ if } i \neq j.$$

A partition of G is called complete if H_i is cyclic for all $i = 1, \dots, n$. The research on groups having a complete partition goes back at least to P. Kontorovich [Sur la representation d'un groupe fini sous la forme d'une somme directe de sous-groupes, I. Rec. Math. (Mat. Sbornik), 5 (47) (1939), 283–296].

In [2] Suzuki considers groups having a complete partition. Examples of such groups are $PGL(2,q)$ and $PSL(2,q)$ where q is a power of a prime. In [2], however, Suzuki determines only nonsimple groups having a complete partition. It is shown first that if G is a nonsimple, nonsolvable finite group with a complete partition then a minimal normal subgroup N of G is of index 2. The proof proceeds by induction on the order of G, since the complete partitionability carries over to its subgroups and even to its factor groups as Suzuki shows.

Suzuki next shows that the Sylow 2-subgroups of G are dihedral, and that for any odd prime p, any two distinct Sylow p-subgroups of G have a trivial intersection. He then uses a counting argument to obtain a configuration in which the group G is a sharply triply transitive permutation group acting on the coset space G/M where M is a suitable subgroup of G obtained in the counting argument mentioned above. Therefore Suzuki is able to use the result of Zassenhaus [Kennzeichnung endlicher linearer Gruppen als Permutationsgruppe, Hamb. Abh., 11(1936), 17–40], who had classified, among other results, all such permutation groups, hence the theorem:

Theorem. *Let G be a nonsimple, nonsolvable finite group with a complete partition. Then G is isomorphic to the full linear fractional group $PGL(2,q)$ where q is a power of an odd prime.*

Character theory is not used in [2]. This paper shows that Suzuki was a young mathematician of foresight. He was able to recognize the importance of the groups $PSL(2,q)$ and Zassenhaus' work. The concept of a group having a partition does not appear to be very important on its own right, but it should be mentioned that the infinite series of new simple groups $Sz(q)$ discovered by Suzuki in 1960 does have a partition, though not a complete partition. Suzuki completes the classification of all (semi) simple groups with a partition in 1961 [18].

As for the paper [5], let us first observe that the subgroups of the simple groups $PSL(2,p)$ for a prime p are of the types: (1) metacyclic groups; (2) the alternating group A_4 of degree 4; (3) the symmetric group S_4 of degree 4; or (4) the alternating group A_5 of degree 5. In [5], Suzuki characterizes $PSL(2,p)$ by this property.

Let G be a finite simple group such that all of its subgroups are of types (1)-(4) mentioned above. Suzuki first shows that G possesses a complete partition in the sense of the paper [2]. Among all papers of Suzuki, the theory of exceptional characters first appeared here in [5]. Using this theory and Brauer's work on a group whose order is divisible by a prime to the first power, Suzuki was able to show that G possesses an irreducible character of degree $\frac{1}{2}(p \pm 1)$ for some prime p. He next applies a result of H.F. Tuan [On groups whose orders contains a prime number to the first power, Ann. of Math., 45(1944), 110–140] to complete the characterization of $PSL(2,p)$.

As he recognized the importance of studying the simple groups $PSL(2,q)$, he began doing research on them from various points of view : in [2] as groups having a partition, in [5] as groups having only a special set of isomorphism classes of subgroups, etc.

Although the papers [2] or [5] of Suzuki might perhaps not be among his better works, if they are considered as stand-alone papers, the line of research in this direction served him well and it culminated in the discovery of the simple groups $Sz(q)$ and the classification of all Zassenhaus groups (which was completed by a joint effort of Zassenhaus, Feit, Ito and Suzuki).

The paper [6] is also part of Suzuki's continuing efforts to understand the simple groups $PSL(2,p)$. Its content is fully explained in the title. Its introduction begins with 'The purpose of this paper is to determine the structure of some finite groups in which all Sylow subgroups of odd order are cyclic.The assumption on Sylow subgroups simplifies the structure of groups considerably, but the structure of 2-Sylow subgroups might be too complicated to make any definite statement on the structure of the groups. In this paper, therefore, we shall make another assumption on 2-Sylow subgroups, $\cdots$'.

In fact, he assumes that the Sylow 2-subgroups of G are either (a) dihedral or (b) generalized quaternion. The Sylow 2-subgroups of $SL(2,p)$ are, as is well known, generalized quaternion if p is odd. Suzuki shows that the group G contains a normal subgroup $G_1 = Z \times L$ of index at most 2 such that $L \cong PSL(2,p)$ if (a) holds, and $L \cong SL(2,p)$ if (b) holds. Moreover, Z is a group of odd order all of whose Sylow subgroups are cyclic. Frobenius and Burnside treated groups such that all of their Sylow subgroups are cyclic and showed that all such groups are solvable, in fact all such groups are metacyclic. Zassenhaus classified all solvable groups with the same assumption on Sylow subgroups for odd primes but with the weaker assumption for the prime 2 that a Sylow 2-subgroups has a cyclic subgroup of index 2.

§3. Theory of exceptional characters

'Perhaps the first mathematician of the post war generation who mastered Brauer's work in group theory was M. Suzuki. He came to the United States in the early fifties and he has made many significant contributions to the theory of simple groups (from W. Feit [R.D. Brauer, Bull (New Series). Amer. Math. Soc., 1(1979), 1–20])'.

Having begun his research on exceptional characters in [5], Suzuki wrote a couple of papers on the subject [13], [19], and several papers in which the theory played a crucial role [6], [8], [9], [10], [17].

In his work on the theory of modular representations, Brauer defined the concept of an exceptional character. Brauer and Suzuki independently extended this concept of exceptional characters at about the same time, around 1950. Although the basic assumption of the theory can be loosened from the one given below, we will show it in the simplest but most important setting.

We are typically interested in a finite group G having an abelian subgroup A such that the centralizer of every nonidentity element of A is contained in A (hence it is equal to A itself and A is a maximal abelian subgroup of G). The simple group $PSL(2,q)$ contains a couple of conjugacy classes of such abelian subgroups. For Suzuki, a motivation to extend the theory of exceptional characters must have come from his investigation of the simple group $PSL(2,q)$. Under this condition on G and on A, the following conditions hold:

(1) A is an abelian TI subgroup of G: i.e. $A \cap A^g = A$ or 1 for every element g of G.

(2) The normalizer $N = N_G(A)$ of A in G is a Frobenius group.

Let $l = [N : A]$ and $w = \frac{|A|-1}{l}$. Then G possesses exactly w conjugacy classes of elements represented by nonidentity elements of A.

The Frobenius group N possesses l irreducible characters of degree 1, all of which contain A in their kernels. In addition to those linear characters, N possesses w irreducible characters not containing A in their kernels, and all of them have degree l. Those are all the irreducible characters of N. Thus N possesses exactly $l + w$ irreducible characters.

We can actually obtain the irreducible characters of N of degree l as follows. Let $\{\psi_i, i = 1, \dots, w\}$ be the complete set of representatives of N-orbits (by conjugation) consisting of nonidentity irreducible characters of A and $\Psi_i = \psi_i^N$ be the corresponding induced character of ψ_i to N. By computing the inner product directly, we see that Ψ_i is an irreducible character of N for all i. We thus obtain w irreducible characters of N of degree l. The remaining irreducible characters of N (of degree 1) will appear as constituents of the induced character of the trivial character of A.

Let $\Psi_i^G, i = 1, \dots, w$ be the corresponding induced characters to G. We compute that $\Psi_i^G(g) = 0$ if g is not conjugate to an element of $A\backslash 1$ and $\Psi_i^G(g) = \Psi_i(a)$ if g is conjugate to an element a of $A\backslash 1$. Thus

$$\langle \Psi_i^G, \Psi_i^G \rangle_G - (\Psi_i^G(1))^2 = \langle \Psi_i, \Psi_i \rangle_N - (\Psi_i(1))^2.$$

Therefore, the norm $||\Psi_i^G||_G$ is almost determined by the norm $||\Psi_i||_N$, but not completely so since $\Psi_i^G(1)$ is an unknown number. If we can find a way to eliminate the ambiguity then it will be nice.

Now assume, in addition to (1) and (2) mentioned above:

(3) $w \geq 2$.

Consider the generalized character $\Psi_i - \Psi_j, i \neq j$, of N. Then we obtain

$$||\Psi_i^G - \Psi_j^G|| = 2$$

since $||\Psi_i^G - \Psi_j^G||_G = ||\Psi_i - \Psi_j||_N = 2$ holds. Therefore, $\Psi_i^G - \Psi_j^G = \epsilon_{ij}(\Theta_i - \Theta_j)$ where Θ_i, Θ_j are irreducible characters of G and $\epsilon_{ij} = \pm 1$. Actually ϵ_{ij} is independent of i, j and so

$$\Psi_i^G - \Psi_j^G = \epsilon(\Theta_i - \Theta_j), \ \epsilon = \pm 1.$$

This implies that

$$\Psi_i^G = \epsilon\Theta_i + \Delta$$

where Δ is a generalized character of G independent of $i = 1, \dots, w$.

The irreducible characters $\Theta_i, i = 1, \dots, w$ obtained above are called *exceptional characters* of G associated with A. (W. Feit was able to extend the exceptional character theory by dropping the condition that A is abelian. Feit still needed that A is nilpotent and is not isomorphic to a certain type of p-group. A further extension was obtained by D. Sibley.)

Exceptional characters satisfy the following properties. Let D be the set of all elements of G not conjugate to any element of $A\backslash 1$.

(I) $\Theta_i(\sigma) = \Theta_j(\sigma)$ if $\sigma \in D$ for every pair i, j. In particular all exceptional characters Θ_i have the same degree.

(II) The exceptional characters are linearly independent on the conjugacy classes $\{C_1, \dots, C_w\}$ of G represented by the elements of $A\backslash 1$: i.e. if $\sum_{i=1}^{w} a_i\Theta_i(\sigma) = 0$ for all $\sigma \in \cup_{i=1}^{w} C_i$, then $a_i = 0$ for all $i = 1, \dots, w$.

(III) If B is another abelian subgroup of G not conjugate to A but satisfying the same property as A does, then the exceptional characters for A are nonexceptional characters for B.

Therefore if G has many nonconjugate abelian subgroups of the same property, then the majority of the irreducible characters of G will be exceptional characters associated with some abelian subgroup A. Using those irreducible characters, one can obtain strong numerical conditions on the order of G.

§4. The CA-paper of Suzuki

Theorem ([8]). *Let G be a finite simple group such that the centralizer of every nonidentity element is abelian. Then the order of G is even.*

Let us quote Thompson first:

'A third strategy (or was it a tactic ?) in OOP (Odd Order Paper) attempted to build a bridge from Sylow theory to character theory. The far shore was marked by the granite of Suzuki's theorem on CA-groups, flanked by W. Feit, M. Hall, Jr. and J.G. Thompson [Finite groups in which the centralizer of any non-identity element is nilpotent, Math. Z., 74(1960), 1–17]. The bridge was built of tamely embedded subsets with their supporting subgroups and associated tau (τ) isometry. The near shore was dotted with the E-theorems and the uniqueness theorems.

... ...

Suzuki's CA-theorem is marvel of cunning. In order to have a genuinely satisfying proof of the odd order theorem, it is necessary, it seems to me, not to assume this theorem. Once one accepts this theorem as a step in a general proof, one seems irresistibly drawn along the path which was followed. To my colleagues who have grumbled about the tortuous proofs in the classification of simple groups, I have a ready answer: find another proof of Suzuki's theorem (from J.G. Thompson [Finite Non-Solvable Groups, in Group Theory:essays for Philip Hall, Academic Press, (1984), 1–12])'

Now let G be a finite group such that the centralizer of every non-identity element is abelian. Let us call such a group G a CA-group. Already in 1920's, it was known that every CA-group is either solvable or simple (L. Weisner [Groups in which the normalizer of every element except the identity is abelian, Bull. Amer. Math. Soc., 31(1925), 413–416]). So let us assume that our CA-group G is nonabelian and simple.

Let g be a nonidentity element of G. Then the centralizer $A = C_G(g)$ is a proper abelian subgroup of G. Let $1 \neq h \in A$. Then $C_G(h) \supset A$. The fact that $C_G(h)$ is abelian forces the equality $C_G(h) = A$, thus A is a maximal abelian subgroup of G, and A is a TI-set. The rudiments of group theory also show that A is a Hall subgroup of G, i.e. $\gcd(|G : A|, |A|) = 1$. If the normalizer $N = N_G(A)$ is equal to A itself, then $N_G(P) = C_G(P)$ for a Sylow p-subgroup P of A for some prime p. Since P is a Sylow p-subgroup of G also, Burnside's theorem implies that G is nonsimple. Thus $N > A$ and N is a Frobenius group. In order to apply the exceptional character theory effectively, we need one more condition : $w \geq 2$ where $w = \frac{|A|-1}{l}, l = [N : A]$. For this purpose, we henceforth assume that G is of odd order as this is the case Suzuki treats. Then $|A|$ and l are both odd, and so w can not be equal to 1. Hence $w \geq 2$ as desired.

Let $\{A_i, i = 1, \dots , n\}$ be a complete set of representatives of the conjugacy classes of maximal abelian subgroups of G and we put $N_i = N_G(A_i)$. We have shown that $N_i > A_i$ and N_i is a Frobenius group for all i. Moreover, every element of $G\backslash 1$ has a representative in $\cup_{i=1}^{n} A_i$.

Since each A_i is a TI-set, we have

$$|G| = 1 + \sum_{i=1}^{n} [G : N_i](|A_i| - 1).$$

Each A_i gives rise to $w_i = +(|A_i| - 1/l_i)$ (where $l_i = [N_i : A_i]$) exceptional characters and so G has $\sum_{i=1}^{n} w_i$exceptional characters in total. On the other hand, G possesses precisely $1 + \sum_{i=1}^{n} w_i$ conjugacy classes. Therefore every nonidentity irreducible character of G is exceptional for some A_i. Suzuki puts all of this information together and starts a counting argument. In three pages, he is able to reach a contradiction.

This CA-paper of Suzuki was received by the editors on December 24, 1954 but was published in 1957. Suzuki knew who was the referee. It was none other than R. Brauer. Apparently Brauer did not understand some argument of Suzuki and left it there for a (great) while. Suzuki submitted a revised version two years later and the paper was published soon.

'At the time its importance was not fully grasped, either by him or by others, as it seemed to be simply an elegant exercise in character theory. However, the result and the methods used had a profound impact on much succeeding work (W. Feit [Obituary written for Michio Suzuki, Notices of Amer. Math. Sci., Vol. 46(1999)]).'

L. Redei [Ein Satz über die endlichen einfachen Gruppen, Acta. Math., 84(1950), 129–153] considered finite simple groups such that every proper subgroup of every maximal subgroup is abelian. He showed that the alternating group of degree 5 is the only such group of even order. One obtains, as a corollary to the main theorem of this paper, that there is no such group of odd order. Moreover, Suzuki proved that the word *abelian* in Redei's theorem can be replaced by *nilpotent* to assert the same conclusion.

Suzuki uses the assumption that G is of odd order only to assert $w \geq 2$ and so this method can go farther under a suitable assumption. In fact, R. Brauer, M. Suzuki, and G.E. Wall, more or less independently proved:

Theorem. *If the centralizer of every element of a finite group G is abelian then either G is solvable or G is isomorphic to $PSL(2, 2^n)$.*

In the published form of the Brauer-Suzuki-Wall Theorem [9], however, it is stated as follows:

Theorem. *Let G be a group of even order which satisfies the condition:*
(1) *If two cyclic subgroups A and B of even order of G have a nontrivial intersection then there exists a cyclic subgroup C of G that contains both A and B.*
(2) $G = [G, G]$.
Then $G \cong PSL(2, q)$ for some prime power q.

One of my colleagues, Ronald Solomon, and I studied the latter theorem but could not conclude that it implies the former. We wrote a letter of inquiry to G.E. Wall, who replied that they worked fairly independently with not a great deal of communication between them. He says also that the BSW paper (published version) was written by R. Brauer who did not have enough time to weld together three rather different versions and that the CA-groups of even order are not covered in any obvious way (in the published version), but they are covered in the 'behind scenes' BSW versions.

§5. Zassenhaus groups

Let V be a 2-dimensional vector space over a field K and let

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL(V)$$

be a 2×2 matrix of nonzero determinant with entries in K. The matrix A acts on V as a linear transformation and so the image of a line (1 dimensional subspace of V) is again a line. Since the structure of $GL(V)$ depends only on the dimension of V and the field K, we write $GL(2, K)$ for $GL(V)$ also.

Let $P_1(K)$ be the set of all lines of V. $GL(2, K)$ acts on $P_1(K)$. The scalar matrices $A = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$ are the only matrices that act trivially on $P_1(K)$. Denote by Z the set of all scalar matrices of $GL(2, K)$. Then the factor group $PGL(2, K) = GL(2, K)/Z$ acts on $P_1(K)$ faithfully.

If $\{u_1, u_2\}$ and $\{v_1, v_2\}$ are any pairs of linearly independent vectors of V, then there is an element $g \in GL(2, K)$ such that $g(u_1) = v_1, g(u_2) = v_2$. This implies that $PGL(2, K)$ is doubly transitive on $P_1(K)$ since if $[u]$ denotes the line spanned by the vector $u \in V$, then $\bar{g}([u_1]) = [v_1], \bar{g}([u_2]) = [v_2]$ where $\bar{g}$ is the image of $g \in GL(2, K)$ in $PGL(2, K)$.

Put $SL(2, K) = \{g \in GL(2, K) \mid \det g = 1\}$ and $PSL(2, K) = SL(2, K)/Z \cap SL(2, K)$. As is easily seen, $PSL(2, K)$ is also doubly transitive on $P_1(K)$. Let us consider subgroups of $G = SL(2, K)$ that leave points of $P_1(K)$ invariant. Let $\{[u_1], [u_2]\}$ be a set of two arbitrary elements of $P_1(K)$. We want to know the structure of the two point stabilizer $G_{\alpha,\beta}; \alpha, \beta \in P_1(K), \alpha \neq \beta$. Since G is doubly transitive, we may assume $\{\alpha = [(1,0)], \beta = [(0,1)]\}$ and we find

$$G_{\alpha,\beta} = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}, \alpha \in K \right\}.$$

In particular, $G_{\alpha,\beta}$ is cyclic. If in addition, $g \in G_{\alpha,\beta}$ fixes a third point, then $g = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ and so every three point stabilizer in $\bar{G} = PSL(2, K)$ is trivial.

Definition. A permutation group G acting on a finite set Ω is called a Zassenhaus group, if
(1) G is doubly transitive on Ω,
(2) the identity element is the only element of G that leaves three distinct points of Ω invariant; and,
(3) G does not have a regular normal subgroup.

Remark. Let G be a permutation group on a finite set Ω. If a subgroup H of G acts transitively on Ω and $|H| = |\Omega|$, then H is called a regular subgroup of G.

As shown above, $G = PSL(2, K)$ acting on $P_1(K)$ is an example of a Zassenhaus group if $|K| \geq 4$. Let G be a Zassenhaus group acting on Ω and let $\alpha \in \Omega$. Then the one point stabilizer $H = G_\alpha$ of α is a transitive but not regular permutation group on $\Omega \backslash \alpha$ such that a two point stabilizer of H on $\Omega \backslash \alpha$ is trivial and so H is a Frobenius group. By Frobenius' theorem, the identity element and the set of all elements of H that do not leave any letter of $\Omega \backslash \alpha$ invariant forms a normal subgroup K of H. Let $C = H_\beta = G_{\alpha,\beta}$. Then H is a semi-direct product of K and C.

Zassenhaus was the first person to study a group having the property described in the definition above. In the paper [op.cit.], Zassenhaus determined the structure of G under some additional assumptions (see below). What Zasssenhaus did was to define an algebraic structure called a *near field* from the one point stabilizer H of G. He then used the structure of G to show that the near field is almost a field. He next constructed a suitable geometry of projective lines over a field and determined the structure of G.

In the paper [Über endliche Fastkörper, Hamb. Abh., 11(1936), 187–220], Zassenhaus was able to determine all near fields of finite order.

This implies that he completely determined all sharply doubly transitive permutation groups.

The complete classification of all Zassenhaus groups was carried out by a combined effort of H.Zassenhaus, W. Feit, N. Ito, and M. Suzuki.

Theorem (H. Zassenhaus [op.cit.]). *Let G be a Zassenhaus group on Ω. Suppose that G is triply transitive on Ω. Then $G \cong PGL(2,q)$, or $PGL^*(2,q^2)$.*

Here $G = PGL^*(2,q^2)$ is a group which is uniquely defined as follows. G contains a normal subgroup of index 2 isomorphic to $PSL(2,q^2)$ and the Sylow 2-subgroups of G are semi-dihedral.

Theorem (H. Zassenhaus [op.cit.]). *Let G be a Zassenhaus group on Ω. Suppose $|G| \geq |\Omega|(|\Omega|-1)(|\Omega|-2)/2$, then $G \cong PGL(2,q)$, $PGL^*(2,q^2)$, or $PSL(2,q)$.*

Theorem (W. Feit [On a class of doubly transitive permutation groups, Ill. J. Math., 4(1960), 170–186]). *Let G be a Zassenhaus group on Ω. Then the Frobenius kernel K of a one point stabilizer $H = G_\alpha$ is a p-group for some prime p. Furthermore if K is abelian, then G is contained in $PGL(2,q)$ or $PGL^*(2,q^2)$ as a normal subgroup of index at most 2.*

With this theorem of Feit, every researcher of the time must have conjectured that every Zassenhaus group is isomorphic to $PSL(2,q)$, $PGL(2,q)$ or $PGL^*(2,q^2)$ where q is a power of a prime p. N. Ito soon settled the cases in which the Frobenius kernel K is a p-group for an odd prime p.

Theorem (N. Ito [On a class of doubly transitive permutation groups, Ill. J. Math., 6(1962), 341–352]). *Let G be a Zassenhaus group on a set of $n+1$ letters. If n is odd, then the Frobenius kernel K of a one point stabilizer $H = G_\alpha$ is abelian (and so the structure of G is determined by Zassenhaus and Feit).*

Therefore the Zassenhaus groups on an even number of letters are now completely classified. Namely, they are isomorphic to

$$PSL(2,q), PGL(2,q) \text{ or } PGL^*(2,q^2), q \text{ odd } > 3.$$

Note that if $q = 3$, then $PSL(2,3)$ and $PGL(2,3)$ have a regular nórmal subgroup. I should mention here that the theorems of Feit and Ito stated above both use the fundamental result proved by Thompson, who solved affirmatively the long standing conjecture: the Frobenius kernel is nilpotent.

We are now left with the case in which $p = 2$ or equivalently $|\Omega| = 1 + 2^n$ for some n. We, however, need a new section to describe this case.

§6. Suzuki's simple groups $Sz(2^n)$

The late '50s must have been an exciting period for young (and old) group theorists, although the competition among them must have been intense also. In 1955, C. Chevalley [Sur certains groupes simples, Tohoku J. Math., 7(1955), 14–66] announced the discovery of several series of new simple groups of finite order. These simple groups are defined using Lie algebras over the ring of integers. The paper of R. Steinberg [Variations on a theme of Chevalley, Pacific J. Math., 9(1959), 875–891] followed, in which he defined several twisted versions of the Chevalley groups and showed that these twisted groups are also simple except for a few cases. After these theorems of Chevalley and Steinberg, no new simple groups were expected to come out from Lie theory.

Suzuki surprised the world by discovering a new series of simple groups, which were soon identified as groups coming from Lie theory, though they were not initially defined as such. These are now known as Suzuki groups $Sz(q)$ where q (≥ 8) is an odd power of 2. $Sz(q)$ is an example of a Zassenhaus group but it was, according to Suzuki, not discovered as a Zassenhaus group.

Groups such that the centralizer of every nonidentity element of G is abelian were all determined by late in the '50s. Feit, M. Hall, and J.G. Thompson [op.cit.] showed, in 1960, that all simple CN-groups (Centralizer-Nilpotent) are of even order. The next problem that Suzuki decided to treat was the determination of all (simple) CN-groups. In doing so, he discovered a new series of simple groups, which turned out to be Zassenhaus groups.

Let $F = F_q$ be a finite field with $q = 2^{2n+1}$ $(n \geq 1)$ elements and set $r = 2^{n+1}$. We have $r^2 = 2q$ and the mapping

$$\theta \,:\, \alpha \to \alpha^r$$

is an automorphism of F and it satisfies $\theta^2 = 2$. In other words,

$$\alpha^{\theta^2} = \alpha^2, \quad \alpha \in F$$

holds. Moreover, we define, for arbitrary elements α, β of F, a 4×4 matrix (α, β) and a subset Q as follows:

$$(\alpha,\beta)=\begin{pmatrix}1&0&0&0\\ \alpha&1&0&0\\ \alpha^{1+\theta}+\beta&\alpha^{\theta}&1&0\\ \alpha^{2+\theta}+\alpha\beta+\beta^{\theta}&\beta&\alpha&1\end{pmatrix},$$
$$Q=Q(q)=\{(\alpha,\beta)\mid\alpha,\beta\in F_q\}.$$

Since the product is

$$(\alpha,\beta)(\gamma,\delta)=(\alpha+\gamma,\ \alpha\gamma^{\theta}+\beta+\delta),$$

Q is a subgroup of order q^2. Let us define, for an element k of the multiplicative groups F^* of the field F, a matrix (k) by:

$$(k)=\begin{pmatrix}\zeta_1&&&0\\ &\zeta_2&&\\ &&\zeta_3&\\ 0&&&\zeta_4\end{pmatrix},$$

where

$$\zeta_1^{\theta}=k^{1+\theta},\quad \zeta_2^{\theta}=k,\quad \zeta_3=\zeta_2^{-1},\quad \zeta_4=\zeta_1^{-1}.$$

If we set

$$K=K(q)=\{(k)\mid k\in F^*\},$$

then, K is a cyclic group of order $q-1$ and is isomorphic to F^*. Since

$$(k)^{-1}(\alpha,\beta)(k)=(\alpha k,\beta k^{1+\theta}),$$

the set theoretical product QK is a subgroup and Q is a normal subgroup of QK. If $k\neq 1$, then the conjugation by the matrix (k) does not leave any element of $Q\backslash 1$ invariant. Let us define another matrix τ as follows:

$$\tau=\begin{pmatrix}0&&&1\\ &&1&\\ &1&&\\ 1&&&0\end{pmatrix}.$$

We have $\tau^2=1$ and, $(k)^{\tau}=(k)^{-1}$.

Denote the subgroup of $GL(4,F)$ generated by $Q(q)$, $K(q)$, τ by:

$$Sz(q)=\langle Q(q),\ K(q),\ \tau\rangle.$$

The family $Sz(q)$ are called Suzuki's simple groups and form an infinite series of new simple groups of finite order. $Sz(q)$ has the following properties:

(1) $|Sz(q)| = q^2(q-1)(q^2+1),\ q = 2^{2n+1},\ n \geq 1.$

(1′) $|Sz(q)|$ is not divisible by 3.

(2) $Sz(q)$ has cyclic subgroups A_+, A_- of order $q \pm r + 1$ respectively and

$$Sz(q) = \underset{g \in G}{\cup}(Q^g \cup K^g \cup A_+^g \cup A_-^g)$$

is a union of subgroups of $Sz(q)$ such that any pair of subgroups have trivial intersection unless they coincide. ($Sz(q)$ has a *partition.*)

(3) If g is an arbitrary nonidentity element of $Sz(q)$, then the centralizer of g in $Sz(q)$ is always nilpotent. ($Sz(q)$ is a CN-group.)

(4) The natural action of $Sz(q)$ on its factor space $Sz(q)/QK$ is doubly transitive and the identity of $Sz(q)$ is the only element that leaves three distinct points of $Sz(q)/QK$ invariant. ($Sz(q)$ is a Zassenhaus group.)

Apparently it was a great surprise to many that the order of $Sz(q)$ is not divisible by 3: it was believed that every nonabelian simple group has order divisible by 6. All the generators $\{(\alpha, \beta),\ (k),\ \tau\}$ of $Sz(q)$ given above leave the bilinear form

$$x_1y_4 + x_2y_3 + x_3y_2 + x_4y_1$$

invariant and so $Sz(q)$ is a subgroup of the 4 dimensional symplectic group $Sp(4, q) = B_2(q)$. The group $B_2(q)$ has a special involutory automorphism σ only if q is an odd power of 2, and

$$Sz(q) = \{g \in B_2(q) \mid g^\sigma = g\}$$

holds. Therefore, $Sz(q)$ could have been constructed naturally through Lie theory. It was, however, discovered by Suzuki in a process of classifying all CN-groups (an important step to determine all Zassenhaus groups), which is independent of Lie theory. W. Feit told me that he, when he was young, uttered the following words to a famous Lie theorist

"It is better to have a good mathematician than a good theory !"

Although the discovery was purely group theoretic, for classification purpose, however, $Sz(q)$ can better be accounted for as a simple group of Lie type and is often denoted by ${}^2B_2(q)$.

Just before Suzuki announced the discovery of a new series of simple groups, he published a two-part paper:

[11] On characterizations of linear groups, I, II, 1959.

Suzuki published two more papers on the same theme.

[23] On characterizations of linear groups, III, 1962.

[32] On characterizations of linear groups, IV, 1968.

In [11, Part I], Suzuki proves:

Theorem. *Let G be a simple group such that the centralizer of every involution is abelian. Then $G \cong PSL(2, 2^n)$.*

The assumption Suzuki actually uses is slightly more general so that he can use induction. The simple group $PSL(2, 2^n)$ does have this property. In fact, $PSL(2, 2^n)$ has the property that the centralizer of every involution is an abelian 2-group. In 1951, K.A. Fowler showed that this property characterizes $PSL(2, 2^n)$. There is a generalization of Fowler's result by Brauer, Suzuki, and Wall. Suzuki puts the characterization of $PSL(2, 2^n)$ in its final shape.

Already in 1900, Burnside gave the following characterization of $PSL(2, 2^n)$.

Theorem (Burnside). *$PSL(2, 2^n)$ is the only simple group of even order such that the order of every element is either odd or equal to 2.*

This result of Burnside had been completely forgotten and was rediscovered by K.A. Fowler half a century later. It is quite surprising that Burnside worked on this relatively modern problem, considering the fact that the line of research did not continue until it was taken up again much later.

In [11, Part II], Suzuki studies the structure of $G = PGL(3, q)$ where $q = 2^n$. G is simple if $3 \not| q-1$. If $3 | q-1$, then G has a normal subgroup of index 3. For example $PSL(3, 4)$, which has the same order as A_8, is a normal subgroup of index 3 of $PGL(3, 4)$. Every involution of G is conjugate to

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

and the centralizer of I in G has order $q^3(q-1)$. In $PSL(3, 4)$, the centralizer of I has order 2^6, hence it is a 2-group.

In this paper, Suzuki shows that $PGL(3, q)$ is characterized by the structure of $C_G(I)$ except for one case when $q = 2$, in which case we obtain $G \cong PGL(3, 2)$ or $G \cong A_6$. A similar characterization of $PGL(3, q)$ where q is a power of a prime satisfying $q \equiv -1 \pmod 3$ was obtained by R. Brauer. With the initial work of Brauer and Suzuki's work that followed, the characterizations of simple groups by the centralizers of involutions began in full force and continued until early in the 1970's.

$C_G(I)$ is isomorphic to the subgroup of G consisting of all matrices of the form:

$$M(\alpha,\beta,\gamma,\delta)=\begin{pmatrix}1&0&0\\ \alpha&\delta&0\\ \beta&\gamma&1\end{pmatrix}$$

where $\alpha,\beta,\gamma,\delta\neq 0$ are elements of a finite field F of characteristic 2.

The matrix product shows

$$M(\alpha,\beta,\gamma,\delta)M(\alpha',\beta',\gamma',\delta')=M(\alpha^*,\beta^*,\gamma^*,\delta^*)$$

where

$$\alpha^*=\alpha+\delta\alpha',\beta^*=\beta+\gamma\alpha'\beta',\gamma^*=\gamma\delta'+\gamma',\delta^*=\delta\delta',$$

Suzuki computes the order of the group G in [11, Part I]. In [11, Part II] he also obtains the order of the group G. Namely $|G|=q^3(q-1)(q+1)(q^3-1)$ in this case. Here also, he uses the exceptional character theory. It is shown that there are elementary abelian subgroups P and L of order q^2 in a Sylow 2-subgroup Q of G. P and L are not conjugate in G. Moreover, G acts doubly transitively on the set $\mathfrak{P}$ consisting of all conjugates of P and also on the set $\mathfrak{L}$ consisting of all conjugates of L. The normalizer $N_G(P)$ of P is of index q^2+q+1 in G and so $|\mathfrak{P}|=q^2+q+1$. The same assertion holds for $\mathfrak{L}$. Suzuki calls the elements of $\mathfrak{P}$ points and the elements of $\mathfrak{L}$ lines. An incidence relation can be defined on the pair $(\mathfrak{P},\mathfrak{L})$ by saying that $P_1\in\mathfrak{P}$ is incident to $L_1\in\mathfrak{L}$ if and only if $P_1\cap L_1\neq 1$. Suzuki next shows that the geometry so defined on $(\mathfrak{P},\mathfrak{L})$ is Desarguesian using Gleason's result. This completes the characterization.

At the time of writing [11], Suzuki was only a year away from discovering $Sz(q), q=2^n$. If we compare his notation for $M(\alpha,\beta,\gamma,\delta)$ of $PGL(3,2^n)$ and their product, and the corresponding quantities (α,β), etc. of $Sz(2^n)$ which is a subgroup of $PGL(4,2^n)$, it appears that Suzuki had good practice in $PGL(3,2^n)$ before he discovered his new simple groups.

§7. ZT-groups and related classification theorems

Suzuki proved several fundamental classification theorems. I will make comments on some of them.

[17] Finite groups with nilpotent centralizers, 1961.

Let us call a finite group G a CN-group, as Feit-Hall-Thompson and then Suzuki did, if the centralizer of every nonidentity element of

G is nilpotent. Let us review some of the results mentioned in the preceding sections. K.A. Fowler investigated the structure of nonsolvable groups with the property that the centralizer of every involution is an abelian 2-group and showed that $PSL(2, 2^n)$ is the only family of simple groups having the property. Suzuki and Wall independently showed that $PSL(2, 2^n)$ is the only family of nonsolvable CA-groups.

Suzuki, in one of his famous papers [8], showed that every simple CA-group is of even order and Feit-Hall-Thompson extended this result to CN-groups: every nonabelian simple CN-group is of even order. Therefore, Suzuki is able to assume that his CN-group G is of even order and so G contains an involution. To classify all CN-group of even order, Suzuki gives another definition: a group G is a CIT-group if the centralizer of every involution is a 2-group.

Suzuki shows that nonsolvable CN-groups are CIT-groups and devotes his efforts to classify all nonsolvable CIT-groups. The property that the group G satisfies CIT is obviously hereditary to all subgroups and even to all sections of G (though a bit of work is necessary to show it), so by using induction on the order of G one can assume that all proper subgroups are of known type.

Theorem ([17]). *A finite group G is a nonabelian simple CIT-group if and only if G is isomorphic to one of the following groups*:
(i) *a Zassenhaus group of odd degree* (*called a ZT-group by Suzuki*),
(ii) $PSL(2, p)$ *where p is a Fermat prime or Mersenne prime,*
(iii) $PSL(2, 9)$,
(iv) $PSL(3, 4)$.

Therefore, all CIT-groups will be classified if all Zassenhaus groups of odd degree are determined. Zassenhaus groups of even degree had already been classified by Zassenhaus, Feit and Ito. Suzuki himself completes the classification for the even degree cases. In this paper [17], Suzuki claims to have shown that if the order of a Zassenhaus group G of odd degree is divisible by 3, then G is isomorphic to $PSL(2, 2^n)$. As already remarked in §6, Suzuki's simple group $Sz(2^n)$ has order not divisible by 3. Later Thompson and Glauberman treated simple groups of order not divisible by 3 and showed that $Sz(q)$ is the only family of simple groups with this property. Therefore, apart from $Sz(q)$, all simple groups have order divisible by 6. Although he writes in the introduction of this paper [17] that only fragmentary results are known for the general Zassenhaus groups of odd degree, he himself finishes the problem before the paper actually went to press. If we use this result (published later), we obtain, as a corollary, that every nonsolvable CIT-group is a CN-group.

Skimming through the paper [17], we can see that all the important classification results that Suzuki later shows are already presented here in their preliminary mode. For example,

Theorem. *A Zassenhaus group of odd degree is a nonabelian simple CIT-group.*

Theorem. *A nonsolvable CN-group is a CIT-group.*

Theorem . *Let G be a CIT-group and S a Sylow 2-group of G. Assume that Sylow 2-groups of G are independent* (*i.e. a TI set*)*. Then we have one of the following:*
(i) *S is normal,*
(ii) *S is cyclic,*
(iii) *S is a generalized quaternion group, or;*
(iv) *G is a Zassenhaus group of odd degree.*

[21] On a class of doubly transitive groups, 1962.

In this paper, the class of finite groups called Zassenhaus groups is completely determined. Classified also are all simple CN-groups. This paper published in the Annals of Mathematics is one of Suzuki's major results. It is memorable to me personally also. As a student at the University of Tokyo in the middle of 1960s, I read this paper in a series of group theory seminars.

Suzuki acknowledges in the introduction of [21] that G. Higman's result on 2-groups is essential for the completion of this work.

Theorem (G. Higman). *Let Q be a 2-group which admits a cyclic group of automorphisms transitive on the set of involutions. Assume that Q is not abelian and contains $q-1$ involutions. If $q > 2$, then Q satisfies the following properties:*
(i) *Q is of exponent* 4, (ii) *the order of Q is either q^2 or q^3, and;* (iii) *if the order of Q is q^2, then Q is isomorphic with one of the groups $S(q;x)$.*

Here the 2-group $S(q;x)$ is defined as follows. Let F be the field GF(q) of q elements where q is a power of 2 ; $q = 2^n$. Let x denote an automorphism of the field F such that $x \neq 1$ and $\alpha^{1+x} = 1$ implies $\alpha = 1$.

Consider the matrices over F of the form

$$(\alpha,\beta)=\begin{pmatrix}1&&\\ \alpha^x&1&\\ \beta&\alpha&1\end{pmatrix}.$$

The product of two matrices is written as

$$(\alpha,\beta)(\gamma,\delta)=(\alpha+\gamma,\alpha\gamma^x+\beta+\delta).$$

Now define

$$S(q;x)=\{(\alpha,\beta)|\alpha,\beta\in F\}.$$

Then $S(q;x)$ is a 2-group of order q^2. The mapping:

$$\psi(\zeta):(\alpha,\beta)\ \rightarrow\ (\zeta\alpha,\zeta^{1+x}\beta)$$

is an automorphism of $S(q;x)$ that fixes no nonidentity element of $S(q;x)$ unless $\zeta=1$. Therefore $S(q;x)$ admits a fixed-point-free automorphism group Z of order $q-1$. Since Z is isomorphic to the multiplicative group of F, Z is cyclic also.

Now assume

(i) G: a Zassenhaus group acting on Ω such that $|\Omega|=1+N$ with N odd,

(ii) $H=G_\alpha$: the subgroup of G consisting of elements fixing a symbol $\alpha\in\Omega$,

(iii) Q: a Sylow 2-subgroup of H,

(iv) K: the subgroup consisting of elements fixing two symbols α and β,

(v) τ: an involution in $N_G(K)$.

Q is a normal subgroup of H and H is a semi-direct product of Q and K. One can prove that τ inverts every element of K, and so K is abelian and hence cyclic.

Suzuki proves:

Proposition. *Q contains two elements σ and ρ such that σ is an involution, σ is a certain power of ρ and:*

$$\tau\sigma\tau=\rho^{-1}\tau\rho,$$

$$\rho^{-1}(\sigma\tau)\rho=(\sigma\tau)^2.$$

Moreover, σ and ρ are unique if H,K, and τ are chosen and fixed.

Suzuki calls the identity obtained in the proposition above the *structure identity* of G. Firstly the case: $\sigma = \rho$ is treated. By counting the number of real elements, Suzuki shows that $|G| = N(N+1)(N-1)$. Therefore G is a sharply triply transitive permutation group. That $G \cong PSL(2, 2^n)$ follows from a theorem of Zassenhaus.

Assuming $G \ncong PSL(2, N)$, Suzuki continues his counting argument for real elements. He shows that if $q-1$ is the number of involutions of Q then $|Q| = q^2 = N$ and $|G| = q^2(q-1)(q^2+1)$. The rest of the paper is devoted to the proof of the uniqueness of the structure of G and that $G \cong Sz(q)$. A very subtle argument involving the structure identity is necessary to show the required uniqueness.

[24] Two characteristic properties of (ZT)-groups, 1963.

In this paper, Suzuki raised the following question: Suppose a proper subgroup H of even order of a finite group G contains the centralizer of every nonidentity element. Then what can we say about the structure of G?

Suzuki shows that if G is not a Frobenius group, then G is a Zassenhaus group of odd degree and H is either a Sylow 2-subgroup or the normalizer of a Sylow 2-subgroup of G.

Note that G is a special case of a group having a *strongly embedded* subgroup. Suzuki had been faithful to Brauer's program, and characterized quite a few simple or almost simple groups by the centralizers of involutions. Suzuki, however, went farther and began to form a concept of a strongly embedded subgroup, which was to be taken up seriously by H. Bender soon.

'The name of Michio Suzuki was forever engraved in my mind when in 1964 Bernd Fischer, who had just become an assistant of Reinhold Baer at Frankfurt, handed me a paper by Suzuki to be studied and presented in Baer's seminar. That paper [23] lies at the intersection of two main streams of Suzuki's work:

(1) Characterize the known simple groups by the centralizer of an involution. (2) Determine doubly transitive permutation groups with a regular fixed point behavior, especially Zassenhaus groups, and Suzuki-transitive groups (the stabilizer of a point has a normal subgroup regular on the remaining points). (H. Bender [Obituary written for Michio Suzuki, Notices of Amer. Math. Soc., Vol.46(1999)).'

We have come to the paper:

[27] On a class of doubly transitive groups, II, 1964.

Having put an end to the classification of all Zassenhaus groups, Suzuki began extending his results to a larger class of simple groups.

He considers:

$(*)$ G is a permutation group on a finite set Ω and the one point stabilizer G_α, for every $\alpha \in \Omega$, contains a normal subgroup acting regularly on the remaining points $\Omega \backslash \alpha$.

If a group G satisfies the condition $(*)$ (Bender calls such a group a Suzuki-transitive group), then G is doubly transitive on Ω. Zassenhaus groups satisfy the condition. In addition to Zassenhaus groups, there is another family of groups that satisfy $(*)$. Let $SU(3,q^2)$ be the totality of all unitary matrices of determinant 1 defined over the field E with q^2 elements. We have $|SU(3,q^2)| = q^3(q^2-1)(q^3+1)$. The group $SU(3,q^2)$ can also be defined as the set of all matrices of determinant 1 that leave the following form invariant.

$$\psi(\vec{x},\vec{y}) = x_1 y_3^q + x_2 y_2^q + x_3 y_1^q.$$

If we define

$$J = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

then

$$SU(3,q^2) = \{A | \bar{A}^t J A = J, det A = 1\}.$$

The subgroup Z consisting of all scalar matrices of $SU(3,q^2)$ is a cyclic group of order $(3, q+1)$. Define $PSU(3,q^2) = SU(3,q^2)/Z$.

Let Ω be the set of all points $\vec{x} = [x_1, x_2, x_3]$ on the projective plane $P^2(q^2)$ such that $\psi(\vec{x},\vec{x}) = 0$. We have $|\Omega| = q^3 + 1$ and $PSU(3,q^2)$ acts doubly transitively on Ω. Moreover, the one point stabilizer has a normal subgroup Q acting regularly on the remaining points.

More precisely, the stabilizer $H = G_\alpha$ of $\alpha = [0,0,1] \in \Omega$ in $G = PSU(3,q^2)$ contains a normal subgroup Q of order q^3 consisting of the projective images of the matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ b & 1 & 0 \\ d & -b^q & 1 \end{pmatrix}, \ b^{1+q} + d + d^q = 0.$$

Q acts regularly on the remaining points $\Omega \backslash \alpha$. Equivalently, G is Suzuki-transitive on the coset space $G/N(Q)$.

To state the main theorem of [27] we need one more assumption:

$(**)$ $|\Omega|$ is odd and the order of the two point stabilizer $G_{\alpha,\beta}$ is odd (hence $G_{\alpha,\beta}$ is solvable).

Suzuki shows that if G satisfies $(*)$, $(**)$ and G is simple, then G is isomorphic to a ZT-group or $PSU(3, q^2)$. Nonsimple cases are also treated by Suzuki. With the completion of this paper [27], Suzuki began to shift his attention to a general classification theorem. But let me make a comment on the following first:

[18] On a finite group with a partition, 1961.

Although he published the paper [1] on the lattices of subgroups of a finite group a little earlier, Suzuki, early in the 1950s, began his mathematical career by investigating finite groups having a partition [2]. For example, the nonsolvable groups $PGL(2, q), PSL(2, q)$ admit a partition. This problem or its solution did not appear to have much impact on finite group theory itself. Suzuki, however, did not lose his interest in the subject. The discovery of $Sz(q)$ by himself and the fact that the Suzuki groups admit a partition must have given him an added impetus to pursue the subject.

I did not make any comments on this subject in §2 and so let us come back to Suzuki's first love again. Throughout this paper, the idea of R. Baer [Partitionen endlicher Gruppen, Math. Z., 75(1961), 333–372] is used and it is so acknowledged.

Repeating the definition given in §2, if a finite group G can be expressed as a union of subgroups U_i with the property $U_i \cap U_j = 1$ if $i \neq j$, then we say G admits a partition:

$$G = \bigcup_{i=1}^{n} U_i, \ \ U_i \cap U_j = 1 \text{ if } i \neq j.$$

In other words, we say G has a partition if every nonidentity element of G is contained in one and only one subgroup in the collection $\{U_i, i = 1, \dots, n\}$. Of course, we, in principle, exclude the cases in which $G = U_i$ or $U_j = 1$ for some i, j. For example, if $\{U_i\}$ is the totality of all maximal cyclic subgroups of $PSL(2, q)$, then it gives a partition of $PSL(2, q)$. The partition of a group G is not necessarily unique. For example, one can use the Sylow p-subgroups of $PSL(2, q)$ where $q = p^n$ for a prime p as members of the set $\{U_i\}$ instead of using cyclic subgroups of the Sylow p-subgroups.

Every subgroup H of G has an induced partition by taking $V_i = H \cap U_i$ and throwing away some unnecessary V_j, provided that $H \not\subset U_i$ for any i.

If $\{U_i\}$ and $\{W_i\}$ are both partitions of G and if for every j, there is an i such that $W_j \subset U_i$, then $\{W_i\}$ is called a *refinement* of $\{U_i\}$. If all conjugates of every member of a partition U_i are again members of $\{U_i\}$, then we say the partition $\{U_i\}$ is *normal.* If a partition $\{U_i\}$ admits no nontrivial refinements, then it is called *minimal.*

Let us see how things unfold.

Lemma. *Every partition has a refinement which is normal.*

In fact, every minimal partition is normal. All one has do is to refine a given partition until it becomes minimal.

Lemma. *If a nontrivial partition $\{U_i\}$ is normal, then the normalizer $N(U_i)$ of each component U_i is larger than U_i unless G is a Frobenius group.*

Suppose $N(U_i) = U_i$ and the partition $\{U_i\}$ is normal. Then the permutation representation of G on $\Omega = G/U_i$ gives rise to a Frobenius group.

Lemma. *If $N(U_i) \neq U_i$, then U_i is nilpotent.*

Let $U = U_i$, $N = N(U)$ and assume $N > U$. Let H be a subgroup of N containing U such that $[H : U] = p$ where p is a prime. The subgroup H admits an inherited partition from G. Thus $H = U \cup (\cup V_j)$ where j ranges over some index set. Since $U \cap V_j = 1$, we have $|V_j| = p$ and $H = V_j U$. In other words, every element of $H \backslash U$ is of order p. If U is a p-group then of course it is nilpotent. Suppose not. Then the subgroup $H_p(H)$ generated by the elements of H which do not have order p is a proper subgroup of H. Hence U is an H_p-group in the sense of Hughes-Thompson [The H_p-problem and the structure of the H_p-groups, Pacific J. Math., 9(1959), 1097–1102]. Hughes and Thompson proved that $H_p(G) = 1, H_p(G) = G$ or $[G : H_p(G)] = p$ and so $H_p(H) = U$ in our case. Kegel [Die Nilpotenz der H_p-Gruppen, Math. Z., 75(1961), 373–376] proved that all H_p-groups are nilpotent. Hence U is nilpotent.

Thus we only need to treat groups having nilpotent partitions, i.e. all components U_i are nilpotent. Baer has shown that if G possesses a nontrivial nilpotent normal subgroup and a nilpotent partition, then G is solvable.

Let N be the largest nilpotent normal subgroup of G. Suppose first that $|N|$ is divisible by two distinct primes. Then N must be contained in one of the components of the partition since every nilpotent group having a nilpotent partition is a p-group. Call the component U that contains N. Since our partition $\{U_i\}$ is normal, $U = N$ must hold. If no element of $G \backslash N$ commutes with any nonidentity element of $N \backslash 1$, then

G is a Frobenius group and N is the Frobenius kernel. In particular, N is a Hall subgroup of G and the centralizer in G of every nonidentity element of N is nilpotent. Therefore, if the centralizer of some element of N is not nilpotent, then some element x of $N\backslash 1$ commutes with an element of $G\backslash N$.

Suzuki analyses this case carefully and eventually proves:

Theorem. *Let G be a non-solvable group with a nilpotent partition. If the centralizer of some involution is not nilpotent, then G is isomorphic with $PGL(2,q)$, q odd.*

Theorem. *Let G be a non-solvable group with a nilpotent partition. If the centralizer of every involution is nilpotent, then G is isomorphic with either $PSL(2,q)$ or $Sz(q)$.*

The major portion of this paper is devoted to the proof of the following theorem.

Theorem. *If G is a nonsolvable group having a normal nilpotent partition, then $|G|$ is even.*

Had Suzuki used the result of Feit-Thompson (which was not available when Suzuki wrote this paper), then this 14 pages paper would have been less than half its length. As in his paper [8], exceptional character theory is the key tool to prove that $|G|$ is even.

Therefore Suzuki has shown that there is no semi-simple group having a partition other than the groups $PGL(2,q), PSL(2,q)$ or $Sz(q)$, thus fulfilling his 'Jugendtraum'. Let us again come back to the main stream of simple group theory.

[28] Finite groups of even order in which Sylow 2-subgroups are independent, 1964.

Theorem. *Suppose that G is a nonabelian simple group satisfying the property that any two distinct Sylow 2-subgroups have only the identity element in common. Then G is isomorphic to $PSL(2,q), PSU(3,q^2)$ or $Sz(q)$ where q is a power of 2.*

[30] Finite groups in which the centralizer of any element of order 2 is 2-closed, 1965.

Theorem. *Let G be a finite nonabelian simple group such that the centralizer of any element of order 2 has a normal Sylow 2-subgroup. Then G is isomorphic to one of the simple groups $PSL(2,p)$; p a Fermat or Mersenne prime, $PSL(2,9)$; $PSL(2,q)$, $Sz(q)$, $PSU(3,q^2)$, or $PSL(3,q)$, q a power of 2.*

The theorems stated above show Suzuki's path from the permutation group theoretic results proved in [21] and [27] to general results which can readily be used for the classification of all simple groups of finite order. In [28] Suzuki reduces to the case in which the group G satisfies the condition of Suzuki-transitive groups, and then applies the main result of [27]. Therefore the characterization method used in [28] was still via the permutation group theory.

In the bibliography of [30], however, something new, which Suzuki had never before used, appeared. [D.G. Higman and J.E. McLaughlin, Geometric ABA-groups, Illinois J. Math., 5(1961), 382–397] and [J. Tits, Theoreme de Bruhat et sous-groupes paraboliques, C.R. Acad. Sci. Paris, 254(1962), 2910–2912] were the new papers required.

In order to prove the theorem stated above, we can assume that there is a pair of Sylow 2-subgroups which have a nonidentity element in common, since otherwise all such simple groups have been treated in [28]. The rest of the proof of the main theorem of [30] divides into two cases.

(i) Sylow 2-subgroups have cyclic center,
(ii) Sylow 2-subgroups have noncyclic center.

If the case (i) holds, Suzuki shows that G is isomorphic to $PSL(2,p)$ where p is a Fermat or a Mersenne prime, or $PSL(2,9)$. If the case (ii) holds, Suzuki shows that G possesses a Bruhat decomposition with its Weyl group isomorphic to the symmetric group of degree three and applies Higman-McLaughlin [op.cit.] to conclude $G \cong PSL(3,q)$, here also q is a power of 2.

Suzuki states, in Introduction, that the main theorem of the paper [30] will give an independent proof of some of the results he obtained earlier. For example, his classification of the CIT-groups is not used in [30]. Not used also are the characterizations of $PSL(3,2^n)$ and of $PSU(3,2^n)$ in terms of the centralizer of an involution. Moreover, he makes a remark that this paper is entirely group theoretic and free from the theory of characters. It is as though Suzuki is announcing to the world that he has at last cut himself off from the bondage of character theory and found a new tool.

In his paper [30], one can see the path in its primitive form, which the classification of all finite simple groups later followed. Case (ii) lead

Suzuki to the groups with BN-pairs and Case (i) and (the case in which any pair of Sylow 2-subgroups have only the identity element in common) lead him to the groups where the prime 2 is more or less isolated (or 2-nonconnected).

This dichotomy was to be followed later for an odd prime p also. In one case, we have a proper subgroup H of G such that H contains a Sylow p-subgroup of G and all its p-local subgroups (the normalizers of p-subgroups). Therefore, H is isolated (with respect to the prime p) in the group G. In the other case, there are no such subgroups and so G is connected through p-local subgroups and their intersections. Hence, for example, some graph or geometry can be associated with G. Bender took up the case in which the prime 2 is nonconnected. He first classified all doubly transitive permutation groups in which no involution stabilizes a point, and then classified all transitive permutation groups in which every involution stabilizes exactly one point. This latter result had a far reaching application for the classification of all finite simple groups. Suppose we are in the latter case and let H be the stabilizer of a point $\alpha \in \Omega$ and let t be an involution of H. Then every element in $C_G(t)$ fixes α and so $C_G(t) \subset H$. In fact, one can show also that the normalizer of every nontrivial 2-subgroup of H is contained in H. Such a proper subgroup H was to be called a strongly embedded subgroup. Bender was able to classify all simple groups having a strongly embedded subgroup.

Although Suzuki must have had his own idea of classifying all finite simple groups, [30] was to become his last general classification theorem. The world of finite group theory was changing rapidly. The solvability of all groups of odd order (Burnside's Conjecture) was shown to hold by Feit and Thompson (1963). Janko found new sporadic simple groups, later named $Janko_1$, $Janko_2$, $Janko_3$ (1965, 1968). The simple groups $Conway_1$, $Conway_2$, $Conway_3$ and $Fischer_1$, $Fischer_2$, $Fischer_3$ were to be discovered soon. The signalizer functor method of Gorenstein-Walter was shaping up. A new generation of young group theorists was coming of age. Stars and superstars were emerging into the field. The middle to the late '60s (and perhaps to early in the '70s) was the period of turbulence for finite group theory. This was also the golden era of group theory.

Suzuki wrote a number of papers whose titles contain the phrase 'Characterization of Linear Groups'. Let us pick up another paper and discuss it briefly.

[35] Characterization of linear groups, 1969.

This is an expanded and improved version of Suzuki's one hour address delivered at one of the AMS meetings in 1967. The purpose is to characterize the simple group $PSL(n, q)$ in terms of the centralizer of an involution.

The theme of this research direction was initiated by Brauer's address at the International Congress of Mathematicians held in 1954. As for $PSL(n, q)$, Brauer himself did the characterization when $n = 2, 3$ and with some restriction on q. A great many papers followed Brauer's. Suzuki himself treated a large number of cases in which q is even.

In this paper, Suzuki talks about its history, which is short but quite readable. He mentions that the following doublets or triplets share the isomorphic centralizer of an involution.

$$(PSL(2,7), A_6), (PSL(3,3), Mathieu_1), (A_{4m}, A_{4m+1}),$$

$$(Janko_2, Janko_3), (A_{12}, A_{13}, S_6(2)), (PSL(5,2), Mathieu_5, Held).$$

There are no examples of four or more simple groups that have isomorphic centralizers of an involution.

In [35], Suzuki proves:

Theorem. *The simple group $PSL(m, 2^n)$ is characterized by the centralizer of an involution in the center of a Sylow 2-subgroup if $m \geq 6$ or $n > 1$.*

The remaining cases not treated in Suzuki's theorem had already been taken care of by others and Suzuki himself.

I believe that I have covered most of his contributions to the theory of finite groups except for his work on subgroup lattices [1], [3], [4] and [7]. For these papers I have too limited a knowledge to make any reasonable comments. I do add that Bender cites Suzuki's work on subgroup lattices as one of the reasons for the honorary degree he received from Kiel University, Germany. Skimming through the list of publications of Suzuki again, I find, however, that there are a few more papers that I should make comments on.

[12] On finite groups of even order whose 2-Sylow subgroup is a quaternion group, 1959.

In this paper, Brauer and Suzuki prove: Let G be a group of finite even order. If the 2-Sylow group P of G is a quaternion group (ordinary or generalized), then G is not simple. The proof is (modular) character theoretic. Groups having a cyclic Sylow 2-subgroup cannot be simple either as had been known since the turn of the century. Therefore if P is a Sylow 2-subgroup of a simple group of even order, then P must contain a Klein's four group ($\cong Z_2 \times Z_2$). We say P is of 2-rank at least two. There are examples of 2-groups of rank two which can be a Sylow 2-subgroup of a simple group. The Brauer-Suzuki theorem was the modern starting point of the classification theorems that dealt with simple groups having Sylow 2-subgroups of low 2-rank.

[34] A simple group of order 448,345,497,600 (1969).

Suzuki made big news with the discovery of a sporadic simple group *Suzuki* of order 448,345,497,600, which was announced in 1967.

Janko's second group $Janko_2$ was constructed by M. Hall using the idea of transitive extensions of rank 3. Other constructions of rank 3 extensions followed. Sporadic simple groups *McLaughlin*, $Fischer_1$, $Fischer_2$, $Fischer_3$, and *Higman-Sims* are examples. Starting from the simple group of Lie type $H = G_2(4)$, Suzuki constructed a rank 3 transitive extension of H of degree 1782.

[38], [39], [41], [44] Gunron (Japanese), 1977, 1978; Group Theory (translation of [38], [39]), 1982, 1986.

Suzuki began writing this book late in the 1960s. Aschbacher, who was at Illinois as a postdoc, says that Suzuki was giving group theory lectures from a draft of that book. It was nearly a 20 year effort from the draft until the completion of its translation.

§8. Group theory in Japan before Suzuki

Michio Suzuki lists Shokichi Iyanaga as his adviser and says that Kenkichi Iwasawa also had a profound influence on him. Let me discuss group theory in Japan before Suzuki briefly.

Let k be a number.field and K/k be its absolute class field: i.e. the Galois group of the abelian extension K/k is isomorphic to the ideal class group of k. It was conjectured by D.Hilbert that every ideal of k extends to a principal ideal of K. This is called the Principal Ideal Theorem. Artin reformulated it into a group theoretical problem (see below). Furtwängler (1930) solved the conjecture affirmatively after a complicated computation and Iyanaga gave a simple proof (1934). (I looked at the Furtwängler's proof. It was indeed complicated. Magnus also published a short proof in 1934. As for the proof of the Principal Ideal Theorem, see [Artin-Tate, Class Field Theory, Benjamin, Inc., 1974].)

Theorem (Principal Ideal Theorem). *Let G be a (not necessarily finite) group whose commutator subgroup* $G' = [G, G]$ *is of finite index in G and is finitely generated. Then the transfer map* $G \to G'/G''$ *is the zero map.*

Iwasawa is of course better known for his work in Lie groups, number theory, etc. But let me mention only the following:

Theorem ([K. Iwasawa, Über die endlicher Gruppen und die Verbände ihrer Untergruppen, J. Univ. Tokyo, 43(1941), 171–199.]). *The maximal subgroup chains of a finite group G all have the same length if and only if G is supersolvable.*

A finite group G is supersolvable if it possesses a normal series

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = 1$$

in which each factor group G_{i-1}/G_i is cyclic of prime order. If a finite group G is supersolvable, it can be shown that any chain of subgroups

$$G = H_0 \supset H_1 \supset \cdots \supset H_s = 1$$

can be refined by inserting further subgroups:

$$H_{i-1} = H_{i-1,0} \supset H_{i-1,1} \supset \cdots \supset H_{i-1,t} = H_i, t = t(i), i = 1, \dots , s$$

such that all indices $[H_{i,j} : H_{i,j+1}]$ are primes. This implies that all maximal chains of subgroups have the same length, which is the total number of primes, counting repetitions, dividing the order of G. Iwasawa's Theorem shows that the converse also holds. The converse is of course nontrivial and the most difficult step is to show that G has a proper normal subgroup.

A monomial representation of a group G is an induced representation Ψ^G where Ψ is a one-dimensional representation of a subgroup H of G. All irreducible representations of a nilpotent group are known to be monomial. The converse is false. We, however, have:

Theorem ([K. Taketa, Über die Gruppen, deren Darstellungen sich sämtlich auf monomiale Gestalt transformieren lassen, Proc. Jap. Imp. Acad., 6(1930), 31–33]). *If every irreducible representation of a finite group G is monomial, then G is solvable.*

As seen above, there were some roots of finite group theory in the prewar Japan. It appears, however, that nobody in Japan was doing serious research on simple groups such as $PSL(2, q)$. Perhaps some people were interested in them but it would be fair to say that no important results came out from their efforts. It is, therefore, quite surprising that in such an environment, Suzuki took up a hard problem, which eventually lead him into the heart and the top of simple group theory.

There must have been time for me ask Suzuki personally how and why he got into the problems concerning $PSL(2, q)$ when nobody else in Japan was doing it. But such an opportunity is now lost for good. I could have asked Iwasawa,who had a great influence on Suzuki, about it, but he too passed away several months after Suzuki died.

§9. Michio Suzuki, my teacher and my mentor

I met Michio Suzuki for the first time in the spring of 1966 when he visited Japan with his family, then 2 year old Kazuko-chan and his wife Naoko Suzuki. D.G.Higman of the University of Michigan came to Japan with the Suzukis also. I was a second year graduate student at the University of Tokyo. I had decided to do group theory as my special field of mathematics in the spring of 1964 when I was a college senior.

It was the time when group theory reached its height and the golden era was continuing. For my decision to do group theory, I was influenced greatly by the work of Suzuki, especially:

(1) Discovery of the new series of simple groups $Sz(q)$.
(2) The classification of Zassenhaus groups (Zassenhaus, Feit, Ito, and Suzuki).
(3) Classification theorems for certain types of simple groups.

Under the supervision of N. Iwahori, I, together with a few other students, began reading [Curtis-Reiner, Representation Theory of Finite Groups and Associative Algebras]. I remember that Iwahori, who had visited the USA a few times, talked enthusiastically about Suzuki's work, Thompson's proof that the Frobenius kernel is nilpotent, the Odd Order Paper of Feit-Thompson, etc. I soon joined in the group theory seminar organized under Iwahori. Among the participants were Takeshi Kondo and Hiroyoshi Yamaki.

I chose Suzuki's classification of Zassenhaus groups of odd degree [21] for my seminar presentation. I next chose Thompson's proof of the nilpotency of the Frobenius kernel [Normal p-complements for finite groups, Math. Z., 72(1960), 332–354]. I found it impossible to read and gave up. Soon afterward fortunately, a shorter proof was published [J.G. Thompson, Normal p-complement for finite groups, J. Alg., 1 (1964), 43–46]. Thompson's new paper was much easier to read than the first one.

Around 1965, Japan was still in a poor state of affairs economically. A Xerox copier was delivered to the department of mathematics but students had to pay all copying cost, which was rather expensive for them. The expenses to participate in symposiums and conferences had to be borne by the students. We students tried to be winners under those conditions, since all Japanese were under the same constraints.

Besides, those who were students in the 1940s and 50s would say that the 60s were far better than their times.

After Suzuki's paper and Thompson's and a few more papers, T. Kondo, H. Yamaki, I and others started reading Feit-Thompson's odd order paper. Soon the group theory seminar lost most of its members. Left in the group were Kondo, Yamaki and myself, just three of us. After 30 years, we three still talk about the struggles we had in reading Feit-Thompson's paper in the seminar room of the basement of a building of the University of Tokyo.

R. Baer visited Japan in the fall of 1965 and other foreign group theorists came to Japan also. H. Wielandt visited Japan at a similar time. But not too many people in Japan were doing group theory and not too many students were going into the theory either. It was still a field of mathematics which did not command too much respect in Japan. My classmates at the University of Tokyo, Shigeru Iitaka, Takushiro Shintani, Takuro Shintani, Takushiro Ochiai, Ryoshi Hotta, went into fields such as algebraic geometry, number theory, differential geometry, and representation theory. But I took up group theory as my field with confidence and enthusiasm, and I have not regretted the decision since.

Suzuki's visit in 1966 to Japan was a very timely event for me. I was a second year graduate student at the University of Tokyo, and Suzuki was only 39 years of age and the peak of his career was continuing. He gave talks for us one after another, all without any compensation. In fact, he had to spend nearly two hours one way in a train to come from his home to the university. We, young group theorists, asked him to give lectures on Bender, Glauberman, Alperin and others. Week after week, Suzuki did everything we asked for.

At the time of his visit, I was working on a research problem. I completed it just as Suzuki was leaving for the USA. Much to my surprise and delight, he suggested that I submit it to the Illinois Journal of Mathematics. In addition to submitting the paper to him, I wrote him letters regularly, to which he gave replies regularly. One of his letters, dated October 23, 1966, contains many unpublished results. At the end of the letter, he writes that he will find time to write more. Apparently I had complained to him that the news on group theory would arrive late in Japan and I wrote him I would like to know them sooner. The letter cited above was his reply.

It was then customary for a graduate student to seek employment after earning the master's degree. I was offered an assistantship at Nagoya University as I was finishing my master's degree. One year after I first met Suzuki and after I had already moved to Nagoya, I received a letter from him in which he said that there would be a special program on finite groups and algebraic groups for the academic year 1968-69 at the Institute for Advanced Study in Princeton, N.J., Suzuki suggested that I apply for a membership of the Institute. He added in the letter that he would write a letter of recommendation. This was an incredible opportunity for me. The Institute at Princeton occupied so high a place in my mind that I did not quite believe what I was reading in his letter.

I and my wife arrived at the Institute on the 10th of September, 1968. The Suzukis arrived shortly afterward. As soon as he arrived, he asked me if I knew the game of bridge. I said no. In fact, I had never heard the word before either. Suzuki then began teaching me and my wife the game of contract bridge. So instead of Gorenstein's group theory book, I had to read Goren's book on contract bridge. Suzuki and his wife invited us over to their place usually twice a week to play bridge until they left for Illinois the next spring.

The following year, Takeshi Kondo came to the Institute also. We played bridge many nights and sometimes days. At some point, number theory friends stopped coming to the games. The rumour had it that Goro Shimura scolded young number theorists who were visiting the Institute at that time. We group theorists kept playing. If Michio Suzuki likes the game so much then it must be a good thing to play.

Suzuki invited me to spend a year at the University of Illinois at Champaign-Urbana after my second year at the Institute. By then Daniel Gorenstein and I had written quite a few joint papers together and I had begun thinking that I would like to stay in the USA as long as possible. Suzuki's invitation to Illinois guaranteed a third year for me in the States and soon afterward Gorenstein and Janko secured a permanent position for me at the Ohio State University starting the academic year of 1971. Over 30 years has passed. It all started from Suzuki's visit to Japan in 1966.

For Michio Suzuki, mathematics came first and research was everything. Apparently, however, he watched football games or basketball games whenever he wanted to have a relaxation. He talked about how good Jonny Unitas and Wilt Chamberlain were. He liked to read mystery stories. Iwasawa also said to me that he liked to read mysteries. Suzuki did not appear to like traveling much. Maybe this is not very precise. He did not mind going out from his home. But apparently, as soon as he went out, he wanted to come back home as quickly as possible.

Suzuki did not write too many research papers after 1980, but he visited Japan quite often. Conferences and symposiums were organized concurrently with his visits. Suzuki gave talks most of the time. At the memorial conference held for Suzuki's 70th birthday in July of 1997, he gave a talk on his new research effort. People must have been surprised to learn of his fresh enthusiasm to do research.

I received a Christmas card from him for the last time in December of 1997, five months after the conference held in his honor. In the card he writes 'I have been learning amstex recently. I can at last print out as I please. I am having fun since the product is very neat.' I am still a beginner in TEX and so apparently he was younger in this respect than me. Continuing his card, he writes 'Take a good care of yourself and have a good new year.'

In February of 1998, the sad news of a cancer in his liver was communicated to me and to the mathematical community of the world. It was a shock to me and to all who knew him. The cancer was discovered early in the month and Suzuki left for Japan immediately. The same doctor who had found nothing wrong in him in the summer of 1997 gave the same diagnosis as the Illinois doctor. The Illinois doctor gave Suzuki three to six months, but the Japanese doctor only two to four months.

As I could not leave for Japan immediately, I wrote several letters to him. In the following month, March 19, I left for Japan as soon as I handed the grades to the math office for the courses that I taught in the winter quarter.

I visited his room, which was a guest room of the International Christian University at Mitaka, Tokyo, Japan. Hiroshi Suzuki (no relation) was a faculty member there and had been taking care of Michio Suzuki and his wife since their arrival in Japan.

'I am happy to be able to see you while I am still well' were his first words. With Mrs. Suzuki and Hiroshi, we talked about many things. Suzuki and I had 30 years of memories together. We would never be able to stop talking. It was hardly believable that Michio Suzuki had only a month or so of his life remaining. But when we were talking about lots of things, I did not think about it. Everything was just as natural. He spoke a lot, sometimes smiling and I did so also. The thought of his short remaining life was not on the surface of the conversation. But when the conversation came to a quiet moment, then I had to think that this happy moment would end soon, much too soon.

Suzuki's incomplete 140 page manuscript was sitting on the table. It was nearly complete and he had been enjoying putting it into the TEX format, but the work had to come to an abrupt stop. Mrs. Suzuki said that Suzuki, many a time, tried, in vain, to continue working on the paper in the hospital or the guest room. As I saw he might be tired for the day, I promised to come back and left the place. Suzuki came to the door of his room. As he bid good-bye, he had a small smile on his face. The cherry trees were visible from the window of his room.

Suzuki would be able to see the cherry blossoms once more very soon. Mrs. Suzuki came down to the front door of the building. She had tears in her eyes when I said good-bye to her. The whole thing was so totally unexpected. I promised I would come back again soon.

With some of my friends I visited Suzuki two more times during my stay of three weeks in Japan. The last one was on April 10. The spring term had already started at my university in the States. Suzuki looked a little weaker than when I first saw him three weeks before. After an hour or so, Suzuki with an apology went back to his bed. I was sorry that I stayed a little too long till he got tired, but I knew this might be the last time for me to see him. I left the room. At the bottom of the stairs, I looked up. Suzuki was there near the top of the stairs. He too knew that this might be the last time, got out from his bed and said good-bye to us. Mrs. Suzuki saw me off at the front door of the guest house. I said I would come back in June, July. She said it would be hard for him to wait that long. I searched for a word. But none came out. She was being as cheerful as she could in front of her husband, but tears began to come down from her eyes and came down profusely. I looked up towards the window of Suzuki's room. The cherry blossoms were changing into tiny green leaves.

Suzuki went back to the hospital on April 18. He was to survive 43 days more. A surprise visitor to the hospital was Helmut Bender. Prior to his visit, Bender did not say anything to anybody. Bender flew from Germany and stayed with Suzuki in the hospital for a few days starting May 18th. Suzuki, with all of his remaining energy, discussed his new research work with Bender. It must have been a beautiful sight, Helmut Bender and Michio Suzuki together talking mathematics, just days before his death.

I had already purchased a plane ticket back to Japan for a June 4th flight. Michio Suzuki, however, passed away May 31. On the same day, though 166 years earlier, Evariste Galois died of a gunshot wound from a duel. The group theory emerged as a respectable field of mathematics largely through the efforts of Galois, and Suzuki was one of those who made it flourish.

The funeral service for Michio Suzuki took place on June 7th and it was a memorable one. Fortunate for the occasion, if it had to happen, was that there was a conference on class field theory honoring Teiji Takagi in Tokyo. Among the people who got together for his funeral were Michio Suzuki's adviser, Shokichi Iyanaga, and Suzuki's friends, Ichiro Satake, Gaishi Takeuchi, Takashi Ono. All of them left Japan in the 50s or early 60s and came to the USA, as Suzuki did.

Longtime friends Noboru Ito and Takeshi Kondo made moving memorial speeches, and I added one too. Ito talked about their friendship during the war and right after the war. Kondo touched on Suzuki's mathematical contributions. Hymns were sung and lines from the Bible were read. Each and every one of us paid tribute to him with a branch of yellow rose, Suzuki's favorite flower.

On September 18th, the memorial service for Michio Suzuki took place at the Chapel of the University of Illinois. Eiichi Bannai, Ronald Solomon, and I attended the service from Columbus, Ohio. Walter Feit, George Glauberman, Henry Leonard, Richard Lyons, Paul Bateman, Everett Dade, and John Walter were present also. Having sent Eiichi off to Japan from the Champaign airport the following day, I went to Suzuki's home. I looked around with emotion. How many hours did I spent in this home during the last 30 years ?

In this room, Michio Suzuki and I listened to Bach and Mozart together. Out from this home, his family and mine went to a McDonald's and ate hamburgers. He talked about how bad their Fighting Illini football team was but how good it once had been, all those things. He lived in the area, Champaign, Illinois, for nearly 45 years. Mrs. Suzuki had never driven a car, never needed it since Michio Suzuki did not mind taking his wife grocery shopping, taking his daughter Kazuko to her nursery school, elementary school, etc. all the time.

One of my colleagues and a friend for nearly 30 years, Ronald Solomon posts in his office a letter he received from Suzuki concerning Gorenstein, Lyons and Solomon's work.

'Dear Ron,

I would like to congratulate you on the publication of the second volume of the classification series which I have just glanced through. It is very well organized and readable. I have an elated feeling that I may be able to understand the proof of the classification in my life time. ....'

To this letter, Solomon replies: Professor Suzuki, I am sorry we were too slow. But I suppose you know a better proof by now.
(R. Solomon [Obituary written for Michio Suzuki, Notices of Amer. Math. Soc., Vol. 46 (1999)])

Suzuki kept his enthusiasm for mathematics and warm interest in the work of his colleagues to the end of his days. He is now gone and will be missed by his family and by those of us who knew him. But his name will forever be with us for his pioneering work.

Acknowledgements.

I thank Ronald Solomon deeply who read this manuscript twice thoroughly and suggested many improvements.

References

[1] Suzuki, Michio, The lattice of subgroups of a finite group, (Japanese) Suugaku (Mathematics), **2** (1950), 189–200.

[2] Suzuki, Michio, On the finite group with a complete partition, J. Math. Soc. Japan, **2** (1950), 165–185.

[3] Suzuki, Michio, On the lattice of subgroups of finite groups, Trans. Amer. Math. Soc., **70** (1951), 345–371.

[4] Suzuki, Michio, On the L-homomorphisms of finite groups, Trans. Amer. Math. Soc., **70** (1951), 372–386.

[5] Suzuki, Michio, A characterization of simple groups $LF(2,p)$, J. Fac. Sci. Univ. Tokyo. Sect. I., **6** (1951), 259–293.

[6] Suzuki, Michio, On finite groups with cyclic Sylow subgroups for all odd primes, Amer. J. Math., **77** (1955), 657–691.

[7] Suzuki, Michio, Structure of a group and the structure of its lattice of subgroups, Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft 10, Springer-Verlag, Berlin-Gotingen-Heidelberg, (1956), 96 pp.

[8] Suzuki, Michio, The nonexistence of a certain type of simple groups of odd order, Proc. Amer. Math. Soc., **8** (1957), 686–695.

[9] Brauer, R., Suzuki, Michio and Wall, G. E., A characterization of the one-dimensional unimodular projective groups over finite fields, Illinois J. Math., **2** (1958), 718–745.

[10] Suzuki, Michio, On finite groups containing an element of order four which commutes only with its powers, Illinois J. Math., **3** (1959), 255–271.

[11] Suzuki, Michio, On characterizations of linear groups, I, II, Trans. Amer. Math. Soc., **92** (1959), 191–219.

[12] Brauer, Richard and Suzuki, Michio, On finite groups of even order whose 2-Sylow group is a quaternion group, Proc. Nat. Acad. Sci. U.S.A., **45** (1959), 1757–1759.

[13] Suzuki, Michio, Applications of group characters, 1959 Proc. Sympos. Pure Math., Vol. 1, pp. 88–99, American Mathematical Society, Providence, R.I..

[14] Suzuki, Michio, (Russian) [Structure of a group and the structure of its lattice of subgroups] Translated from the English by L. E. Sadovskiĭ, edited by B. I. Plotkin Izdat. Inostr. Lit., Moscow, 1960, 158 pp.

[15] Suzuki, Michio, A new type of simple groups of finite order, Proc. Nat. Acad. Sci. U.S.A., **46** (1960), 868–870.

[16] Suzuki, Michio, Investigations on finite groups, Proc. Nat. Acad. Sci. U.S.A., **46**, (1960), 1611–1614.

[17] Suzuki, Michio, Finite groups with nilpotent centralizers, Trans. Amer. Math. Soc., **99** (1961), 425–470.

[18] Suzuki, Michio, On a finite group with a partition, Arch. Math., **12** (1961), 241–254.

[19] Suzuki, Michio, Applications of group characters, 1962, Proc. Sympos. Pure Math., Vol. VI, pp.101–105, American Mathematical Society, Providence, R.I..

[20] Suzuki, Michio, Contributions to the theory of finite groups, 1962 Proc. Sympos. Pure Math., Vol. VI, pp. 107–109, American Mathematical Society, Providence, R.I..

[21] Suzuki, Michio, On a class of doubly transitive groups, Ann. of Math., (2) **75** (1962), 105–145.

[22] Suzuki, Michio, On generalized (ZT)-groups, Arch. Math., **13**(1962), 199–202.

[23] Suzuki, Michio, On characterizations of linear groups, III, Nagoya Math. J., **21** (1962), 159–183.

[24] Suzuki, Michio, Two characteristic properties of (ZT)-groups, Osaka Math. J., **15** (1963), 143–150.

[25] Suzuki, Michio, On the existence of a Hall normal subgroup, J. Math. Soc. Japan, **15** (1963), 387–391.

[26] Suzuki, Michio, A class of doubly transitive permutation groups, 1963 Proc. Internat. Congr. Mathematicians (Stockholm, 1962), 285–287, Inst. Mittag-Leffler, Djursholm.

[27] Suzuki, Michio, On a class of doubly transitive groups, II, Ann. of Math., (2) **79** (1964), 514–589.

[28] Suzuki, Michio, Finite groups of even order in which Sylow 2-groups are independent, Ann. of Math., (2), **80** (1964), 58–77.

[29] Suzuki, Michio, A characterization of the 3-dimensional projective unitary group over a finite field of odd characteristic, J. Algebra, **2** (1965), 1–14.

[30] Suzuki, Michio, Finite groups in which the centralizer of any element of order 2 is 2-closed, Ann. of Math., (2), **82** (1965) ,191–212.

[31] Suzuki, Michio, Transitive extensions of a class of doubly transitive groups, Nagoya Math. J., **27** (1966), 159–169.

[32] Suzuki, Michio, On characterizations of linear groups, IV, J. Algebra, **8** (1968), 223–247.

[33] Suzuki, Michio, A characterization of the simple groups PSL(2, q), J. Math. Soc. Japan, **20** (1968), 342–349.

[34] Suzuki, Michio, A simple group of order, $448,345,497,600$, 1969, Theory of Finite Groups (Symposium, Harvard Univ., Cambridge, Mass., 1968), 113–119, Benjamin, New York.

[35] Suzuki, Michio, Characterizations of linear groups, Bull. Amer. Math. Soc., **75** (1969), 1043–1091.

[36] Suzuki, Michio, Characterizations of some finite simple groups, Actes du Congr. International des Mathematiciens (Nice, 1970), Tome 1, 371–373. Gauthier-Villars, Paris, 1971.

[37] Suzuki, Michio, A transfer theorem, J. Algebra, **51** (1978), 608–618.

[38] Suzuki, Michio, Gun ron, Vol. 1 (Japanese) [Group theory, Vol. 1] Gendai Suugaku [Modern Mathematics], **18**, Iwanami Shoten, Tokyo, 1977, xii+408 pp. (loose errata).

[39] Suzuki, Michio, Gun ron, Vol. 2 (Japanese) [Group theory, Vol. 2] Gendai Suugaku [Modern Mathematics], **19**, Iwanami Shoten, Tokyo, (1978), pp. i-vi and 409–951.

[40] Suzuki, Michio, Finite groups with a split BN-pair of rank one, The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979), 139–147, Proc. Sympos, Pure Math., **37**, Amer. Math. Soc., Providence, R.I., 1980.

[41] Suzuki, Michio, Group theory, I, Translated from the Japanese by the author, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], **247**, Springer-Verlag, Berlin-New York, 1982, xiv+434 pp., ISBN: 3-540-10915-3.

[42] Suzuki, Michio, Classification of finite simple groups (Japanese), Suugaku, **34** (1982), no. 3, 193–210.

[43] Suzuki, Michio, The values of irreducible characters of the symmetric group, The Arcata Conference on Representations of Finite Groups (Arcata, Calif., 1986), 317–319, Proc. Sympos. Pure Math., **47**, Part 2, Amer. Math. Soc., Providence, R.I., 1987.

[44] Suzuki, Michio, Group theory, II, Translated from the Japanese, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science], **248**, Springer-Verlag, New York-Berlin, 1986, x+621 pp., ISBN: 0-387-10916-1.

[45] Suzuki, Michio, Solvable generation of finite groups, Hokkaido Math. J., **16** (1987), no. 1, 109–113.

[46] Suzuki, Michio, A remark on finite groups having a split BN-pair of rank one with characteristic two, J. Algebra, **112** (1988), no. 1, 240–249.

[47] Suzuki, Michio, Elementary proof of the simplicity of sporadic groups, Group theory (Singapore, 1987), 195–206, de Gruyter, Berlin-New York, 1989.

Department of Mathematics
The Ohio State University
Columbus, OH 43210
U.S.A.

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 41–207

On the Prime Graph of a Finite Simple Group An Application of the Method of Feit-Thompson-Bender-Glauberman

Michio Suzuki

Introduction The theorem alluded to in the subtitle is the Odd Order Theorem of Feit-Thompson [FT] which states that all finite groups of odd order are solvable. For the remarkable proof, they invented a revolutionary new method which was influential to the development of finite group theory in the last 30 odd years. Recently, Bender and Glauberman [BG] have published a highly polished proof covering the group theoretical portion of the proof of the Odd Order Theorem.

By design, their proof is by contradiction. From the start they work on the hypothetical minimal simple group of odd order and study its properties. Thus, all the wonderful intermediate results are properties of the hypothetical group, and hence they may be vacuous. One of the goals of this paper is to show that this is not so; their method does give positive results and all the intermediate results are in fact properties of some real groups.

We consider the prime graph $\Gamma(G)$ of a finite group $G$. This is the graph defined as follows. The set of vertices of $\Gamma(G)$ is the set $\pi(G)$ of the primes dividing the order $|G|$ of $G$. If $p, q \in \pi(G)$, we join $p$ and $q$ by an edge in $\Gamma(G)$ if and only if $p \neq q$ and $G$ has an element of order $pq$.

The classification of finite simple groups has several interesting consequences on the prime graph of a finite group. The following is one of them.

Theorem A. *Let Δ be a connected component of the prime graph $\Gamma(G)$ of a finite group $G$, and let $\varpi$ be the set of primes in Δ. Assume that $\Delta \neq \Gamma(G)$ and $2 \notin \varpi$. Then, Δ is a clique.*

Usually, we identify Δ with $\varpi$ and abuse the terms, saying $\varpi$ is a connected component of the graph $\Gamma(G)$. Theorem A has not been stated

Received May 31, 1998.

in the literature in this form. But, the works of Gruenberg and Kegel [GK] and Williams [W] together with properties of Frobenius groups yield Theorem A. The classification of finite simple groups is used in two separate places of its proof. The first is in the proof of the following theorem.

Theorem B. *Theorem A holds for a finite simple group.*

The second use of the classification is to prove the following lemma.

Lemma. *Let G be a finite simple group. Then, $\pi(\operatorname{Out} G)$ is contained in the connected component of the prime graph $\Gamma(G)$ that includes the prime 2.*

This is fairly easy to check because $\operatorname{Out} G$ for a simple group G is not too complicated. The checking of Theorem B is more complex.

The purpose of this work is to show that the method of Feit, Thompson, Bender, and Glauberman can be adapted to give a proof of Theorem B without using the classification of finite simple groups.

Actually, Williams [W] has checked the following result for a finite simple group.

Theorem C. *Let Δ be a connected component of the prime graph $\Gamma(G)$ of a finite simple group G. Let ϖ be the set of primes in Δ. Assume that $\Delta \neq \Gamma(G)$ and $2 \notin \varpi$. Then, G contains a nilpotent Hall ϖ-subgroup H that is isolated in G.*

A subgroup H of any group G is called *isolated* in G if $1 \neq H \neq G$ and for every element $x \in H^{\sharp}$, we have

$$C_G(x) \subseteq H.$$

Theorem B is weaker than Theorem C which may be considered a local version of the Odd Order Theorem. It would be nice if our method would be able to prove Theorem C.

Originally, Gruenberg and Roggenkamp [GR] are led to study the prime graph, in particular its connectivity, through their work on the decomposition of the augmentation ideal of the integral group ring of a finite group. Specifically they considered the following three conditions on a finite group G.

(1) G has an isolated subgroup.
(2) The augmentation ideal decomposes as a right $\mathbb{Z}G$-module.
(3) The prime graph $\Gamma(G)$ is not connected.

Gruenberg and Roggenkamp [GR] proved that (1) $\Rightarrow$ (2) $\Rightarrow$ (3). Using Theorem C, Williams [W] was able to prove that (3) $\Rightarrow$ (1). If ϖ is a connected component of the prime graph $\Gamma(G)$ such that $2 \notin \varpi$ and $\varpi \neq \Gamma(G)$, it is not necessarily true that G has a Hall ϖ-subgroup that is isolated.

1. The Beginning of the Proof

Let G be a finite group and let $\varpi \subseteq \pi(G)$ be the set of primes of a connected component Δ of the prime graph $\Gamma(G)$. Assume that

$$\varpi \neq \pi(G) \quad \text{and} \quad 2 \notin \varpi.$$

These conditions and notation are used throughout this paper. The starting point of the proof is the following proposition.

Proposition 1. *Let P be a nonidentity ϖ-subgroup of G. If $N_G(P)$ is of even order, then G has an abelian Hall ϖ-subgroup that is isolated in G.*

Proof. Since $2 \notin \varpi$, P is of odd order. By assumption, there is an element t of order 2 that normalizes P. Since ϖ is a connected component and $2 \notin \varpi$, the element t acts regularly on P. This yields that

$$x^t = x^{-1} \quad \text{for} \quad x \in P.$$

Thus, P is abelian. If $x \in P^\sharp$, $C_G(x)$ is a ϖ-group and is normalized by t. It follows that $A = C_G(x)$ is abelian and the element t inverts every element of A. If $y \in A^\sharp$, the same argument proves that $C_G(y)$ is abelian. Since $A = C_G(x) \subseteq C_G(y)$, we have $C_G(y) = A$. Therefore, A is an abelian subgroup that is isolated in G. It is known that every isolated subgroup is a Hall subgroup. Q.E.D.

Therefore, to prove Theorem B, we may assume that every ϖ-local subgroup is of odd order. From now on we use the following notation and assumptions in addition to the ones already stated.

Let G be a finite simple group. Let

$$\mathcal{M} = \{M \mid M \text{ is a maximal } \varpi\text{-local subgroup of } G\},$$

define

$$\mathcal{M}(H) = \{M \in \mathcal{M} \mid H \subseteq M\}$$

for any subgroup H of G, and assume that *every subgroup $M \in \mathcal{M}$ is of odd order.*

The set of subgroups $\mathcal{M}$ satisfies properties which are similar to the properties of the set of all maximal subgroups of the hypothetical minimal simple group of odd order studied by [FT] and [BG]. We remark that the situation considered here does occur in real groups. For example, if p is a prime such that $p \equiv 3 \pmod 4$, the alternating group A_p satisfies the condition for $\varpi = \{p\}$.

2. The Local Analysis of $\mathcal{M}$

We can apply the method of Bender and Glauberman to study the subgroups in $\mathcal{M}$. The subgroups in $\mathcal{M}$ are of odd order; hence, they are solvable by the Odd Order Theorem. By definition, $M \in \mathcal{M}$ is a ϖ-local subgroup. It follows that $F(M)$, the Fitting subgroup of M, is a ϖ-subgroup. Let $p \in \pi(G)$ and let $P \in Syl_p(M)$. If P is not cyclic, P contains an elementary abelian p-subgroup A of order p^2. Then, A normalizes $N = O_{\varpi}(M)$ which is not 1. By a well-known proposition (Proposition 1.16 [BG]),

$$N = \langle C_N(x) \mid x \in A^\sharp \rangle.$$

It follows that $p \in \varpi$. Thus, if M is not a ϖ-group, M has a cyclic Sylow p-subgroup for every $p \in \pi(M) \setminus \varpi$, Thus, $M \in \mathcal{M}$ is almost a ϖ-subgroup. However, I call attention to the following point. For $M \in \mathcal{M}$, the set $\sigma(M)$ of primes is defined in [BG] as

$$\sigma(M) = \{p \in \pi(M) \mid N_G(P) \subseteq M \text{ for some } P \in Syl_p(M)\}$$

(p.70 [BG]). The important set in our case is

$$\sigma_0(M) = \sigma(M) \cap \varpi$$

and the subgroup we should study is

$$M_{\sigma_0} = O_{\sigma_0(M)}.$$

It is proved that M_{σ_0} is a Hall $\sigma_0(M)$-subgroup of M.

Proposition 2. *All the statements of the sections* $7 - 15$ *of* [*BG*] *hold with proper changes in the hypotheses and conclusions.*

The *types* of subgroups in $\mathcal{M}$ are defined as in pp.128–129 [BG] with the following three changes.

(II*iv*) should read: $V \neq 1$ and if V is a ϖ-group, then

$$N_G(V) \not\subseteq M.$$

(II*v*) should read: $N_G(A) \subseteq M$ for every nonidentity subgroup A of M' such that $C_H(A) \neq 1$.

(III*iii*) should read: V is an abelian ϖ-group and $N_G(V) \subseteq M$.

Then, $M \in \mathcal{M}$ is of type I, II, III, IV, or V. We have the following two theorems which are the goal of the local analysis.

Theorem I. *Either every subgroup in $\mathcal{M}$ is of type I or all the following conditions are true.*

(1) *G contains a cyclic subgroup $W = W_1 \times W_2$ with the property that $N_G(W_0) = W$ for every nonempty subset W_0 of $W - \{W_1, W_2\}$. Also, $W_i \neq 1$ for $i = 1, 2$.*

(2) *There are two subgroups S and T in $\mathcal{M}$ such that S and T are of type II, III, IV, or V, $S \cap T = W$, S is not conjugate to T in G, and either S or T (it may be both) is of type II.*

(3) *Every $M \in \mathcal{M}$ is either of type I or conjugate to S or T in G.*

There are other conditions which S and T must satisfy. For each $M \in \mathcal{M}$, two particular subsets $A(M)$ and $A_0(M)$ of M are defined (cf. p.124 and p.131 [BG]). The notation M_F for each $M \in \mathcal{M}$ denotes the normal nilpotent Hall subgroup of maximal order of M.

Theorem II. *For a subgroup $M \in \mathcal{M}$, let $X = A(M)$ or $A_0(M)$, and let*

$$D = \{x \in X^\sharp \mid C_G(x) \nsubseteq M\}.$$

Then, $D \subseteq M_{\sigma_0}$, $|\mathcal{M}(C_G(x))| = 1$ for all $x \in D$, and the following conditions are satisfied.

(T*i*) *Whenever two elements of X are conjugate in G, they are conjugate in M.*

(T*ii*) *If D is not empty, there are ϖ-subgroups $M_1, \dots, M_n$ in $\mathcal{M}$ of type I or II such that with $H_i = (M_i)_F$,*

(a) $(|H_i|, |H_j|) = 1$ *for* $i \neq j$,

(b) $M_i = H_i(M \cap M_i)$ *and* $M \cap H_i = 1$,

(c) $(|H_i|, |C_M(x)|) = 1$ *for all* $x \in X^\sharp$,

(d) *$A_0(M_i) - H_i$ is a nonempty TI-set in G with normalizer M_i, and*

(e) *if $x \in D$, then there is a conjugate y of x in D and an index i such that*

$$C_G(y) = C_{H_i}(y) C_M(y) \subseteq M_i.$$

If $y \in D$ with $C_G(y) \subseteq M_i$, then $y \in A(M_i)$.

(T*iii*) *If some M_i in (Tii) has type II, then M is a ϖ-group and is a Frobenius group with cyclic Frobenius complement, and M_F is not a TI-set in G.*

3. Application of Character Theory

We can study subgroups of $\mathcal{M}$ using character theory as in [FT]. The following are the major steps.

Proposition 3. *There is no subgroup $M \in \mathcal{M}$ of type V.*

Proposition 4. *Every subgroup $M \in \mathcal{M}$ of type I is a Frobenius group.*

This is very powerful. Suppose that $M \in \mathcal{M}$ is not a Frobenius group. Then, any supporting subgroup M_i for M in Theorem II is of type I by (*Tiii*). Then, Proposition 4 yields that M_i is a Frobenius group. However, it is easy to see that $A_0(M_i) = H_i$ for a Frobenius group. This contradicts (*Tii*)(*d*). Therefore, there is no supporting subgroup. It follows that X is a TI-set in G. This gives a very tight control on the imbedding of any M that is not a Frobenius group. In particular, we can study the subgroups in $\mathcal{M}$ which are of type II, III, or IV. The final result is the following.

Theorem III. *Let G be a finite simple group with disconnected prime graph $\Gamma(G)$. Let ϖ be a connected component such that $2 \notin \varpi$. Then, one of the following two cases occurs.*

(1) *G contains a nilpotent Hall ϖ-subgroup that is isolated in G.*
(2) *We have $\varpi = \{p, q\}$ for some primes p and q, and G has a self-normalizing cyclic subgroup of order pq.*

If the second case occurs, there are many more conditions the primes p and q must satisfy. It may be possible to eliminate the case (2) without referring to the classification of finite simple groups. In any case, Theorem III implies Theorem B.

Theorem IV. *Let G be a finite simple group with disconnected prime graph $\Gamma(G)$. Let Δ be a connected component consisting of odd primes. Then, Δ is a clique.*

4. Lemmas

For the most part, we will follow the notation and terminology in [BG]. Exceptions are noted in the body of the paper. As usual, for a prime $p \in \pi(G)$, we denote by

$$Syl_p(G)$$

the set of all Sylow p-subgroups of G.

Let X be a group and Y a subgroup of X. As in [BG], a *complement* Z of Y in X is defined to be a subgroup Z of X satisfying the two conditions

$$Y \cap Z = 1 \quad \text{and} \quad X = YZ.$$

We have the following well-known lemma.

Lemma. *Let X be a group and Y a subgroup of X. Suppose that Y has a complement Z in X. If U is a subgroup of X such that $Y \subseteq U \subseteq X$, then Y has a complement in U.*

Proof. We will show that $U \cap Z$ is a complement of Y in U. Let $W = U \cap Z$. Then, clearly $Y \cap W = 1$. We have

$$U = X \cap U = YZ \cap U.$$

Since $Y \subseteq U$, the Dedekind law yields that

$$YZ \cap U = Y(Z \cap U) = YW.$$

This proves that Y has a complement W in U. Q.E.D.

Next, we will state five lemmas which are used freely throughout this paper. Their proofs can be found at the end of the introduction.

Lemma A. *If $P \neq 1$ is a ϖ-group, so is $C_G(P)$.*

Lemma B. *Suppose a noncyclic elementary abelian p-group E acts on a subgroup $H \neq 1$.*

(1) *If H is a ϖ-group, then $p \in \varpi$.*
(2) *If $p \in \varpi$ and H is a p'-group, then H is a ϖ-group.*

Lemma C. *Assume $2 \notin \varpi$. If there exists a ϖ-local subgroup of even order, then G contains an isolated abelian Hall ϖ-subgroup.*

Lemma D. *A ϖ-group $\neq 1$ is contained in a ϖ-local subgroup.*

Lemma E.

(1) *If $M \in \mathcal{M}$ and a pi-subgroup $K \neq 1$ is normal in M, then $M = N_G(K)$.*
(2) *If $M \in \mathcal{M}$, then $N_G(M) = M$.*
(3) *If $M \in \mathcal{M}$ normalizes a ϖ-group $H \neq 1$, then $H \subseteq M$ and $M = N_G(H)$.*

Furthermore, we will collect here a few fundamental lemmas which are explicitly stated in the body of the paper. The terminology and notation are given there, as are the proofs.

Lemma F (See §4, page 9). *If $M \in \mathcal{M}$ and $p \in \pi(M) \cap \varpi'$, then M has a cyclic p-Sylow subgroup.*

Lemma G (See §4, page 12). *If $M \in \mathcal{M}$, then M is a ϖ-group except when*

(1) *M is a Frobenius group such that the Frobenius kernel of M is a Hall ϖ-subgroup of M, or*
(2) *M has the following structure: M/M' is a cyclic ϖ-group, $M_\alpha = M_\beta = M_{\sigma_0} \neq 1$ is a nilpotent ϖ-group, and M'/M_β is a non-identity cyclic ϖ'-group that is a Hall subgroup of M. Both M' and M/M_β are Frobenius groups.*

In the case (1), the Frobenius kernel of M is M_{σ_0} and it is either M' or $M_\alpha = M_\beta$.

Lemma H (See §6, page 17). *Let $M \in \mathcal{M}$. If $\tau_2(M) \neq \emptyset$, then M is a ϖ-group. If M is not a ϖ-group, then $r_p(M) \leq 1$ for all $p \notin \sigma_0(M)$.*

We also need some lemmas about the fusion of elements (§11, page 66). Our hypotheses are weaker than those in [BG], and these lemmas guarantee that the same results still hold.

Lemma I. *Let $M \in \mathcal{M}$ and let X be an F-set of M. Every element of $X^\sharp$ is conjugate to an element of D^* in M.*

Lemma J.

(1) *Every element g of M_i is conjugate in M_i to an element of the form $xh = hx$ where $x \in M \cap M_i$ and $h \in H_i$.*
(2) *Suppose that g is an element of M_i with $C_{H_i}(g) \neq 1$. Assume that g is conjugate in M_i to an element of the form hx where $x \in M \cap M_i$ and $h \in C_{H_i}(x)$, and at the same time, g is conjugate to an element of the annex $A(y)$ with $y \in D_j$. Then, $j = i$ and the element x is conjugate to y in M_i. In particular, $x \in D_i$ and $g \in A(M_i)$.*

Finally, we prove Lemmas A through E.

The first three lemmas give a few basic properties of connected components of prime graphs.

Lemma A. *Let G be a group and let ϖ be a connected component (or a union of connected components) of the prime graph $\Gamma(G)$ of G. If $P \neq 1$ is a ϖ-subgroup of G, then $C_G(P)$ is a ϖ-group.*

Proof. Let $p \in \pi(P)$. Then, $p \in \varpi$. Take any $q \in \pi(C_G(P))$. We will show $q \in \varpi$. We may assume $q \neq p$. There are elements x and y such that x is an element of P of order p and y is an element of $C_G(P)$ of order q. Since x and y commute, the product xy has order pq. Thus, (p, q) is an edge of the prime graph $\Gamma(G)$. This proves that q lies in the same connected component as the prime $p \in \varpi$. Hence, $q \in \varpi$. Q.E.D.

Lemma B. *Let G be a group and let ϖ be a connected component* (or a union of connected components) *of the prime graph $\Gamma(G)$ of G. Let p be a prime. Suppose that a noncyclic elementary abelian p-subgroup E normalizes a subgroup H of G.*

(1) *If H is a ϖ-group $\neq 1$, then $p \in \varpi$.*
(2) *If $p \in \varpi$ and H is a p'-group, then H is a ϖ-group.*

Proof. By our assumptions, $K = HE$ is a subgroup and $H \lhd K$.

(1) Suppose that H is a ϖ-group $\neq 1$. If $p \in \pi(H)$, then $p \in \varpi$. Suppose that $p \notin \pi(H)$. Then, H is a p'-group. By Proposition 1.16 [BG],

$$H = \langle C_H(x) \mid x \in E^\sharp \rangle.$$

Since $H \neq 1$, $P = C_H(x) \neq 1$ for some $x \in E^\sharp$. Then, $x \in C_G(P)$ where $P \neq 1$ is a ϖ-group. By Lemma A, $C_G(P)$ is a ϖ-group, so in particular, the order of x is a ϖ-number. This proves $p \in \varpi$.

(2) Let $q \in \pi(H)$ and $Q \in Sy\ell_q(H)$. Then, $q \neq p$ and Q is a Sylow q-subgroup of K. By the Frattini argument, $K = HN_K(Q)$. Therefore, a conjugate of E normalizes Q. We may replace E by a conjugate (in K) and assume that E normalizes Q. Since Q is a p'-group, Proposition 1.16 [BG] yields

$$Q = \langle C_Q(x) \mid x \in E^\sharp \rangle.$$

Since $\langle x \rangle$ is a ϖ-group by assumption, Lemma A implies that $C_Q(x)$ is a ϖ-group. Therefore, $q \in \varpi$. This proves that H is a ϖ-group. Q.E.D.

Lemma C. *Let G be a group and ϖ a connected component of the prime graph $\Gamma(G)$. Suppose that the prime 2 is not contained in ϖ and that there is a ϖ-local subgroup of even order. Then, G contains an abelian Hall ϖ-subgroup A that is isolated. Furthermore, any ϖ-element is conjugate to an element of A and the centralizer of any ϖ-element is abelian.*

Proof. By assumption, there is a pair (H, t) of a ϖ-subgroup H and an element t of order 2 that normalizes H. We have a lemma: For any pair (H, t) consisting of a ϖ-subgroup H and an element t of order 2 that normalizes H, t inverts every element of H and consequently, H is abelian. This follows from the lemma of Burnside ((1.9) [S II] p. 131). Note that since $2 \notin \varpi$, $C_H(t) = 1$ by Lemma A. By a first application of the above lemma, the element t inverts every element x of $H^\sharp$, i.e. $txt^{-1} = x^{-1}$. It follows that t normalizes $A = C_G(x)$. By Lemma A, A is a ϖ-subgroup of G. Take $y \in A^\sharp$. A second application of the lemma proves that $C_G(y)$ is abelian. Since A is abelian, $A \subseteq C_G(y)$. By the definition of A, $A = C_G(x)$ for some $x \in A^\sharp$. Thus, the abelian group $C_G(y)$ must coincide with A, i.e. A satisfies the property that if $y \in A^\sharp$, then $C_G(y) = A$. An easy application of Sylow's Theorem yields that A is a Hall subgroup of G.

If $A \cap uAu^{-1} \neq 1$ for some $u \in G$, then take a nonidentity element y of $A \cap uAu^{-1}$ and consider $C_G(y)$. Then, $A = C_G(y) = uAu^{-1}$. Thus, A is isolated.

We will show that $\varpi = \pi(A)$. Suppose that $\varpi \neq \pi(A)$. Then, there is a pair of primes (p, q) such that $p \in \pi(A)$, $q \in \varpi - \pi(A)$, and (p, q) is an edge of the prime graph $\Gamma(G)$. Therefore, there are elements a, b such that a is of order p, b is of order q, $a \in A^\sharp$, and a commutes with b. It follows that $b \in C_G(a) = A$. This contradicts the choice of q with $q \notin \pi(A)$. We have shown that A is a *varpi*-Hall subgroup of G that is isolated.

If z is any ϖ-element, $\langle z \rangle$ is conjugate to a subgroup of A by a theorem of Wielandt [W 1954]. The last assertion follows. Q.E.D.

We will also need the following properties of $\mathcal{M}$.

Lemma D. *Let G be a group and π a set of primes. Any π-subgroup $H \neq 1$ is contained in a maximal π-local subgroup.*

Proof. By definition, $K = N_G(H)$ is a π-local subgroup of G. Let M be a π-local subgroup of maximal order that contains K. Then, M is a maximal π-local subgroup such that $H \subseteq M$. Q.E.D.

Lemma E.

(1) *If $M \in \mathcal{M}$ and a π-subgroup $K \neq 1$ is normal in M, then $N_G(K) = M$.*

(2) *If $M \in \mathcal{M}$, then $N_G(M) = M$.*

(3) *If $M \in \mathcal{M}$ normalizes a π-subgroup $H \neq 1$ of G, then $H \subseteq M$ and $M = N_G(H)$.*

Proof. (1) By assumption, $N_G(K)$ is a π-local subgroup that contains M. Since $M \in \mathcal{M}$, we get $N_G(K) = M$.

(2) Let $K = O_\pi(M)$. Then, K is a π-subgroup $\neq 1$ of G. Hence, $M = N_G(K)$ by (1). Since $K \operatorname{char} M$, $N_G(M) \subseteq N_G(K)$. Hence, $N_G(M) = M$.

(3) By assumption, $N_G(H)$ is a π-local subgroup that contains M. Since $M \in \mathcal{M}$, we have $N_G(H) = M$. Q.E.D.

Chapter I. Local Analysis

We begin the local analysis of the simple groups G that satisfies the basic assumptions. We need the following notation.

Notation. Let G be a simple group with disconnected prime graph $\Gamma = \Gamma(G)$. Let ϖ be a connected component of Γ that consists of odd primes. We fix the following notation:

$$\begin{aligned} \mathcal{M} &= \text{the set of all maximal } \varpi\text{-local subgroups,} \\ \mathcal{M}(H) &= \text{the set of } M \in \mathcal{M} \text{ such that } H \subseteq M, \\ \mathcal{U} &= \text{the set of all proper subgroups } H \subseteq G \text{ such that } |\mathcal{M}(H)| = 1. \end{aligned}$$

The **basic assumptions** are

$$2 \notin \varpi$$

and

the set $\mathcal{M}$ *consists of subgroups of odd order.*

Thus, if $M \in \mathcal{M}$, then M is a solvable group of odd order.

The above notation and the basic assumptions are in force throughout this paper, not just in Chapter I.

Chapter I contains 10 sections and is organized as follows. Section m of this chapter corresponds to Section $m+6$ of [BG]. Lemma (Theorem, Proposition, or Corollary) $m.k$ of Section m of this paper corresponds to Lemma (Theorem, Proposition, or Corollary) $(m+6).k$ in [BG]. Proof may sometimes be obtained from the proof of the corresponding lemma in [BG] simply by changing the reference to Lemma $n.k$ to Lemma $(n-6).k$ of this paper when $n > 6$. If this is the case, the proof is usually omitted by referring to [BG].

§1. The Transitivity Theorem

Hypothesis 1.1. (1) The group A is a noncyclic subgroup of G with $O_{\varpi}(A) \neq 1$, and $\pi = \pi(A)$.

(2) Whenever X is a ϖ-local subgroup of the group G such that $A \subseteq X$, we have

$$O_{\pi'}(X) = \langle \text{И}_X(A;\pi') \rangle.$$

Let $K = O_{\pi'}(C_G(A))$ as in [BG]. Then, *K is the set of all π'-elements in $C_G(A)$.* This is proved as follows. Let $B = O_{\varpi}(A)$. By Hypothesis 1.1 (1), $B \neq 1$. Hence, $C_G(A) \subseteq C_G(B) \subseteq N_G(B)$. This implies that $N_G(B) = X$ is a ϖ-local subgroup that contains A. Let x be a π'-element of $C_G(A)$. Then, $\langle x \rangle$ is a π'-subgroup of X that is A-invariant. By (2), $\langle x \rangle \subseteq O_{\pi'}(X)$. Therefore,

$$\langle x \rangle \subseteq C_G(A) \cap O_{\pi'}(X) \subseteq O_{\pi'}(C_G(A)) = K.$$

Conversely, if $x \in K$, then x is a π'-element of $C_G(A)$. Q.E.D.

Lemma 1.1. *Assume Hypothesis* 1.1. *Suppose, for a prime $q \in \pi' \cap \varpi$, that Q_1, $Q_2 \in \text{И}^*_G(A;q)$ and that there exists a ϖ-local subgroup H of G such that*

$$A \subseteq H, H \cap Q_1 \neq 1, \quad \textit{and} \quad H \cap Q_2 \neq 1.$$

Then, $Q_2 = {Q_1}^k$ for some $k \in K$.

Proof. We proceed by induction on $|G|_q/|Q_1 \cap Q_2|$. If this number is 1, then Q_1 and Q_2 are Sylow subgroups of G with $|Q_1 \cap Q_2| = |Q_1| = |Q_2|$. This implies $Q_1 = Q_2 = {Q_1}^k$ with $k = 1 \in K$. Proceed by induction. By the basic assumptions, H is a solvable group. Hence, the A-invariant q-subgroup $H \cap Q_1$ is contained (in $O_{\pi'}(H)$ by Hypothesis 1.1 and so) in an A-invariant Sylow q-subgroup R_1 of $O_{\pi'}(H)$. Similarly, $H \cap Q_2 \subseteq R_2$ where R_2 is an A-invariant Sylow q-subgroup of $O_{\pi'}(H)$. By Proposition 1.5 [BG], ${R_1}^h = R_2$ for some $h \in O_{\pi'}(H) \cap C_G(A)$. Since h is a π'-element of $C_G(A)$, the remark after Hypothesis 1.1 yields $h \in K$.

Take $Q_3 \in \text{И}^*_G(A;q)$ such that $R_2 \subseteq Q_3$. Since $h \in K$, $Q_1^h \in \text{И}_G(A;q)$. We have $1 \neq (Q_1 \cap H)^h = {Q_1}^h \cap H \subseteq {R_1}^h = R_2 \subseteq Q_3$ and $1 \neq Q_2 \cap H \subseteq R_2 \subseteq Q_3$. Therefore, $1 \neq {Q_1}^h \cap H \subseteq {Q_1}^h \cap Q_3$ and $1 \neq Q_2 \cap H \subseteq Q_2 \cap Q_3$.

If $Q_1 \cap Q_2 = 1$, we are done as in [BG]. Suppose that $Q = Q_1 \cap Q_2 \neq 1$. Since q is assumed to be in ϖ, $N_G(Q)$ is a ϖ-local subgroup that contains A and we may assume $H = N_G(Q)$. The proof of Lemma 7.1 [BG] applies now without change. Q.E.D.

Theorem 1.2. *Assume Hypothesis* 1.1 *and let* $q = \pi' \cap \varpi$. *Suppose* $m(Z(A)) \geq 3$. *Then, K acts transitively on* $\text{И}^*_G(A;q)$.

Proof. By hypothesis, $Z(A)$ contains an elementary abelian p-subgroup B of order p^3 for some prime p. Since B centralizes $O_\varpi(A)$ and $O_\varpi(A) \neq 1$, we have $p \in \varpi \cap \pi$. So, $p \neq q$. The proof of Theorem 7.2 [BG] yields the result if we apply Lemma 1.1 to the ϖ-local subgroup $N_G(\langle z \rangle)$ at the end. Q.E.D.

Theorem 1.3. *Assume Hypothesis* 1.1 *and let* $q \in \pi' \cap \varpi$. *Suppose* $r(Z(A)) \geq 2$ *and* $q \in \pi(C_G(A))$. *Then, K acts transitively on* $\text{И}^*_G(A;q)$.

Proof. The proof of Theorem 7.3 [BG] applies here if we use Lemma 1.1 with the ϖ-local subgroup $N_G(\langle x \rangle)$ for some $x \in B$ with $C_{Q_1}(x) \neq 1$. Q.E.D.

Theorem 1.4. *Assume Hypothesis* 1.1 *and let* $q \in \pi' \cap \varpi$. *Suppose that P is a π-subgroup of G that contains A as a subnormal subgroup and that K acts transitively on* $\text{И}^*_G(A;q)$. *Then,*

(a) $C_K(P) = O_{\pi'}(C_G(P))$,

(b) $O_{\pi'}(C_G(P))$ *acts transitively on* $\text{И}^*_G(P;q)$,

(c) $\text{И}^*_G(P;q) \subseteq \text{И}^*_G(A;q)$, *and*

(d) *for every* $Q \in \text{И}^*_G(P;q)$, *we have* $P \cap N_G(P)' \subseteq N_G(Q)'$ *and* $N_G(P) = O_{\pi'}(C_G(P))(N_G(P) \cap N_G(Q))$.

Proof. Since A is subnormal in P, we have $O_\varpi(A) \subseteq O_\varpi(P)$. Therefore, $O_\varpi(P) \neq 1$ and P is contained in a ϖ-local subgroup. Note that, by the basic assumptions, $|P|$ is odd so P is solvable. The subgroup P satisfies the condition that is obtained from Hypothesis 1.1 replacing A by P.

Since $C_G(P) \subseteq C_G(A)$, $O_{\pi'}(C_G(P))$ is a set of π'-elements of $C_G(A)$. Hence, $O_{\pi'}(C_G(P)) \subseteq K \cap C_G(P) = C_K(P)$. On the other hand, $C_K(P) = O_{\pi'}(C_G(A)) \cap C_G(P) \subseteq O_{\pi'}(C_G(P))$. We have proved (a).

To prove the parts (b) and (c) we use induction on $|P:A|$. Let

$$1 = P_0 \lhd P_1 \lhd \cdots \lhd P_{n-1} \lhd P_n = P$$

be a composition series of P through A. If $A = P_{n-1}$ (or $A = P_n$), the proof of Theorem 7.4 [BG] for the case $k > n-2$ yields (b) and (c). If $A \neq P_{n-1}$, let $B = P_{n-1}$. Note that B satisfies the condition obtained from Hypothesis 1.1 by replacing A by B. The parts (b) and (c) follow by induction as in [BG].

In order to prove (d), take any $Q \in \mathit{И}^*_G(P;q)$ and let $L = N_G(P) \cap N_G(Q)$. If $x \in N_G(P)$, then $Q^x \in \mathit{И}^*_G(P;q)$. By (b), $Q^x = Q^y$ for some $y \in O_{\pi'}(C_G(P))$. Hence, $xy^{-1} \in N_G(Q) \cap N_G(P) = L$. Therefore,

$$N_G(P) = LO_{\pi'}(C_G(P)) = LC_K(P).$$

Since $O_{\pi'}(C_G(P)) = C_K(P) \lhd N_G(P)$, we have $N_G(P) = C_K(P)L$.

Note that $N_G(P)$ is contained in a ϖ-local subgroup, so by the basic assumptions, $N_G(P)$ is solvable of odd order. Lemma 6.5 [BG] with (G, K, U, H) replaced by $(N_G(P), O_{\pi'}(C_G(P)), L, P)$ yields $P \cap N_G(P)' = P \cap L' \subseteq L' \subseteq N_G(Q)'$. Q.E.D.

Proposition 1.5. *Suppose $p \in \varpi$ and A is an abelian p-subgroup of G. Assume that either* (1) $A = \{x \in C_G(A) \mid x^p = 1\}$ *and every ϖ-local subgroup of G has p-length* 1, *or* (2) $A \in SCN_2(P)$ *for some $P \in Sy\ell_p(G)$. Then, A satisfies Hypothesis* 1.1.

Proof. We can use the same method as in the proof of Theorem 7.5 [BG]. The proof in [BG] utilizes the centralizer $C_G(b)$ of an element b of order p. This subgroup need not be ϖ-local. However, it is contained in the ϖ-local subgroup $N_G(\langle b \rangle)$. Since the index $|N_G(\langle b \rangle) : C_G(\langle b \rangle)|$ is prime to p, we may replace $C_G(b)$ by $N_G(\langle b \rangle)$ without affecting the argument. Q.E.D.

Theorem 1.6 (Transitivity Theorem). *Suppose $p \in \varpi$, $A \in SCN_3(p)$, and $q \in p' \cap \varpi$. Then, $O_{p'}(C_G(A))$ acts transitively on $\mathit{И}^*_G(A;q)$ by conjugation.*

§2. The Fitting Subgroup of a Maximal ϖ-Local Subgroup

This section corresponds to Section 8 of [BG]. We begin with the following remark. Let H be a ϖ-local subgroup of G. By the basic assumptions, H is a solvable group of odd order. Let $F = F(H)$ be the Fitting subgroup of H. Since $O_\varpi(H) \neq 1$, we have $O_\varpi(F) \neq 1$. This implies that $\pi(F) \subseteq \varpi$ as F is nilpotent and is the direct product of its Sylow subgroups.

Theorem 2.1. *Suppose $M \in \mathcal{M}$, $p \in \pi(F(M))$, and $A_0 \in \mathcal{E}^*_p(F(M))$. Assume that $m(A_0) \geq 3$. Let $P \in Sy\ell_p(M)$.*

(a) *If $F(M)$ is not a p-group, then $C_{F(M)}(A_0) \in \mathfrak{U}$.*
(b) *If $F(M)$ is a p-group, then $P \in Sy\ell_p(G)$ and every element of $SCN_3(P)$ is contained in $F(M)$ and belongs to $\mathfrak{U}$.*

Proof. (a) Let $F = F(M)$, $\pi = \pi(F)$ and $A = C_F(A_0)$. Then $\pi(A) = \pi$ because $Z(F) \subseteq C_F(A_0) = A \subseteq F$. Note that for every $q \in \pi$,

$$C_G(A) \subseteq C_G(A_q) \subseteq C_G(Z(F)_q) \subseteq N_G(Z(F)_q) = M.$$

The last equality comes from Lemma E (1) since $Z(F)_q$ is a nonidentity normal ϖ-subgroup of M. The notation N_π stands for $O_\pi(N)$ of a nilpotent group N as in [BG].

We will show that $C_G(A)$ is a π-subgroup. Suppose that x is a π'-element of $C_G(A)$. Let $C = C_F(x)$. By the first paragraph, $x \in M$. Since $A \subseteq C$, $C_F(C) \subseteq C_F(A) \subseteq C_F(A_0) = A \subseteq C$. By Proposition 1.10 [BG] , $x \in C_M(F) = C_M(F(M)) \subseteq F$. Since x is a π'-element with $\pi = \pi(F)$, we get $x = 1$. Thus, $C_G(A)$ is a π-subgroup of M.

We prove the following lemma. *Let p be any prime, X a solvable subgroup of G and P a p-subgroup of X. Then,*

$$O_{p'}(N_G(P)) \cap X \subseteq O_{p'}(X).$$

Proof. Let $Y = O_{p'}(N_G(P)) \cap X$. Then,

$$Y = O_{p'}(N_G(P)) \cap N_X(P) \subseteq O_{p'}(N_X(P)).$$

Since $P \subseteq X$, we have $[O_{p'}(N_X(P)), P] \subseteq O_{p'}(N_X(P)) \cap P = 1$. Hence,

$$O_{p'}(N_X(P)) \subseteq O_{p'}(C_X(P)).$$

By Proposition 1.15 [BG], $O_{p'}(C_X(P)) \subseteq O_{p'}(X)$.

This proves $Y \subseteq O_{p'}(X)$. Q.E.D.

With this lemma on hand, we verify Hypothesis 1.1 for A. Take an arbitrary ϖ-local subgroup X that contains A and $Y \in \mathcal{U}_X(A;\pi')$. Take any $q \in \pi$. By the first paragraph of the proof, $C_Y(A_q) \subseteq M$. Since Y is an A-invariant π'-subgroup,

$$[C_Y(A_q), A] \subseteq Y \cap [M, A] = Y \cap F = 1.$$

Hence, $C_Y(A_q) \subseteq C_G(A)$. Since $C_G(A)$ is a π-group, we have $C_Y(A_q) = 1$. Thus, by Proposition 1.6 [BG], $Y = C_Y(A_q)[Y, A_q] = [Y, A_q]$. By hypothesis, $|\pi| \geq 2$. Take $r \neq q$ in π. Since $N_G(Z(F)_q) = M$ by Lemma E (1), $A_r \subseteq F_r \subseteq O_{q'}(M)$: and: $A_r \subseteq O_{q'}(N_G(Z(F)_q)) \cap X$.

Since $Z(F) \subseteq A \subseteq X$, Lemma implies

$$A_r \subseteq O_{q'}(X) \quad \text{for any } q \neq r \text{ in } \pi. \tag{1}$$

Since $Y = [Y, A_r]$, we have $Y \subseteq O_{q'}(X)$ for all $q \in \pi$. Hence, $Y \subseteq \bigcap_{q\in\pi} O_{q'}(X) = O_{\pi'}(X)$. This proves Hypothesis 1.1 for A.

We will prove that $\text{И}^*_G(A;q) = \{1\}$ for every $q \in \pi' \cap \varpi$. Take $q \in \pi' \cap \varpi$. Since $m(Z(A)) \geq m(A_0) \geq 3$, Theorem 1.2 implies that $O_{\pi'}(C_G(A))$ acts transitively on $\text{И}^*_G(A;q)$. But, $C_G(A)$ is a π-group, so $O_{\pi'}(C_G(A)) = 1$. Thus, $\text{И}^*_G(A;q) = \{Q\}$ for some q-subgroup Q of G. Since F is nilpotent, $A \lhd\lhd F$. By Theorem 1.4 (c), $\text{И}^*_G(F;q) \subseteq \text{И}^*_G(A;q)$. Therefore, $\text{И}^*_G(F;q) = \{Q\}$ and M normalizes Q. By Lemma E (3), $Q \subseteq M$. Hence, $Q \lhd M$ and $Q \subseteq F(M)$. Since $\pi = \pi(F(M))$ and $q \in \pi'$, we have $Q = 1$. Thus, $\text{И}^*_G(A;q) = \{1\}$ for $q \in \pi' \cap \varpi$.

To prove $A \in \mathfrak{U}$, take $H \in \mathcal{M}(A)$. Let $D = F(H)$ and $\sigma = \pi(D)$. We will prove first $\sigma = \pi$. Since A normalizes D, the last paragraph yields $\sigma \subseteq \pi$. By definition of D, $O_{\sigma'}(H) = 1$. We have

$$O_{\sigma'}(Z(F)) \subseteq O_{\sigma'}(A) = \langle A_r \mid r \in \pi \cap \sigma' \rangle.$$

By (1) for $X = H$, $A_r \subseteq O_{q'}(H)$. Hence

$$\langle A_r \mid r \in \pi \cap \sigma' \rangle \subseteq \bigcap\nolimits_{q \in \sigma} O_{q'}(H) = O_{\sigma'}(H) = 1.$$

It follows that $\pi \cap \sigma'$ is empty, i.e. $\pi \subseteq \sigma$. Thus, $\sigma = \pi$.

For each $q \in \pi$, $O_{q'}(A) = \langle A_r \mid r \neq q \rangle \subseteq O_{q'}(H)$. So,

$$[D_q, O_{q'}(A)] \subseteq [D_q, O_{q'}(H)] = 1. \tag{2}$$

Hence, $D_q \subseteq C_G(O_{q'}(A)) \subseteq N_G(O_{q'}(A)) = M$. The last equality is by Lemma E (1). This proves $D \subseteq M$.

The formula (2) implies that A_p centralizes $O_{p'}(D)$. Since $O_{p'}(D) = F(O_{p'}(H))$, Proposition 1.4 [BG] implies that A_p centralizes $O_{p'}(H)$. Hence, $O_{p'}(H) \subseteq C_G(A_p) \subseteq M$ by the first paragraph of the proof. By Lemma E (1) for H, $O_{p'}(H) \subseteq O_{p'}(N_G(D_p)) \cap M$. Since $D_p \subseteq M$, the lemma applies to get $O_{p'}(H) \subseteq O_{p'}(M)$.

We will prove that $O_{p'}(M) \subseteq O_{p'}(H)$. Since A_0 is a p-subgroup of F, we have $O_{p'}(F) \subseteq C_G(A_0) = A$. Thus, $O_{p'}(F) = O_{p'}(A)$. By (2), D_p centralizes $O_{p'}(A) = O_{p'}(F) = F(O_{p'}(M))$. Proposition 1.4 [BG] shows that D_p centralizes $O_{p'}(M)$, i.e. $O_{p'}(M) \subseteq C_G(D_p) \subseteq N_G(D_p) = H$. The last equality is by Lemma E (1) applied to $H \in \mathcal{M}$. Therefore,

$$O_{p'}(M) \subseteq O_{p'}(N_G(Z(F)_p)) \cap H.$$

We have $Z(F)_p \subseteq O_{q'}(A) \subseteq C_G(D_q) \subseteq H$.

The lemma gives us $O_{p'}(M) \subseteq O_{p'}(H)$. Therefore, $O_{p'}(M) = O_{p'}(H)$ and $M = N_G(O_{p'}(M)) = N_G(O_{p'}(H)) = H$. This proves that $A \in \mathfrak{U}$.

(b) The proof of Part (b) of Theorem 8.1 [BG] is applicable. Note that we must take $q \in p' \cap \varpi$ to apply the Transitivity Theorem 1.6 and

that an A-invariant p'-subgroup is a ϖ-subgroup by Lemma B (2).
Q.E.D.

§3. The Uniqueness Theorem

Theorem 3.1. *Suppose that p is a prime, $M \in \mathcal{M}$, $B \in \mathcal{E}_p(M)$, and B is not cyclic. Assume that* (a) *$C_G(b) \subseteq M$ for all $b \in B^\sharp$ or* (b) *$\langle И_G(B; p') \rangle \subseteq M$. Then, $B \in \mathfrak{U}$.*

Proof. Since $O_\varpi(M) \neq 1$ and B normalizes $O_\varpi(M)$, Lemma B (1) implies $p \in \varpi$. If $K \in И_G(B; p')$, Lemma B (2) proves that K is a ϖ-group. In particular, $O_{p'}(M)$ is a ϖ-subgroup. It follows that if $O_{p'}(M) \neq 1$, then $M = N_G(O_{p'}(M))$ by Lemma E (1). With these remarks, the proof of Theorem 9.1 [BG] shows the validity of the conclusion of Theorem 3.1. Q.E.D.

Corollary 3.2. *Suppose that $L \in \mathfrak{U}$, K is a subgroup of $C_G(L)$, and $r(K) \geq 2$. Then, $K \in \mathfrak{U}$ if one of the following conditions holds:*

(a) *$r_p(K) \geq 2$ for some $p \in \varpi$,*
(b) *$\pi(L) \cap \varpi$ is nonempty, or*
(c) *K is contained in some $M \in \mathcal{M}$.*

Proof. Let $\mathcal{M}(L) = \{H\}$. Take $B \in \mathcal{E}_p^2(K)$ for some prime p. If (a) holds, take $p \in \varpi$. If (b) holds, take $q \in \pi(L) \cap \varpi$ and an element x of L of order q. The element x centralizes B. Since $q \in \varpi$, we have $p \in \varpi$. If (c) holds, B normalizes $O_\varpi(M) \neq 1$. Then, $p \in \varpi$ by Lemma B (1). Thus, we have $p \in \varpi$ in all cases.

For each $b \in B^\sharp$, we have $L \subseteq C_G(b) \subseteq N_G(\langle b \rangle)$. Since $p \in \varpi$, $N_G(\langle b \rangle)$ is a ϖ-local subgroup. Since $\mathcal{M}(L) = \{H\}$, we have

$$C_G(b) \subseteq N_G(\langle b \rangle) \subseteq H$$

for all $b \in B^\sharp$. By Theorem 3.1, $B \in \mathfrak{U}$ and $\mathcal{M}(B) = \{H\}$. Since $B \subseteq K$, we have $\mathcal{M}(K) = \{H\}$ and $K \in \mathfrak{U}$. Q.E.D.

Corollary 3.3. *Suppose that $p \in \varpi$, A is an abelian p-subgroup of G, and B is a noncyclic p-subgroup of G. Assume that $A \in \mathfrak{U}$, $m(A) \geq 3$, and $r_p(C_G(B)) \geq 3$. Then, $B \in \mathfrak{U}$.*

Proof. Take $B^* \in \mathcal{E}_p^3(C_G(B))$ and let P be a Sylow p-subgroup of G that contains B^*. Replacing A by a conjugate, if necessary, we can assume that $A \subseteq P$. The proof of Corollary 9.3 [BG] shows $B \in \mathfrak{U}$.
Q.E.D.

Lemma 3.4. *Suppose that p is a prime, $M \in \mathcal{M}$, and $r_p(F(M)) \geq 3$. Then, $\mathcal{U}$ contains every abelian p-subgroup of rank at least three.*

Proof. The assumptions imply $p \in \varpi$ by Lemma B (1). Lemma follows from Theorem 2.1 and Corollaries 3.2 and 3.3 as in the proof of Lemma 9.4 [BG] . Q.E.D.

Lemma 3.5. *Suppose $p \in \varpi$ and $A \in SCN_3(p)$. Then, $A \in \mathcal{U}$.*

Proof. Since $p \in \varpi$, $C_G(A)$ is a ϖ-group (Lemma A). By Lemma D, $\mathcal{M}(C_G(A))$ is not empty. Let M be an arbitrary element of $\mathcal{M}(C_G(A))$, and let $F = F(M)$. We assume that $A \notin \mathcal{U}$. By Lemma 3.4, we have $r_p(F) \leq 2$.

Choose a prime q as follows: if $r(F) \leq 2$, let q be the largest primes in $\pi(M)$; if $r(F) \geq 3$, let q be some prime for which $r_q(F) \geq 3$. If $r(F) \leq 2$, Theorem 4.20 (c) [BG] implies $O_q(M) \in Syl_q(M)$. In all cases, $O_q(M) \neq 1$. Then, $q \in \varpi$, for if $q \notin \varpi$, $O_q(M)$ would centralize $O_\varpi(M) \neq 1$ contradicting Lemma A.

Since $q \in \varpi$, we have $M = N_G(O_q(M))$ by Lemma E (1). If $r(F) \leq 2$, then $O_q(M)$ is indeed a Sylow q-subgroup of G. Thus, $r_q(G) \leq 2$. Since $r_p(G) \geq 3$, we have $q \neq p$. If $r(F) \geq 3$, then $r_q(F) \geq 3$ while $r_p(F) \leq 2$. Thus, $q \neq p$ in all cases.

Let P be a Sylow p-subgroup of $N_G(A)$ and let R be a subgroup of $P \cap M$ that contains A. Then R normalizes $O_q(M)$. Take $Q \in \mathcal{V}^*_G(R; q)$ such that $O_q(M) \subseteq Q$. We will prove $Q \subseteq N_G(Q) \subseteq M$.

If $r(F) \geq 3$, the definition of the prime q implies $r_q(F(M)) \geq 3$, so Lemma 3.4 applies with q in place of p. Since $O_q(M)$ contains an abelian subgroup of rank at least three, $O_q(M) \in \mathcal{U}$ by Lemma 3.4. Since $O_q(M) \subseteq Q \subseteq N_G(Q)$, we have $N_G(Q) \subseteq M$. On the other hand, if $r(F) \leq 2$, then $Q = O_q(M) \lhd M$. Hence, the claim holds in all cases.

We will prove next $N_G(A) \subseteq M$ and $N_G(P) \subseteq M$.

By definition, R is a p-subgroup so $A \lhd\lhd R$. By Theorem 1.6, $O_{p'}(C_G(A))$ acts transitively on $\mathcal{V}^*_G(A; q)$. By Proposition 1.5, A satisfies Hypothesis 1.1. By Theorem 1.4, $O_{p'}(C_G(R))$ acts transitively on $\mathcal{V}^*_G(R; q)$. Note that $C_G(R) \subseteq C_G(A) \subseteq M$.

Take $x \in N_G(R)$. Then, $Q^x \in \mathcal{V}^*_G(R; q)$. Hence,

$$Q^x = Q^y \quad \text{for some} \quad y \in O_{p'}(C_G(R)) \subseteq M.$$

We have $xy^{-1} \in N_G(Q) \subseteq M$. This implies that $x = (xy^{-1})y \in M$. Thus, $N_G(R) \subseteq M$. By taking $R = A$, we have $P \subseteq N_G(A) \subseteq M$. By taking $R = P$, we have $N_G(P) \subseteq M$.

Let $P_0 = [P, N_G(P)]$ and $D = O_{p'}(F)$. Then, $P_0 \neq 1$ (Theorem 1.18 [BG]). We will prove that P_0 centralizes D. Suppose that P_0 does not centralize D. By Proposition 1.16 [BG],

$$D = \langle C_D(B) \mid B \subseteq \Omega_1(A), \quad \Omega_1(A)/B \text{ cyclic}\rangle.$$

Take $B \subseteq \Omega_1(A)$ such that $\Omega_1(A)/B$ is cyclic and P_0 does not centralize $C_D(B)$. Since $A \in SCN_3(p)$, B is not cyclic. Since $A \notin \mathcal{U}$, we have $B \notin \mathcal{U}$. By Theorem 3.1, there exist $y \in B^\sharp$ and $L \in \mathcal{M}$ such that $C_G(y) \subseteq L$ and $C_G(y) \nsubseteq M$. Since $C_G(A) \subseteq C_G(b) \subseteq L$, we can apply the preceding argument, with L in place of M, to conclude that $N_G(P) \subseteq L$. Hence,

$$N_G(P) \subseteq M \cap L \quad \text{and} \quad P_0 \subseteq (N_G(P))' \subseteq (M \cap L)'.$$

Since $D \cap L \lhd M \cap L$, no subgroup of $D \cap L$ lies in $\mathcal{U}$. As $D = O_{p'}(F(M))$, Lemma 3.4 implies that $r(D \cap L) \leq 2$. Thus, by Corollary 4.19 [BG], P_0 centralizes every chief factor U/V of $L \cap M$ for which $U \subseteq D \cap L$. Since $D \cap L$ is a p'-subgroup, Lemma 1.9 [BG] shows that P_0 centralizes $D \cap L$. However, $D \cap L \supseteq D \cap C_G(y) \supseteq C_D(B)$ and $C_D(B)$ is not centralized by P_0. This contradiction shows that P_0 centralizes D.

We claim that $\{M\} = \mathcal{M}(N_G(P_0))$. Suppose that $r(F) \geq 3$. Since $r_p(F) \leq 2$, we have $r(D) \geq 3$. By Lemma 3.4 applied to a prime q with $r_q(D) \geq 3$, D contains some subgroup in $\mathcal{U}$. Thus, $D \in \mathcal{U}$. Since $M = N_G(D)$, we have $\mathcal{M}(D) = \{M\}$. We have $D \subseteq C_G(P_0) \subseteq N_G(P_0)$ so $\mathcal{M}(N_G(P_0)) = \{M\}$.

Suppose that $r(F) \leq 2$. By Theorem 4.20 [BG], $M' \subseteq F$. We have shown that $P \subseteq N_G(P) \subseteq M$.

Since M/F is abelian, $FP \lhd M$ and $M = O_{p'}(M)N_M(P)$. Since $P_0 = [P, N_G(P)] \lhd N_G(P)$ and $O_{p'}(M)$ centralizes P_0, we have $P_0 \lhd M$. This yields $\{M\} = \mathcal{M}(N_G(P_0))$.

We will complete the proof as in [BG]. Since $A \notin \mathcal{U}$, it follows that $\Omega_1(A) \notin \mathcal{U}$. By Theorem 3.1, there exists $x \in \Omega_1(A)^\sharp$ such that $C_G(x) \nsubseteq M$. Take $H \in \mathcal{M}(C_G(x))$. Then, $C_G(A) \subseteq C_G(x) \subseteq H$. Since M was chosen arbitrary from $\mathcal{M}(C_G(A))$, we can apply the previous argument to H in place of M to conclude

$$\{H\} = \mathcal{M}(N_G(P_0)) = \{M\}$$

that is a contradiction. This completes the proof of Lemma 3.5.

Q.E.D.

Theorem 3.6 (The Uniqueness Theorem). *Suppose that K is a subgroup of G with $r(K) \geq 2$. Assume that $r_p(K) \geq 3$ for some $p \in \varpi$*

or $r_p(C_G(K)) \geq 3$ for some $p \in \varpi$. Then, $K \in \mathcal{U}$. In particular, if $A \in \mathcal{E}_p^2(G) \setminus \mathcal{E}^*(G)$, for some prime $p \in \varpi$, then $A \in \mathcal{U}$.

Proof. Assume that $r_p(K) \geq 3$ for some $p \in \varpi$. Take $B \in \mathcal{E}_p^3(K)$ of order p^3. Let P be a Sylow p-subgroup of G that contains B. By Lemma 5.1 [BG], there exists $A \in SCN_3(P)$. Since $p \in \varpi$, Lemma 3.5 implies $A \in \mathcal{U}$. Since B is abelian, $B \subseteq C_G(B)$. Corollary 3.3 implies $B \in \mathcal{U}$. Therefore, $K \in \mathcal{U}$.

Assume that $r_p(C_G(K)) \geq 3$ for some $p \in \varpi$. Let $L = C_G(K)$. Then, the first paragraph of the proof shows $L \in \mathcal{U}$. Since $\pi(L) \cap \varpi$ is nonempty, Corollary 3.2 implies $K \in \mathcal{U}$. Q.E.D.

§4. The Subgroups M_α and M_σ

For each $M \in \mathcal{M}$, we define the sets of primes $\alpha(M)$, $\beta(M)$ and $\sigma(M)$, and the subgroups M_α, M_β, and M_σ as in [BG], page 70. In addition, we use the notation

$$\sigma_0(M) = \sigma(M) \cap \varpi \quad \text{and} \quad M_{\sigma_0} = O_{\sigma_0(M)}(M).$$

Lemma F. *Let $M \in \mathcal{M}$ and $p \in \pi(M)$. If $p \notin \varpi$, then M has a cyclic Sylow p-subgroup.*

Proof. By the basic assumptions, p is odd. If a Sylow p-subgroup S of M is not cyclic, then S contains an elementary abelian p-subgroup E that is not cyclic ([S], II page 59, (4.4)). The group E normalizes $O_\varpi(M)$ which is a nonidentity ϖ-subgroup. By Lemma B (1), we have $p \in \varpi$. Q.E.D.

Theorem 4.1. *Suppose $M \in \mathcal{M}$, $p \in \sigma(M)$, and X is a nonempty subset of $G^\sharp$ such that $\langle X \rangle$ is a p-subgroup of G.*

(a) *If $X \subseteq M$, $g \in G$, and $X^g \subseteq M$, then $g = cm$ for some $c \in C_G(X)$ and $m \in M$.*
(b) *The subgroup $C_G(X)$ acts transitively by conjugation on the set $\{M^g \mid g \in G \text{ and } X \subseteq M^g\}$.*
(c) *If X is a subgroup of M, then $N_G(X) = N_M(X)C_G(X)$.*
(d) *If X is a Sylow p-subgroup of M, then $X \subseteq M^g$ implies $g \in M$ (so M is the only conjugate of M that contains X).*
(e) *If $X \subseteq M$, $C_G(X) \subseteq M$, $g \in G$, and $X \subseteq M^g$, then $M = M^g$ and $g \in M$.*

There is only a small difference between our Theorem 4.1 and the corresponding Theorem 10.1 [BG]. To prove (b), we may replace X by

$\langle X\rangle$ and assume that X is a nontrivial p-subgroup of G (as in [BG]). The argument in [BG] proves the result. Note that in the case when $r(P) \geq 3$, we have $p \in \varpi$. This justifies the use of the Uniqueness Theorem on the top of page 72 [BG].

Theorem 4.2. *Let $M \in \mathcal{M}$. Then,*

(a) *M_α is a Hall $\alpha(M)$-subgroup of M and of G,*
(b) *M_σ is a Hall $\sigma(M)$-subgroup of M and of G,*
(c) *$M_\alpha \subseteq M_{\sigma_0} \subseteq M_\sigma \subseteq M'$,*
(d) *$r(M/M_\alpha) \leq 2$ and M'/M_α is nilpotent,*
(e) *$M_{\sigma_0} \neq 1$, and*
(f) *M_{σ_0} is a Hall $\sigma_0(M)$-subgroup of M and of G.*

Proof. The proof is the same as that of Theorem 10.2 [BG]. We will repeat it here because the results are so basic.

The basic assumptions imply that M is a solvable group of odd order. So, M contains a Hall $\alpha(M)$-subgroup $M(\alpha)$. Take $p \in \alpha(M)$ and $P \in Syl_p(M(\alpha))$. By definition of $\alpha(M)$, $r(P) \geq 3$. So, by Lemma F, $p \in \varpi$. The Uniqueness Theorem implies $P \in \mathcal{U}$. In particular, we have $N_G(P) \subseteq M$. Thus, $p \in \sigma(M)$; in fact, $p \in \sigma_0(M)$. Since p is arbitrary in $\alpha(M)$, we have $\alpha(M) \subseteq \sigma_0(M) \subseteq \sigma(M)$. Also, $N_G(P) \subseteq M$ implies that $P \in Syl_p(G)$. Thus, $M(\alpha)$ is a Hall $\alpha(M)$-subgroup of G.

Let $M(\sigma)$ be a Hall $\sigma(M)$-subgroup of M that contains $M(\alpha)$. Take $p \in \sigma(M)$ and $P \in Syl_p(M(\sigma))$. By definition of $\sigma(M)$, we have $N_G(P) \subseteq M$ so $P \in Syl_p(G)$. Hence, $M(\sigma)$ is a Hall $\sigma(M)$-subgroup of G.

By Theorem 1.17 [BG],

$$P \cap G' = \langle x^{-1}y \mid x, y \in P \text{ and } x \text{ is conjugate to } y \text{ in } G\rangle$$
$$P \cap M' = \langle x^{-1}y \mid x, y \in P \text{ and } x \text{ is conjugate to } y \text{ in } M\rangle.$$

Since G is simple, $P \cap G' = P$. If $x, y \in P$ and $y = x^g$ for some $g \in G$, then Theorem 4.1 (a) yields that $g = cm$ where $c \in C_G(x)$ and $m \in M$. This implies $x^g = x^m = y$. It follows that $P = P \cap G' = P \cap M' \subseteq M'$. Since p is arbitrary in $\sigma(M)$, we have $M(\sigma) \subseteq M'$.

Consider the group M/M_α. Since $M_\alpha = O_{\alpha(M)}(M)$, we have

$$M_\alpha \subseteq M(\alpha) \subseteq M(\sigma) \subseteq M'.$$

Consider the normal subgroup F of M such that $M_\alpha \subseteq F$ and $F/M_\alpha = F(M/M_\alpha)$. Then, F/M_α is nilpotent and it is an $\alpha(M)'$-group. The extension of F over M_α splits by the Schur-Zassenhaus Theorem. Hence,

F/M_α is isomorphic to a subgroup of M. Since F/M_α is an $\alpha(M)'$-group, we have $r(F/M_\alpha) \leq 2$. By Theorem 4.20 [BG],

$$M'/M_\alpha = (M/M_\alpha)' \subseteq F(M/M_\alpha) = F/M_\alpha.$$

This implies that M'/M_α is nilpotent. Therefore, any Hall subgroup of M'/M_α is a characteristic subgroup. Since the subgroups $M(\sigma)/M_\alpha$ and $M(\alpha)/M_\alpha$ are normal subgroups of M/M_α, both $M(\sigma)$ and $M(\alpha)$ are normal subgroups of M. It follows that

$$M_\alpha = M(\alpha) \quad \text{and} \quad M_\sigma = M(\sigma).$$

This proves (a) and (b). The last statement (f) is proved in a similar way. We have also (c) and (d). To prove (e), we may assume $M_\alpha = 1$. Then, $r(M) \leq 2$. By Theorem 4.20 [BG], $O_q(M) \in Syl_q(M)$ for the largest prime q of $\pi(M)$. This implies $q \in \sigma(M)$. We need only to note that $q \in \varpi$ as $O_\varpi(M) \neq 1$. Q.E.D.

Lemma 4.3. *Suppose $M \in \mathcal{M}$, X is an $\alpha(M)'$-subgroup of M, and $r(C_{M_\alpha}(X)) \geq 2$. Then, $C_M(X) \in \mathcal{U}$.*

Lemma 4.4. *Suppose $M \in \mathcal{M}$, $p \in \pi(M)$, and $P \in Syl_p(M)$.*

(a) *If p divides $|M/M'|$, then $p \notin \sigma(M)$.*

(b) *Assume $p \notin \sigma(M)$ and $M_\alpha \neq 1$. Then, there exists $x \in \Omega_1(Z(P))^\sharp$ such that $\{M\} \neq \mathcal{M}(C_G(x))$ and $C_{M_\alpha}(x)$ is a Z-group.*

(c) *Assume $p \notin \sigma(M)$ and $r_p(M) = 2$. Then, p is not ideal and $\mathcal{E}_p^2(M) \subseteq \mathcal{E}_p^*(M)$.*

The proof of Lemma 10.4 [BG] applies here. Note that the assumptions of Part (c) imply $p \in \varpi$ by Lemma F. So, the use of the Uniqueness Theorem is justified. On the fourth line of the proof of (b) in [BG], Z stands for $\Omega_1(Z(P))$.

Lemma 4.5. *Suppose that $M \in \mathcal{M}$, $p \in \sigma(M)'$, and X is a nonidentity p-subgroup of G with $N_G(X) \subseteq M$. Then, $r_p(M) = 2$, p is not ideal, and if $|X| = p$, there exists $A \in \mathcal{E}_p^2(M)$ that contains X.*

Proof. The assumptions imply $X \subseteq M$. Since $\alpha(M) \subseteq \sigma(M)$, we have $r_p(M) \leq 2$. Let $P \in Syl_p(M)$ that contains X. If $r_p(M) = 1$, P is cyclic. Then, X is a characteristic subgroup of P. So, we have $N_G(P) \subseteq N_G(X) \subseteq M$. This contradicts the assumption that $p \notin \sigma(M)$. Therefore, $r_p(M) = 2$ and p is not ideal by Lemma 4.4. If $X = \Omega_1(Z(P))$, then we have $N_G(P) \subseteq N_G(X) \subseteq M$. So, if $|X| = p$, $X \neq \Omega_1(Z(P))$ and $X\Omega_1(Z(P)) \in \mathcal{E}_p^2(P)$. Q.E.D.

Theorem 4.6. *Let $M \in \mathcal{M}$. Then, M has p-length one for every $p \in \pi(M)$.*

We have followed the usage in [BG] so a group H is said to have p-length one for a given prime p if $H/O_{p',p}(H)$ is a p'-group.

Corollary 4.7. *Suppose that $p \in \pi(G) \cap \varpi$ and $P \in Syl_p(G)$. The following propositions hold.*

(a) *Take V to be any complement of P in $N_G(P)$. Then we have*

$$P = [P, V] \subseteq N_G(P)'.$$

(b) *Suppose $r(P) \leq 2$. Then, either P is abelian or P is the central product of a nonabelian subgroup P_1 of order p^3 and exponent p and a cyclic subgroup P_2 for which $\Omega_1(P_2) = Z(P_1)$.*

(c) *Suppose $Q \subseteq P$, $x \in G$, and $Q^x \subseteq P$. Then, $Q^x = Q^y$ for some element $y \in N_G(P)$.*

(d) *For every subgroup Q of P, the group $N_P(Q)$ is a Sylow p-subgroup of $N_G(Q)$.*

(e) *Suppose R is a p-subgroup of G and $Q \subseteq P \cap R$ and $Q \lhd N_G(P)$. Then $Q \lhd N_G(R)$.*

Proof. Since $p \in \varpi$, $N_G(P)$ is a ϖ-local subgroup. Take $M \in \mathcal{M}(N_G(P))$. By Theorem 4.6, M has p-length one, so $P \subseteq O_{p',p}(M)$. By the definition of $\sigma(M)$, we have $p \in \sigma(M)$. Theorem 4.2 shows that $P \subseteq M_\sigma \subseteq M'$. The rest of the proof is the same as that of Corollary 10.7 [BG]. Q.E.D.

Lemma 4.8. *Let $M \in \mathcal{M}$. Then the following hold.*

(a) *M_β is a Hall $\beta(M)$-subgroup of M and of G.*

(b) *M' and M_σ have nilpotent Hall $\beta(M)'$-subgroups.*

(c) *For each prime $p \in \pi(M) \setminus \beta(M)$, M' and M_σ have normal p-complements and p is the largest prime divisor of $|M/O_{p'}(M)|$.*

Corollary 4.9. *Let $M \in \mathcal{M}$.*

(a) *Suppose that p and q are distinct primes in $\pi(M) \setminus \beta(M)$ and X is a q-subgroup of M. Assume $X \subseteq M'$ or $p < q$. Then,*

(1) *X centralizes a Sylow p-subgroup of M_σ,*

(2) *if $p \in \alpha(M)$ and $X \neq 1$, then $q \in \varpi$ and $C_M(X) \in \mathcal{U}$, and*

(3) *if $X \in Syl_q(M')$, then $N_M(X)'$ contains a Sylow p-subgroup of M'.*

(b) *If $H \in \mathcal{M} \setminus \{M\}$ and $N_G(S) \subseteq H \cap M$ for some Sylow subgroup S of G, then $M = (H \cap M)M_\beta$ and $\alpha(M) = \beta(M)$.*

The proof of Corollary 10.9 [BG] can be used to prove this corollary. We shall add a few lines to verify the statement (2).

Suppose that $p \in \alpha(M)$ and $X \neq 1$. By (1), X centralizes a Sylow p-subgroup P of M_α. Since $p \in \alpha(M)$, we have $P \neq 1$ and $r(P) \geq 3$. By the Uniqueness Theorem, $P \in \mathfrak{U}$. Note that $p \in \varpi$. Since a nonidentity q-subgroup X centralizes a p-subgroup P, we have $q \in \varpi$. Since $P \subseteq C_M(X)$, $P \in \mathfrak{U}$ implies $C_M(X) \in \mathfrak{U}$.

Lemma G. *If $M \in \mathcal{M}$, then M is a ϖ-group except when*

(1) *M is a Frobenius group such that the Frobenius kernel of M is a Hall ϖ-subgroup of M, or*

(2) *M has the following structure: M/M' is a cyclic ϖ-group, $M_\alpha = M_\beta = M_{\sigma_0}$ is a nilpotent ϖ-group, and M'/M_β is a nonidentity cyclic ϖ'-group.*

In the case (1), the Frobenius kernel is M_{σ_0} and it is either M' or M_β. If it is M_β, then we have $M_\alpha = M_\beta$. In the case (2), both M' and M/M_β are Frobenius groups with Frobenius kernels M_β and M'/M_β, respectively.

Proof. By definition of $\beta(M)$, we have $M_\beta \subseteq M_\alpha \subseteq M'$ and M_β is a ϖ-group. By Lemma 4.8, M'/M_β is nilpotent. Hence, M'/M_β is either a ϖ-group or a ϖ'-group.

Suppose that M'/M_β is a ϖ-group. Then, M' is a ϖ- group. If M/M' is a ϖ-group, so is M. If M/M' is a ϖ'-group, then by Lemma A, $x \in (M')^\sharp$ satisfies $C_G(x) \subseteq M'$. This shows that M is a Frobenius group with Frobenius kernel M'. In this case, M' is nilpotent by a theorem of Thompson. If $p \in \pi(M')$, a Sylow p-subgroup P of M' is a Sylow p-subgroup of M and $P \lhd M$. It follows that $N_G(P) = M$ and $p \in \sigma_0(M)$. This proves that $M' = M_{\sigma_0}$.

Suppose that M'/M_β is a ϖ'-group. If M/M' is a ϖ'-group, so is M/M_β. We see that M is a Frobenius group with Frobenius kernel M_β. In this case, $M_\alpha = M_\beta$ because M_α is a ϖ-group, and $M_\beta = M_{\sigma_0}$ because M_β is nilpotent.

Finally, assume that M/M' is a ϖ-group. Then, M' is a Frobenius group with M_β as Frobenius kernel and M/M_β is a Frobenius group with Frobenius kernel M'/M_β. Thus, M'/M_β is nilpotent (as a Frobenius kernel) and $r(M'/M_\beta) = 1$ (as a Frobenius complement in M'). It follows that M'/M_β is cyclic. The abelian group M/M' satisfies $r(M/M') = 1$ because it is a Frobenius complement in M/M_β. Thus, M/M' is cyclic, too. This proves Lemma G. Q.E.D.

Proposition 4.10. *Suppose that p and q are distinct primes, $A \in$*

$\mathcal{E}_p^2(G) \cap \mathcal{E}_p^*(G)$, and $Q \in \mathcal{U}_G^*(A;q)$. Assume that $p \in \varpi$ and $q \in \pi(C_G(A))$. Then for some $P \in Syl_p(G)$ that contains A,

(a) $N_G(P) = O_{p'}(C_G(P))(N_G(P) \cap N_G(Q))$,

(b) $P \subseteq N_G(Q)'$, *and*

(c) *if Q is cyclic or $\mathcal{E}^2(Q) \cap \mathcal{E}^*(Q)$ is not empty, then P centralizes Q.*

Proof. Since $p \in \varpi$ and $q \in \pi(C_G(A))$, we have $q \in \varpi$. Since A is a maximal elementary abelian p-subgroup of G, we have $A = \{x \in C_G(A) \mid x^p = 1\}$. Hence, by Proposition 1.5, A satisfies Hypothesis 1.1. Since $m(Z(A)) = 2$, Theorem 1.3 yields that $O_{p'}(C_G(A))$ acts transitively on $\mathcal{U}_G^*(A;q)$. Take $P_1 \in Syl_p(G)$ such that $A \subseteq P_1$. Then, Theorem 1.4 shows

$$\mathcal{U}_G^*(P_1;q) \subseteq \mathcal{U}_G^*(A;q)$$

and for every $Q_1 \in \mathcal{U}_G^*(P_1;q)$, we have $P_1 \cap N_G(P_1)' \subseteq N_G(Q_1)'$ and

$$N_G(P_1) = O_{p'}(C_G(P_1))(N_G(P_1) \cap N_G(Q_1)).$$

Since both Q and Q_1 lie in $\mathcal{U}_G^*(A;q)$, we have $Q_1^x = Q$ for some $x \in O_{p'}(C_G(A))$. Let $P = P_1^x$. Then, P satisfies (a).

Since $p \in \varpi$, Corollary 4.7 shows that $P \subseteq N_G(P)'$. Therefore,

$$P = P \cap N_G(P)' \subseteq N_G(Q)'.$$

This proves (b). To prove (c), note that the hypothesis of (c) implies that Q is narrow. Apply Theorem 5.5 (a) [BG] to the subgroup $N_G(Q)/C_G(Q)$ of $\operatorname{Aut} Q$. It follows that $(N_G(Q)/C_G(Q))'$ is a q-group. Since $P \subseteq N_G(Q)'$, we have $P \subseteq C_G(Q)$. This proves (c). Q.E.D.

Proposition 4.11. *Suppose $M \in \mathcal{M}$ and K is a $\sigma_0(M)'$-subgroup of M. Then*

(a) *if M is a ϖ-group, $K \notin \mathcal{U}$;*

(b) $r(C_K(M_{\sigma_0})) \leq 1$;

(c) *$C_K(M_{\sigma_0}) \cap M'$ is a cyclic normal subgroup of M; and*

(d) *if $p \in \sigma_0(M)'$, $P \in \mathcal{E}_p^1(N_M(K))$, $C_{M_{\sigma_0}}(P) = 1$, and K is an abelian p'-group, then $[K,P]$ centralizes M_{σ_0} and is a cyclic normal subgroup of M.*

Proof. There is a small difference between this and Proposition 10.11 [BG]. If M is a ϖ-group, we have $\sigma_0(M) = \sigma(M)$ and for every subgroup P of M, $N_G(P)$ is a ϖ-local subgroup. The proof of Part (a) in [BG] is valid in our case.

To prove (b), suppose $r_p(C_K(M_{\sigma_0})) \geq 2$ for some prime p. Then,

$$p \in \pi(K) \subseteq \sigma_0(M)'.$$

By Lemma G, M is a ϖ-group. Thus, $\sigma_0(M) = \sigma(M)$ and Part (a) implies $K \notin \mathcal{U}$. The argument in the proof of Part (b) of Proposition 10.11 [BG] gives us $p \in \sigma(M)$. However, $p \in \pi(K) \subseteq \sigma(M)'$. This contradiction proves (b).

For (c) and (d), read σ_0 for σ in the proof of Proposition 10.11 [BG]. The assertions are proved. Q.E.D.

Lemma 4.12. *Suppose M, $H \in \mathcal{M}$ and H is not conjugate to M in G. Then,*

(a) *$M_\alpha \cap H_\sigma = 1$ and $\alpha(M)$ is disjoint from $\sigma(H)$, and*
(b) *if M_σ is nilpotent, then $M_\sigma \cap H_\sigma = 1$ and $\sigma(M)$ is disjoint from $\sigma(H)$.*

Proof. The proof is similar to the one of Lemma 10.12 [BG].

Suppose that $p \in \sigma_0(M) \cap \sigma(H)$. Then some Sylow p-subgroup S of G lies in M and in a conjugate H^g of H. Then, $S \in M \cap H^g$ and $M \neq H^g$ by assumption. Since $p \in \varpi$, the Uniqueness Theorem yields that $r(S) \leq 2$. Thus, $p \notin \alpha(M)$. This proves (a).

Assume that M_σ is nilpotent. Suppose $\sigma(M) \cap \sigma(H)$ is not empty. Take a prime p in $\sigma(M) \cap \sigma(H)$. As before, some Sylow p-subgroup P lies in M and in some conjugate H^x of H. Then, $M \neq H^x$ and $N_G(P) \subseteq M \cap H^x$. In particular, P is not normal in M, so M_σ is not nilpotent. Q.E.D.

Lemma 4.13. *Suppose $p \in \varpi$, $A \in \mathcal{E}_p^2(G) \cap \mathcal{E}_p^*(G)$, and P is a nonabelian p-subgroup of G that contains A. Let $Z_0 = \Omega_1(Z(P))$ and $A_0 \in \mathcal{E}^1(A)$ such that $A_0 \neq Z_0$. Then,*

(a) *$Z_0 \in \mathcal{E}^1(A)$,*
(b) *$C_P(A) = A_0 \times Z$ with Z a cyclic subgroup that contains Z_0, and*
(c) *$N_P(A)$ acts transitively by conjugation on $\mathcal{E}^1(A) \setminus \{Z_0\}$.*

Proof. Let S be a Sylow p-subgroup that contains P. Since $p \in \varpi$, we can apply Lemma 4.7 (b) when $r(S) \leq 2$. The proof of Lemma 10.13 [BG] will prove this lemma. Q.E.D.

Proposition 4.14. *Let $M \in \mathcal{M}$, $p \in \beta(M)$, and $P \in Syl_p(M)$.*

(a) *The sets $\mathcal{E}_p^2(P) \cap \mathcal{E}_p^*(P)$ and $\mathcal{E}_p^2(G) \cap \mathcal{E}_p^*(G)$ are empty.*
(b) *Every p-subgroup R of G such that $r(R) \geq 2$ lies in $\mathcal{U}$.*

(c) *If X is a subgroup of P, then $N_P(X) \in \mathfrak{U}$.*

(d) *For every nonidentity $\beta(M)$-subgroup Y of M, $N_G(Y) \subseteq M$.*

Proof. (a) By the definition of $\beta(M)$, $\mathcal{E}_p^2(G) \cap \mathcal{E}_p^*(P)$ is empty for the Sylow p-subgroup P of M. If $A \in \mathcal{E}_p^2(G) \cap \mathcal{E}_p^*(G)$, take a Sylow p-subgroup Q of G such that $A \subseteq Q$. Then, $Q^g = P$ for some $g \in G$. Thus, $A^g \subseteq Q^g = P$ and $A^g \in \mathcal{E}_p^2(P) \cap \mathcal{E}_p^*(P)$. This is a contradiction.

(b) We can assume $R \subseteq P$ by choosing a conjugate of R. Take $A \in \mathcal{E}_p^2(R)$. By (a), there is $B \in \mathcal{E}_p^*(P)$ such that $A \subseteq B$ and $m(B) \geq 3$. Since $B \subseteq C_G(A)$, we have $r_p(C_G(A)) \geq 3$. Since $p \in \beta(M) \subseteq \varpi$, the Uniqueness Theorem yields $A \in \mathfrak{U}$. Therefore, we have $R \in \mathfrak{U}$.

(c) Let $Q = N_P(X)$. If $r(Q) \geq 2$, then $Q \in \mathfrak{U}$ by (b). Suppose that $r(Q) = 1$. Then, Q is cyclic, X chra Q, and $N_P(Q) \subseteq N_G(X) = Q$. Since P is a p-group, this implies $Q = P$ contrary to the assumption that $p \in \beta(M)$.

(d) Let $q \in \pi(F(Y))$ and $X = O_q(Y)$. We can assume that $q = p$ and $X \subseteq P$. Then, by (c), $N_P(X) \in \mathfrak{U}$. Since $N_G(X)$ is ϖ-local, we have $N_G(X) \subseteq M$ and $N_G(Y) \subseteq N_G(X) \subseteq M$.

§5. Exceptional Subgroups of $\mathcal{M}$

The following conditions and notation are used throughout this section.

Hypothesis 5.1. Suppose $M \in \mathcal{M}$, $p \in \sigma(M)'$, $A_0 \in \mathcal{E}_p^1(M)$, and

$$N_G(A_0) \subseteq M.$$

By Lemma 4.5, $r_p(M) = 2$ and $A_0 \subseteq A$ for some $A \in \mathcal{E}_p^2(M)$. Let P be a Sylow p-subgroup of M that contains A. Since $r_p(M) = 2$ for $p \in \sigma(M)'$, Lemma G implies that M is a ϖ-group. As $p \in \sigma(M)'$, $N_G(P) \nsubseteq M$ and since $C_G(A) \subseteq C_G(A_0) \subseteq N_G(A_0) \subseteq M$, we have $A \in \mathcal{E}_p^*(G)$.

We will fix the subgroups A and P throughout this section.

Lemma 5.1. *Suppose that $g \in G \setminus M$, $A \subseteq M^g$, $q \in \sigma(M)$, and that Q_1 and Q_2 are A-invariant Sylow q-subgroups of M_σ and ${M_\sigma}^g$, respectively. Then,*

(a) *$Q_1 \cap Q_2 = 1$, and*

(b) *if $X \in \mathcal{E}^1(A)$, then $C_{Q_1}(X) = 1$ or $C_{Q_2}(X) = 1$.*

Proof. As remarked at the beginning of this section, Hypothesis 5.1 implies that M is a ϖ-group. Thus, if $Q_1 \cap Q_2 \neq 1$, the subgroup $Q_1 \cap Q_2$ is a ϖ-group $\neq 1$. Also, $C_G(X)$ is a ϖ-group by Lemma A. Thus, if either (a) or (b) is false, there is a ϖ-local subgroup H such that

$$H \cap Q_1 \neq 1 \quad \text{and} \quad H \cap Q_2 \neq 1.$$

(Cf. Lemma D.) By Lemma 1.1, we have $Q_2 = {Q_1}^k$ for some element $k \in C_G(A)$. The rest of the proof is the same as that of Lemma 11.1 [BG]. Q.E.D.

Corollary 5.2. *Suppose $g \in G \setminus M$ and $A \subseteq M^g$. Then,*

(a) $M_\sigma \cap M^g = 1$, *and*
(b) $M_\sigma \cap C_G({A_0}^g) = 1$.

Theorem 5.3. *The group M_σ is nilpotent.*

Corollary 5.4. *Suppose $H \in \mathcal{M}(A)$ and $M_\sigma \cap H_\sigma \neq 1$. Then, $M = H$.*

Theorem 5.5. *The Sylow p-subgroups of M are abelian.*

Corollary 5.6. *We have*

(a) $A = \Omega_1(P)$,
(b) $C_{M_\sigma}(A) = 1$, *and*
(c) *there exist subgroups A_1, $A_2 \in \mathcal{E}_p^1(A)$ such that $A_1 \neq A_2$ and $C_{M_\sigma}(A_1) = C_{M_\sigma}(A_2) = 1$.*

Theorem 5.7. *We have $M_\sigma A \lhd M$.*

§6. The Subgroup E

Let E denote a complement of M_σ in M, which will be fixed for discussion. We use the notation τ_i and E_i as defined in [BG], Section 12.

Lemma 6.1. (a) *E' is nilpotent.*

(b) $E_3 \subseteq E'$ *and* $E_3 \lhd E$.
(c) *If* $E_2 = 1$, *then* $E_1 \neq 1$.
(d) E_1 *and* E_3 *are cyclic.*
(e) $E = E_1E_2E_3$, $E_{12} = E_1E_2$, $E_2E_3 \lhd E$, *and* $E_2 \lhd E_{12}$.
(f) $C_{E_3}(E) = 1$.
(g) *If* $p \in \tau_2(M)$ *and* $A \in \mathcal{E}_p^2(M)$, *then* $A \in \mathcal{E}_p^*(G)$ *and* $p \notin \beta(G)$.

Lemma 6.2. *Suppose that $M \in \mathcal{M}$, p is a prime, X is a nonidentity p-subgroup of M, and $M^* \in \mathcal{M}(N_G(X))$. Then,*

(a) *$p \in \sigma(M^*) \cup \tau_2(M^*)$, and*

(b) *if $p \in \sigma(M)$ and $M \neq M^*$, or if $p \in \tau_1(M) \cup \tau_3(M)$, then M^* is not conjugate to M in G.*

Proof. (a) Suppose that $p \notin \sigma(M^*)$. Then, Lemma 4.5 applied to M^* implies that $r_p(M^*) = 2$. This proves $p \in \tau_2(M^*)$.

(b) Suppose that M^* is conjugate to M. Then, $\sigma(M) = \sigma(M^*)$ and $\tau_i(M) = \tau_i(M^*)$ for $i = 1, 2, 3$. Therefore, if $p \in \tau_1(M) \cup \tau_3(M)$, we have a contradiction to (a). Suppose that $p \in \sigma(M)$. Then, by Theorem 4.1(b), M^* and M are conjugate by an element x of $C_G(X)$: $M = (M^*)^x$. Since $C_G(X) \subseteq N_G(X) \subseteq M^*$, we have $M = M^*$. This proves (b). Q.E.D.

Remark. If $p \in \varpi$, a subgroup M^* is available; however, if $p \in \varpi$ is not assumed, Lemma 6.2 holds only when there is a ϖ-local subgroup that contains $N_G(X)$.

Lemma 6.3. *Suppose $M^* \in \mathcal{M} \setminus \{M\}$, p is a prime, $A \in \mathcal{E}_p^2(M \cap M^*)$, and $N_G(A_0) \subseteq M^*$ for some $A_0 \in \mathcal{E}^1(A)$.*

(a) *If $p \notin \sigma(M)$, then A centralizes $M_\sigma \cap M^*$.*

(b) *If $p \in \sigma(M) \setminus \alpha(M)$, then A centralizes $M_\alpha \cap M^*$.*

Proposition 6.4. *Suppose $M \in \mathcal{M}$, p is a prime and $A \in \mathcal{E}_p^2(M)$. Then,*

(a) *$C_G(A) \subseteq M$, and*

(b) *if $\mathcal{M}(N_G(A_0)) \neq \{M\}$ for every $A_0 \in \mathcal{E}^1(A)$, then $p \in \sigma(M)$, $M_\alpha = 1$, and M_σ is nilpotent.*

Proof. By assumption, $r_p(M) \geq 2$ so $p \in \varpi$. Thus, for every $X \in \mathcal{E}^1(A)$, $N_G(X)$ is a ϖ-local subgroup. The proof of Proposition 12.4 [BG] can be adapted to yield the results. However, this is basic so we repeat the argument.

Suppose that $\mathcal{M}(N_G(A_0)) = \{M\}$ for some $A_0 \in \mathcal{E}^1(A)$. Then, $C_G(A) \subseteq C_G(A_0) \subseteq N_G(A_0) \subseteq M$. This proves (a) in this case.

For the remainder of proof, we may assume that $\mathcal{M}(N_G(X)) \neq \{M\}$ for every $X \in \mathcal{E}^1(A)$. For a fixed $X \in \mathcal{E}^1(A)$, choose

$$M^* = M^*(X) \in \mathcal{M}(N_G(X)) \setminus \{M\}.$$

Since $C_M(X) \subseteq M \cap M^*$, the Uniqueness Theorem implies

$$r(C_M(A)) \le r(C_M(X)) \le 2.$$

We claim that $p \in \sigma(M)$. Suppose $p \notin \sigma(M)$. Then, Lemma 6.3(a) implies that $C_{M_\sigma}(X) \subseteq M_\sigma \cap M^* \subseteq C_M(A)$. This holds for every $X \in \mathcal{E}^1(A)$. By Proposition 1.16 [BG], $M_\sigma = \langle C_{M_\sigma}(X) \mid X \in \mathcal{E}^1(A)\rangle$. Since $C_{M_\sigma}(X) \subseteq C_M(A)$ for every $X \in \mathcal{E}^1(A)$, we have $M_\sigma \subseteq C_M(A)$ which contradicts Proposition 4.11 (b). Thus, we have $p \in \sigma(M)$.

Let P be a Sylow p-subgroup of M_σ that contains A and let $Z = \Omega_1(Z(P))$. Since $r(C_M(A)) \le 2$, we have $Z \subseteq A$. Take $X \in \mathcal{E}^1(Z)$. Then, $P \subseteq C_M(X)$ and $r(P) \le r(C_M(X)) \le 2$. This proves that $p \in \sigma(M) \setminus \alpha(M)$. We apply the same argument as before to M_α. Again for any $X \in \mathcal{E}^1(A)$, choose $M^* \in \mathcal{M}(N_G(X)) \setminus \{M\}$. Then, Lemma 6.3 (b) implies that $C_{M_\alpha}(X) \subseteq M_\alpha \cap M^* \subseteq C_M(A)$. It follows that $M_\alpha = \langle C_{M_\alpha}(X) \mid X \in \mathcal{E}^1(A)\rangle \subseteq C_M(A)$. This implies $M_\alpha = 1$ because $r(C_M(A)) = 2$. By Theorem 4.2 (d), $M' = M'/M_\alpha$ is nilpotent. Since $M_\sigma \subseteq M'$, M_σ is nilpotent. This proves (b).

Since M_σ is nilpotent, we have $P \lhd M$. Hence,

$$Z = \Omega_1(Z(P)) \lhd M.$$

Since $Z \subseteq A$, we have $C_G(A) \subseteq C_G(Z) \subseteq N_G(Z) = M$. The last equality comes from Lemma E (1). This completes the proof of Proposition 6.4. Q.E.D.

We state a corollary of Lemma G.

Lemma H. *Let $M \in \mathcal{M}$.*

(1) *If $\tau_2(H) \ne \emptyset$, then M is a ϖ-group.*
(2) *If M is not a ϖ-group, then $r_p(M) \le 1$ for all $p \notin \sigma_0(M)$.*

This follows immediately from the structure of subgroups in $\mathcal{M}$ which are not ϖ-groups given in Lemma G.

Theorem 6.5. *Suppose $M \in \mathcal{M}$ and $\tau_2(M) \ne \emptyset$. Let $p \in \tau_2(M)$ and $A \in \mathcal{E}_p^2(M)$. Then, M is a ϖ-group and the following hold:*

(a) *M_σ is nilpotent,*
(b) *M has abelian Sylow p-subgroups and every Sylow p-subgroup P of M such that $A \subseteq P$ satisfies $\Omega_1(P) = A$ and $N_G(P) \not\subseteq M$,*
(c) *$M_\sigma A \lhd M$,*
(d) *$C_{M_\sigma}(A) = 1$,*
(e) *$M_\sigma \cap M^* = 1$ for every $M^* \in \mathcal{M}(A) \setminus \{M\}$, and*
(f) *there exists $A_1 \in \mathcal{E}^1(A)$ such that $C_{M_\sigma}(A_1) = 1$.*

Proof. Since $\tau_2(M) \neq \emptyset$, M is a ϖ-group by Lemma H. Hence, for any $X \in \mathcal{E}^1(A)$, $N_G(X)$ is a ϖ-local subgroup. Since $p \notin \sigma(M)$, Proposition 6.4 (b) implies that $\mathcal{M}(N_G(A_0)) = \{M\}$ for some $A_0 \in \mathcal{E}^1(A)$. Thus, we have Hypothesis 5.1 for A_0 and M. The results of Section 5 prove Theorem 6.5 except (e).

To prove (e), take $M^* \in \mathcal{M}(A) \setminus \{M\}$. If $N_G(A_0) \subseteq M^*$ for some $A_0 \in \mathcal{E}^1(A)$, Lemma 6.3 (a) shows that A centralizes $M_\sigma \cap M^*$. On the other hand, $C_{M_\sigma}(A) = 1$ by (d). This proves $M_\sigma \cap M^* = 1$. If $N_G(X) \nsubseteq M^*$ for every $X \in \mathcal{E}^1(A)$, the hypothesis of Proposition 6.4 (b) is satisfied for M^*. Hence, we have $p \in \sigma(M^*)$ and $M^*{}_\sigma$ is nilpotent. It follows that $A \subseteq O_p(M^*)$ and $[M_\sigma \cap M^*, A] \subseteq M_\sigma \cap O_p(M^*) = 1$ because $p \notin \sigma(M)$. So, $M_\sigma \cap M^* \subseteq C_{M_\sigma}(A) = 1$. Q.E.D.

Corollary 6.6. *Suppose $M \in \mathcal{M}$ and $\tau_2(M) \neq \emptyset$. Let $p \in \tau_2(M)$ and $A \in \mathcal{E}_p^2(E)$. Then,*

(a) *$A \lhd E$ and $\mathcal{E}_p^1(E) = \mathcal{E}^1(A)$,*
(b) *$C_G(A) \subseteq N_M(A) = E$ and $N_G(A) \nsubseteq M$,*
(c) *$\mathcal{M}(C_G(X)) = \{M\}$ for each $X \in \mathcal{E}^1(A)$ such that $C_{M_\sigma}(X) \neq 1$,*
(d) *$C_{M_\sigma}(x) = 1$ for each $x \in E_3{}^\sharp$,*
(e) *$C_{M_\sigma}(x) = 1$ for each $x \in C_{E_1}(A)^\sharp$, and*
(f) *if $M^* \in \mathcal{M}$ is not conjugate to M, then $M_\sigma \cap M^*{}_\sigma = 1$ and $\sigma(M^*)$ is disjoint from $\sigma(M)$.*

Proof. As before, Lemma H implies that M is a ϖ-group. Since E is a complement of M_σ, Theorem 6.5 (c) implies $A \lhd E$. If $X \in \mathcal{E}_p^1(E)$, then AX is a p-subgroup of E. Let P be a Sylow p-subgroup of E such that $AX \subseteq P$. By Theorem 6.5 (b), we have $\Omega_1(P) = A$. Since $X \subseteq \Omega_1(P)$, $X \subseteq A$. This proves $\mathcal{E}_p^1(E) = \mathcal{E}^1(A)$. This proves (a).

We have $C_G(A) \subseteq M$ by Proposition 6.4 (a). Thus, $C_G(A) \subseteq N_M(A)$. By (a), $E \subseteq N_M(A)$. It follows from the Dedekind law that

$$N_M(A) = N_M(A) \cap M_\sigma E = N_{M_\sigma}(A)E.$$

We have $[N_{M_\sigma}(A), A] \subseteq M_\sigma \cap A = 1$, so $N_{M_\sigma}(A) \subseteq C_{M_\sigma}(A) = 1$ by Theorem 6.5 (d). This proves that $N_M(A) = E$. If P is any Sylow p-subgroup of M that contains A, then $A = \Omega_1(P)$ by Theorem 6.5 (b). Hence, $N_G(P) \subseteq N_G(A)$. Since $N_G(P) \nsubseteq M$ by Theorem 6.5 (b), we have $N_G(A) \nsubseteq M$. This proves (b).

Suppose $C_{M_\sigma}(X) \neq 1$ and $\mathcal{M}(C_G(X)) \neq \{M\}$ for some $X \in \mathcal{E}^1(A)$. Take M^* such that $C_G(X) \subseteq M^* \neq M$. Since $A \subseteq C_G(X)$, Theorem 6.5 (e) implies that $M_\sigma \cap M^* = 1$. Hence,

$$C_{M_\sigma}(X) \subseteq M_\sigma \cap C_G(X) \subseteq M_\sigma \cap M^* = 1.$$

This contradiction proves (c).

For (d) and (e), we may assume that $\langle x\rangle = X$ is a q-group for some prime $q \in \tau_1(M) \cup \tau_3(M)$. As remarked at the beginning of the proof, $q \in \varpi$ so we can take $M^* \in \mathcal{M}(N_G(X))$. By Lemma 6.2, M^* is not conjugate to M. In particular, $M^* \neq M$. Since A and E_3 are normal subgroups of E with $A \cap E_3 = 1$, A centralizes E_3. Thus, $A \subseteq C_G(X) \subseteq M^*$ in all cases. By Theorem 6.5 (e), we have $M_\sigma \cap M^* = 1$. Therefore,

$$C_{M_\sigma}(X) \subseteq M_\sigma \cap C_G(X) \subseteq M_\sigma \cap M^* = 1.$$

This proves (d) and (e).

Since M_σ is nilpotent (cf. Theorem 6.5 (a)), Lemma 4.12 (b) yields (f). Q.E.D.

Theorem 6.7. *Suppose that $M \in \mathcal{M}$, $p \in \tau_2(M)$, $A \in \mathcal{E}_p^2(E)$, and assume that G has nonabelian Sylow p-subgroups. Then,*

(a) $\tau_2(M) = \{p\}$,

(b) $A_0 = C_A(M_\sigma)$ *has order* p *and satisfies* $F(M) = M_\sigma \times A_0$,

(c) *every* $X \in \mathcal{E}_p^1(E) \backslash \{A_0\}$ *satisfies* $C_{M_\sigma}(X) = 1$ *and* $C_G(X) \not\subseteq M$,

(d) A_0 *has a complement* E_0 *in* E, *and*

(e) $\pi(C_{E_0}(x)) \subseteq \tau_1(M)$ *for every* $x \in M_\sigma{}^\sharp$.

Proof. The assumptions of this theorem imply that M is a ϖ-group (by Lemma H). The argument of the proof of Theorem 12.7 [BG] proves the assertions. We paraphrase a few points in the argument.

The subgroup A_0 was defined as an element of $\mathcal{E}^1(A)$ such that $C_{M_\sigma}(A_0) \neq 1$. It is proved to be the unique element with $C_{M_\sigma}(A_0) \neq 1$. We have $A_0 = C_A(M_\sigma)$. Since $A \lhd E$ by Corollary 6.6 (a), E normalizes A_0. Note that $M_\sigma \lhd M$. Clearly, M_σ normalizes A_0, so $M = M_\sigma E$ normalizes A_0. Thus, $A_0 \lhd M$ and A_0 is a part of the Fitting subgroup $F(M)$. Apply Lemma 6.2 taking each $q \in \pi(F(M))$ and $X = O_q(M)$. Then, $M \in \mathcal{M}(N_G(X))$ and $q \in \sigma(M) \cup \tau_2(M)$. This proves that $\pi(F(M)) = \sigma(M) \cup \{p\}$ as M_σ is nilpotent (Theorem 6.5 (a)) and $\tau_2(M) = \{p\}$ by (a). Q.E.D.

Lemma 6.8. *Suppose that $M \in \mathcal{M}$, $p \in \tau_2(M)$, $A \in \mathcal{E}_p^2(E)$, and S is a Sylow p-subgroup of G that contains A. Assume that S is abelian. Then,*

(a) E_2 *is an abelian normal subgroup of* E,

(b) E_2 *is a Hall* $\tau_2(M)$-*subgroup of* G,

(c) $S \subseteq N_G(S)' \subseteq F(E) \subseteq C_G(S) \subseteq E$ *and* $S = O_p(E)$,

(d) $N_G(A) = N_G(S) = N_G(E_2) = N_G(E_2E_3) = N_G(F(E)) \not\subseteq M$,

(e) *every* $X \in \mathcal{E}^1(E_1)$ *for which* $C_{M_\sigma}(X) = 1$ *lies in* $Z(E)$, *and*
(f) *we have* $C_S(X) \lhd N_G(S)$ *and* $[S, X] \lhd N_G(S)$ *for every subgroup* X *of* $N_G(S)$.

Proof. As before, the assumptions imply that M is a ϖ- group. By Theorem 6.7 (a), each $p \in \tau_2(M)$ satisfies the assumption that G has abelian Sylow p-subgroups. Since $S \subseteq C_G(A) \subseteq E$ by Corollary 6.6 (b), E_2 is a Hall $\tau_2(M)$-subgroup of G. This proves (b).

By Corollary 6.6 (a), we have $E \subseteq N_G(A)$.

Clearly, $A \subseteq O_p(N_G(A)) \subseteq S$. Hence, A is contained in the center of $F(N_G(A))$. Thus,

$$F(N_G(A)) \subseteq C_G(A) \subseteq E \subseteq N_G(A).$$

This proves two properties. One is $F(N_G(A)) \subseteq F(C_G(A)) \subseteq F(E)$, and the other property is $r(F(N_G(A))) \leq r(E) \leq 2$. By Theorem 4.20 [BG], we have $N_G(A)' \subseteq F(N_G(A))$. It follows that $E \lhd N_G(A)$, so $F(E) \subseteq F(N_G(A))$. We have $F(N_G(A)) = F(C_G(A)) = F(E)$. By Theorem 6.5 (b), we have $A = \Omega_1(S)$, so $N_G(S) \subseteq N_G(A)$. Moreover, Corollary 4.7 (a) shows $S \subseteq N_G(S)'$. It follows that

$$S \subseteq N_G(S)' \subseteq N_G(A)' \subseteq F(N_G(A)) = F(E).$$

This implies that $S = O_p(E)$ and $F(E) \subseteq C_G(S) \subseteq C_G(A) \subseteq E$. We have proved (c). As remarked earlier, $S = O_p(E)$ for every $p \in \tau_2(M)$. This implies $E_2 \lhd E$ and (a) holds.

Let $K = E_2E_3$. Then, $E_3 \lhd E$ by Lemma 6.1 (a). Since $E_2 \lhd E$ and $E_2 \cap E_3 = 1$, we have $K = E_2E_3 = E_2 \times E_3$. Since E_3 is cyclic by Lemma 6.1 (d) and E_2 is abelian, K is a Hall subgroup of $F(E)$. Each subgroup in the series

$$A \subseteq S \subseteq E_2 \subseteq E_2E_3 \subseteq F(E)$$

is characteristic in its successor. Since $F(E) = F(N_G(A))$, we have (d).

By (d), $K \lhd N_G(K) = N_G(S)$. Also, $N_G(S)' \subseteq F(E) \subseteq C_G(K)$ by (c). Let $X \in \mathcal{E}^1(E_1)$ be a subgroup such that $C_{M_\sigma}(X) = 1$. Then, $N_G(S)'X \lhd N_G(S)$ and $N_G(S)' \subseteq C_G(K)$. Consider $Y = [K, X]$. Then, it is a subgroup of K and

$$Y = [K, X] = [K, N_G(S)'X] \lhd N_G(S).$$

Thus, $N_G(Y) \supseteq N_G(S)$ so we have $N_G(Y) \nsubseteq M$. On the other hand, Proposition 4.11 (d) applies to X and shows that $Y = [K, X] \lhd M$. If $Y \neq 1$, then Y is a nonidentity normal ϖ-subgroup of M. This would imply $N_G(Y) = M$ by Lemma E (1). However, we have shown that $N_G(Y) \not\subseteq M$. This contradiction proves $[K, X] = 1$. Since $E = E_1 K$ and E_1 is cyclic (Lemma 6.1), we have $X \subseteq Z(E)$. This proves (e).

To prove (f), note that for any subgroup X of $N_G(S)$,

$$C_G(S)X \lhd N_G(S)$$

because $N_G(S)' \subseteq C_G(S)$ by (c). Then, $C_S(X) = C_S(C_G(S)X) \lhd N_G(S)$ and $[S, X] = [S, C_G(S)X] \lhd N_G(S)$. Q.E.D.

Corollary 6.9. *Suppose $M \in \mathcal{M}$, $p \in \tau_2(M)$, $A \in \mathcal{E}_p^2(E)$, $q \in \tau_1(M)$, $Q \in \mathcal{E}_q^1(E)$, $C_{M_\sigma}(Q) = 1$, and $[A, Q] \neq 1$. Let $A_0 = [A, Q]$ and $A_1 = C_A(Q)$. Then, G has nonabelian Sylow p-subgroups. We have*

(a) *$A_0 \in \mathcal{E}^1(A)$ and $A_0 = C_A(M_\sigma) \lhd M$,*
(b) *A_0 is not conjugate to A_1 in G, and*
(c) *$A_1 \in \mathcal{E}^1(A)$ and $C_G(A_1) \not\subseteq M$.*

Proof. If G has abelian Sylow p-subgroups, Lemma 6.8 (e) implies either $C_{M_\sigma}(Q) \neq 1$ or $[A, Q] = 1$. Thus, G has nonabelian Sylow p-subgroups.

Since A is abelian, we have $A = A_0 \times A_1$ by Proposition 1.6 [BG]. Proposition 4.11 (d) with (p, P, K) replaced by (q, Q, A) yields that $A_0 = [A, Q] \neq 1$ is a cyclic normal subgroup of M. It follows that $A_0 \subseteq C_A(M_\sigma)$. Theorem 6.7 (b) yields (a).

This implies that $A_1 \in \mathcal{E}^1(A)$. Then, Theorem 6.7 (c) proves (c). Since $r_q(M) = 1$ and Q does not centralize A_0, $C_G(A_0)$ is a q'-group. Therefore, (b) holds. Q.E.D.

Corollary 6.10. *Let $M \in \mathcal{M}$.*

(a) *Every nilpotent $\sigma(M)'$-subgroup of M is abelian.*
(b) *The groups E_2 and E' are abelian.*
(c) *Suppose $p \in \tau_2(M)$ and $A \in \mathcal{E}_p^2(E)$. Then, $E_2 E_3 \subseteq C_E(A) \lhd E$ and $\pi(E/C_E(A)) \subseteq \tau_1(M)$.*
(d) *Suppose $p \in \sigma(M)$ and P is a noncyclic p-subgroup of M. Then, $N_G(P) \subseteq M$.*
(e) *Suppose $x \in M^\sharp$, $\pi(\langle x \rangle) \subseteq \tau_2(M)$, and $C_{M_\sigma}(x) \neq 1$. Then, $\mathcal{M}(C_G(x)) = \{M\}$.*

Proof. We will paraphrase the proof of Part (e); the remainder is straightforward (cf. the proof of Corollary 12.10 [BG]).

The group M contains an abelian Hall $\tau_2(M)$-subgroup E_2 (Theorems 6.7 (a) and 6.5 (b), and Lemma 6.8 (a)). This implies that any

$\tau_2(M)$-subgroup of M is conjugate to a subgroup of E_2. Since $\langle x \rangle$ is a $\tau_2(M)$-subgroup of M, $\langle x \rangle$ is conjugate to a subgroup of E_2 in M. Thus, we may assume that $x \in E_2$.

We have $\tau_2(M) \neq \emptyset$. By Lemma H, M is a ϖ-group. So, $C_G(x)$ is contained in a ϖ-local subgroup and contains $A \in \mathcal{E}_p^2(E)$ for some $p \in \tau_2(M)$. If $C_G(x) \subseteq M^* \in \mathcal{M}(C_G(x)) \setminus \{M\}$, Theorem 6.5 (e) yields that $C_{M_\sigma}(x) \subseteq M_\sigma \cap N^* = 1$. This proves (d). Q.E.D.

Lemma 6.11. *Suppose $M \in \mathcal{M}$, $p \in \tau_2(M)$, $A \in \mathcal{E}_p^2(E)$, and $M^* \in \mathcal{M}(N_G(A))$. Then,*

(a) $\tau_2(M) \subseteq \sigma(M^*) \setminus \beta(M^*)$,

(b) $\pi(E/C_E(A)) \subseteq \tau_1(M^*) \cup \tau_2(M^*)$, *and*

(c) *if $q \in \pi(E/C_E(A)) \cap \pi(C_E(A))$, then $q \in \tau_2(M^*)$, some Sylow p-subgroup of G is normal in M^*, and M^* contains an abelian Sylow q-subgroup of G.*

Proof. As before M is a ϖ-group. The proof of (a) and (b) is similar to the corresponding proof of Lemma 12.11 [BG]. We paraphrase the proof of Part (c).

Let $q \in \pi(E/C_E(A)) \cap \pi(C_E(A))$ and $Q \in Syl_q(E)$. Corollary 6.10 (c) yields $q \in \tau_1(M)$. It follows that Q is cyclic. Since $A \lhd E$ by Corollary 6.6 (a), we have $C_E(A) \lhd E$. Hence, $Q \cap C_E(A)$ is a Sylow q-subgroup of $C_E(A)$. Thus, we have $Q_0 = \Omega_1(Q) \subseteq C_E(A)$ and $Q_0 \neq Q$.

By Corollary 6.6 (b), $C_G(A) \subseteq E$ so $C_G(A)$ has a cyclic Sylow q-subgroup. The Frattini argument yields

$$N_G(A) = C_G(A)(N_G(A) \cap N_G(Q_0)).$$

Take $M^{**} \in \mathcal{M}(N_G(Q_0))$. Since $Q_0 \subseteq C_E(A)$, we have $A \subseteq N_G(Q_0)$. Proposition 6.4 applied to M^{**} yields that $C_G(A) \subseteq M^{**}$. The above displayed formula shows $N_G(A) \subseteq M^{**}$. By (b) and Lemma 6.2 (a) both applied to A and M^{**}, the prime q lies in $\sigma(M^{**}) \cup \tau_2(M^{**})$ and in $\tau_1(M^{**}) \cup \tau_2(M^{**})$. Therefore, $q \in \tau_2(M^{**})$. The part (a) applied to M^* and then to M^{**} shows that $p \in \sigma(M^*)$ and $p \in \sigma(M^{**})$. Since $q \in \tau_2(M^{**})$, we can apply Corollary 6.6 for M^{**}. The part (f) implies that M^* is conjugate to M^{**}; otherwise we would have $\sigma(M^*) \cap \sigma(M^{**}) = \emptyset$. Since $A \subseteq M^* \cap M^{**}$, Theorem 4.1 (b) shows that M^{**} is conjugate to M^* by an element of $C_G(A)$. But, $C_G(A) \subseteq M^{**}$ so we have $M^{**} = M^*$. Thus, $q \in \tau_2(M^*)$.

It follows from Theorem 6.5 (a) that $(M^*)_\sigma$ is nilpotent. Since $p \in \sigma(M^*) \setminus \beta(M^*)$ by (a), $O_p(M^*)$ is a Sylow p-subgroup of M^* and of G. This proves the second statement.

Since $q \in \tau_2(M^*)$, Theorem 6.5 (b) applied to M^* yields that M^* has abelian Sylow q-subgroups. Note that $Q_0 \lhd Q$ so $Q \subseteq M^{**} = M^*$. Let E^* be a complement of $(M^*)_\sigma$ in M^* that contains Q. Let S be a Sylow q-subgroup of E^* that contains Q. We will show that $S \in Sy\ell_q(G)$.

Suppose that G has nonabelian Sylow q-subgroups. Theorem 6.7 applied to M^* yields the following. Among the elements of $\mathcal{E}^1(S)$, there is a unique subgroup X_0 such that $C_{M^*_\sigma}(X_0) \neq 1$ (Theorem 6.7 (c)). This subgroup X_0 has a complement E_0 in E^* (Part (d)). We have $A \subseteq M^*_\sigma \cap C_G(Q_0)$. Therefore, we must have $X_0 = Q_0$. Since Q_0 has a complement E_0 in E^*, the Dedekind law shows that $E_0 \cap Q$ must be a complement of Q_0 in Q. Since $Q \neq Q_0$ and Q is cyclic, Q_0 has no complement in Q. This is a contradiction. Thus, G has abelian Sylow q-subgroups. By Lemma 6.8 (b), we have $S \in Sy\ell_q(G)$. This completes the proof. Q.E.D.

Theorem 6.12. *Suppose $M \in \mathcal{M}$ and $C_{M_{\sigma_0}}(e) = 1$ for each $(\tau_1(M) \cup \tau_3(M))$-element $e \in E^\sharp$. Then,*

(a) *E contains an abelian normal subgroup A_0 such that $C_E(x) \subseteq A_0$ for every $x \in (M_{\sigma_0})^\sharp$, and*

(b) *E contains a subgroup E_0 of the same exponent as E such that $E_0 M_{\sigma_0}$ is a Frobenius group with Frobenius kernel M_{σ_0}.*

Proof. If $E_2 = 1$, then $E = E_1 E_3$ acts regularly on M_{σ_0}. Therefore, with $A_0 = 1$ and $E_0 = E$, (a) and (b) hold.

Assume that $\tau_2(M)$ is not empty. Then, by Lemma H, M is a ϖ-group. Take $p \in \tau_2(M)$. If G has nonabelian Sylow p-subgroups, then Theorem 6.7 provides subgroups A_0 and E_0 as required. Note that (c) implies that $C_{M_\sigma}(x) = 1$ for every p-element x of ${E_0}^\sharp$. Thus, we can assume the hypotheses, notation and conclusions of Lemma 6.8.

By assumptions, $C_E(x)$ is a $\tau_2(M)$-group for every $x \in {M_\sigma}^\sharp$. By Lemma 6.8 (a) and (b), E contains an abelian normal Hall $\tau_2(M)$-subgroup E_2. Hence, we have $C_E(x) \subseteq E_2$ for every $x \in {M_\sigma}^\sharp$. Thus, $A_0 = E_2$ satisfies (a).

For each $p \in \tau_2(M)$, we have a normal abelian subgroup S of rank two such that S is a Sylow p-subgroup of E and of G (Lemma 6.8 (a) and (b)). We will prove that for each $p \in \tau_2(M)$ there is a cyclic normal subgroup $Z = Z_p$ of E having the same exponent as S and satisfying the condition $C_{M_\sigma}(z) = 1$ for every $z \in Z^\sharp$.

We remark that the last centralizer condition is equivalent to

$$C_{M_\sigma}(\Omega_1(Z)) = 1.$$

and this condition is automatically satisfied if Z is a nonidentity cyclic subgroup of S such that $\Omega_1(Z) \lhd N_G(S)$. The first claim is trivial. To prove the second, suppose that $C_{M_\sigma}(\Omega_1(Z)) \neq 1$. Corollary 6.6 (c) for $X = \Omega_1(Z)$ yields $\mathcal{M}(C_G(X)) = \{M\}$. Since $\Omega_1(Z) \lhd N_G(S)$, we have

$$N_G(S) \subseteq N_G(\Omega_1(Z)) \subseteq M.$$

This contradicts Lemma 6.8 (d).

Assume that $C_E(S) = E$. Since S is abelian of rank 2, $S = Y \times Z$ for some cyclic subgroups Y and Z. We choose the notation $|Y| \leq |Z|$. If $|Y| < |Z|$, $\Omega_1(Z)$ is characteristic in S. Then, $\Omega_1(Z) \lhd N_G(S)$ so $Z = Z_p$ satisfies the required property. (Since $C_E(S) = E$, any subgroup of S is normal in E.) If $|Y| = |Z|$, we can take a factor Z in such a way that $\Omega_1(Z)$ is equal to any given $A_1 \in \mathcal{E}^1(S)$ and, by Theorem 6.5 (f), at least one such A_1 satisfies $C_{M_\sigma}(A_1) = 1$. This completes the proof in the case $C_E(S) = E$.

Assume that $C_E(S) \neq E$. Take $q \in \pi(E/C_E(S))$ and let $Q_1 \in Sy\ell_q(E)$ and $Q \in Sy\ell_q(N_G(S))$ such that $Q_1 \subseteq Q$. The definition of q implies $C_S(Q_1) \neq S$. Let $A = \Omega_1(S)$. Then, $A \in \mathcal{E}^2(S)$. By Proposition 1.6 [BG], Q_1 does not centralize A. Therefore, by Corollary 6.10 (c), $q \in \tau_1(M)$ and Q_1 is cyclic. Since $C_S(Q_1) \neq S$ and $C_G \subseteq E$, we have

$$Q_0 = C_Q(S) \subsetneqq Q_1.$$

Suppose that Q/Q_0 acts regularly on S. Then, Proposition 3.9 [BG] shows that Q/Q_0 is cyclic. Hence, $\Omega_1(Q/Q_0) \subseteq Q_1/Q_0$ and $\Omega_1(Q) \subseteq Q_1$. Since Q_1 is cyclic, $\Omega_1(Q) \subseteq Q_1$ implies that Q is cyclic, too. Thus, $r_q(N_G(S)) = 1$. On the other hand, since $q \in \tau_1(M)$, the assumption of this theorem implies that $C_{M_\sigma}(\Omega_1(Q_1)) = 1$. Hence, by Lemma 6.8 (e), $\Omega_1(Q_1)$ lies in $Z(E)$ so $\Omega_1(Q_1)$ centralizes A.

If $M^* \in \mathcal{M}(N_G(A))$, $S \subseteq N_G(A) \subseteq M^*$. So, S is a Sylow p-subgroup of M^*. Now,Lemma 6.11 (c) yields $q \in \tau_2(M^*)$, $S \lhd M^*$, and M^* contains an abelian Sylow q-subgroup of G. This implies that $r_q(N_G(S)) \geq 2$. This contradiction proves that Q/Q_0 does not act regularly on S. Therefore, $1 \neq C_S(X) \neq S$ for some subgroup X of Q. By Proposition 1.6 (d) [BG], we have $S = S_0 \times S_1$ where $S_0 = C_S(X)$ and $S_1 = [S, X]$. Since $r(S) = 2$, both S_0 and S_1 are cyclic. By Lemma 6.8 (f), both S_0 and S_1 are normal in $N_G(S)$. Define $Z = S_0$ if $|S_0| \geq |S_1|$ and $Z = S_1$ if $|S_0| < |S_1|$. Then, Z has the required properties.

Define E_0 to be the product of E_1E_3 and $\prod Z_p$ for all $p \in \tau_2(M)$. Then, E_0 satisfies the requirements of (b). Q.E.D.

Theorem 6.13. *Let $p \in \varpi$. Then, every nonabelian p-subgroup of G lies in $\mathcal{U}$.*

Proof. The proof of Theorem 12.13 [BG] works. We just add some details. Let $p \in \varpi$ and let P be a nonabelian p-subgroup of maximal order that lies in two distinct subgroups M and M^* of $\mathcal{M}$. Then, by Corollary 6.10, $N_G(P) \subseteq M \cap M^*$. It follows that $P \in Syl_p(G)$ and $r(P) = 2$. By Corollary 4.7 (b), P contains a nonabelian subgroup Q of order p^3 and of exponent p and $Z(Q) = \Omega_1(Z(P))$. Let $Z = Z(Q)$ and $K = C_{M_\sigma}(Z)$. It is proved that $K \subseteq M^*$. By Corollary 4.9 (b), $M = (M \cap M^*)M_\alpha$. This implies that $M_\alpha \neq 1$. Similarly, we have $(M^*)_\alpha \neq 1$.

Apply Lemma 6.5 (b) with (K, U, H, G) replaced by $(M_\alpha, M \cap M^*, Z, M)$ to conclude $N_M(Z) = C_{M_\alpha}(Z)(N_M(Z) \cap M^*) \subseteq M^*$. It follows that

$$\mathcal{M}(N_G(Z)) \neq \{M\};$$

otherwise, we would have $N_G(Z) = N_M(Z) \subseteq M \cap M^*$.

Take any $A \in \mathcal{E}_p^2(Q)$ and apply Proposition 6.4 (b) to M, and then M^*. Since $M_\alpha \neq 1$, the hypothesis of Proposition 6.4 (b) does not hold. Thus, there is a subgroup $A_0 \in \mathcal{E}^1(A)$ such that $\mathcal{M}(N_G(A_0)) = \{M\}$. Since Z does not satisfy this condition, we have $A_0 \neq Z$. Similarly, there is a subgroup $A_0^* \in \mathcal{E}^1(A) \setminus \{Z\}$ which satisfies $\mathcal{M}(N_G(A_0^*)) = \{M^*\}$. By the property of the group Q, A_0^* is conjugate to A_0 in Q. This would imply that $\mathcal{M}(N_G(A_0^*))$ would be conjugate to $\mathcal{M}(N_G(A_0))$ by an element of $Q \subseteq M \cap M^*$, so $M^* = M$. This contradiction proves Theorem 6.13. Q.E.D.

Corollary 6.14. *Suppose $M \in \mathcal{M}$, $p \in \sigma(M)$, $X \in \mathcal{E}_p^1(M)$, and $P \in Syl_p(M_\sigma)$. Assume that $p \in \beta(M)$ or $X \subseteq M_\sigma{}'$. Then, $p \in \varpi$ and $\mathcal{M}(C_G(X)) = \mathcal{M}(P) = \{M\}$.*

Proof. We may assume that X is a subgroup of P. First, we prove a lemma: *under the assumptions of Corollary 6.14, if $p \notin \beta(M)$, then we have $X \subseteq P'$.* If $p \notin \beta(M)$, the assumption implies that $X \subseteq M_\sigma{}'$. The group M_σ/M_β is nilpotent by Lemma 4.8 (b). Since $P \cap M_\beta = 1$, we have $X \subseteq M_\sigma{}' \cap P = P'$ proving the lemma.

This lemma implies that if $p \notin \beta(M)$, P is nonabelian; in particular, P is not cyclic so $r(P) \geq 2$. Thus, $p \in \varpi$ by Lemma F. If $p \in \beta(M)$, we have $p \in \varpi$. This proves $p \in \varpi$ in all cases.

Suppose that $r(C_P(X)) \geq 3$. By the Uniqueness Theorem, we have $C_P(X) \in \mathcal{U}$. Since $C_P(X) = C_G(X) \cap P$, both $C_G(X)$ and P lie in $\mathcal{U}$. Then, we have

$$\mathcal{M}(C_G(X)) = \mathcal{M}(P) = \{M\}.$$

Suppose that $r(C_P(X)) \leq 2$. If $r(P) \geq 3$, P is narrow by Corollary 5.4 [BG]; so $p \notin \beta(M)$. By the lemma, we have $X \subseteq P'$. On the other hand, if p is narrow and $r(C_P(X)) \leq 2$ for some $X \in \mathcal{E}^1(P)$, Theorem 5.3 (d) shows $X \cap P' = 1$. This contradicts $X \subseteq P'$. Hence, $r(P) \leq 2$ and $p \notin \beta(M)$. The lemma yields that P is nonabelian.

By Corollary 4.7 (b), P is the central product and satisfies $P' \subseteq Z(P)$. We have $P \subseteq C_M(X)$ because $X \subseteq P'$. Since P is nonabelian, $P \in \mathfrak{U}$ by Theorem 6.13. This implies that $C_G(X) \in \mathfrak{U}$ and completes the proof. Q.E.D.

Proposition 6.15. *Suppose $M \in \mathcal{M}$, $q \in \sigma(M)$, X is a nonidentity q-subgroup of M, and $M^* \in \mathcal{M}(N_G(X)) \setminus \{M\}$. Let S be a Sylow q-subgroup of $M \cap M^*$ that contains X. Then, S, M, and M^* satisfy the following conditions.*

(a) *M^* is not conjugate to M in G.*

(b) *$N_G(S) \subseteq M$.*

(c) *S is a Sylow q-subgroup of M^*.*

(d) *If $q \in \sigma(M^*)$, then* (1) $M^* = (M \cap M^*)M^*_\beta$, (2) $\tau_1(M^*) \subseteq \tau_1(M) \cup \alpha(M)$, and (3) $M_\beta = M_\alpha \neq 1$.

(e) If $q \notin \sigma(M^*)$, then (1) $q \in \tau_2(M^*)$, (2) $\pi(M) \cap \sigma(M^*) \subseteq \beta(M^*)$, and (3) $M \cap M^*$ is a complement to M^*_σ in M^*.

Proof. The assertions follow as in the proof of Proposition 12.15 [BG]; we will paraphrase the proof of (e).

Suppose that $q \notin \sigma(M^*)$. By Lemma 6.2 (a) applied to q, we have $q \in \tau_2(M^*)$. Lemma H shows that M^* is a ϖ-group. Since $S \in Syl_q(M^*)$ by (c), Theorem 6.5 proves $A = \Omega_1(S) \in \mathcal{E}^2(S)$.

Let E^* be a complement of M^*_σ in M^* that contains A. By Theorem 6.5 (e) and Corollary 6.6 (a) with (p, M) replaced by (q, M^*), $M^*_\sigma \cap M = 1$ and $A \lhd E^*$. By Corollary 6.10 (d), we have $N_G(A) \subseteq M$. This implies that $E^* \subseteq N_G(A) \subseteq M$. Thus,

$$M \cap M^* = M \cap M^*_\sigma E^* = (M \cap M^*_\sigma)E^* = E^*.$$

This proves (3).

Suppose that $p \in \pi(M) \cap \sigma(M^*)$ and $p \notin \beta(M^*)$. By Corollary 6.6 (b) applied to M^*, we have $C_G(A) \subseteq E^*$. Since $p \in \sigma(M^*)$, the group $C_G(A)$ is a p'-group.

By (a), M is not conjugate to M^*. Therefore, Corollary 6.6 (f) applied to M^* and q proves that $\sigma(M^*)$ is disjoint from $\sigma(M)$. This implies first $p \neq q$ because $p \in \sigma(M^*)$ and $q \in \sigma(M)$, and secondly $p \notin \beta(M)$ as $\beta(M) \subseteq \sigma(M)$. By (1), $q \in \tau_2(M^*)$ so $q \notin \beta(G)$ by Lemma 6.1 (g) with p replaced by q. We can apply Corollary 4.9 to M^*. If $p < q$, the q-subgroup A of M^* centralizes a Sylow p-subgroup of

M^*_σ. Since $p \in \sigma(M^*)$, $C_G(A)$ has order divisible by p. This contradicts the earlier statement that $C_G(A)$ is a p'-group. Thus, we have $q < p$. We apply Corollary 4.9 to M interchanging p and q. We conclude that a Sylow p-subgroup P of M centralizes a Sylow q-subgroup Q of M_σ. Since $p \in \pi(G)$, we have $P \neq 1$. We may replace Q and P by conjugates and suppose that $A \subseteq Q$. We get a contradiction that $1 \neq P \subseteq C_G(A)$. This completes the proof of (e). Q.E.D.

Corollary 6.16. *Let $M \in \mathcal{M}$ and E a complement of M_σ in M. Suppose that Y is a $\sigma(M)$-subgroup of G such that $O_\varpi(Y) \neq 1$. Then, Y is conjugate to a subgroup of M_σ and for every $p \in \pi(E) \cap \beta(G)'$ and every $H \in \mathcal{M}(Y)$ not conjugate to M in G,*

(a) *$r_p(N_H(Y)) \leq 1$, and*
(b) *if $p \in \tau_1(M)$, then $p \notin \pi(N_H(Y)')$.*

Proof. With the extra condition that $O_\varpi(Y) \neq 1$ Y is contained in a ϖ-local subgroup, so it is solvable. We can take a nonidentity characteristic q-subgroup X of Y for some prime $q \in \sigma_0(M)$. Since M contains a Sylow q-subgroup of G, we may replace Y by some conjugate if necessry, and assume that $X \subseteq M_\sigma$.

First we prove the following lemma as part of the proof of (a). *Let $H \in \mathcal{M}(Y)$. If H is not conjugate to M in G, then for any prime $p \in \pi(E) \cap \beta(G)'$, we have $r_p(H \cap M) \leq 1$.*

Suppose $r_p(H \cap M) \geq 2$ and take $A \in \mathcal{E}^2_p(H \cap M)$. Then $p \in \tau_2(M)$ and by Theorem 6.5 (e) we have $M_\sigma \cap H = 1$ in contradiction to

$$1 \neq X \subseteq M_\sigma \cap H.$$

This proves the lemma.

To prove Corollary 6.16, we assume first that $N_G(X) \subseteq M$. In this case we have $Y \subseteq N_G(X) \subseteq M$. Since M/M_σ is a $\sigma(M)'$-group and Y is a $\sigma(M)$-group, we have $Y \subseteq M_\sigma$. Let $p \in \pi(E) \cap \beta(G)'$ and let $H \in \mathcal{M}(Y)$ such that H is not conjugate to M in G. By the lemma, $r_p(H \cap M) \leq 1$. Since $N_H(Y) \subseteq N_G(Y) \subseteq N_G(X) \subseteq M$, we have $N_H(Y) \subseteq H \cap M$. This implies $r_p(N_H(Y)) \leq r_p(H \cap M) \leq 1$. If $p \in \tau_1(M)$, M' is a p'-group (by definition of $\tau_1(M)$). Then, (b) holds because $N_H(Y)' \subseteq (H \cap M)' \subseteq M'$.

In the remainder of the proof we assume that $N_G(X) \not\subseteq M$. Since X is a ϖ-group, there is $M^* \in \mathcal{M}(N_G(X))$. Since $N_G(X) \not\subseteq M$, we have $M^* \neq M$. By Proposition 6.15, M^* is not conjugate to M in G, $q \in \sigma(M^*) \cup \tau_2(M^*)$, and if $q \in \tau_2(M^*)$, then $\pi(M) \cap \sigma(M^*) \subseteq \beta(M^*)$. Moreover, if K is defined to be M^*_β or M^*_σ according as $q \in \sigma(M^*)$ or

$q \in \tau_2(M^*)$, then $M^* = (M \cap M^*)K$. We claim that K is a $\sigma(M)'$-group. If $q \in \sigma(M^*)$, $K = M^*_\beta \subseteq M^*_\alpha$ and by Lemma 4.12 (a), $\alpha(M^*)$ is disjoint from $\sigma(M)$. If $q \in \tau_2(M^*)$, we have $K = M^*_\sigma$ and $\sigma(M^*) \cap \sigma(M) = \emptyset$ by Corollary 6.6 (f) with M replaced by M^*. Thus, K is a $\sigma(M)'$- group.

Since $Y \subseteq N_G(X)$, the $\sigma(M)$-group Y is contained in $M^* = (M \cap M^*)K$. Since K is a normal $\sigma(M)'$-group, the Schur-Zassenhaus Theorem shows that Y is conjugate to a subgroup of $M \cap M^*$. Since Y is a $\sigma(M)$-group, Y is contained in $M_\sigma \cap M^*$ which is a normal Hall $\sigma(M)$-subgroup of $M \cap M^*$. This proves the first assertion of Corollary 6.16.

Take $p \in \pi(E) \cap \beta(G)'$ and $H \in \mathcal{M}(Y)$ that is not conjugate to M in G. We claim that K is a p'-group. This is clear if $K = (M^*)_\beta$ because $p \notin \beta(G)$. On the other hand, if $K = (M^*)_\sigma$, we have $q \in \tau_2(M^*)$ so p cannot divide $|(M^*)_\sigma|$ because $\pi(M) \cap \sigma(M^*) \subseteq \beta(M^*)$ and $p \notin \beta(M^*)$. Thus, K is a p'-group. Since $N_H(Y) \subseteq N_G(Y) \subseteq M^*$ and M^* is not conjugate to M in G, we may assume $H = M^*$. In this case, we have $H = (H \cap M)K$. Since K is a p'-group, $H \cap M$ contains a Sylow p-subgroup of H. The lemma at the beginning of the proof shows that $r_p(H \cap M) \leq 1$. Thus, we have $r_p(N_H(Y)) \leq r_p(H) \leq 1$. This proves (a).

If $p \in \tau_1(M)$, then $p \notin \pi(M')$. It follows that $(H \cap M)'$ is a p'-group. Clearly, we have $N_H(Y)' \subseteq H' \subseteq (H \cap M)'K$. Therefore, $N_H(Y)'$ is a p'-group. Q.E.D.

Lemma 6.17. *Let $M \in \mathcal{M}$ and E a complement of M_σ in M. Then, we have $C_{M_\sigma}(E) \subseteq (M_\sigma)'$, $[M_\sigma, E] = M_\sigma$, and for every $g \in G \setminus M$, the group $M_\sigma \cap M^g$ is a cyclic $\beta(M)'$-group intersecting $(M_\sigma)'$ trivially.*

Lemma 6.18. *Suppose $M \in \mathcal{M}$, $p \in \tau_1(M)$, $P \in \mathcal{E}^1_p(M)$, $q \in p'$, and Q is a nonidentity P-invariant q-subgroup of M such that $C_Q(P) = 1$ and $\mathcal{M}(N_G(Q)) \neq \{M\}$.*

(a) *If $M_\alpha \neq 1$ and $q \notin \alpha(M)$, then $C_{M_\alpha}(P) \neq 1$ and $C_{M_\alpha}(PQ) = 1$.*

(b) *If $Q \in Syl_q(M)$, then $\alpha(M) = \beta(M)$ and we have the situation of* (a).

Proof. We will rewrite the first paragraph of the proof of Lemma 12.18 [BG]; the remainder of the proof can be adapted directly.

Suppose that $M_\alpha \neq 1$ and $q \notin \alpha(M)$. We will prove that

$$r(C_{M_\alpha}(Q)) \leq 1.$$

Suppose that $r(C_{M_\alpha}(Q)) \geq 2$. Then, $C_{M_\alpha}(Q)$ is a ϖ-group so by Lemma A, Q is a ϖ-group. Lemma 4.3 with X replaced by Q yields that $C_M(Q) \in \mathcal{U}$. Since $q \in \varpi$, $\mathcal{M}(N_G(Q))$ is not empty and, by assumption, contains $H \in \mathcal{M}$ different from M. Thus,

$$C_M(Q) \subseteq N_G(Q) \subseteq H \neq M,$$

so $C_M(Q) \notin \mathcal{U}$. This contradiction proves $r(C_{M_\alpha}(Q)) \leq 1$.

We prove $r(C_{M_\alpha}(P)) \leq 1$. Suppose that $r(C_{M_\alpha}(P)) \geq 2$. The same argument as above yields that $p \in \varpi$ and $C_M(P) \in \mathcal{U}$. Since $p \in \tau_1(M)$, P is contained in a cyclic Sylow p-subgroup S of M. Since $p \notin \sigma(M)$, we have $N_G(S) \nsubseteq M$ Thus, $N_G(S) \subseteq N_G(P) \nsubseteq M$.

We can find $H \in \mathcal{M}(N_G(P))$ because $p \in \varpi$. Then, $H \neq M$ and

$$C_M(P) \subseteq N_G(P) \subseteq H \neq M.$$

Thus, $C_M(P) \notin \mathcal{U}$. This proves $r(C_{M_\alpha}(P)) \leq 1$. Q.E.D.

Lemma 6.19. *Let $M \in \mathcal{M}$ and E a complement of M_σ in M. Then, the group E' centralizes a Hall $\beta(M)'$-subgroup of M_σ.*

§7. Prime Action

This section corresponds Section 13 of [BG]. Troughout this section, s subgroup $M \in \mathcal{M}$ and a complement E of M_σ in M will be fixed.

Lemma 7.1. *Suppose that $M^* \in \mathcal{M}$, $p \in \pi(E) \cap \pi(M^*)$, $p \notin \tau_1(M^*)$, $[M_\sigma \cap M^*, M \cap M^*] \neq 1$, and M^* is not conjugate to M in G. Then,*

(a) *every p-subgroup of $M \cap M^*$ centralizes $M_\sigma \cap M^*$,*
(b) *$p \notin \tau_2(M^*)$, and*
(c) *if $p \in \varpi \cap \tau_1(M)$, then $p \in \beta(G)$.*

Proof. Since $[M_\sigma \cap M^*, M \cap M^*] \subseteq M_\sigma \cap (M^*)'$, there is $q \in \sigma(M) \cap \pi((M^*)')$. Then, $q \neq p$ because $p \in \pi(E)$. Let Y be a Sylow q-subgroup of $(M^*)'$. By Lemma 4.8, $(M^*)'/(M^*)_\beta$ is nilpotent so $(M^*)_\beta Y \lhd M^*$. The Frattini argument yields $M^* = (M^*)_\beta N_{M^*}(Y)$.

In order to prove (b), suppose $p \in \tau_2(M^*)$. Then, $r_p(N_{M^*}(Y)) = 2$ because $N_{M^*}(Y)$ covers $M^*/(M^*)_\beta$. Moreover, M^* is a ϖ-group by Lemma H. It follows that $q \in \varpi$. Lemma 6.1 (g) yields that $p \notin \beta(G)$. Corollary 6.16 (a) can be applied to get $r_p(N_{M^*}(Y)) \leq 1$. This contradiction proves (b).

To prove (c), suppose that $p \in \beta(G)'$. By (b) and the assumptions, $p \in \sigma(M^*) \cup \tau_3(M^*)$. Therefore, $p \in \pi((M^*)')$. We have $(M^*)' =$

$(M^*)_\beta(N_{M^*}(Y))'$. Hence, $N_{M^*}(Y)'$ contains a p-subgroup $P \neq 1$. We will show that this is a contradiction. Let S be a Sylow p-subgroup of $(M^*)'$. Since $(M^*)'/(M^*)_\beta$ is nilpotent, $(M^*)_\beta S \lhd M^*$ and $P \subseteq (M^*)_\beta S$. We claim that $q \in \varpi$. If $q \in \beta(M^*)$, this is trivial. If $q \notin \beta(M^*)$, $(M^*)_\beta S$ is a q'-group. Recall that $p \neq q$. Now, $[Y, P] \subseteq Y \cap (M^*)_\beta S = 1$ because $P \subseteq N_G(Y)$ and $P \subseteq (M^*)_\beta S$. Since $P \neq 1$ is a p-group and $p \in \varpi$, we have $q \in \varpi$. We can apply Corollary 6.16 (b) which yields that if $p \in \tau_1(M)$, then $p \notin \pi(N_{M^*}(Y))$. This contradiction proves (c).

The statement (a) follows as in [BG]. Q.E.D.

Corollary 7.2. *Suppose that $p \in \tau_1(M) \cup \tau_3(M)$, P is a nonidentity p-subgroup of M, and $M^* \in \mathcal{M}(N_G(P))$. Then,*

(a) *every p-subgroup of $M \cap M^*$ centralizes $M_\sigma \cap M^*$,*
(b) *every $\tau_1(M^*)'$-subgroup of $E \cap M^*$ centralizes $M_\sigma \cap M^*$, and*
(c) *if $[M_\sigma \cap M^*, M \cap M^*] \neq 1$, then $p \in \sigma(M^*)$ and in the case $p \in \varpi \cap \tau_1(M)$, we even have $p \in \beta(M^*)$.*

Corollary 7.3. *The following statements hold.*

(a) *Let $P \in Syl_p(E)$ for some $p \in \pi(E) \cap \varpi$. Assume that P is cyclic. Then, P acts in a prime manner on M_σ.*
(b) *If $\varpi \cap \tau_3(M) \neq \emptyset$, E_3 acts in a prime manner on M_σ.*

Proof. Let $P_1 = \Omega_1(P)$. If $x \in P^\sharp$, then $P_1 \subseteq \langle x \rangle \subseteq P$. By assumption, $p \in \tau_1(M) \cup \tau_3(M)$. Therefore, we have $N_G(P) \nsubseteq M$ Since $p \in \varpi$, there exists $M^* \in \mathcal{M}(N_G(P))$. We have $P \subseteq M \cap M^*$. By Corollary 7.2 (a), P centralizes $M_\sigma \cap M^*$. Thus,

$$M_\sigma \cap M^* \subseteq C_{M_\sigma}(P) \subseteq C_{M_\sigma}(x) \subseteq C_{M_\sigma}(P_1).$$

On the other hand, $C_{M_\sigma}(P_1) \subseteq N_G(P_1) \subseteq M^*$, so $C_{M_\sigma}(P_1) \subseteq M_\sigma \cap M^*$. It follows that $C_{M_\sigma}(x) = M_\sigma \cap M^*$ for every $x \in P^\sharp$. This proves (a).

The proof of (b) is similar. Take $X \in \mathcal{E}^1(E_3)$ with $p \in \varpi$ and $M^* \in \mathcal{M}(N_G(X))$. We have $E_3 \subseteq E'$ by Lemma 6.1 (b). Since $E \subseteq N_G(X) \subseteq M^*$, E_3 is a subgroup of $(M^*)'$; in particular, E_3 is a $\tau_1(M^*)'$-subgroup. If $x \in {E_3}^\sharp$ satisfies $X \subseteq \langle x \rangle$, then we have

$$C_{M_\sigma}(E_3) = C_{M_\sigma}(x) = C_{M_\sigma}(X) = M_\sigma \cap M^*.$$

If $p \in \varpi$ for one prime p in $\tau_3(M_3)$, then $\tau_3(M) \subseteq \varpi$. Hence, for any element $x \in {E_3}^\sharp$, we have $C_{M_\sigma}(x) = C_{M_\sigma}(E_3)$. This proves (b).

Q.E.D.

Theorem 7.4. *Suppose that $p \in \varpi$, $p \in \tau_1(M)$, $P \in \mathcal{E}^1(E)$, $r \in \pi(E)$, and $R \in \mathcal{E}^1_r(C_E(P))$. Then, $C_{M_\sigma}(P) \subseteq C_{M_\sigma}(R)$.*

Proof. By assumption, we have $RP = R \times P$ so $r \in \varpi$. Since $p \in \tau_1(M)$, we have $N_G(P) \not\subseteq M$. We can take $M^* \in \mathcal{M}(N_G(P))$ because $N_G(P)$ is a ϖ-local subgroup. By Lemma 6.2, $p \in \sigma(M^*) \cup \tau_2(M^*)$ (by (a)) and M^* is not conjugate to M in G (by (b)), In particular, $M^* \neq M$.

By Corollary 7.2 (a), P centralizes $M_\sigma \cap M^*$. as in the proof of Corollary 7.3, we have $C_{M_\sigma}(P) = M_\sigma \cap M^*$. This implies that $M_\sigma \cap M^*$ is a ϖ-group by Lemma A. Since $R \subseteq M \cap M^*$, the $\sigma(M)'$-group PR normalizes $M_\sigma \cap M^*$. Therefore, for each $q \in \pi(M_\sigma \cap M^*)$, there is a PR-invariant Sylow q-subgroup S of $M_\sigma \cap M^*$. Then, $S \notin \mathcal{U}$ so S is abelian by Theorem 6.13. Note that $q \in \varpi$.

We have to show that R centralizes S. We will derive a contradiction by assuming that R does not centralize S. Let $Q = [S, R]$ and assume that $Q \neq 1$. Then, $S = Q \times C_S(R)$ and $C_Q(R) = 1$ (because S is abelian). Since $S \subseteq M_\sigma \cap M^*$,

$$Q = [S, R] \subseteq [M_\sigma \cap M^*, M \cap M^*] \neq 1.$$

By Corollary 7.2, we obtain $p \in \beta(M^*)$ from (c) and $r \in \tau_1(M^*)$ from (b).

We check that all the assumptions of Lemma 6.18 (a), except the one about $\mathcal{M}(N_G(Q))$, are satisfied for (M^*, r, R, q, Q) in place of (M, p, P, q, Q). But, since $p \in \beta(M^*)$, one of the conclusions is violated, i.e. $P \subseteq C_{M^*_\alpha}(RQ) \neq 1$. It follows that $\mathcal{M}(N_G(Q)) = \{M^*\}$.

By Lemma 6.2 (a), we have $q \in \sigma(M^*) \cup \tau_2(M^*)$. We can apply Proposition 6.15 for $Q = X$. If $q \in \tau_2(M^*)$, Part (e) applies so $M \cap M^*$ is a complement of $(M^*)_\sigma$ in M^*. However, this is not true because

$$P \subseteq (M^*)_\sigma \cap M = (M^*)_\sigma \cap (M \cap M^*) \neq 1.$$

It follows that $q \in \sigma(M^*)$. Hence, by Proposition 6.15 (d), we have

$$r \in \pi(E) \cap (\tau_1(M) \cup \alpha(M)) = \tau_1(M)$$

and $M_\alpha \neq 1$. Since $q \in \sigma(M^*)$, Lemma 4.12 (a) yields $q \notin \alpha(M)$. Thus, if R does not centralize S, we have $q \notin \alpha(M)$. It follows that $C_{M_\alpha}(P) \subseteq C_{M_\alpha}(R)$ and $r \in \tau_1(M)$. We can interchange p and r to get $C_{M_\alpha}(R) \subseteq C_{M_\alpha}(P)$. Then, $C = C_{M_\alpha}(P) = C_{M_\alpha}(R)$, so

$$C = C_{M_\alpha}(P) = C_{M_\sigma}(P) \cap M_\alpha = M_\alpha \cap M^*$$

because $C_{M_\sigma}(P) = M_\sigma \cap M^*$. The group S normalizes C. Hence,

$$[C, R, S] = [S, C, R] = 1.$$

By the Three Subgroup Theorem we have $[R, S, C] = 1$. Thus, $Q = [R, S]$ centralizes C. It follows that $C = C_{M_\alpha}(R) = C_{M_\alpha}(RQ)$. On the other hand, Lemma 6.18 (a) for M, r, R, q and Q in place of M, p, P, q and Q yields $C_{M_\alpha}(R) \neq C_{M_\alpha}(RQ)$. This contradiction proves Theorem 7.4. Q.E.D.

Theorem 7.5. *Suppose that $\varpi \cap \tau_1(M) \neq \emptyset$. Then, E_1 acts in a prime manner on M_σ.*

Proof. Since E_1 is cyclic, the assumption yields that E_1 is a ϖ-group. For each $p \in \tau_1(M)$, let $P \in \mathcal{E}^1(E_1)$. By Theorem 7.4, the group $C = C_{M_\sigma}(P)$ does not depend on p. If P_1 is any p-subgroup of E_1, we have $C_{M_\sigma}(P_1) = C$ by Corollary 7.3 (a). It follows that $C_{M_\sigma}(X) = C$ for any subgroup X of E_1. Q.E.D.

Lemma 7.6. *Suppose $1 \neq P \subseteq E_1$, $q \in \sigma(M)$, and $X \in \mathcal{E}_q^1(C_{M_\sigma}(P))$. Let $S \in Syl_q(M_\sigma)$. Assume either $P = E_1$ or $\varpi \cap \tau_1(M) \neq \emptyset$. Then, $q \in \varpi$ and $\mathcal{M}(C_G(X)) = \mathcal{M}(S) = \{M\}$.*

Proof. If $q \in \beta(M)$ or $X \subseteq (M_\sigma)'$, Corollary 6.14 yields the conclusion of the lemma. We will derive a contradiction by assuming $q \notin \beta(M)$ and $X \nsubseteq (M_\sigma)'$. If $\varpi \cap \tau_1(M) \neq \emptyset$, E_1 acts in a prime manner on M_σ by Theorem 7.5. Therefore, we may assume that $P = E_1$.

Since $q \notin \beta(M)$, by Lemma 6.19, E' centralizes some Sylow q-subgroup of M_σ. The group E is a $\sigma(M)'$-group that normalizes a $\sigma(M)$-subgroup $C_{M_\sigma}(E')$. Hence, E normalizes some Sylow q-subgroup of $C_{M_\sigma}(E')$. We may replace S by a conjugate without affecting the conclusion. Thus, we may assume that S is normalized by E and centralized by E'.

The group $SE_1 \subseteq SE$ is a Hall $\{q, \tau_1(M)\}$-subgroup of M. Therefore, the subgroup XE_1 of M is conjugate to a subgroup of SE_1. Thus, for some $x \in M$, $(XE_1)^x = X^x E_1^x \subseteq SE_1$ Then, E_1^x and E_1 are Hall subgroups of SE_1, so they are conjugate in SE_1. We may assume that $E_1^x = E_1$. Since $XE_1 = X \times E_1$, we have $X^x \subseteq C_M(E_1^x) = C_M(E_1)$. Also, we have $X^x \subseteq S$ because S is a normal Sylow q-subgroup of SE_1. It follows that $X^x \in \mathcal{E}_q^1(C_{M_\sigma}(P))$ and $X^x \subseteq S$. By replacing X and S by conjugates, we may assume that

$$X \subseteq S \subseteq C_{M_\sigma}(E').$$

By Lemma 6.17, $C_{M_\sigma}(E) \subseteq (M_\sigma)'$. Since $X \not\subseteq (M_\sigma)'$, X does not centralize E, but does centralize E_1 and E'. It follows that $E \neq E_1E'$. Since $E_3 \subseteq E'$ and $E = E_1E_2E_3$ by Lemma 6.1, we have $E_2 \neq 1$. By Lemma H, M is a ϖ-group.

Take $p \in \tau_2(M)$ and $A \in \mathcal{E}_p^2(E)$. We have $A \lhd E$ by Corollary 6.6 (a) and $C_{M_\sigma}(A) = 1$ by Theorem 6.5 (d). Since A is abelian, $A = A_0 \times [A, E_1]$ with $A_0 = C_A(E_1)$. Since $[A, E_1] \subseteq E'$, $[A, E_1]$ centralizes X. Furthermore, Theorem 7.4 shows that A_0 centralizes X. Thus, $X \subseteq C_{M_\sigma}(A)$ and $C_{M_\sigma}(A) \neq 1$. This contradicts Theorem 6.5 (d).

Q.E.D.

Lemma 7.7. *Suppose that $E_1 \neq 1$, $E_3 \neq 1$, and that E_1 does not act regularly on E_3. Then, we have one of the following two cases.*

(1) *We have $\tau_3(M) \cap \varpi = \emptyset$, M is a Frobenius group with Frobenius kernel $M_\alpha = M_\beta = M_{\sigma_0}$, M_α is a ϖ-group, and M/M_α is a ϖ'-group.*

(2) *We have $\tau_3(M) \cap \varpi \neq \emptyset$, M is a ϖ-group and the group E_1E_3 acts in a prime manner on M_σ.*

Proof. By assumption, there exist primes p and r such that $P \in \mathcal{E}^1(E_1)$ centralizes $R \in \mathcal{E}_r^1(E_3)$. These primes p and r lie in the same connected component of the prime graph of G.

Suppose that $\tau_3(M) \cap \varpi = \emptyset$. Then, M is not a ϖ- group. By Lemma G, we have (1).

Suppose that $\tau_3(M) \cap \varpi \neq \emptyset$. Since E_3 is cyclic by Lemma 6.1 (d), we have $\tau_3(M) = \pi(E_3) \subseteq \varpi$. Since M'/M_β is nilpotent by Lemma 4.8 and $\tau_3(M) \subseteq \pi(M'/M_\beta)$by Lemma 6.1 (b), the group M'/M_β is a ϖ-group. The remark at the beginning of the proof shows $\tau_1(M) \cap \varpi \neq \emptyset$. Since $\tau_1(M) \subseteq \pi(M/M')$, M/M' is a ϖ-group. This proves that M is a ϖ-group.

The remainder of the proof is similar to that of Lemma 13.7 [BG]. Since M is a ϖ-group, we can apply Corollary 7.3 and Theorems 7.4 and 7.5. We assume

$$C_{M_\sigma}(P) \neq C_{M_\sigma}(R)$$

and we will obtain a contradiction. We have $1 \neq R \subseteq E_3$ and $C_{M_\sigma}(R) \neq 1$. If $\tau_2(M) \neq \emptyset$, Corollary 6.6 (d) would yield $C_{M_\sigma}(R) = 1$. Therefore, $\tau_2(M) = \emptyset$ and $E = E_1E_3$. Since R char $E_3 \lhd E$ by Lemma 6.1, we have $R \lhd E$. We can take $M^* \in \mathcal{M}(N_G(R))$ since $N_G(R)$ is a ϖ- local subgroup. We have $N_G(R) \not\subseteq M$ so $M^* \neq M$. By our hypothesis,

$$1 \neq [C_{M\sigma}(R), P] \subseteq [M_\sigma \cap M^*, E_1].$$

If $C = C_{E_1}(M_\sigma \cap M^*)$, the above displayed formula yields $C \neq E_1$. On the other hand, C centralizes $M_\sigma \cap M^*$. Since E_1 acts in a prime manner on M_σ by Theorem 7.5, we have $C = 1$, Corollary 7.2 with p and P replaced by r and R yields $\pi(E_1) \subseteq \tau_1(M^*)$ from (b) and $r \in \sigma(M^*)$ from (c). Thus, E_1 is contained in a Hall $\tau_1(M^*)$-subgroup $(E^*)_1$ of M^* and $1 \neq P \subseteq C_{E^*_\sigma}(R)$ where $R \subseteq (M^*)_\sigma$. Since $\tau_1(M^*) \cap \varpi \neq \emptyset$, E^*_1 acts in a prime manner on $(M^*)_\sigma$ by Theorem 7.5. Therefore, E^*_1 centralizes R. Since $E_1 \subseteq E^*_1$, R centralizes E_1. It follows that $R \subseteq C_{E_3}(E)$ because $R \subseteq E_3$ and $E = E_1E_3$. Recall that E_3 is cyclic. However, $C_{E_3}(E) = 1$ by Lemma 6.1 (f). This proves Lemma 7.7. Q.E.D.

Lemma 7.8. *The following configuration is impossible:*

(1) $M, M^* \subseteq \mathcal{M}$ *and* M^* *is not conjugate to* M *in* G,

(2) $p \in \tau_1(M) \cap \tau_1(M^*)$ *and* $P \in \mathcal{E}^1(M \cap M^*)$,

(3) Q *and* Q^* *are* P*-invariant Sylow subgroups (possibly for different primes) of* $M \cap M^*$,

(4) $C_Q(P) = 1$ *and* $C_{Q^*}(P) = 1$, *and*

(5) $N_G(Q) \subseteq M^*$ *and* $N_G(Q^*) \subseteq M$.

Proof. Assume this configuration. It follows from (3) and (5) that Q is a nonidentity Sylow q-subgroup for some prime q different from p and Q^* is a Sylow subgroup of M^*. By Lemma 6.18 (b), we have $\alpha(M) = \beta(M)$, $M_\alpha \neq 1$, and $q \notin \alpha(M)$. Furthermore, by (a) of the same lemma, $C_{M_\alpha}(P) \neq 1$ and $C_{M_\alpha}(PQ) = 1$. Since $C_{M_\alpha}(P) \neq 1$ and $\alpha(M) \subseteq \varpi$, we have $p \in \varpi$ by Lemma A.

Proposition 1.6 [BG] yields that $Q = C_Q(P)[Q, P]$. By (4),

$$Q = [Q, P] \subseteq M' \cap (M^*)'.$$

Theorem 4.2 (d) shows that M'/M_α is nilpotent. It follows that $M_\alpha Q \lhd M$ and the Frattini argument yields $M = M_\alpha N_M(Q)$.

This implies that $N_M(Q)$ contains a Hall $\alpha(M)'$-subgroup K of M. Since $q \notin \alpha(M)$ and $p \in \tau_1(M)$, PQ is an $\alpha(M)'$-subgroup of $N_M(Q)$. We may choose K so that $PQ \subseteq K$. Note that we have

$$M = M_\alpha K, M_\alpha \cap K = 1, \quad \text{and} \quad PQ \subseteq K \subseteq N_M(Q).$$

We claim that $C_M(P) = C_{M_\alpha}(P)C_K(P)$. Take an element of $C_M(P)$ and write it xy with $x \in M_\alpha$ and $y \in K$. This is a unique expression of this sort. For any $z \in P$,

$$xy = z^{-1}(xy)z = (z^{-1}xz)(z^{-1}yz).$$

Since $z^{-1}xz \in M_\alpha \lhd M$ and $z^{-1}yz \in K$, we have $z^{-1}xz = x$ and $z^{-1}yz = y$. This proves $C_M(P) \subseteq C_{M_\alpha}(P)C_K(P)$. The reverse containment is obvious. This proves the claim.

Let H be a Hall $(\beta(M) \cup \beta(M^*))$-subgroup of $C_G(P)$. Recall that $p \in \varpi$, so $C_G(P)$ is contained in a ϖ-local subgroup and it is solvable. Take any $s \in \pi(F(H))$ and $t \in \pi F(C_{M_\beta}(P)))$. By symmetry between M and M^*, we may fix notation and can assume $s \in \beta(M)$. We may choose H so that $C_{M_\beta}(P) \subseteq H$. Let $X = O_s(H)$ and $Y = O_t(C_{M_\beta}(P))$. We will show that $H \subseteq M$.

Since $s \in \beta(M)$, M contains a Sylow s-subgroup of G. Hence, some conjugate M^g with $g \in G$ contains X. By Proposition 4.14 (d), applied to M^g and X, we have $M^g \supseteq N_G(X) \supseteq H \supseteq Y$.

The same argument applied to M and Y yields $M \supseteq N_G(Y) \supseteq C_G(Y)$. Since $Y \subseteq M \cap M^g$, it follows from Theorem 4.1 (b) that $M^g = M^h$ for some element $h \in C_G(Y) \subseteq M$. Thus, $M = M^g \supseteq H$.

Take $r \in \beta(M^*) \cap \pi(H)$. By Lemma 4.12 (a), $r \notin \sigma(M)$. Note that M^* is not conjugate to M by (1). Moreover, since $H \subseteq M$, $r \in \pi(C_M(P))$. Since $C_M(P) = C_{M_\alpha}(P)C_K(P)$, $K \subseteq N_M(Q)$, and $r \notin \alpha(M) \subseteq \sigma(M)$, we have $r \in \pi(C_K(P))$. Therefore, there is a subgroup $R \in \mathcal{E}_r^1(N_M(Q) \cap C_G(P))$. Then, $R \subseteq N_G(Q) \subseteq M^*$ and $r \in \beta(M^*)$. Proposition 4.14 (d) applied to $R \subseteq M^*$ yields $N_G(R) \subseteq M^*$.

The subgroup $PR = P \times R$ is a $\sigma(M)'$-subgroup of M. Hence, PR is conjugate to a subgroup of E in M. Since $p \in \varpi$, we can apply Theorem 7.4 to obtain

$$1 \neq X \subseteq C_{M_\sigma}(P) \subseteq C_{M_\sigma}(R) \subseteq M^*.$$

We claim that $[X, Q] = 1$. We have $X \subseteq M_\alpha \cap M^*$ and $M_\alpha \cap M^*$ is a Q-invariant q'-subgroup because $q \notin \alpha(M)$. Therefore, $[X, Q]$ is a q'-group. We have $Q \subseteq (M^*)'$ and $(M^*)'/(M^*)_\alpha$ is nilpotent by Theorem 4.2 (d). Hence, $(M^*)_\alpha Q \lhd M^*$.

It follows that $[X, Q] \subseteq [X, (M^*)_\alpha Q] \subseteq (M^*)_\alpha Q$. Since $[X, Q]$ is a q'-group, we have $[X, Q] \subseteq (M^*)_\alpha$. On the other hand, $X \subseteq M_\beta$ because $s \in \beta(M)$. Therefore, $[X, Q] \subseteq [M_\beta, Q] \subseteq M_\beta \subseteq M_\alpha$. Lemma 4.12 yields $M_\alpha \cap (M^*)_\alpha = 1$. Thus, we have $[X, Q] = 1$.

Since $X \subseteq H \subseteq C_{M_\alpha}(P)$, we have $1 \neq X \subseteq C_{M_\alpha}(PQ)$. This contradicts the fact that $C_{M_\alpha}(PQ) = 1$. Q.E.D.

Theorem 7.9. *Suppose M, $M^* \in \mathcal{M}$ and M^* is not conjugate to M in G. Then, $\sigma(M)$ is disjoint from $\sigma(M^*)$.*

Theorem 7.10. *Suppose that some $P \in \mathcal{E}^1(E)$ does not centralize E_3. Then, $\tau_1(M) \subseteq \varpi$ and the following hold.*

(a) *E_1 acts regularly on E_3.*

(b) *E_3 acts regularly on M_{σ_0}.*
(c) $C_{M_{\sigma_0}}(P) \neq 1$.

Proof. We remark that the assumption implies $E_3 \neq 1$. Suppose $\tau_1(M) \cap \varpi = \emptyset$. Then, by Lemma G, M is a Frobenius group. The Frobenius kernel is either M' or M_α. In the first case, we have $M' = M_\sigma$ and $E_3 = 1$. On the other hand, if the Frobenius kernel is M_α, the group E is a subgroup of a Frobenius complement. Hence, by the structure of a Frobenius complement, every subgroup of prime order in E is normal in E. In particular, P centralizes E_3. Thus, we have $\tau_1(M) \cap \varpi \neq \emptyset$. In this case, we have $\tau_1(M) \subseteq \varpi$ because E_1 is cyclic.

Suppose that $\tau_1(M) \subseteq \varpi$ but M is not a ϖ-group. Then, Lemma G yields that M/M' is a ϖ-group, M'/M_α is a ϖ'-group and M_α is a ϖ-group. Since $E_3 \subseteq E' \subseteq M'$ by Lemma 6.1 (b), E_3 is a ϖ'-group. Since E_1 is a ϖ-group ($\tau_1(M) \subseteq \varpi$), we have (a).

Lemma G yields $M_\alpha = M_{\sigma_0}$. Hence, M_{σ_0} is a ϖ-group and we have (b). The Frobenius group PE_3 acts on M_α with $C_{M_\alpha}(E_3) = 1$. Theorem 3.10 [BG] yields that $C_{M_\alpha}(P) \neq 1$. This proves (c).

If M is a ϖ-group, the proof of Theorem 13.10 [BG] shows the validity of (a), (b) and (c). Q.E.D.

Corollary 7.11. *Suppose $E_3 \neq 1$ and E_3 does not act regularly on M_{σ_0}. Then, M is a ϖ-group with $\tau_2(M) = \emptyset$. We have* (a) $E_1 \neq 1$, (b) $E = E_1E_3$, (c) E acts in a prime manner on M_σ, and (d) every $X \in \mathcal{E}^1(E)$ is normal in E.

Proof. If $\tau_2(M) \neq \emptyset$, Corollary 6.6 (d) yields that E_3 acts regularly on M_σ. This is false, so we have $\tau_2(M) = \emptyset$. Lemma 6.1 yields (a) and (b). It follows from Theorem 7.10 (b) that every $P \in \mathcal{E}^1(E_1)$ centralizes E_3. This implies (d) because $E = E_1E_3$ and E_1 is cyclic.

By assumption some nonidentity element of E_3 centralizes a ϖ-subgroup. Therefore, $\tau_3(M) \cap \varpi \neq \emptyset$ by Lemma A. By Lemma 7.7 (2), M is a ϖ-group and (c) holds. Q.E.D.

Lemma 7.12. *Suppose $p \in \tau_1(M)$, $P \in \mathcal{E}^1(E)$, $q \in \tau_2(M)$, $A \in \mathcal{E}^2_p(E)$, and $C_A(P) \neq 1$. Then, $C_{M_\sigma}(P) = 1$.*

Proof. Since $\tau_2(M) \neq \emptyset$, M is a ϖ-group by Lemma H. The proof of Lemma 13.12 [BG] may be adapted to this case. Q.E.D.

Lemma 7.13. *Suppose that $p \in \tau_1(M) \cup \tau_3(M)$, $P \in \mathcal{E}^1(E)$, and $C_{M_\sigma}(P) \neq 1$. Then, for every $M^* \in \mathcal{M}(N_G(P))$, we have $p \in \sigma(M^*)$.*

Proof. Once $p \in \tau_2(M^*)$ is assumed, M^* is a ϖ-group by Lemma H. The proof of Lemma 13.13 [BG] works. Q.E.D.

§8. Subgroups of Type $\mathcal{P}$ and Counting Arguments Prime Action

Warning. We will use the notation of [BG] with *one major change.* Let $\kappa(M)$ be the set of primes $p \in \tau_1(M) \cup \tau_3(M)$ such that

$$C_{M_{\sigma_0}}(P) \neq 1 \quad \text{for some} \quad P \in \mathcal{E}_p^1(M).$$

This definition makes $\kappa(M) \subseteq \varpi$. Since we never use the set defined to be $\kappa(M)$ in [BG], we use the same notation for a different meaning. We divide the set $\mathcal{M}$ into three parts $\mathcal{M}_{\mathcal{F}}$, $\mathcal{M}_{\mathcal{P}_1}$, and $\mathcal{M}_{\mathcal{P}_2}$ just as in [BG]. However, the set $\kappa(M)$ is used in the sense defined above.

The notion of *σ-decomposition* and of *σ-length* of an element must also be modified: we replace $\sigma(M)$ used in their definitions in [BG] by $\sigma_0(M)$. For example, we define

$$\mathcal{M}_\sigma(g) = \{M \in \mathcal{M} \mid g \in M_{\sigma_0}\}.$$

However, we use the same notation as that of [BG]. Note that our definition coincides with theirs if g is a ϖ-element. As in [BG], we have $\ell_\sigma(g) = 1$ for a ϖ-element $g \in G$ if and only if $\mathcal{M}_\sigma(g)$ is not empty.

Lemma 8.1. *Suppose that $M \in \mathcal{M} \setminus \mathcal{M}_{\mathcal{P}_1}$. Take any $p \in \pi(M) \setminus \{\sigma(M), \kappa(M)\}$, let $S \in Syl_p(M)$ and let $A = \Omega_1(S)$. Then, $|A| \leq p^2$, $C_{M_{\sigma_0}}(A) = 1$, and M_{σ_0} is nilpotent.*

Proof. We have $\pi(M) \setminus \sigma(M) = \tau_1(M) \cup \tau_2(M) \cup \tau_3(M)$. If $p \in \tau_2(M)$, M is a ϖ-group by Lemma H. Lemma 8.1 follows from (b), (d) and (a) of Theorem 6.5.

If $p \in \tau_1(M) \cup \tau_3(M)$, we have $r_p(M) \leq 1$ so $|A| = p$. Since $p \notin \kappa(M)$, $C_{M_{\sigma_0}}(A) = 1$ and this implies that M_{σ_0} is nilpotent by Thompson's Theorem 3.7 [BG]. Q.E.D.

Proposition 8.2. *Suppose $M \in \mathcal{M}_{\mathcal{P}}$. Let K be a Hall $\kappa(M)$-subgroup of M and define $K^* = C_{M_\sigma}(K)$. Then, $K^* \subseteq M_{\sigma_0}$ and the following hold.*

(a) *The group K acts in a prime manner on M_σ, and acts regularly on some abelian Hall $(\kappa(M) \cup \sigma_0(M))'$-subgroup U of M.*

(b) *For every $X \in \mathcal{E}^1(K)$,*

  (1) *$N_M(X) = N_M(K) = K \times K^*$, and*

  (2) *$X \subseteq (M^*)_\sigma$ for each $M^* \in \mathcal{M}(N_G(X))$. In particular, we have $N_G(X) \not\subseteq M$.*

(c) *$K^* \neq 1$ and every $X \in \mathcal{E}^1(K^*)$ satisfies $\mathcal{M}(C_G(X)) = \{M\}$.*

(d) *Every $g \in G \setminus M$ satisfies $K^* \cap M^g = 1$ and every $g \in M \setminus (K \times K^*)$ satisfies $K \cap K^g = 1$.*

(e) *For every prime $p \in \pi(K^*)$ and every $S \in Syl_p(M_{\sigma_0})$,*

$$\mathcal{M}(S) = \{M\} \quad \textit{and} \quad S \nsubseteq K^*.$$

(f) *Every $\sigma_0(M)$-subgroup Y of G satisfying $Y \cap K^* \neq 1$ lies in M_{σ_0}.*

(g) *If $M \in \mathcal{M}_{\mathcal{P}_2}$, then $\sigma_0(M) = \beta(M)$, K has prime order, and M_{σ_0} is a nilpotent TI-subgroup of G.*

Proof. Although the proof of Proposition 14.2 [BG] is applicable, we include some details.

We prove (a) and (b1). Take a complement E of M_σ that contains K. Suppose that

$$\kappa(M) \cap \tau_3(M) \neq \emptyset.$$

Then, $E_3 \neq 1$ and E_3 does not act regularly on M_{σ_0}. By Corollary 7.11, M is a ϖ-group, $E_1 \neq 1$, $E = E_1E_3$, E acts in a prime manner on M_σ, and every $X \in \mathcal{E}^1(E)$ is normal in E. Since $E = E_1E_3$ acts in a prime manner on M_σ, we have $\kappa(M) = \pi(E)$. Therefore, $K = E$ and K acts in a prime manner on M_σ. In this case, $\pi(M) = \sigma(M) \cup \kappa(M)$. So, $U = 1$ satisfies (a). If $X \in \mathcal{E}^1(K)$, we have $X \lhd E$. It follows from $M = M_\sigma E$ that

$$N_M(X) = N_{M_\sigma}(X)E = C_{M_\sigma}(X)E.$$

Since K acts in a prime manner on M_σ, we have $C_{M_\sigma}(X) = C_{M_\sigma}(K) = K^*$. Thus, $N_M(X) = K \times K^*$. Therefore, (a) and (b) hold in the case $\kappa(M) \cap \tau_3(M) \neq \emptyset$.

Suppose that $\kappa(M) \cap \tau_3(M) = \emptyset$. Then, $\kappa(M) \subseteq \tau_1(M)$ and $\varpi \cap \tau_1(M) \neq \emptyset$. Theorem 7.5 shows that E_1 acts in a prime manner on M_σ. Thus, $\kappa(M) = \tau_1(M)$ and we may choose $K = E_1$. To prove (a), we need to find U. Suppose that M is not a ϖ-group. Since $\tau_1(M) = \kappa(M) \subseteq \varpi$, M is a group of type (2) in Lemma G. Then, we have

$$\pi(M) \setminus \{\kappa(M), \sigma_0(M)\} = \pi(M) \cap \varpi'.$$

There is an E_1-invariant complement U of M_α in M'. Since $U \cong M'/M_\beta$ is cyclic, U satisfies (a).

Assume that M is a ϖ-group. Then, $\sigma_0(M) = \sigma(M)$ and

$$\pi(M) \setminus \{\kappa(M), \sigma_0(M)\} = \tau_2(M) \cup \tau_3(M).$$

We will show that $U = E_2E_3$ satisfies (a). Since $K = E_1$, U is K-invariant. Assume $E_2 \neq 1$. If E_1 does not act regularly on E_2, some

$P \in \mathcal{E}^1(E_1)$ satisfies $C_A(P) \neq 1$ for some $A \in \mathcal{E}^2(E_2)$. Lemma 7.12 yields $C_{M_\sigma}(P) = 1$ contrary to the fact that $K = E_1$ acts in a prime manner on M_σ. Thus, E_1 acts regularly on E_2. If E_1 does not act regularly on E_3, some $P \in \mathcal{E}^1(E_1)$ centralizes some $R \in \mathcal{E}^1(E_3)$. Since M is assumed to be a ϖ-group, Theorem 7.4 yields that

$$1 \neq C_{M_\sigma}(P) \subseteq C_{M_\sigma}(R).$$

This would imply $\tau_3(M) \cap \kappa(M) \neq \emptyset$ in contradiction to the hypothesis of this case. Thus, $E_1 \neq 1$ acts regularly on E_2E_3. It follows from Theorem 3.7 [BG] that E_2E_3 is nilpotent. By Corollary 6.10 (a), E_2E_3 is abelian. This proves (a).

It follows from the structure of the group M discussed in the proof of (a) that every $X \in \mathcal{E}^1(K)$ is normal in K, M is the semidirect product of M_{σ_0} and UK, and $N_{UK}(X) = K$. We have

$$N_M(X) = N_{M_{\sigma_0}}(X)K = C_{M_{\sigma_0}}(X)K = C_{M_{\sigma_0}}(K)K = K^* \times K.$$

This proves (b1).

Lemma 7.13 yields the first part of (b2). We have $M \notin \mathcal{M}(N_G(X))$, since $X \subseteq E_1$. This proves (b2).

The parts (c), (d), (e) and (f) are proved as in the proof of Proposition 14.2 [BG]. For (f), recall that M_{σ_0} is a normal Hall subgroup of M_σ. Hence, M_{σ_0} contains all $\sigma_0(M)$-subgroup of M_σ.

For the proof of (g), suppose that $U \neq 1$. Then, (a) implies that KU is a Frobenius group with Frobenius kernel U. Suppose that M is not a ϖ-group. Then, by Lemma G, U is a ϖ'-group, so $M_{\sigma_0}U$ is a Frobenius group with Frobenius kernel M_{σ_0}. Hence, $C_{M_\sigma}(U) = 1$ and M_{σ_0} is nilpotent. Thus, the nonidentity Frobenius group KU acts on a nilpotent group M_{σ_0} and K acts in a prime manner on M_{σ_0}. It follows from Theorem 3.10 [BG] that K has prime order. By Lemma G, we have $M_\beta = M_{\sigma_0}$. Lemma 6.17 shows that for every $g \in G \setminus M$, the group $M_{\sigma_0} \cap M^g$ is a $\beta(M)'$-group. Since $M_{\sigma_0} = M_\beta$, $M_{\sigma_0} \cap M^g$ is a $\beta(M)$-group. This proves that $M_{\sigma_0} \cap M^g = 1$ for every $g \in G \setminus M$. Thus, M_{σ_0} is a TI-subgroup of G.

Suppose finally that M is a ϖ-group In this case, we have $U = E_2E_3$. Lemma 8.1 shows that $C_{M_\sigma}(U) = 1$ and M_σ is nilpotent. Since K acts in a prime manner on M_σ by (a), Lemma 3.10 [BG] yields that K has prime order. We have $U = [U, K] \subseteq E'$. By Lemma 6.19, U centralizes a Hall $\beta(M)'$-subgroup of M_σ. Since $C_{M_\sigma}(U) = 1$, a Hall $\beta(M)'$-subgroup equals 1. Therefore, $M_\beta = M_\sigma$ and $\beta(M) = \sigma(M)$. Lemma 6.17 implies that $M_{\sigma_0} \cap M^g = 1$ for every $g \in G \setminus M$. This completes the proof of Proposition 8.2. Q.E.D.

Corollary 8.3. *Suppose $M \in \mathcal{M}$, $x \in {M_{\sigma_0}}^\sharp$, and x' is a nonidentity $\sigma(M)'$-element of $C_M(x)$. Then, either*

(1) $\pi(\langle x'\rangle) \subseteq \kappa(M)$ *and* $C_G(x) \subseteq M$, *or*
(2) $\pi(\langle x'\rangle) \subseteq \tau_2(M)$, $\ell_\sigma(x') = 1$, *and* $\mathcal{M}(C_G(x')) = \{M\}$.

Theorem 8.4. *Suppose that x is a ϖ-element of $G^\sharp$ such that $\mathcal{M}_\sigma(x)$ is not empty. Then, $C_G(x)$ has a normal Hall subgroup $R(x)$ that acts sharply transitively on $\mathcal{M}_\sigma(x)$ by conjugation. Furthermore, if $|\mathcal{M}_\sigma(x)| > 1$, then $C_G(x)$ lies in a unique subgroup $N = N(x) \in \mathcal{M}$ and for every $M \in \mathcal{M}_\sigma(x)$,*

(a) $R(x) = C_{N_\sigma}(x) \neq 1$,
(b) $C_G(x) = C_M(x)R(x)$,
(c) $\pi(\langle x\rangle) \subseteq \tau_2(N) \subseteq \sigma_0(M)$,
(d) $\pi(M) \cap \sigma(N) \subseteq \beta(N)$,
(e) $M \cap N$ *is a complement of* N_σ *in* N, *and*
(f) N *is a* ϖ*-group in* $\mathcal{M}_{\mathcal{F}} \cup \mathcal{M}_{\mathcal{P}_2}$.

Proof. The proof of Theorem 14.4 [BG] may be modified with some changes to yield this theorem. We will present the details here. If $|\mathcal{M}_\sigma(x)| = 1$, we can let $R(x) = 1$ and finish the proof. So, we will assume $|\mathcal{M}_\sigma(x)| > 1$ in the remainder of proof.

Since x is a ϖ-element with $\mathcal{M}_\sigma(x) \neq \emptyset$, we can take $M \in \mathcal{M}_\sigma(x)$, $q \in \pi(\langle x\rangle)$, $X \in \mathcal{E}_q^1(\langle x\rangle)$, and $N \in \mathcal{M}(N_G(X))$. Note that $\mathcal{M}_\sigma(x) \subseteq \mathcal{M}_\sigma(X)$ and

$$C_G(x) \subseteq N_G(\langle x\rangle) \subseteq N_G(X) \subseteq N.$$

We will show that $\mathcal{M}_\sigma(X)$ consists of conjugates of M and that $C_G(X)$ acts transitively on $\mathcal{M}_\sigma(X)$ by conjugation. Let $L \in \mathcal{M}_\sigma(X)$. Then, $X \subseteq M_\sigma \cap L_\sigma$. Theorem 7.9 yields that L is conjugate to M. Since $q \in \sigma(M)$ and X is a q-group, Theorem 4.1 (b) yields that $C_G(X)$ acts transitively on $\mathcal{M}_\sigma(X)$. In particular, $C_G(X) \nsubseteq M$ and $N \neq M$.

Since $N \neq M$, Proposition 6.15 (a) applies to N and yields that N is not conjugate to M. Then, by Theorem 7.9, $\sigma(N)$ is disjoint from $\sigma(M)$. It follows that $q \notin \sigma(N)$. Proposition 6.15 (e) now yields that $q \in \tau_2(N)$ and the conditions (d) and (e) of this theorem hold. Since $q \in \tau_2(N)$, $\tau_2(N)$ is not empty. Therefore, $N \notin \mathcal{M}_{\mathcal{P}_1}$ and N is a ϖ-group by Lemma H. This proves (f).

We will prove that $R(x)$ acts sharply transitively on $\mathcal{M}_\sigma(x)$. We have shown that if $L \in \mathcal{M}_\sigma(x)$, then $L = M^u$ with $u \in C_G(X) \subseteq N$. Since $N = (M \cap N)N_\sigma$ by (e), we may choose $u \in N_\sigma$. Then,

$$(x^{-1}ux)^{-1}M(x^{-1}ux) = M^{ux} = L^x = L = M^u.$$

However, if $M^u = M^v$ for $u, v \in N_\sigma$, then $uv^{-1} \in N_G(M) \cap N_\sigma$. Since $N_G(M) = M$ by Lemma E, we have $uv^{-1} \in M \cap N_\sigma = 1$ by (e). We apply this twice. First, the displayed formula yields that if $L = M^u$ with $u \in N_\sigma$, then $u \in R(x)$. Thus, $R(x)$ acts transitively on $\mathcal{M}_\sigma(x)$. Secondly, $M^u = M$ with $u \in R(x)$ implies $u = 1$. Thus, $R(x)$ is sharply transitive. Since $|\mathcal{M}_\sigma(x)| > 1$, we have (a). Since $R(x) \subseteq C_G(x)$ and $R(x)$ is transitive on $\mathcal{M}_\sigma(x)$, we have

$$C_G(x) = (C_G(x) \cap N_G(M))R(x) = C_M(x)R(x).$$

This proves (b).

We prove next $\mathcal{M}(C_G(x)) = \{N\}$. Since $R(x) \neq 1$, there is an element $y \in {N_{\sigma_0}}^\sharp$ such that $y \in C_G(x)$. Apply Corollary 8.3 to (N, y, x) in place of (M, x, x'). Since x is a $\sigma(M)$-element, it is a $\sigma(N)'$-element. Since $q \in \pi(\langle x\rangle) \cap \tau_2(N)$, we have the second case of Corollary 8.3. Thus, $\pi(\langle x\rangle) \subseteq \tau_2(N)$ and $\mathcal{M}(C_G(x)) = \{N\}$.

It remains to prove (c). We have just proved $\pi(\langle x\rangle) \subseteq \tau_2(N)$. Take $p \in \tau_2(N)$. By (e) and Corollary 6.6 (a), there is $A \in \mathcal{E}_p^2(M \cap N)$ such that $A \lhd M \cap N$. Then, $x \in N_{M_\sigma}(A)$. Since $r_p(M) \geq 2$, we have $p \in \sigma(M) \cup \tau_2(M)$. If $p \in \tau_2(M)$, $N_{M_\sigma}(A) = C_{M_\sigma}(A) = 1$ by Corollary 6.5 (d). This contradiction proves $p \in \sigma(M)$. In fact, $p \in \sigma_0(M)$ because N is a ϖ- group by (f). Q.E.D.

We will use the notation $\widetilde{M}$ to mean

$$\{xx' \mid x \in {M_{\sigma_0}}^\sharp \quad \text{and} \quad x' \in R(x)\}.$$

This is slightly different from the usage in [BG].

Lemma 8.5. *The following hold.*

(a) *If x and y are distinct ϖ-elements of $G^\sharp$ of σ-length one, then $xR(x) \cap yR(y) = \emptyset$.*

(b) *If M_1 and M_2 are elements of $\mathcal{M}$ not conjugate in G, then $\widetilde{M_1} \cap \widetilde{M_2} = \emptyset$.*

(c) *If $M \in \mathcal{M}$, then $|\mathcal{C}_G(\widetilde{M})| = (|M_{\sigma_0}| - 1)|G : M|$.*

Proof. (a) Suppose that $g = xx'$ with $\ell_\sigma(x) = 1$ and $x' \in R(x)$ lies in $yR(y)$ and $x \neq y$. Write $g = yy'$ with $y' \in R(y)$. Since y is a σ-factor of the element g, we have $y = x'$, so $x' \neq 1$. Therefore, $|\mathcal{M}_\sigma(x)| > 1$. Take $M \in \mathcal{M}(C_G(y))$. Then, $y' = x \in M_\sigma$ and $M \in \mathcal{M}_\sigma(x)$. Take $N \in \mathcal{M}(C_G(x))$. Then, $x' = y \in N_\sigma \cap M$ which is 1 by Theorem 8.4 (e). This contradicts $y \neq 1$.

The parts (b) and (c) follow as in the proof of Lemma 14.4 [BG].
Q.E.D.

Lemma 8.6. *Each nonidentity ϖ-element g satisfies exactly one of the following two conditions*:

(1) $g = xx'$ *with* $\ell_\sigma(x) = 1$ *and* $x' \in R(x)$, *or*

(2) $g = yy'$ *with* $\ell_\sigma(y) = 1$ *and* y' *is a nonidentity* $\kappa(M)$*-element of* $C_M(y)$ *for some* $M \in \mathcal{M}_\sigma(y)$.

Proof. Suppose that both (1) and (2) hold for some ϖ-element $g \neq 1$. We will derive a contradiction. Take $N \in \mathcal{M}(C_G(x))$ and $L \in \mathcal{M}_\sigma(x)$. Since y is a σ-factor of g, we have $y = x$ or $y = x'$. Suppose $y = x$. We may choose $L = M$. Since $y = x$, we have $x' = y' \neq 1$. By Theorem 8.4, $|\mathcal{M}_\sigma(x)| = |R(x)| > 1$ and. by Part (e),

$$x' = y' \in N_\sigma \cap M = 1.$$

This contradicts $y' \neq 1$. Suppose next $y = x'$. Then, we have $y' = x$ and it is a $\kappa(M)$-element and at the same time a $\tau_2(N)$-element by Theorem 8.4 (c). Since $1 \neq y = x' \in M_\sigma \cap N_\sigma$, N is conjugate to M by Theorem 7.9. Therefore, we have $\tau_2(N) = \tau_2(M)$ Since $\kappa(M) \cap \tau_2(M) = \emptyset$, we have a contradiction $y' = 1$.

We will prove that either (1) or (2) holds for every g. Suppose that no decomposition of type (1) or (2) is possible and we will derive a contradiction. We have $\ell_\sigma(g) > 1$ since the choice of $x = g$ and $x' = 1$ provides (1) if $\ell_\sigma(g) = 1$. Let x be a σ-factor of g with $\ell_\sigma(x) = 1$, and write $g = xx'$. We prove a lemma: *under the hypothesis of this paragraph, no subgroup* $M \in \mathcal{M}_\sigma(x)$ *contains* g.

Suppose $g \in M$. Then, $x' \in M$ and $x' \neq 1$ because $\ell_\sigma(g) > 1$. Since x is a σ-factor of the element g, x' is a $\sigma(M)'$-element but not a $\kappa(M)$-element because $g = xx'$ does not satisfy (2). Therefore, we must have the case (2) of Corollary 8.3. Thus, we have $\ell_\sigma(x') = 1$ and $\mathcal{M}(C_G(x')) = \{M\}$. It follows that

$$x \in M_\sigma \cap C_G(x') = R(x').$$

This implies that $g = xx'$ is a decomposition of type (1) with (x', x) in place of (x, x'). This is a contradiction and proves the lemma.

Let x be a σ-factor of the element g with $\ell_\sigma(x) = 1$ and write $g = xx'$. Then, x is a power of g. Take $M \in \mathcal{M}_\sigma(x)$ and $N \in \mathcal{M}(C_G(x))$. Then, $g \in C_G(x) \subseteq N$. By the lemma, none of the σ-factor of g of σ-length one lies in N_σ. It follows that g is a $\sigma(N)'$-element of N. We have $x = x^g \in M \cap M^g$ and $g \notin M$ (by the lemma). Thus, $|\mathcal{M}_\sigma(x)| > 1$ and, by Theorem 8.4 (e), $M \cap N$ is a complement of N_σ in N. Since g is a $\sigma(N)'$-element, $g \in (M \cap N)^u$ for some element $u \in N$. Thus, $g \in M^u$. Since x is a power of g, we have $x \in M^u$. However, x is a $\sigma(M)$-element.

Since $\sigma(M) = \sigma(M^u)$, we have $x \in M_\sigma{}^u$. This contradicts the Lemma. Q.E.D.

Theorem 8.7. *Suppose $M \in \mathcal{M}_\mathcal{P}$ and K is a Hall $\kappa(M)$-subgroup of M. Let $K^* = C_{M_\sigma}(K)$, $k = |K|$, $k^* = |K^*|$, $Z = K \times K^*$, and $\widehat{Z} = Z \setminus (K \cup K^*)$. Then, for some other $M^* \in \mathcal{M}_\mathcal{P}$ that is not conjugate to M, we have*

(a) *$\mathcal{M}(C_G(X)) = \{M^*\}$ for every $X \in \mathcal{E}^1(K)$,*

(b) *K^* is a Hall $\kappa(M^*)$-subgroup of M^* and a Hall $\sigma_0(M)$-subgroup of M^*,*

(c) *$K = C_{M^*_\sigma}(K^*)$ and $\kappa(M) = \tau_1(M)$,*

(d) *Z is cyclic and for every $x \in K^\sharp$ and $y \in (K^*)^\sharp$,*

$$M \cap M^* = Z = C_M(x) = C_{M^*}(y) = C_G(xy),$$

(e) *$\widehat{Z}$ is a TI-subset of G with $N_G(\widehat{Z}) = Z$, $\widehat{Z} \cap M^g$ empty for all $g \in G \setminus M$, and*

$$|\mathcal{C}_G(\widehat{Z})| = (1 - \frac{1}{k} - \frac{1}{k^*} + \frac{1}{kk^*})|G| > \frac{1}{2}|G|,$$

(f) *M or M^* lies in $\mathcal{M}_{\mathcal{P}_2}$ and, accordingly, K or K^* has prime order,*

(g) *every $H \in \mathcal{M}_\mathcal{P}$ is conjugate to M or M^* in G, and*

(h) *M' is a complement of K in M and $M' = M_{\sigma_0}U$ where U is the subgroup defined in Proposition 8.2 (a).*

Proof. Although the proof of Theorem 14.7 [BG] is adequate to cover this theorem, we will paraphrase their proof of this miraculous theorem. By the hypothesis, $M \in \mathcal{M}_\mathcal{P}$. Thus, $\kappa(M)$ is not empty and $K \neq 1$.

We begin the proof with the following lemma which is not really necessary. *If $X \in \mathcal{E}^1(K)$, then $N_G(X) \in \mathcal{U}$.* Suppose $H, L \in \mathcal{M}(N_G(X))$. By Proposition 8.2 (b2), $X \subseteq H_\sigma \cap L_\sigma$. It follows from Theorem 7.9 that $L = H^g$ for some $g \in G$. Since $C_G(X) \subseteq N_G(X) \subseteq H$, Theorem 4.1 (e) with H in place of M yields $L = H^g = H$. This completes the proof of the lemma.

Let $M_1, M_2, \ldots, M_n$ be the distinct subgroups in $\mathcal{M}$ that contain $N_G(X)$ for some $X \in \mathcal{E}^1(K)$. For each i, take $X_i \in \mathcal{E}^1(K)$ such that $M_i \in \mathcal{M}(N_G(X_i))$. By Proposition 8.2 (b), we have $\pi(X_i) \subseteq \sigma_0(M_i)$ and

$$Z = K \times K^* \subseteq N_G(X_i) \subseteq M_i.$$

Since $\pi(X_i) \subseteq \pi(K) = \kappa(M) \subseteq \sigma(M)'$, none of M_i is conjugate to M in G. Therefore, by Theorem 7.9, $\sigma(M)$ is disjoint from $\sigma(M_i)$. Thus, K^* is a $\sigma(M_i)'$-subgroup of M_i.

Take $X^* \in \mathcal{E}^1(K^*)$. By Proposition 8.2 (c), $\mathcal{M}(C_G(X^*)) = \{M\}$. Apply Corollary 8.3 to $M_i \in \mathcal{M}$, $x \in X_i{}^\sharp$, and $x' \in X^{*\sharp}$. All the assumptions of Corollary 8.3 are satisfied. Since $\mathcal{M}(C_G(X^*)) \neq \{M_i\}$, we have the first case: $\pi(X^*) \subseteq \kappa(M_i)$. We can take X^* arbitrary in $\mathcal{E}^1(K^*)$, so $\pi(K^*) \subseteq \kappa(M_i)$.

Let K_i be a Hall $\kappa(M_i)$-subgroup of M_i that contains X^*, and define $K_i^* = C_{M_{i_\sigma}}(K_i)$. Recall that K_i is a Z-group and that, by Proposition 8.2 (b1) for M_i, every subgroup in $\mathcal{E}^1(K_i)$ is normal in K_i. We claim that $K^* \subseteq K_i$. This is proved as follows. Since K^* is a $\kappa(M_i)$-subgroup of a solvable group M_i, $K^* \subseteq (K_i)^g$ for some $g \in M_i$. Then, X^* and X^{*g} are normal subgroups of the same prime order in the Z-group $(K_i)^g$. Hence, we have $X^* = (X^*)^g$. Thus, $g \in N_{M_i}(X^*) = N_{M_i}(K_i)$ by Proposition 8.2 (b1) for M_i. This implies $K^* \subseteq (K_i)^g = K_i$.

Since $X^* \subseteq K^*$ and $K \subseteq M_i$, we have

$$K \subseteq C_{M_i}(X^*) \subseteq N_{M_i}(X^*) = K_i \times K_i^*.$$

Therefore, $K \times K^* \subseteq K_i \times K_i^*$. Similarly, with M_i, K_i, X^*; M, K, and X_i in place of M, K, X_i; M_i, K_i, and X^*, we have $K_i \times K_i^* \subseteq K \times K^*$. We need to check a few relations: $X^* \subseteq K_i$, $M \in \mathcal{M}(N_G(X^*))$ and

$$X_i \subseteq K \quad \text{where} \quad X_i \in \mathcal{E}^1(K_i^*).$$

We check the last one. We have $X_i \subseteq K \subseteq K_i \times K_i^*$, $\pi(X_i) \subseteq \sigma_0(M_i)$, and K_i^* is a Hall $\sigma_0(M_i)$-subgroup of $K_i \times K_i^*$. Therefore, $X_i \subseteq \mathcal{E}^1(K_i^*)$. It follows that $K \times K^* = K_i \times K_i^*$ for each i. Let $M_0 = M$, $K_0 = K$, and $K_0^* = K^*$. Take $X_0^* \in \mathcal{E}^1(K^*)$. Then, by Proposition 8.2 (c), $\mathcal{M}(C_G(X_0^*)) = \{M_0\}$. For each $X_i^* \in \mathcal{E}^1(K_i^*)$ we have $\mathcal{M}(C_G(X_i^*)) = \{M_i\}$. It follows that $K_i^* \cap K_j^* = 1$ if $i \neq j$. Otherwise, we would have $\{M_i\} = \mathcal{M}(C_G(X)) = \{M_j\}$ for $X \in \mathcal{E}^1(K_i^* \cap K_j^*)$.

We claim that $Z = K_0^* \times K_1^* \times \cdots \times K_n^*$. Let Z_0 be the subgroup of Z generated by the subgroups K_i^*. For each i, we have $Z = K_i \times K_i^*$ where K_i^* is a $\sigma(M_i)$-group and K_i is a $\sigma(M_i)'$-group. Therefore, K_i^* is a normal Hall subgroup of Z. If $i \neq j$, we have shown $K_i^* \cap K_j^* = 1 (i \neq j)$. Then, K_i^* and K_j^* with $i \neq j$ have relatively prime orders and centralize each other. It follows that

$$Z_0 = K_0^* \times K_1^* \times \cdots \times K_n^*.$$

We will show that $Z = Z_0$. First, we prove that every $X \in \mathcal{E}^1(Z)$ is contained in some K_i^*. Since $Z = K_0 \times K_0^*$ and $(|K_0|, |K_0^*|) = 1$, either

$X \subseteq K_0^*$ or $X \subseteq K_0$. Suppose $X \subseteq K_0 = K$. It follows from the definition of the subgroups M_i that

$$\mathcal{M}(N_G(X)) = \{M_i\}$$

for some i (cf. the lemma at the beginning of the proof). By Proposition 8.2 (b1) for M_i, we have $X \subseteq (M_i)_\sigma$. Since K_i^* is the normal Hall $\sigma(M_i)$-subgroup of Z, we have $X \subseteq K_i^*$. Take any element $x \in Z$ of order p^e where p is a prime. Let $X \in \mathcal{E}^1(\langle x \rangle)$. Then, $X \subseteq K_i^*$ for some i. Hence, $p \in \pi(K_i^*)$ and $\langle x \rangle$ is a $\sigma(M_i)$-subgroup. This implies $x \in K_i^*$ as before.

Finally, let y be an arbitrary element of Z of order n. If $n = \prod {p_i}^{e_i}$ is the canonical decomposition of the integer n into the product of powers of distinct primes $p_1, \ldots, p_m$, we have $y = x_1 \ldots x_m$ where x_i is a power of the element y and the order of x_i is ${p_i}^{e_i}$. Then, $x_i \in Z$ so each x_i lies in Z_0 and we have $Z = Z_0$.

The subgroups K_i^* are distinct and each is a normal Hall subgroup of Z. It follows that the groups M_i are pairwise not conjugate in G. By Theorem 7.9, $\sigma(M_i)$ is disjoint from $\sigma(M_j)$ if $j \neq i$. Since K_j^* is a $\sigma(M_j)$-group, K_j^* is a $\sigma(M_i)'$-group for $j \neq i$. Therefore, we have $K_j^* \subseteq K_i$ for $j \neq i$, so if we let $W = \prod_{j \neq i} K_j^*$, $W \subseteq K_i$. The groups K_i and W are complements of K_i^* in Z. This implies $K_i = W$.

For every element $z \in Z$, the factorization $z = \prod z_i$ with $z_i \in K_i^*$ is the σ-decomposition of z.

Define $T = Z \setminus \{K_0^*, K_1^*, \ldots, K_n^*\}$. Note that $z \in Z$ is in T if and only if $z = yy'$ with $y \in K_i^{*\sharp}$ and $y' \in {K_i}^\sharp$ for some index i. In this case, y' is a nonidentity $\kappa(M_i)$-element of $C_{M_i}(y)$ with $\ell_\sigma(y) = 1$. Thus, we have the case (2) of Lemma 8.6. It follows that $T \cap \widetilde{H} = \emptyset$ for any $H \in \mathcal{M}$. Thus, $\mathcal{C}_G(T) \cap \mathcal{C}_G(\widetilde{M_i}) = \emptyset$ for each i. Since M_i are not conjugate to each other, Lemma 8.5 yields

$$\mathcal{C}_G(\widetilde{M_i}) \cap \mathcal{C}_G(\widetilde{M_j}) = \emptyset \quad \text{if} \quad i \neq j.$$

We will prove that T is a TI-subset of G with $N_G(T) = Z$. Suppose that $t \in T$, $g \in G$, and $t^g \in Z$. Write $t = yy' = y'y$ with $y \in K_i^{*\sharp}$ and $y' \in {K_i}^\sharp$ for some i. Then, y^g and $(y')^g$ are powers of t^g. Hence, $y^g \in K_i^* \cap (M_i)^g$. By Proposition 8.2 (d) for M_i, we have $g \in M_i$. Then, $y'^g \in K_i \cap (K_i)^g$. The same proposition yields that $g \in Z$. This proves that T is a TI-subset of G with $N_G(T) = Z$.

We count the number of elements in $\mathcal{C}_G(T)$. With $z = |Z|$, $k_i = |K_i|$, and $k_i^* = |K_i^*|$, we have

$$\begin{aligned}|\mathcal{C}_G(T)| &= |T||G : N_G(T)| \\ &= (z - 1 - \sum_{i=0}^{n}(k_i^* - 1))|G : Z| \\ &= (1 + \frac{n}{z} - \sum_{i=0}^{n} \frac{1}{k_i})|G|.\end{aligned}$$

Suppose that all the subgroups M_i lie in $\mathcal{P}_1$. Then $M_i = M_{i\sigma_0}K_i$ so $|M_i| = |M_{i\sigma_0}||K_i|$. By Lemma 8.5,

$$\begin{aligned}|\mathcal{C}_G(\widetilde{M_i})| &= (|M_{i\sigma_0}| - 1)|G : M_i| \\ &= (\frac{1}{k_i} - \frac{1}{|M_i|})|G| \geq (\frac{1}{k_i} - \frac{1}{2z})|G|.\end{aligned}$$

The last inequality comes from $Z \subsetneqq M_i$. Since the sets $\mathcal{C}_G(T)$, $\mathcal{C}_G(\widetilde{M_0})$, $\ldots$, $\mathcal{C}_G(\widetilde{M_n})$ are pairwise disjoint,

$$\begin{aligned}|G^\sharp| &\geq |\mathcal{C}_G(T)| + \sum_{i=0}^{n} |\mathcal{C}_G(\widetilde{M_i})| \\ &\geq ((1 + \frac{n}{z} - \sum_{i=0}^{n} \frac{1}{k_i}) + \sum_{i=0}^{n}(\frac{1}{k_i} - \frac{1}{2z}))|G| \\ &> |G|\end{aligned}$$

and this contradiction proves that some M_i is of type $\mathcal{P}_2$.

If M_i is of type $\mathcal{P}_2$, Proposition 8.2 (g) yields that K_i is of prime order and $M_{i\sigma_0}$ is nilpotent. Therefore, $K_i = K_j^*$ for $j \neq i$ and we have $n = 1$.

Since $K_i^* \subseteq M_{i\sigma_0}$, K_i^* is nilpotent. Furthermore,

$$Z = K_i \times K_i^* = K_j \times K_j^*,$$

$K_j = K_i^*$, $K_i = K_j^*$ and $r(K_i^*) = 1$. It follows that the nilpotent group K_i is cyclic. Since K_i is of prime order, $Z = K_i \times K_i^*$ is cyclic. This proves the first statement of (d).

Since $n = 1$, we have $T = \widehat{Z}$. Suppose $g \in G \setminus M$ and $T \cap M^g \neq \emptyset$. Take $uv \in T \cap M^g$ with $u \in K^\sharp$ and $v \in K^{*\sharp}$. Then, any power of uv lies in M^g so in particular, $v \in K^{*\sharp} \cap M^g$. This contradicts Proposition

8.2 (d). We have

$$
\begin{aligned}
|\mathcal{C}_G(T)| &= (1 - \frac{1}{k} - \frac{1}{k^*} + \frac{1}{kk^*})|G| \\
&= (1 - \frac{1}{k})(1 - \frac{1}{k^*})|G| \geq \frac{8}{15}|G| > \frac{1}{2}|G|
\end{aligned}
$$

because k and k^* are odd integers ≥ 3 and $k \neq k^*$. This proves (e).

With $M^* = M_1$, we have proved (f). We will prove (g). Suppose that $H \in \mathcal{M}_{\mathcal{P}}$. Let L be a Hall $\kappa(H)$-subgroup of H, $L^* = C_{H_\sigma}(L)$, and $S = L \times L^* \setminus \{L, L^*\}$. We have $|\mathcal{C}_G(T)| > |G|/2$ and $|\mathcal{C}_G(S)| > |G|/2$. It follows that $\mathcal{C}_G(T) \cap \mathcal{C}_G(S) \neq \emptyset$.

Replacing M and H by conjugates, we may assume that $T \cap S$ is not empty. Then, $L^* \cap K_i^* \neq 1$ for some i. If $Y \in \mathcal{E}^1(L^* \cap K_i^*)$ then Proposition 8.2 (c) yields $\{H\} = \mathcal{M}(C_G(Y)) = \{M_i\}$. This proves (g).

We will prove (a)¿ If $X \in \mathcal{E}^1(K)$, then $X \in \mathcal{E}^1(K_1^*)$ because $K_1^* = K$. Proposition 8.2 (c) yields $\mathcal{M}(C_G(X)) = \{M_1\} = \{M^*\}$.

Since $K^* = K_1$, K^* is a Hall $\kappa(M^*)$-subgroup of M^*. This is the first statement of (b). Clearly, K^* is a $\sigma_0(M)$-subgroup of M^*. Let H be a Hall $\sigma_0(M)$-subgroup of M^* that contains K^*. The subgroup H is a $\sigma_0(M)$-subgroup such that $H \cap K^* \neq 1$. By Proposition 8.2 (f), we have $H \subseteq M_{\sigma_0}$. Hence, $[H, K] \subseteq [M_{\sigma_0}, K] \subseteq M_{\sigma_0}$. On the other hand, $H \subseteq M^*$ and $K = K_1^* \subseteq (M^*)_\sigma$. It follows that

$$[H, K] \subseteq [M^*, (M^*)_\sigma] \subseteq (M^*)_\sigma,$$

and $[H, K] \subseteq M_{\sigma_0} \cap (M^*)_\sigma$. But, M is not conjugate to M^*, so by Theorem 7.9, $[H, K] = 1$. Therefore, $H \subseteq C_{M_\sigma}(K) = K^*$. This proves $H = K^*$. Thus, (b) holds.

To prove (c) and (h), let U be the subgroup defined in Proposition 8.2 (a). Since K acts regularly on U, we have $U = [U, K] \subseteq M'$. Since $M_{\sigma_0} \subseteq M'$, $M_{\sigma_0}U \subseteq M'$. On the other hand, $M_{\sigma_0}U$ is a normal subgroup of M with $M/M_{\sigma_0} \cong K$. Since K is cyclic by the first part of (d) which we have proved, $M_{\sigma_0}U$ contains M'. Therefore, we have $M_{\sigma_0}U = M'$ and K is a complement of M' in M. This proves (h).

Moreover, K is a cyclic Hall subgroup of M such that $\pi(K) \cap \pi(M') = \emptyset$. By defintion, we have

$$\kappa(K) = \pi(K) = \tau_1(M).$$

Since $K = K_1^*$ and $K^* = K_1$, we have $K = C_{M-\sigma^*}(K^*)$. This proves (c).

It remains to prove the second part of (d). By (b), K^* is a Hall $\sigma_0(M)$-subgroup of M^*. Therefore, $K^* = M_{\sigma_0} \cap M^*$. It follows that

$K^* = M_{\sigma_0} \cap M^* \lhd M \cap M^*$ and, by Proposition 8.2 (b1),

$$M \cap M^* \subseteq N_{M^*}(K^*) = K \times K^*.$$

Since $K \times K^* \subseteq M \cap M^*$, we have $M \cap M^* = K \times K^* = Z$.

If $x \in K^\sharp$ and $y \in K^{*\sharp}$, (a) yields $C_G(x) \subseteq M^*$ so $C_M(x) \subseteq M \cap M^* = Z$. Since Z is cyclic by the first part of (d), we have

$$C_M(x) = Z.$$

Similarly, $C_{M^*}(y) = Z$. Moreover, $C_G(xy) = C_G(x) \cap C_G(y) \subseteq M \cap M^*$. This implies $C_G(xy) = Z$ and completes the proof of (d). Q.E.D.

Remark. From now on, we reserve the notation M^* or K^* to denote the subgroups given in Theorem 8.7 for the subgroup M in $\mathcal{M}_{\mathcal{P}}$.

Corollary 8.8. *The subgroups in $\mathcal{M}_{\mathcal{P}_1}$, if any, are all conjugate in G and, if $\mathcal{M}_{\mathcal{P}}$ is not empty, then $\mathcal{M}_{\mathcal{P}}$ contains exactly two conjugacy classes of subgroups.*

Corollary 8.9. *Choose a system of representatives $M_1, M_2, \ldots, M_n \in \mathcal{M}$ from each conjugacy class of subgroups of $\mathcal{M}$.*

(a) *If $\mathcal{M}_{\mathcal{P}}$ is empty, then the set of ϖ-elements of $G^\sharp$ is the disjoint union of the sets $\mathcal{C}_G(\widetilde{M_i})$ for $i = 1, 2, \ldots, n$.*

(b) *If $\mathcal{M}_{\mathcal{P}}$ is not empty, the set of ϖ-elements of $G^\sharp$ is the disjoint union of $\mathcal{C}_G(\widehat{Z})$ and the sets $\mathcal{C}_G(\widetilde{M_i})$ for $i = 1, 2, \ldots, n$ with $\widehat{Z}$ as in Theorem 8.7.*

Corollary 8.10. *For every ϖ-element $g \in G$ we have $\ell_\sigma(g) \leq 2$.*

Lemma 8.11. *Suppose that $M \in \mathcal{M}_{\mathcal{F}}$, E is a complement of M_σ in M, $q \in \pi(E)$, and $Q \in \mathcal{E}_q^1(E)$. Assume that $Q \not\subseteq F(E)$. Then, M is a ϖ-group with $\tau_2(M) \neq \emptyset$. Take $p \in \tau_2(M)$, $A \in \mathcal{E}_p^2(E)$ and $H \in \mathcal{M}(N_G(A))$. Then, $A_0 = [E, Q] = C_A(M_\sigma) \in \mathcal{E}_p^1(A)$and $E = A_0 C_E(Q)$. Moreover, either*

(1) *$q \in \tau_2(H)$ and $\mathcal{M}(C_G(Q)) = \{H\}$, or*

(2) *$q \in \kappa(H)$ and $H \in \mathcal{M}_{\mathcal{P}_1}$.*

Proof. Suppose $\tau_2(M) = \emptyset$. Then, M is a Frobenius group and E is a Frobenius complement. From the structure of Frobenius complement, we get $Q \subseteq F(E)$. This contradicts the assumption $Q \not\subseteq F(E)$. Therefore, $\tau_2(M) \neq \emptyset$ and, by Lemma H, M is a ϖ-group.

Let $p \in \tau_2(M)$ and take $A \in \mathcal{E}_p^2(E)$. By Corollary 6.6 (a), we have $A \lhd E$ and $\mathcal{E}_p^1(E) = \mathcal{E}_p^1(A)$. Since $Q \nsubseteq F(E)$, we have $q \notin \tau_2(M)$. By Lemma 6.1, E_3 is a cyclic normal Hall $\tau_3(M)$-subgroup of E. Thus, $q \notin \tau_3(M)$. Therefore, we have $q \in \tau_1(M)$.

Let S be a Sylow p-subgroup of G that contains A. Suppose that S is abelian. Since $q \in \tau_1(M)$ and M is a Frobenius group, we can apply Lemma 6.8 (e) to conclude that Q lies in $Z(E) \subseteq F(E)$. This contradiction proves that S is nonabalian.

By Theorem 6.7 (b), $A_0 = C_A(M_\sigma)$ has order p and satisfies $F(M) = M_\sigma \times A_0$. Let $K = [E, Q]$. Then, $K \subseteq E'$ and E' is abelian by Corollary 6.10 (b). It follows that K is an abelian q'-group. Therefore, because $KQ \lhd E$, the Frattini argument yields $E = KN_E(Q)$. Since $[Q, N_E(Q)]$ is a q'-subgroup of Q, we have $N_E(Q) = C_E(Q)$ and $E = KC_E(Q)$. This implies $K = [E, Q] = [K, Q]$. Now, Proposition 4.11 (d) with q and Q in place of p and P yields that $[K, Q] = K$ is a cyclic normal subgroup of M that centralizes M_σ¿ It follows that $K \subseteq F(M) \cap E = A_0$. We have $K \neq 1$ because $Q \nsubseteq Z(E)$. Therefore, we have $K = A_0$.

Take $H \in \mathcal{M}(N_G(A))$. Since $A = [A, Q] \times C_A(Q)$ and $[A, Q] = A_0$, we have $C_A(Q) \in \mathcal{E}^1(A)$. Lemma 6.11 yields that $p \in \sigma_0(H) \setminus \beta(H)$ and $q \in \tau_1(H) \cup \tau_2(H)$. Recall that $p \in \tau_2(M)$ and $p \in \varpi$.

Suppose $q \in \tau_2(H)$. Since $C_A(Q) \neq 1$ and $A \subseteq H_{\sigma_0}$, Corollary 6.10 (e) for H and Q in place of M and $\langle x \rangle$ yields $\mathcal{M}(C_G(Q)) = \{H\}$. This is the case (1).

If $q \in \tau_1(H)$, $C_A(Q) \neq 1$ and $A \subseteq H_{\sigma_0}$ imply $q \in \kappa(H)$. Since $q \in \sigma_0(H)$, we have $\sigma_0(H) \neq \beta(H)$. Proposition 8.2 (g) for H yields that $H \in \mathcal{M}_{\mathcal{P}_1}$. Thus, we have the case (2). Q.E.D.

Corollary 8.12. *Suppose $M \in \mathcal{M}_{\mathcal{P}_2}$. Let K, M^*, and K^* be as in Theorem 8.7 and U as in Proposition 8.2 (a). Suppose $r \in \pi(U)$ and $R \in Syl_r(U)$.*

(a) *If M is not a ϖ-group, there is no $H \in \mathcal{M}(N_G(R))$ and $H \neq M$.*
(b) *If M is a ϖ-group, $\mathcal{M}(N_G(R))$ is not empty. For any $H \in \mathcal{M}(N_G(R))$, H is a ϖ-group in $\mathcal{M}_{\mathcal{F}}$ such that $U \subseteq H_\sigma$, $M \cap H = UK$, $N_H(U) \nsubseteq M$, $K \subseteq F(H \cap M^*)$, and $H \cap M^*$ is a complement of H_σ in H.*

Proof. Suppose that $N \in \mathcal{M}_{\mathcal{P}_2}$. Then, $U \neq 1$ and there exists $r \in \pi(U)$. Let $H \in \mathcal{M}(N_G(R))$ and $H \neq M$. We will prove that H is not conjugate to M or M^*.

Suppose that $H = M^g$ for some $g \in G$. Then, $R \in Syl_r(H)$. Since $N_G(R) \subseteq H$, we have $r \in \sigma(H)$. Since $C_G(R) \subseteq N_G(R) \subseteq H$, Theorem

4.1 (e) with R and H in place of X and M yields $H = M^g = M$. Thus, H is not conjugate to M in G.

Suppose $H = (M^*)^g$ for some $g \in G$. Then, $K \subseteq (M^*)^g = H$. Proposition 8.2 (d) with M and K^* replaced by M^* and K (cf. Theorem 8.7 (b) and (c)) yields $g \in M^*$. Thus, $H = (M^*)^g = M^*$. The nonabelian group KU is contained in $M \cap H$. However, $H = M^*$ so $M \cap H = M \cap M^*$ that is cyclic by Theorem 8.7 (d). Hence, H is not conjugate to M^* either.

To prove (a), suppose that there is a subgroup $H \neq M$ such that

$$H \in \mathcal{M}(N_G(R)).$$

Then, H is not conjugate to M or M^*. By Theorem 8.7 (g), we have $H \in \mathcal{M}_{\mathcal{F}}$. By assumption, M is not a ϖ-group. Hence, by Lemma G, U is a ϖ'-group. It follows that H is not a ϖ-group. Lemma G yields that H is a Frobenius group with Frobenius kernel that is a ϖ-group. In particular, H is ϖ-closed. However, $UK \subseteq H$ and the subgroup UK is not ϖ-closed. This contradiction proves (a).

To prove (b), take $H \in \mathcal{M}(N_G(R))$. Since M is a ϖ-group, we have $r \notin \sigma(M)$ so $N_G(R) \nsubseteq M$. It follows that $H \neq M$. The first part of the proof shows that H is not conjugate to M or M^*. By Theorem 8.7 (g), we have $H \in \mathcal{M}_{\mathcal{F}}$.

Since $M \in \mathcal{M}_{\mathcal{P}_2}$, we have $U \neq 1$. Proposition 8.2 (g) implies that K has prime order, say q. Note that $q \in \varpi$ because M is a ϖ-group. We will prove that H is a ϖ-group. If H is not a ϖ-group, Lemma G implies that H is a Frobenius group and the Frobenius kernel of H is a Hall ϖ-subgroup. Since UK is a ϖ-subgroup of H, UK is contained in the Frobenius kernel of H. Since UK is not nilpotent, we have a contradiction. Thus, H is a ϖ-group.

Since H is not conjugate to M^*, Theorem 7.9 implies that $\sigma(M^*)$ is disjoint from $\sigma(H)$. By Theorem 8.7 (c), we have $q = |K| \in \sigma(M^*)$. Hence, $q \notin \sigma(H)$. It follows that K lies in some complement D of H_σ in H. We will prove that $K \subseteq F(D)$.

Suppose $K \nsubseteq F(D)$. By Lemma 8.11 with (H, D, K) in place of (M, E, Q), there is a subgroup $L \in \mathcal{M}$ such that either $q \in \tau_2(L)$ and $\mathcal{M}(C_G(K)) = \{L\}$, or $q \in \kappa(L)$ and $L \in \mathcal{M}_{\mathcal{P}_1}$. If $L \in \mathcal{M}_{\mathcal{P}_1}$, then L must be conjugate to M or M^* by Theorem 8.7 (g). Note that L is not conjugate to M^* because $q \in \sigma(M^*)$. Hence, L is conjugate to M. This contradicts the assumption that $M \in \mathcal{M}_{\mathcal{P}_2}$. Therefore, we have $\mathcal{M}(C_G(K)) = \{L\}$. However, Theorem 8.7 (a) yields $C_G(K) \subseteq M^*$. This is a contradiction as $M^* \neq L$. Thus, we have $K \subseteq F(D)$.

It follows that K is subnormal in D. We claim that this implies $D \subseteq M^*$. We will prove that if $K \subseteq L \subseteq M^*$, then $N_G(L) \subseteq M^*$. If

$g \in N_G(L)$, then $K \subseteq L = L^g \subseteq (M^*)^g$. Then, Proposition 8.2 (d) with (M, K^*) replaced by (M^*, K) yields $g \in M^*$. By obvious induction, if K is subnormal in D, then $D \subseteq M^*$.

The subgroup U is a q'-group satisfying $U = [U, K]$. Since

$$K \subseteq O_q(D)H_\sigma \lhd H,$$

we get

$$U = [U, K] \subseteq U \cap O_q(D)H_\sigma \subseteq H_\sigma.$$

We will prove next $M \cap H = UK$. Clearly, $UK \subseteq M \cap H$. Since UK is a complement of M_σ in M, we have $M \cap H = XUK$ where $X = M_\sigma \cap H \lhd M \cap H$. Then, since $U \subseteq H_\sigma$,

$$[X, U] \subseteq M_\sigma \cap H_\sigma = 1$$

because M is not conjugate to H (by Theorem 7.9). On the other hand, Lemma 8.1 with M and $p \in \pi(U)$ yields that $C_{M_\sigma}(U) = 1$. Thus, $X = 1$ and we have $M \cap H = UK$.

By Lemma 8.1 with H and q in place of M and p yields that H_σ is nilpotent. Since $M \cap H = UK$ and $U \subseteq H_\sigma$, we have $M \cap H_\sigma = U$. Thus, if U is a proper subgroup of H_σ, then $N_H(U) \not\subseteq M$ by a fundamental property of nilpotent groups. On the other hand, if $U = H_\sigma$, $N_H(U) = H$ and certainly $N_H(U) \not\subseteq M$.

It remains to show that $D = H \cap M^*$. We have seen that $D \subseteq H \cap M^*$. Suppose that $H \cap M^* \neq D$. Then, $H_\sigma \cap M^* \neq 1$. Since $K \subseteq (M^*)_\sigma$,

$$[H_\sigma \cap M^*, K] \subseteq H_\sigma \cap (M^*)_\sigma = 1.$$

It follows from the definition of the set $\mathcal{M}_\mathcal{F}$ that $H \in \mathcal{M}_\mathcal{F}$ implies $q \in \tau_2(H)$. Then, Theorem 6.5 (e) for H yields $H_\sigma \cap M^* = 1$ contradicting the earlier inequality. This proves $D = H \cap M^*$. Q.E.D.

Lemma 8.13. *Assume that x is a ϖ-element such that $|\mathcal{M}_\sigma(x)| > 1$. Let $N = N(x)$ be as in Theorem 8.4 and $M \in \mathcal{M}_\sigma(x)$.*

(a) *If $\sigma(N) \cap \pi(M) \neq \emptyset$, then $M \in \mathcal{M}_\mathcal{F}$ and $\tau_2(M) = \emptyset$. In this case, M is a Frobenius group with Frobenius kernel M_{σ_0}.*

(b) *If $y \in (M_{\sigma_0})^\sharp$ and $C_G(y) \not\subseteq M$, then $|\mathcal{M}_\sigma(y)| > 1$ and $N(y)$ is defined. If $N(y)^g = N$ for some $g \in G$, then $N(y)^m = N$ for some $m \in M$.*

Proof. (a) By Theorem 8.4 (f), N is a ϖ-group in $\mathcal{M}_\mathcal{F} \cup \mathcal{M}_{\mathcal{P}_2}$. Take $q \in \sigma(N) \cap \pi(M)$, $Q \in \mathcal{E}_q^1(M)$, and $H \in \mathcal{M}(N_G(Q))$. Since $\sigma(M)$

is disjoint from $\sigma(N)$, $q \notin \sigma(M)$ so Q lies in some complement E of M_σ in M. By Theorem 8.4 (d),

$$q \in \sigma(N) \cap \pi(M) \subseteq \beta(N) \subseteq \beta(G).$$

Therefore, N contains a Sylow q-subgroup of G. By Sylow's Theorem, $Q \subseteq N^g$ for some $g \in G$. Corollary 6.14 with N^g, q, and Q in place of M, p, and X yields $\mathcal{M}(C_G(Q)) = \{N^g\}$. Note that $q \in \beta(N^g)$. It follows that $H = N^g$. By Lemma 6.1 (g) and Theorem 8.4 (c),

$$\pi(\langle x \rangle) \subseteq \tau_2(N) \subseteq \sigma_0(M) \setminus \beta(M).$$

In particular, $\sigma_0(M) \neq \beta(M)$. Hence, Proposition 8.2 (g) yields $M \notin \mathcal{M}_{\mathcal{P}_2}$. Suppose that $M \in \mathcal{M}_{\mathcal{P}_1}$. Then, $\pi(M) = \sigma(M) \cup \kappa(M)$. Since $q \notin \sigma(M)$, we have $q \in \kappa(M)$. There is a subgroup $M^* \in \mathcal{M}$ with properties stated in Theorem 8.7. We may take a Hall $\kappa(M)$-subgroup of M that contains Q. Define $Q^* = C_{M_\sigma}(Q)$. Then, $Q^* \subseteq M_{\sigma_0}$ and by Proposition 8.2 (b1) and Theorem 8.7 (b), Q^* is a Hall $\sigma_0(M)$-subgroup and a Hall $\kappa(M^*)$-subgroup of M^*. It follows that $M_{\sigma_0} \cap M^* = Q^*$and $\sigma_0(M) \cap \pi(M^*) = \kappa(M^*)$. On the other hand, Theorem 8.7 (a) yields

$$\mathcal{M}(C_G(Q)) = \{M^*\}.$$

Therefore, $M^* = N^g$ and $\pi(M^*) = \pi(N)$. Since $x \in M_{\sigma_0} \cap N$,

$$\pi(\langle x \rangle) \subseteq \sigma_0(M) \cap \pi(N).$$

By Theorem 8.4 (c), $\pi(\langle x \rangle) \subseteq \tau_2(N) \not\subseteq \kappa(N)$. Since $M^* = N^g$, we have $\kappa(N) = \kappa(M^*)$ and $\sigma_0(M) \cap \pi(N) \not\subseteq \kappa(M^*)$. This contradiction proves that $M \notin \mathcal{M}_{\mathcal{P}}$. Thus, $M \in \mathcal{M}_{\mathcal{T}}$.

Suppose that $\tau_2(M)$ is not empty. Take any $p \in \tau_2(M)$. By Lemma 6.1 (g), $p \notin \beta(G)$. Theorem 8.4 yields

$$\pi(M) \cap \sigma(N) \subseteq \beta(N) \quad \text{and} \quad \tau_2(N) \subseteq \sigma_0(M).$$

Therefore, $p \notin \sigma(N) \cup \tau_2(N)$. It follows that $r_p(N) \leq 1$. The rest of proof is as in [BG]. Q.E.D.

§9. The Subgroup M_F

Let $M \in \mathcal{M}$. We will choose a Hall $\kappa(M)$-subgroup K and a complement U of KM_{σ_0} in M that is K-invariant. If $M \in \mathcal{M}_{\mathcal{P}}$, the subgroup U is defined in Proposition 8.2 (a). If $M \in \mathcal{M}_{\mathcal{T}}$, $k = 1$ and U can be any complement of M_{σ_0} in M. We will choose one and fix it throughout the discussion. In addition, M_F denotes the largest normal nilpotent Hall subgroup of M. The notation is fixed in the rest of this paper. The subgroup UK is a complement of M_{σ_0} in M.

Lemma 9.1. *The following conditions hold.*

(a) $UM_{\sigma_0} \lhd M = KUM_{\sigma_0}$, *$K$ is cyclic,* $M_{\sigma_0} \subseteq M'$, *and* M'/M_{σ_0} *is abelian.*

(b) *If* $K \neq 1$, *then* $M' = UM_{\sigma_0}$ *and U is abelian.*

(c) *If X is a nonidentity subgroup of U such that* $C_{M_{\sigma_0}}(X) \neq 1$, *then*

$$\mathcal{M}(C_G(X)) = \{M\}$$

and X is a cyclic $\tau_2(M)$*-subgroup.*

(d) *The group* $\langle C_U(x) \mid x \in (M_{\sigma_0})^\sharp \rangle$ *is abelian.*

(e) *If* $U \neq 1$, *then U contains a subgroup U_0 of the same exponent as U such that* $U_0M_{\sigma_0}$ *is a Frobenius group with Frobenius kernel* M_{σ_0}.

Proof. Since U is K-invariant, $UM_{\sigma_0} \lhd M$. If $K \neq 1$, Theorem 8.7 (d) implies that K is cyclic. By Theorem 4.2 (c),

$$M_\alpha \subseteq M_{\sigma_0} \subseteq M_\sigma \subseteq M'.$$

Part (d) of the same theorem implies that M'/M_{σ_0} is nilpotent. By the definition of the sets $\tau_i(M)$, Theorem 6.5 (b), and Lemma F, the group M'/M_{σ_0} has abelian Sylow subgroups. Therefore, M'/M_{σ_0} is abelian. This proves (a).

If $K \neq 1$, we have $U = [U,K] \subseteq M'$. Then, $M' = UM_{\sigma_0}$ and $U \cong M'/M_{\sigma_0}$. Hence, U is abelian and we have (b).

To prove (c), take nonidentity elements x' and x such that

$$x' \in X \text{ and } x \in C_{M_{\sigma_0}}(X)^\sharp.$$

Since $x' \in U^\sharp$, $\pi(\langle x' \rangle) \nsubseteq \kappa(M)$. By Corollary 8.3, we have $\pi(\langle x' \rangle) \subseteq \tau_2(M)$ and $\mathcal{M}(C_G(x')) = \{M\}$. It follows that X is an abelian $\tau_2(M)$-subgroup. If $r_p(X) > 1$ for some prime p, take $A \in \mathcal{E}_p^2(X)$. Theorem 6.5 (d) yields $C_{M_\sigma}(A) = 1$. Then,

$$C_{M_{\sigma_0}}(X) \subseteq C_{M_\sigma}(A) = 1$$

contrary to the hypothesis. Therefore, $r_p(X) \leq 1$ for all primes and X is cyclic. Taking the element x' to be a generator of X, we have $\mathcal{M}(C_G(X)) = \{M\}$.

If $K \neq 1$, U is abelian by (b). In this case, (d) is trivial. Suppose that $K = 1$. In this case, U is a complement of M_{σ_0}. Let $V = U \cap M_\sigma$. Then, V is a complement of M_{σ_0} in M_σ, and V is a Hall $\sigma(M)$-subgroup of U such that $V \lhd U$. There is a complement E of V in U. It follows that E is a complement of M_σ in M.

If $\sigma_0(M) = \sigma(M)$, we have $U = E$ and Theorem 6.12 yields (d) and (e). If $\sigma_0(M) \neq \sigma(M)$, V is a nontrivial ϖ'-group that acts regularly on M_{σ_0}. By Lemma H, $\tau_2(M) = \emptyset$. Since $K = 1$, the group E acts regularly on M_{σ_0}. It follows that $U = EV$ acts regularly on M_{σ_0}. Thus, $U = U_0$ satisfies (e), while the subgroup defined in (d) is 1.

It remains to prove (e) in the case $K \neq 1$. If M is not a ϖ-group, U is a ϖ'-group by Lemma G. It follows that $U_0 = U$ satisfies (e). Suppose that M is a ϖ-group. Then, $M_{\sigma_0} = M_\sigma$ and $\kappa(M) = \tau_1(M)$ by Theorem 8.7 (c). We may assume that $U = E_2E_3$.

Since $\kappa(M) = \tau_1(M)$, E_3 acts regularly on M_σ. The group E_2 is an abelian group of rank 2. We use the same argument as that of the proof of Theorem 6.12. Take $p \in \tau_2(M)$ and $S \in Syl_p(E_2)$. If G has nonabelian Sylow p-subgroups, then Theorem 6.7 provides a subgroup S_0 of the same exponent as S that acts regularly on M_σ. Furthermore, we have $E_2 = S$ (by Theorem 6.7 (a)). So, $U_0 = S_0E_3$ satisfies the condition (e). We can assume that S is a Sylow p-subgroup of G for every $p \in \tau_2(M)$. We write $S = Y \times Z$ for some cyclic subgroups with $|Y| \leq |Z|$. If $|Y| < |Z|$, then $C_{M_\sigma}(\Omega_1(Z)) = 1$ (cf. the proof of Theorem 6.12). If $|Y| = |Z|$, we can choose Z to satisfy the same condition. Then, the product U_0 of all those cyclic factors and E_3 satisfies the condition (e). Q.E.D.

Theorem 9.2. *For every $M \in \mathcal{M}$, we have*

$$1 \neq M_F \subseteq M_{\sigma_0} \subseteq M_\sigma \subseteq M'.$$

Suppose $M_F \neq M_{\sigma_0}$, and let $p = |K|$, $K^* = C_{M_\sigma}(K)$, and $q = |K^*|$. Then,

(a) *$M \in \mathcal{M}_{\mathcal{P}_1}$ and $M_\sigma = M'$,*
(b) *p and q are primes and $q \in \pi(M_F) \cap \beta(M)$,*
(c) *M has a normal Sylow q-subgroup Q, so $K^* \subseteq Q$,*
(d) *a complement D of Q in M' is nilpotent,*
(e) *$Q_0 = C_Q(D) \lhd M$,*
(f) *$\overline{Q} = Q/Q_0$ is a minimal normal subgroup of M/Q_0 and is elementary abelian of order q^p, and*
(g) *$M'' = (M_\sigma)' \subseteq F(M) = QC_M(Q) = C_M(\overline{Q}) = C_{M_\sigma}(\overline{K^*}) \subseteq M_\sigma$.*

Proof. This theorem has assumptions slightly different from those of Theorem 15.2 [BG]. However, the proof is almost identical. Since M

is a ϖ-local subgroup, $O_{\varpi}(M) \neq 1$. Therefore, the Fitting subgroup $F(M)$ of M is a ϖ-group. It follows that $M_F \subseteq M_{\sigma_0}$. Since $M_{\sigma_0} \neq 1$ by Theorem 4.2 (e), we have $M_F \neq 1$ if $M_F = M_{\sigma_0}$. Therefore, we may assume $M_F \neq M_{\sigma_0}$. Lemma 8.1 yields that $M \in \mathcal{M}_{\mathcal{P}_1}$, i.e. $K \neq 1$ and $M = KM_{\sigma}$. Then, $M/M_{\sigma} \cong K$. Since K is cyclic by Theorem 8.7 (d), we have $M' \subseteq M_{\sigma}$. Therefore, $M_{\sigma} = M'$ and (a) is proved.

We can continue the proof along the line adapted from the proof of Theorem 15.2 [BG]. Q.E.D.

Corollary 9.3. *Suppose H is a Hall subgroup of M_{σ} such that $\pi(H) \cap \varpi \neq \emptyset$. Then,*

(a) *$C_M(H) = C_{M_{\sigma_0}}(H)X$ with X a cyclic $\tau_2(M)$-subgroup, and*

(b) *if H is a ϖ-group, any two elements of H conjugate in G are already conjugate in $N_M(H)$.*

Proof. Since H contains a nontdentity ϖ-subgroup, $C_M(H)$ is a ϖ-group by Lemma A. If $x \neq 1$ is a $\kappa(M)$-element, $C_{M_{\sigma}}(x)$ is conjugate to K^* and does not contain any Hall subgroup of M_{σ} by Proposition 8.2 (d). It follows that $C_M(H) = C_{M_{\sigma_0}}(H)X$ where X is a $(\sigma_0(M) \cup \kappa(M))'$-subgroup . By Lemma 9.1, X is conjugate to a subgroup of U and, since $C_{M_{\sigma_0}}(X) \neq 1$, X is a cyclic $\tau_2(M)$-subgroup.

Suppose that $x, y \in H$, $g \in G$, and $x = y^g$. Then, $x \in M \cap M^g$ and $M = M^{gc}$ for some element $c \in C_G(x)$ by Theorem 8.4. Then $m = gc \in M$ by Lemma E (2) and $x = y^m$. This proves (b) in the case $H \lhd M$.

Suppose the H is not normal in M. Then $M_F \neq M_{\sigma_0}$ and we can use Theorem 9.2 as in the proof of Corollary 15.3 [BG] to finish the proof. Q.E.D.

Corollary 9.4. *Suppose that H is a nonidentity nilpotent Hall subgroup of G. If H is a ϖ-group, then there is a subgroup $M \in \mathcal{M}$ such that $H \subseteq M_{\sigma_0}$.*

Proof. Let S be a nonidentity Sylow subgroup of H and let $M \in \mathcal{M}(N_G(S))$. Then, we have $S \subseteq M_{\sigma_0}$. By Corollary 9.3 (a), $C_M(S) = C_{M_{\sigma_0}}X$ where X is a cyclic $\tau_2(M)$-subgroup of M. If $p \in \tau_2(M)$, Sylow p-subgroups of M are not cyclic. Hence, X contains no Sylow subgroup of G. A nilpotent Hall subgroup H is written $H = S \times L$ where L is a product of Sylow subgroups of G. Since $H \subseteq N_G(S) \subseteq M$, we have $L \subseteq C_M(S)$. It follows that $L \subseteq C_{M_{\sigma_0}}(S)$ because X is a $\sigma_0(M)'$-subgroup that contains no Sylow subgroup of G. This proves that $H = S \times L \subseteq M_{\sigma_0}$. Q.E.D.

Corollary 9.5. *Let $H = M_F$ and $Y = O_{\sigma_0(M)'}(F(M))$. Then,*

(a) *Y is a cyclic $\tau_2(M)$-subgroup of $F(M)$,*
(b) *$M'' \subseteq F(M) = C_M(H)H = F(M_{\sigma_0}) \times Y = F(M_\sigma) \times Y$,*
(c) *$H \subseteq M'$ and M'/H is nilpotent, and*
(d) *if $K \neq 1$, then $F(M) \subseteq M'$.*

Proof. (a) We have $H \subseteq F(M) \subseteq HC_M(H)$. By Corollary 9.3 (a), a Hall $\sigma_0(M)'$-subgroup of $C_M(H)$ is a cyclic $\tau_2(M)$-subgroup. This implies (a).

(b) Clearly, we have $F(M) = F(M_{\sigma_0}) \times Y = F(M_\sigma) \times Y$. Suppose $H = M_{\sigma_0}$. Then, $M'' \subseteq M_{\sigma_0}$ by Lemma 9.1 (a). Thus,

$$M'' \subseteq F(M) = H \times Y \subseteq HC_M(H) = M_{\sigma_0} \times X \lhd M$$

where X is a cyclic $\tau_2(M)$-group by Corollary 9.3 (a). Since $H = M_{\sigma_0}$, $M_{\sigma_0} \times X$ is a nilpotent normal subgroup of M. Hence, $M_{\sigma_0} \times X \subseteq F(M)$. Thus, $HC_M(H) = F(M)$ in this case. Suppose $H \neq M_{\sigma_0}$. By Theorem 9.2, M has a normal Sylow q-subgroup Q such that $Q \subseteq H$ and

$$M'' \subseteq F(M) = F(M_{\sigma_0}) \times Y \subseteq HC_M(H) \subseteq HC_M(Q) \subseteq QC_M(Q) = F(M).$$

Theorem 9.2 (g) yields the first containment and the last equality.

(c) If $H = M_{\sigma_0}$, Theorem 4.2 (c) and (d) yield the conclusions. If $H \neq M_{\sigma_0}$, Theorem 9.2 yields that $M' = M_\sigma$ contains H and M'/H is nilpotent (Part (d)).

(d) If $K \neq 1$, M' is a complement of K in M by Theorem 8.7 (h). Thus, M/M' is a $\kappa(M)$-group. By (c), we have $H \subseteq M_\sigma \subseteq M'$. By Corollary 9.3, $C_M(H) \subseteq M_\sigma X$ where X is a $\tau_2(M)$-group. It follows that $F(M) = HC_M(H) \subseteq M'$. Q.E.D.

Corollary 9.6. *Suppose $M \in \mathcal{M}_{\mathcal{P}}$. Then, $K^* = C_{M_\sigma}(K)$ is a nonidentity cyclic subgroup of M_F and M''. Furthermore, M_F is not cyclic.*

Proof. By definition, K is a ϖ-group. Therefore, $K^* \subseteq M_{\sigma_0}$. If $M_F = M_{\sigma_0}$, certainly $K^* \subseteq M_F$. If $M_F \neq M_{\sigma_0}$, Theorem 9.2 yields that $K^* \subseteq Q$ for some $Q \subseteq Sy\ell_q(M)$. Since $Q \lhd M$, we have $Q \subseteq M_F$. Thus, $K^* \subseteq M_F$ in all cases.

Since $M \in \mathcal{M}_{\mathcal{P}}$, we have $K \neq 1$. Theorem 8.7 (h) yields that M' is a complement of K. Thus, M' is a normal Hall $\kappa(M)'$-subgroup of M. By Lemma 6.3 [BG], $K^* \subseteq C_{M'}(K) \subseteq M''$.

By Proposition 8.2 (c) and Theorem 8.7 (d), $K^* \neq 1$ and K^* is cyclic. Finally, we will prove that M_F is not cyclic. If M_F is cyclic, Theorem 9.2 yields that $M_{\sigma_0} = M_F$ because Q in Theorem 9.2 is noncyclic (by (f)). Then, $F(M) = M_F \times Y$ is cyclic by Corollary 9.5 (a) and (b). This implies $M'' = 1$ which contradicts $K^* \subseteq M''$. Hence, M_F is not cyclic. Q.E.D.

Theorem 9.7. *Suppose that $F(M)$ is not a TI-subset of G. Let $H = M_F$ and define*

$$X = F(M) \cap F(M)^g \neq 1 \quad \textit{for some} \quad g \in G \setminus M.$$

Let E, E_1, E_2 and E_3 be as in Section 6. Then,

(a) *$M \in \mathcal{M}_{\mathcal{F}} \cup \mathcal{M}_{\mathcal{P}_1}$ and $H = M_{\sigma_0}$;*
(b) *$X \subseteq H$, X is cyclic, and H is a $\beta(M)'$-group;*
(c) *$M' \subseteq F(M) = M_{\sigma_0} times Y$ where Y is as in Corollary 9.5;*
(d) *$E_3 = 1$, $E_2 \lhd E = E_1E_2$, and E_1 is cyclic; and*
(e) *one of the following conditions holds:*
  (1) *$M \in \mathcal{M}_{\mathcal{F}}$ and H is abelian of rank 2,*
  (2) *$|X| = p$ is a prime in $\sigma_0(M) \setminus \beta(M)$, $O_p(H)$ is not abelian, $O_{p'}(H)$ is cyclic, and the exponent of M/H divides $q-1$ for every $q \in \pi(H)$, or*
  (3) *$|X| = p$ is a prime in $\sigma_0(M) \setminus \beta(M)$, $O_{p'}(H)$ is cyclic, $O_p(H)$ has order p^3 and exponent p and is not abelian, $M \in \mathcal{M}_{\mathcal{P}_1}$, and $|M/H|$ divides $p+1$.*

Proof. We remark first that $F(M)$ is a ϖ-group so any prime in $\pi(X)$ lies in ϖ. Take $p \in \pi(X)$ and $X_1 \in \mathcal{E}_p^1(X)$. We will show that $O_p(M)$ is not cyclic. If $O_p(M)$ were cyclic, X_1 would be the unique subgroup of order p in $F(M)$ as well as in $F(M)^g$. This would imply $M = N_G(X_1) = M^g$ so $g \in M$. Thus, $O_p(M)$ is not cyclic. Corollary 9.5 (a) yields that $p \in \sigma_0(M)$. Since p is arbitrary in $\pi(X)$, we have $\pi(X) \subseteq \sigma_0(M)$. Hence, $X \subseteq M_{\sigma_0} \cap M^g$. By Lemma 6.17, X is a cyclic $\beta(M)'$-subgroup. In particular, $\sigma_0(M) \neq \beta(M)$ and by Proposition 8.2 (g), we have $M \notin \mathcal{M}_{\mathcal{P}_2}$. Thus, the first part of (a) is proved.

Since $X_1 \subseteq M \cap M^g$, Theorem 4.1 yields $C_G(X_1) \not\subseteq M$. This implies that $C_H(X_1) \notin \mathcal{U}$ where $H = M_F$. Since $\langle H, X_1 \rangle \subseteq F(M)$, $O_{p'}(H)$ centralizes X_1. Theorem 6.13 and the Uniqueness Theorem yield that every Sylow subgroup of $O_{p'}(H)$, and hence $O_{p'}(H)$ itself, is abelian of rank ≤ 2. Let $P = O_p(H)$. Then, $X_1 \subseteq P$ and $C_P(X_1)$ is abelian of rank ≤ 2. Therefore, H is a $\beta(M)'$-group. If $H \neq M_{\sigma_0}$, Theorem 9.2 (b) and (c) yield that a Sylow q-subgroup Q is normal in M and $q \in \pi(M_F) \cap \beta(M)$. This contradiction proves that $H = M_{\sigma_0}$. Thus, (a) holds.

If M is a ϖ-group, certainly $M_\sigma = M_{\sigma_0}$. If M is not a ϖ-group, M is not a group of type (2) in Lemma G because a group of type (2) satisfies $\sigma_0(M) = \beta(M)$. Similarly, if M is a group of type (1) in Lemma G, we have $M' = M_\sigma = M_F$. Thus, we have $M_\sigma = M_{\sigma_0}$ even if M is not s ϖ-group. Since $M_{\sigma_0} = H$, M_σ is a nilpotent $\beta(M)'$-subgroup of M. By Lemma 6.19, the group E' centralizes M_σ. Since E' is nilpotent by Lemma 6.1 (a), we have

$$M' = M_\sigma E' = M_\sigma \times E' \subseteq F(M) = M_{\sigma_0} \times Y$$

where Y is a cyclic $\tau_2(M)$-subgroup (by Corollary 9.5). Hence, E' is a $\tau_2(M)$-group. Since $E_3 \subseteq E'$, we have $E_3 = 1$. This proves (c) and (d).

The last part (e) can be proved by adapting the proof of the corresponding part of Theorem 15.7 [BG]. Q.E.D.

Theorem 9.8. *Suppose that we have the situation of Corollary* 8.12 *and assume that* M *is a* ϖ*-group. Thus,* $M \in \mathcal{M}_{\mathcal{P}_2}$*,* K, M^**, and* K^* *are as in Theorem* 8.7 *and* U *is as in Proposition* 8.2 *(a). Suppose that* $R \in Syl_r(U)$ *for some* $r \in \pi(U)$ *and* $H \in \mathcal{M}(N_G(R))$*. Furthermore, suppose that* $\tau_2(H)$ *is not empty. Then, for* $|K| = q$*,* q *is the unique prime in* $\tau_2(M)$ *and* $\tau_2(M)$ *is empty.*

Proof. By Corollary 8.12, H is a ϖ-group such that

$$U \subseteq H_\sigma, M \cap H = UK, K \subseteq F(H \cap M^*),$$

and $H \cap M^*$ is a complement of H_σ in H. By Theorem 8.2 (g), $q = |K|$ is a prime. Let $D = H \cap M^*$. Then, D is a complement of H_σ in H by Corollary 8.12 (b).

By assumption, $\tau_2(H)$ is not empty so we can choose $A \in \mathcal{E}^2(D)$. Corollary 6.6 (a) yields $A \subseteq F(D)$. Since $K \subseteq F(D)$, $[A, K] = 1$ if A is not a q-group. If A is a q-group, Theorem 6.5 (b) implies that $K \subseteq A$ so $[A, K] = 1$ trivially. If $A \subseteq M^*_\sigma$, then $\pi(A) \subseteq \tau_2(M^*)$. Theorem 6.5 (d) for M^* yields $C_{M^*_\sigma}(A) = 1$. This contradicts $[A, K] = 1$ because $K \subseteq M^*_\sigma$. Hence, we have $A \subseteq M^*_\sigma$.

We claim that $F(M^*)$ contains A as well as a Sylow q-subgroup Q of M^*. If $(M^*)_F = (M^*)_{\sigma_0}$, this is certainly true because $(M^*)_{\sigma_0} \subseteq F(M^*)$. On the other hand, if $(M^*)_F \neq (M^*)_{\sigma_0}$, $F(M^*)$ contains a Sylow q-subgroup Q of M^* by Theorem 9.2 (c). Also, the part (g) of the same theorem quoted above yields that $F(M^*) = C_{M^*_\sigma}(\overline{K})$ which contains A. This proves the claim.

We prove next that $q \notin \beta(G)$. If A is a q-group, Lemma 6.1 (g) implies $q \notin \beta(G)$. If A is not a q-group, then we have $[Q, A] = 1$ because both Q and A are subgroups of a nilpotent group $F(M^*)$. Since $A \notin \mathcal{U}$, we have $Q \notin \mathcal{U}$ by Corollary 3.2 (a). This proves $q \notin \beta(G)$.

Theorem 9.2 (b) yields $(M^*)_F = (M^*)_{\sigma_0}$. Since $\sigma_0(M^*) \neq \beta(M^*)$, $M^* \in \mathcal{M}_{\mathcal{P}_1}$ by Proposition 8.2 (g). Therefore, we have $M^* = (M^*)_{\sigma_0}K^*$. By Lemma 6.17,

$$K = C_{M^*_{\sigma_0}}(K^*) \subseteq (M^*)_{\sigma_0}{}'.$$

Since $(M^*)\sigma_0 = (M^*)_F$ is nilpotent, $K \subseteq Q'$. Hence, Q is nonabelian and, by Theorem 6.13, $Q \in \mathcal{U}$. Since $A \notin \mathcal{U}$, Lemma 3.2 yields that $[Q, A] \neq 1$. Therefore, A is a q-group. Since Q is nonabelian, we have $\tau_2(H) = \{q\}$ by Theorem 6.7 (a).

The remaining statements are proved as in [BG]. Q.E.D.

Corollary 9.9. *Let $x \in M^\sharp_{\sigma_0}$ and $N \in \mathcal{M}(C_G(x))$. Assume that $C_G(x) \nsubseteq M$ and $N \notin \mathcal{M}_{\mathcal{F}}$. Take $r \in \pi(\langle x \rangle)$ and $X \in \mathcal{E}^1_r(\langle x \rangle)$. Then, both M and N are ϖ-groups. Furthermore, for a suitable choice of a complement E of M_σ in M,*

(a) *$M \in \mathcal{M}_{\mathcal{F}}$ and $N \in \mathcal{M}_{\mathcal{P}_2}$,*

(b) *E is cyclic and M is a Frobenius group with Frobenius kernel M_σ, and*

(c) *$r \in \tau_2(N)$, $N_E(X) \subseteq E \cap N$ and $|E \cap N| = |N/N'|$.*

Proof. Take $y \in C_G(x) \setminus M$. Then, $M, M^y \in \mathcal{M}_\sigma(x)$ and $M \neq M^y$. Hence, we are in the situation of Theorem 8.4 with $|\mathcal{M}_\sigma(x)| > 1$. Therefore,

$$C_{N_\sigma}(x) \neq 1, \mathcal{M}(C_G(x)) = \{N\}, r \in \tau_2(N) \cap \sigma_0(M),$$

N is a ϖ-group in $\mathcal{M}_{\mathcal{F}} \cup \mathcal{M}_{\mathcal{P}_2}$, and $M \cap N$ is a complement of N_σ in N. By assumption, we have $N \in \mathcal{M}_{\mathcal{P}_2}$.

Let K_1 be a Hall $\kappa(N)$-subgroup of N. Since $M \cap N$ is a complement of N_σ in N, we can take $K_1 \subseteq M \cap N$. By Proposition 8.2 (g) and (a), $|K_1|$ is a prime and there is an abelian complement U_1 of K_1 in $M \cap N$ for which $C_{U_1}(K_1) = 1$ and $U_1 \lhd M \cap N$.

Let $R \in Syl_r(M \cap N)$. Then, $R \subseteq U_1$ and $R \in Syl_r(N)$. Since

$$r \in \tau_2(N) \subseteq \sigma_0(M),$$

R is not cyclic and, by Corollary 6.10 (d), $N_G(R) \subseteq M$. Corollary 8.12 (b) with N, K_1, U_1, and M in place of M, K, U, and H yields that M is a ϖ-group in $\mathcal{M}_{\mathcal{F}}$ with $M \cap N = U_1K_1$. This proves (a).

By Lemma 8.1, M_{σ_0} is nilpotent. Since $R \subseteq U_1 \subseteq M$ and $r \in \sigma(M)$, we have $R \subseteq M_\sigma$. The group RK_1 is not nilpotent. Therefore, $K_1 \nsubseteq M_\sigma$.

Since $|K_1|$ is a prime, we have $K_1 \cap M_\sigma = 1$. We choose E to satisfy $K_1 \subseteq E$. Theorem 9.8 with N and M in place of M and H implies that if $\tau_2(M)$ is not empty, then $\tau_2(N)$ is empty. However, $\tau_2(N)$ is not empty, so $\tau_2(M)$ must be empty, i.e. $E_2 = 1$ for M. The element x is contained in M_σ and $C_G(x) \nsubseteq M$. Since M_σ is nilpotent, $F(M)$ is not a TI-subset of G. By Theorem 9.7 (d), we have $E_3 = 1$. It follows that $E = E_1$ and it is cyclic. Since $M \in \mathcal{M}_\mathcal{F}$, $\kappa(M)$ is empty. This implies that E acts regularly on $M_\sigma = M_{\sigma_0}$. Thus, M is a Frobenius group with Frobenius kernel M_σ.

We have shown that $r \in \tau_2(N)$. Since $C_G(x) \subseteq N_G(X)$, we have $N_G(X) \subseteq N$. Therefore, $N_E(X) \subseteq E \cap N$. The choice of E implies

$$K_1 \subseteq E \cap N \subseteq M \cap N = U_1 K_1.$$

Since $C_{U_1}(K_1) = 1$, we have $K_1 = C_{E \cap N}(K_1)$. This implies $K_1 = E \cap N$ because E is cyclic. It follows from Theorem 8.7 (h) that $|E \cap N| = |K_1| = |N/N'|$. Q.E.D.

§10. The Main Results

Theorem A. *Let $M \in \mathcal{M}$. Then, the following conditions are satisfied by M.*

(1) *M has a unique normal Hall $\sigma_0(M)$-subgroup M_{σ_0} which is also a Hall $\sigma_0(M)$-subgroup of G.*

(2) *M has a cyclic Hall $\kappa(M)$-subgroup K.*

(3) *KM_{σ_0} has a K-invariant complement U in M, i.e.*

$$UM_{\sigma_0} \lhd M = KUM_{\sigma_0} \quad \textit{and} \quad U \lhd UK.$$

(4) *$C_U(k) = 1$ for every $k \in K^\sharp$.*

(5) *$K^* = C_{M_{\sigma_0}}(K) \neq 1$ and if $K \neq 1$, then $C_M(k) = K \times K^*$ for every $k \in K^\sharp$.*

(6) *$1 \neq M_F \subseteq M_{\sigma_0} \subseteq M' \subset M$ and M'/M_F is nilpotent.*

(7) *$M'' \subseteq F(M) = C_M(M_F)M_F$ and if $K \neq 1$, then $F(M) \subseteq M'$.*

(8) *If $M_F \neq M_{\sigma_0}$, then $U = 1$, $F(M)$ is a TI-subgroup in G, and K has prime order.*

Proof. The group M_{σ_0} is defined as $O_{\sigma_0(M)}(M)$. Hence, $M_{\sigma_0} \lhd M$. Theorem 4.2 (f) yields (1); a normal Hall subgroup is unique. If $\kappa(M)$ is empty, $K = 1$ and the conditions (2), (3), (4) and (5) are trivially satisfied. If $\kappa(M)$ is not empty, $M \in \mathcal{M}_\mathcal{P}$. Then, Proposition 8.2 (a) implies the conditions (3) and (4), and Proposition 8.2 (c) yields $K^* \neq 1$;

while Theorem 8.7 (d) yields (2) and the second part of the condition (5).

Theorem 9.2 proves the first part of (6). If $M_F = M_{\sigma_0}$, Theorem 4.2 (c) and (d) imply the second part of (6). If $M_F \neq M_{\sigma_0}$, Theorem 9.2 (d) yields the result. The condition (7) has been proved in Corollary 9.5 (b) and (d). Theorem 9.2 (a) and (b) yield the first and third conditions of (8), respectively, while Theorem 9.7 (a) implies the second condition. Q.E.D.

To state further results, we need the following notation:

$$\widehat{M_\sigma} = \{a \in M \mid C_{M_{\sigma_0}}(a) \neq 1\}.$$

Note that this definition is slightly different from that in [BG]. We also define $A(M)$ and $A_0(M)$ as in [BG]; however, we use the set $\widehat{M_\sigma}$ defined above in the definition of the sets $A(M)$ and $A_0(M)$. Thus, the sets $A(M)$ and $A_0(M)$ are different from the sets in [BG] even though they are denoted by the same notation. In particular, $\widehat{M_\sigma}$ consists of ϖ-elements.

If $M \in \mathcal{M}$ is not a ϖ-group, we can determine these sets from Lemma G. The result is contained in the following table:

Type	K	U	M_{σ_0}	$\widehat{M_\sigma}$	$A(M)$	$A_0(M)$
(1)	1	a Z-group	M_{σ_0}	M_{σ_0}	M_{σ_0}	M_{σ_0}
(2)	$\neq 1$	*cyclic*	M_{σ_0}	$M_{\sigma_0} \cup \mathcal{C}_M(Z)$	M_{σ_0}	$M_{\sigma_0} \cup \mathcal{C}_M(\widehat{Z})$

Theorem B. *Let $M \in \mathcal{M}$. The following conditions are satisfied by M.*

(1) *Every Sylow subgroup of U is abelian of rank at most 2.*

(2) *$\langle U \cap \widehat{M_\sigma} \rangle$ is abelian.*

(3) *U has a subgroup U_0 that has the same exponent as U and satisfies $U_0 \cap \widehat{M_\sigma} = 1$.*

(4) *$\mathcal{M}(C_G(X)) = \{M\}$ for every nonidentity subgroup X of U such that $C_{M_{\sigma_0}}(X) \neq 1$.*

(5) *The set $A(M) \setminus M_{\sigma_0}$ is either empty or a TI-subset of G with normalizer M.*

Proof. It follows from the definition of the subgroup U (at the beginning of Section 9) that $\pi(U) = \pi(M) \setminus \{\kappa(M), \sigma_0(M)\}$. Take $p \in \pi(U)$ and $S \in Sy\ell_p(U)$. If $p \in \tau_1(M) \cup \tau_3(M)$, then S is cyclic by the definition of the sets $\tau_i(M)$. If $p \in \tau_2(M)$, S is abelian of rank 2 by Theorem 6.5 (b). Finally, if $p \in \sigma(M) \setminus \sigma_0(M)$, S is cyclic by Lemma F. This proves (1).

Lemma 9.1 (d), (e) and (c) imply the conditions (2), (3) and (4), respectively. Suppose that the set $B = A(M) \setminus M_{\sigma_0}$ is not empty. The table before Theorem B shows that M is a ϖ-group. Since U is a Hall subgroup of $M_{\sigma_0}U$, every element g of $M_{\sigma_0}U$ can be written uniquely as a product of a $\sigma_0(M)$-element x and a $\pi(U)$-element v such that $g = xv = vx$. We say that v is the $\pi(U)$-component of the element g. It is a power of g, and v is conjugate to an element of U in M by the Schur-Zassenhaus Theorem.

Suppose that $g \in B$. Then, $g \notin M_{\sigma_0}$ so the $\pi(U)$-component v is not the identity. Also, $g \in B$ implies $C_{M_{\sigma_0}}(g) \neq 1$. It follows that $C_{M\sigma_0}(v) \neq 1$. If v is conjugate to an element u of U in M, we have $v = u^y$ for some $y \in M$ and $u \neq 1$. Then, Theorem B (4) yields that $\mathcal{M}(C_G(u)) = \{M\}$ because $u \neq 1$ and $C_{M_{\sigma_0}}(u) \neq 1$. Since $v = u^y$ with $y \in M$, we have $\mathcal{M}(C_G(v)) = \{M\}$. Thus, $g \in B$ implies $\mathcal{M}(C_G(v)) = \{M\}$ for the $\pi(U)$-component of g. Therefore, if $g \in B \cap B^h$ for some $h \in G$, then

$$\{M\} = \mathcal{M}(C_G(v)) = \{M^h\}.$$

This implies $M = M^h$ and $h \in M$. This proves (5). Q.E.D.

Theorem C. *Let $M \in \mathcal{M}_{\mathcal{P}}$ so $K \neq 1$. The following conditions hold.*

(1) *U is abelian. If M is a ϖ-group, $N_G(U) \not\subseteq M$. If $\sigma(M) \neq \sigma_0(M)$, then $N_G(U) \subseteq M$.*

(2) *K^* is cyclic, $1 \neq K^* \subset M_F$, but M_F is not cyclic.*

(3) *$M' = UM_{\sigma_0}$ and $K^* \subseteq M''$.*

(4) *There exists a unique subgroup $M^* \in \mathcal{M}_{\mathcal{P}}$ such that $K = C_{M^*_\sigma}(K^*)$ and K^* is a Hall $\kappa(M^*)$-subgroup of M^*.*

(5) *$\mathcal{M}(C_G(X)) = \{M\}$ and $\mathcal{M}(C_G(Y)) = \{M^*\}$ for all subgroups $X \subseteq K^*$ and $Y \subseteq K$ of prime order.*

(6) *$M \cap M^* = Z = K \times K^*$ and Z is cyclic.*

(7) *M or M^* is of type $\mathcal{P}_2$ and every subgroup $H \in \mathcal{M}_{\mathcal{P}}$ is conjugate to M or M^* in G.*

(8) *$\widehat{Z}$ is a TI-subset of G with $N_G(\widehat{Z}) = Z$.*

(9) *$\mathcal{C}_M(\widehat{Z})$ is equal to $A_0(M) \setminus A(M)$ and is a TI-subset of G with normalizer M.*

(10) *If $U \neq 1$, then K has prime order and $F(M)$ is a TI-subset of G that contains M_{σ_0}.*

(11) *If $U = 1$, then K^* has prime order.*

Proof. Proposition 8.2 (a) shows that U is abelian. The second statement of (1) follows from Corollary 8.12 (b), while the last one is obvious from the definitions.

Proposition 8.2 (c) implies the second condition of (2) and the first one in (5). Corollary 9.6 proves the remaining conditions of (2) and the last condition of (3). The most of the other conditions (3)—(9) follow from Theorem 8.7. Thus, the first condition of (3) follows from the part (h), (4) from the parts (b) and (c), the uniqueness of M^* and the second part of (5) from (a), the condition (6) from (d), the condition (7) from (f) and (g), the conditions (8) and the second part of (9) from (e) and the first part of (9) follows from the definitions.

Consider the conditions (10). The first one follows from Proposition 8.2 (g). Since $U \neq 1$, we have $M \in \mathcal{M}_{\mathcal{P}_2}$. Theorem 9.7 (a) now yields that $F(M)$ is a TI-subset of G. Then, $M_{\sigma_0} = M_F$ so $M_{\sigma_0} \subseteq F(M)$ by Theorem 9.2 (a).

The assumption $U = 1$ of (11) implies that $M \in \mathcal{M}_{\mathcal{P}_1}$. By Theorem 8.7 (f), $M^* \in \mathcal{M}_{\mathcal{P}_2}$ and K^* has prime order. Q.E.D.

Theorem D. *Let $M \in \mathcal{M}$. The following conditions are satisfied by M.*

(1) *Whenever two elements of M_{σ_0} are conjugate in G, they are conjugate in M.*

(2) *For every $g \in G \setminus M$, the group $M_\sigma \cap M^g = M_\sigma \cap (M_\sigma)^g$ is cyclic.*

(3) *For every $x \in (M_{\sigma_0})^\sharp$, $C_M(x)$ is a Hall subgroup of $C_G(x)$ and has a normal complement $R(x)$ in $C_G(x)$ that acts sharply transitively by conjugation on the set $\{M^g \mid g \in G, x \in M^g\}$.*

(4) *If $x \in (M_{\sigma_0})^\sharp$ and $C_G(x) \not\subseteq M$, then $\mathcal{M}(C_G(x)) = \{N\}$ for some ϖ-group $N = N(x) \in \mathcal{M}$ such that $R(x) = C_{N_\sigma}(x)$, $N_{\sigma_0} = N_F$, $x \in A(N) \setminus N_{\sigma_0}$, $N \in \mathcal{M}_{\mathcal{F}} \cup \mathcal{M}_{\mathcal{P}_2}$, and $M \cap N$ is a complement of N_σ in N. If $N \in \mathcal{M}_{\mathcal{P}_2}$, then M is a ϖ-group in $\mathcal{M}_{\mathcal{F}}$ that is a Frobenius group with cyclic Frobenius complement and Frobenius kernel $M_\sigma = M_F$. Furthermore, M_F is not a TI-subset in G.*

Proof. Corollary 9.3 (b) with H replaced by M_{σ_0} yields the condition (1), while Lemma 6.17 implies (2).

The assumptions of (3) and (4) imply that $\mathcal{M}_\sigma(x)$ is not empty. Therefore, Theorem 8.4 yields (3) and the most parts of (4). In particular, $N \notin \mathcal{M}_{\mathcal{P}_1}$. Then, Theorem 9.2 (a) applied to N proves that $N_{\sigma_0} = N_F$. We have $\pi(\langle x \rangle) \subseteq \tau_2(N)$. Since $N \notin \mathcal{M}_{\mathcal{P}_1}$, either $N = N_{\sigma_0}U$ or $N_{\sigma_0}U$ is a normal complement of K where U and K are defined as a Hall $(\sigma_0(N), \kappa(N))'$-subgroup and a Hall $\kappa(N)$-subgroup of N, respectively. Recall that if $K \neq 1$, K is a Hall $\tau_1(N)$-subgroup of N by Theorem 8.7 (c). Thus, $\pi(\langle x\rangle) \subseteq \tau_2(N)$ implies that $x \in N_{\sigma_0}U$. This proves that $x \in A(N) \setminus N_{\sigma_0}$.

If $N \in \mathcal{M}_{\mathcal{P}_2}$, Corollary 9.9 yields that $M \in \mathcal{M}_{\mathcal{F}}$ and M is a Frobenius group with Frobenius kernel M_{σ_0}. We have $M_{\sigma_0} = M_F$ by Theorem 9.2 (a). Since $C_G(x) \nsubseteq M$ and $x \in M_{\sigma_0} = M_F$. M_F is not a TI-subset of G. Q.E.D.

Theorem E. *For each $x \in (M_{\sigma_0})^\sharp$, let $R(x)$ be as in Theorem D. Define*

$$\widetilde{M} = \{xR(x) \mid x \in (M_{\sigma_0})^\sharp\}.$$

Then,

(1) $|\mathcal{C}_G(\widetilde{M})| = (|M_{\sigma_0}| - 1)|G : M|$.

Let $M_1, \ldots, M_n$ be a set of subgroups in $\mathcal{M}$ such that every subgroup of $\mathcal{M}$ is conjugate in G to exactly one of the M_i. Then,

(2) *ϖ is the disjoint union of the sets $\sigma_0(M_i)$.*

(3) *Let $\widetilde{G}$ be the union of the sets $\mathcal{C}_G(\widetilde{M_i})$. Then, $\widetilde{G}$ is the disjoint union of the sets $\mathcal{C}_G(\widetilde{M_i})$.*

If $\mathcal{M}_{\mathcal{P}}$ is empty, $\widetilde{G}$ is the set of the nonidentity ϖ-elements of G. If $\mathcal{M}_{\mathcal{P}}$ is not empty and $M \in \mathcal{M}_{\mathcal{P}}$, then the set of nonidentity ϖ-elements of G is the disjoint union of $\widetilde{G}$ and $\mathcal{C}_G(\widehat{Z})$ where $\widetilde{Z}$ is as defined in Theorem 8.7.

Proof. If $p \in \varpi$, take $P \in Syl_p(G)$ and $M \in \mathcal{M}(N_G(P))$. We have $p \in \sigma_0(M)$. If $H \in \mathcal{M}$ is not conjugate to M, $\sigma(H)$ is disjoint from $\sigma(M)$ by Theorem 7.9. Thus, ϖ is the disjoint union of the sets $\sigma_0(M_i)$.

The remaining assertions of this theorem follow from Lemma 8.5 and Corollary 8.9. Q.E.D.

We define the type of a subgroup as in [BG] pp.128–129 with the following three changes.

We change (II*iv*), (II*v*) and (III*iii*) to read

(II*iv*) $V \neq 1$ and, if V is a ϖ-group, $N_G(V) \nsubseteq M$.

(II*v*) $N_G(A) \subseteq M$ for every nonidentity subgroup A of M' such that $C_H(A) \neq 1$.

(III*iii*) V is an abelian ϖ-group and $N_G(V) \subseteq M$.

Proposition 10.1. *Let M be an element of $\mathcal{M}$.*

(a) *$M \in \mathcal{M}_{\mathcal{F}}$ if and only if M is of type I.*

(b) *$M \in \mathcal{M}_{\mathcal{P}_2}$ if and only if M is of type II.*
(c) *$M \in \mathcal{M}_{\mathcal{P}_1}$ and $M_F \neq M_{\sigma_0}$ if and only if M is of type III or IV.*
(d) *$M \in \mathcal{M}_{\mathcal{P}_1}$ and $M_F = M_{\sigma_0}$ if and only if M is of type V.*
(e) *$M' = M_{\sigma_0}U$ if and only if M is not of type I.*
(f) *$M_F = M_{\sigma_0}$ if and only if M is of type I, II, or V.*

Proof. (a) Suppose that $M \in \mathcal{M}_{\mathcal{F}}$. This means that $K = 1$ and $U \neq 1$ in the notation of this section. As in [BG], let H denote M_F. Since $U \neq 1$, Theorem A (8) yields that $M_{\sigma_0} = M_F = H$. Thus, U is a complement of H in M. We have $H \neq M$ because $U \neq 1$. By Theorem A (6), $H \neq 1$ so we have the condition (I*i*). The conditions (I*ii*), (I*iii*) and (I*iv*) are Theorem B (2),(3) and (1), respectively. We need to prove (I*v*). Suppose that H is not a TI-subset of G. Then, $F(M)$ is not a TI-subset of G. Since $M \in \mathcal{M}_{\mathcal{F}}$, the case (3) of Theorem 9.7 (e) does not occur. Suppose that neither (a) nor (b) hold in (I*v*). Then, we have the case (2) of Theorem 9.7 (e). Then, for every $q \in \pi(H)$, either $q \in \sigma_0(M) \setminus \beta(M)$, or M has a cyclic Sylow q-subgroup. Thus, $q \in \pi^*$. Furthermore, the exponent of M/H divides $q-1$. Since $O_{p'}(H)$ is cyclic for one prime $p \in \pi(H)$, M satisfies the condition (I*v*). Therefore, every subgroup in $\mathcal{M}_{\mathcal{F}}$ is of type I.

Conversely, suppose that M is of type I. Suppose that $\kappa(M) \neq \emptyset$. Let K be a Hall $\kappa(M)$-subgroup of M and $K^* = C_{M_\sigma}(K)$. Then, by Theorem C (2), $K^* = C_H(K) \neq 1$. We will prove that $C_H(K) = 1$ contrary to the above inequality.

Since $K \cap H \subseteq K \cap M_{\sigma_0} = 1$, there is a complement E of H in M that contains K. Since K is a cyclic Hall subgroup of M by Theorem A (2), (I*iii*) implies that K acts regularly on H by conjugation. Thus, $C_H(K) = 1$. This contradiction proves that every subgroup of type I lies in $\mathcal{M}_{\mathcal{F}}$.

(b) Suppose that $M \in \mathcal{M}_{\mathcal{P}}$, i.e. $K \neq 1$. By Theorem C (3), $M' = UM_{\sigma_0}$, so M' is a normal complement of K. Hence, M' is a Hall $\kappa(M)'$-subgroup of M. It contains H because $H \subseteq M_{\sigma_0} \subseteq M'$ by Theorem A (6). Thus, M satisfies (T1).

Define $W_1 = K$, $W_2 = K^*$, and let V be a K-invariant complement of H in M'. If $M_{\sigma_0} = H$, then choose $V = U$. By Theorem A (6), V ($\cong M'/H$) is nilpotent. This proves the condition (T2) for M. The group H is not cyclic by Theorem C (2). The remaining parts of (T3) follow from Theorem A (7). Since $K^* \subseteq M_{\sigma_0} \subseteq M'$, we have

$$KK^* \cap M' = (K \cap M')K^* = K^*.$$

This, together with Theorem A (5), implies (T4); while Theorem C (8) yields (T5).

Suppose that A_0 and A_1 are subgroups of prime order in V such that

$$(A_0)^g = A_1,\ g \in G \setminus M,\ C_H(A_0) \neq 1, \text{ and } \quad C_H(A_1) \neq 1.$$

If $H = M_{\sigma_0}$, then $V = U$. Hence, by Theorem B (4), we have

$$\{M\} = \mathcal{M}(C_G(A_1)) = \mathcal{M}(C_G(A_0))^g = \{M^g\}.$$

This would imply $g \in M$ by Lemma E. Therefore, we have $H \neq M_{\sigma_0}$. Theorem A (8) yields $U = 1$ and

$$A_i \subseteq V \subseteq M' = UM_{\sigma_0} = M_{\sigma_0}.$$

By Theorem D (1), A_0 and A_1 are conjugate in M. This proves that M satisfies (T6).

Assume that $M \in \mathcal{M}_{\mathcal{P}_2}$. Then, $K \neq 1$ and $U \neq 1$. Theorem A (8) yields $M_{\sigma_0} = H$ so $V = U$. We will check the conditions in (T7) for $M \in \mathcal{M}_{\mathcal{P}_2}$. By Theorem C (10), $W_1 = K$ has prime order and $F(M)$ is a TI-subset in G. Since $F(M) = C_M(H)H$ by Theorem A (7), we have (T7)(*ii*). Theorem C (1), together with Theorem B (1), yields that U is abelian of rank ≤ 2. This is (II*iii*).

Since $M \in \mathcal{M}_{\mathcal{P}_2}$, we have $V = U \neq 1$. Suppose that U is a ϖ-group. Then, M is a ϖ-group and Theorem C (1) yields $N_G(U) \not\subseteq M$. This proves (II*iv*).

To prove (II*v*), let A be a nonidentity subgroup of M' such that $C_H(A) \neq 1$. Since $M' = HU$, we have $A = XY$ where $X = A \cap H$ is a normal Hall subgroup of A and Y is a complement of X in A. Then, $N_G(A) \subseteq N_G(X)$. If $X \neq 1$, we have $N_G(X) \subseteq M$ because $F(M)$ is a TI-subset of G. In this case, $N_G(A) \subseteq M$. Suppose $X = 1$. Then $A = Y$ is a $\sigma_0(M)'$-group and it is conjugate to a subgroup of U in M. We may assume, by replacing A by a conjugate in M if necessary, that $A \subseteq U$. Since $C_H(A) \neq 1$, Theorem B (4) yields that $\mathcal{M}(C_G(A)) = \{M\}$. Therefore, $N_G(A) \subseteq M$. This proves (II*v*). Thus, a group in $\mathcal{M}_{\mathcal{P}_2}$ is of type II.

Assume that $M \in \mathcal{M}_{\mathcal{P}_1}$, i.e. $K \neq 1$ but $U = 1$. In this case, we have $V \subseteq M' = M_{\sigma_0}$. Therefore, V is a ϖ-group. Suppose that $V \neq 1$. Recall that V is defined as a complement of H in M'. Thus, in this case, we have $H \neq M_{\sigma_0}$. Hence, by Theorem A (8), conditions (*i*) and (*ii*) of (T7) hold. Since V is a Hall subgroup, V contains a Sylow p-subgroup P of G. Since $P \subseteq V \subseteq M_{\sigma_0}$, we have $p \in \sigma_0(M)$ and $N_G(P) \subseteq M$. By (T2), V is nilpotent. Hence,

$$N_G(V) \subseteq N_G(P) \subseteq M.$$

Thus, $M \in \mathcal{M}_{\mathcal{P}_1}$ with $V \neq 1$ is of type III or IV according as V is abelian or not.

Finally, suppose that $M \in \mathcal{M}_{\mathcal{P}_1}$ and $V = 1$. In this case, we have $H = M_{\sigma_0} = M'$. Suppose that H is not a TI-subset of G. Then, $F(M)$ is not a TI-subset of G. Theorem 9.7 (e) implies that M satisfies one of the three conditions. Since $M \in \mathcal{M}_{\mathcal{P}_1}$, the first condition does not hold. Hence, M is of type V.

Suppose that M is a group of type II, III, IV, or V. Then, M' is a Hall subgroup of M with a cyclic complement W_1 by (T1) and (T2). The group W_1 is a cyclic Hall subgroup of M such that $C_H(W_1) = W_2 \neq 1$. This implies $\pi(W_1) \subseteq \kappa(M)$. Thus, $\kappa(M) \neq \emptyset$ and $M \in \mathcal{M}_{\mathcal{P}}$. The group M has a series of characteristic subgroups $H \subseteq M_{\sigma_0} \subseteq M'$. The type of M is determined by the properties of this series. The type is V if and only if $H = M'$. The type is IV if and only if the group M'/H is nonabelian.

For the remaining types, M'/H is abelian. The type is III if and only if M'/H is an abelian ϖ-group and $N_G(V) \subseteq M$. Thus, the type of a group in $\mathcal{M}_{\mathcal{P}}$ is uniquely defined. Therefore, the statements (b), (c), and (d) hold. The other parts of Proposition 10.1 are proved as in [BG]. Q.E.D.

Theorem I. *Let H be a nilpotent Hall subgroup of G. Suppose that H is a ϖ-group. Then, two elements of H are conjugate in G if and only if they are conjugate in $N_G(H)$.*

Either every subgroup in $\mathcal{M}$ is of type I or all of the following conditions are true.

(a) *G contains a cyclic subgroup $W = W_1 \times W_2$ with the property that $N_G(W_0) = W$ for every nonempty subset W_0 of $W \setminus \{W_1, W_2\}$. Also, $W_i \neq 1$ for $i = 1, 2$.*

(b) *There are two subgroups S and T in $\mathcal{M}$ not of type I such that*

$$S = W_1 S',\ T = W_2 T',\ S' \cap W_1 = T' \cap W_2 = 1 \text{ and } S \cap T = W.$$

(c) *$M \in \mathcal{M}$ is either of type I or conjugate to S or T.*

(d) *S or T is of type II.*

(e) *Both S and T are of type II, III, IV, or V.*

(f) *The group S is not conjugate to T in G.*

Proof. Let H be a nilpotent Hall subgroup of G, and assume that H is a ϖ-group. In order to prove the first statement, we may assume $H \neq 1$. By Corollary 9.4, there is a subgroup $M \in \mathcal{M}$ such that $H \subseteq M_{\sigma_0}$. We will show that $N_G(H) \subseteq M$. Take a prime $p \in \pi(H)$ and $P \in Syl_p(H)$. Since H is a Hall subgroup of G, we have $P \in Syl_p(G)$.

It follows from the definition of $\sigma_0(M)$ that $N_G(P) \subseteq M$. Since H is nilpotent, $N_G(H) \subseteq N_G(P)$ so $N_G(H) \subseteq M$ as claimed.

Corollary 9.3 (b) implies that any two elements of H which are conjugate in G are already conjugate in $N_M(H)$. Since $N_G(H) \subseteq M$, we have $N_M(H) = N_G(H)$ and the first statement is proved.

Suppose that there is a subgroup $M \in \mathcal{M}$ not of type I. Then, $M \in \mathcal{M}_{\mathcal{P}}$ by Proposition 10.1 (a). Let $M = S$, $M^* = T$, $K = W_1$, and $K^* = W_2$. The group M satisfies the conditions (T1)—(T6) by Proposition 10.1 (a). These conditions imply that W_1 and W_2 are nonidentity cyclic subgroups of relatively prime orders. Condition (T4) yields

$$W = W_1W_2 = W_1 \times W_2.$$

Hence, W is cyclic. Condition (T5) yields the first condition (a) of Theorem I. By Theorems C (4), C (6), and C (7), together with (T1) and (T2), S and T satisfy the conditions (b), (c) and (d). The last two conditions follow from Proposition 10.1 and Theorem 8.7. Q.E.D.

We state here the definition of the sets $A(M)$ and $A_0(M)$ for each $M \in \mathcal{M}$. Let $H = M_F$.

If M is of type I, then

$$A(M) = A_0(M) = \bigcup_{x \in H^\sharp} C_M(x).$$

If M is of type II,

$$A(M) = \bigcup_{x \in H^\sharp} C_{M'}(x);$$

while if M is of type III, IV, or V,

$$A(M) = M'.$$

If M is not of type I, then

$$A_0(M) = A(M) \cup \mathcal{C}_M(\widehat{W}).$$

Theorem II. *For a subgroup $M \in \mathcal{M}$, let $X = A(M)$ or $X = A_0(M)$, and let*

$$D = \{x \in X^\sharp \mid C_G(x) \not\subseteq M\}.$$

Then, $D \subseteq M_{\sigma_0}$, $|\mathcal{M}(C_G(x))| = 1$ for all $x \in D$, and the following conditions are satisfied.

(F*i*) *Whenever elements of X are conjugate in G, they are conjugate in M.*

(F*ii*) *If D is not empty, then there are ϖ-subgroups $M_1, \dots, M_n$ of $\mathcal{M}$ of type I or II such that with $H_i = (M_i)_F$,*

(a) $(|H_i|, |H_j|) = 1$ *for* $i \neq j$,

(b) $M_i = H_i(M \cap M_i)$ *and* $M \cap H_i = 1$,

(c) $(|H_i|, |C_M(x)|) = 1$ *for all* $x \in X^\sharp$,

(d) $A_0(M_i) \setminus H_i$ *is a nonempty TI-subset of G with normalizer M_i, and*

(e) *if $x \in D$, then there is a conjugate y of x in D and an index i such that $C_G(y) = C_{H_i}(y)C_M(y) \subseteq M_i$. If $y \in D$ with $C_G(y) \subseteq M_i$, then $y \in A(M_i)$.*

(F*iii*) *If some M_i in* (F*ii*) *has type II, then M is a ϖ-group and is a Frobenius group with cyclic Frobenius complement, and M_F is not a TI-subset in G.*

Proof. For any $M \in \mathcal{M}$, $A_0(M)$ is a disjoint union of the sets

$$M_{\sigma_0}, A(M) \setminus M_{\sigma_0}, \text{ and } A_0(M) \setminus A(M).$$

The order of an element of M_{σ_0} involves only primes in $\sigma_0(M)$, the order of an element of $A(M) \setminus M_{\sigma_0}$ involves no prime of $\kappa(M)$ and some prime in $\pi(U)$ which is disjoint from $\sigma_0(M)$, and the order of an element of $A_0(M) \setminus A(M)$ involves a prime of $\kappa(M)$. Thus, an element of any of these sets is not conjugate to an element of one of the other two sets. By Theorems B (5) and C (9), the latter two sets are TI-subsets of G with normalizer M if not empty. Therefore, we have $D \subseteq M_{\sigma_0}$. Thus, if $x \in D$, then x is a ϖ-element with $M \in \mathcal{M}_\sigma(x)$. In fact, we have $|\mathcal{M}_\sigma(x)| > 1$ because $C_G(x) \nsubseteq M$. Theorem 8.4 yields $|\mathcal{M}(C_G(x))| = 1$.

It follows from the definition of the set X that $X \setminus M_{\sigma_0}$ is either empty or a TI-subset of G with normalizer M as remarked earlier. Therefore, Theorem D(1) implies (F*i*).

Assume that D is not empty. For each $x \in D$, let $N(x)$ be the element of $\mathcal{M}(C_G(x))$. By Theorem D (4), $N(x)$ is a ϖ-group of type I or II. Let $\mathcal{A}$ be the collection of all such subgroups $N(x)$ and let $\{M_1, \dots, M_n\}$ be a subset of $\mathcal{A}$ such that each $N \in \mathcal{A}$ is conjugate in G to exactly one M_i. The last condition (F*iii*) follows from Theorem D (4).

We will prove (F*ii*). Take some M_i. Theorem D (4) yields that $(M_i)_{\sigma_0} = H_i$ and $M \cap M_i$ is a complement of H_i in M_i. This proves (b). By Theorem E (2), the sets $\sigma(M_i)$ are pairwise disjoint which implies (a).

By Theorem D (4), $x \in A(M_i) \backslash H_i$. Thus, $A(M_i) \backslash H_i$ is a nonempty TI-subset of G with normalizer M_i (by Theorem B (5)). If $A_0(M_i) \neq A(M)$, then $A_0(M_i) \setminus A(M)$ is also a TI-subset (by Theorem C (9)) and does not fuse to $A(M)$. This proves that $A_0(M_i) \setminus H_i$ is a nonempty TI-subset of G with normalizer M_i.

To prove (e), let $x \in D$. Then, the subgroup $N(x)$ is conjugate to M_i for some i, so $N(x)^g = M_i$ for some $g \in G$. By Lemma 8.13 (b), we may take $g \in M$. Then, $y = x^g \in D$ and $N(x) = M_i$. By Theorem 8.4 (b), we have

$$C_G(y) = C_{H_i}(y) C_M(y) \subseteq M_i.$$

If M_i is of type I, certainly $y \in A(M_i)$. Suppose that M_i is of type II. Theorem 8.4 (c) yields $\pi(\langle y \rangle) \subseteq \tau_2(M_i)$. Since M_i is of type II, Theorem 8.7 (h) and (c) yield $y \in (M_i)'$. Hence, $y \in A(M_i)$ in this case, too.

It remains to prove (c). Suppose $x \in X^\sharp$ and $(|H_i|, |C_M(x)|) \neq 1$ for some i. Then, $\pi(M) \cap \sigma_0(M_i)$ is not empty. By Lemma 8.13 (a), M is a Frobenius group with Frobenius kernel M_{σ_0}. Hence,

$$A_0(M) = M_{\sigma_0} = X \quad \text{and} \quad C_M(x) \subseteq M_{\sigma_0}.$$

It follows that $\sigma_0(M) \cap \sigma_0(M_i)$ is not empty. By Theorem E (2), M is conjugate to M_i in G. However, this is a contradiction because $\tau_2(M) = \emptyset$ by Lemma 8.13 (a), while $\tau_2(M_i) \neq \emptyset$ by Theorem 8.4 (c). Q.E.D.

Chapter II. Application of Character Theory

We continue to study the structure and embedding of the subgroups in $\mathcal{M}$ and use the notation introduced in Chapter I. We will follow most of the terms and notation of [BG] and [FT]; however, I follow the practice of denoting elements of groups by the lower case letters and subsets by the capitals. For a group H, let

$$\mathrm{Irr}(H)$$

denote the set of all irreducible characters of the group H over the field $\mathbb{C}$ of complex numbers. If X is a subset of H,

$$I(X)$$

denotes the set of virtual characters which vanish outside X. The subset of $I(X)$ consisting of those virtual characters which take zero at the identity will be important and denoted by

$$I_0(X).$$

Sometimes, the set of complex valued class functions which vanish outside X will be considered; it is denoted by $C(X)$. The subset of those class functions taking value zero at the identity is denoted $C_0(X)$.

When H is a subgroup of a group G, the *induction* φ^G and the *restriction* θ_H of class functions are defined as usual. If the groups involved are clear from the context, the notation φ^* for the induction may be used.

Our starting point is Theorems I and II of Section 10, Chapter I. Theorem I asserts that every subgroup $M \in \mathcal{M}$ is of type I, II, III, IV, or V. The definition of groups of each type is stated in [BG] but we have made three changes in Section 10, Chapter I; we will be using the modified definition in Chapter II. Theorem II concerns the embedding of the subgroups of $\mathcal{M}$. We say that a subset X of M is an *F-set* (or satisfies Feit-Thompson-Sibley-Bender-Glauberman conditions) if M and X satisfy the conditions (Fi), (Fii) and (Fiii) of Theorem II. Theorem II simply says that both $X = A(M)$ and $X = A_0(M)$ are F-sets of M. In [BG], it is suggested to call $A(M)$ and $A_0(M)$ tamely imbedded subsets. I choose a different term because there is another tamely imbedded subset in [FT] and I have added two conditions to (Fii).

The set of subgroups $\{H_1, H_2, \ldots, H_n\}$ in (Fii) is called the set of *supporting subgroups* of the F-set X. Sometimes we abuse the term and may call subgroups $\{M_1, \ldots, M_n\}$ are also supporting subgroups.

If X is an F-set of M, we will use the following notation throughout Chapter II. Let D be the set defined by

$$D = \{x \in X^\sharp \mid C_G(x) \not\subseteq M\}.$$

If D is empty, X is a TI-subset of M. If X is either $A(M)$ or $A_0(M)$, and if D is not empty, then Theorem II yields that $D \subseteq M_{\sigma_0}$. Therefore, the set D does not depend on whether $X = A(M)$ or $X = A_0(M)$. The following notation is used.

$$D_0 = \{x \in X \mid C_G(x) \subseteq M\}$$

and for $i > 0$,

$$D_i = \{x \in D \mid C_G(x) \subseteq M_i\}$$

where M_i is one of the supporting subgroups of the set X. We have abused the notation already. It is convenient to define

$$H_0 = \{1\}, M_0 = M, \quad \text{and} \quad D^* = \bigcup\nolimits_{i=0}^{n} D_i.$$

As in [FT], we define for $i \geq 0$ and $x \in D_i$

$$A_x = A(x) = \{hx \mid hx = xh, h \in H_i\}.$$

Note that each $A(x)$ consists of nonidentity elements. We call a subset of the form $A(x)$ for some $x \in D^*$ an *annex.* For an F-set X of M, we call the set of elements of G which are conjugate to an element of some annex $A(x)$ for $x \in D^*$ the *territory* of X. Sometimes, we abuse the term and call it the territory of M. A class function θ on G is called *well-behaved* if θ takes a constant value on each annex. The well behaved class functions will play an important role in the following discussion.

§11. Preparation from Character Theory

First we paraphrase the proof of Lemma 4.5 [FT] because it is basic to our work. Afterwards, we define the basic character correspondence τ and prove its properties. This part corresponds to Section 9 of [FT].

For convenience, we state Lemma 4.5 [FT]:

Lemma. *Let H be a normal subgroup of the group X and let θ be an irreducible character of H. Suppose X contains a normal subgroup X_0 such that the inertia group $I(\theta) \subseteq X_0$ and such that X_0/H is abelian. Then θ^* is a sum of irreducible characters of X which have the same degree and occur with the same multiplicity in θ^*. This common degree is a multiple of $|X : I(\theta)|$. If furthermore H is a Hall subgroup of X_0, then θ^* is a sum of $|I(\theta) : H|$ distinct irreducible characters of degree $|X : I(\theta)|\theta(1)$.*

We need a lemma.

Lemma. *Let M be a group, $H \lhd M$, $\theta \in \mathrm{Irr}(H)$, and let $I = I(\theta)$ be the inertia group of θ in M. If $\theta^I = \sum a_i\lambda_i$ where a_i are positive integers and λ_i are distinct irreducible characters of the group I, then λ_i^M are distinct irreducible characters of M and*

$$\theta^M = \sum a_i\lambda_i^M.$$

By the reciprocity theorem, $(\lambda_i)_H$ contains the character θ with exact multiplicity a_i. Since $H \lhd I$, $(\lambda_i)_H$ is a sum of the conjugates of θ. It follows from the definition of the inertia group that θ is the only conjugate of θ in I. Thus, we have

$$(\lambda_i)_H = a_i\theta;$$

in particular, $\lambda_i(1) = a_i\theta(1)$.

Let ξ be an irreducible component of λ_i^M. Then, ξ_I involves λ_i. Hence, ξ_H contains $a_i\theta$. Since $H \lhd M$, ξ_H contains all the $|M : I|$ conjugates of θ with the same multiplicity. It follows that

$$\xi(1) \geq a_i|M : I|\theta(1) = |M : I|\lambda_i(1) = \lambda_i^M(1).$$

Since ξ is an irreducible component of λ_i^M, we have $\lambda_i^M = \xi$, i.e. λ_i^M is irreducible. The preceding proof yields that $(\lambda_i^M)_H$ involves θ exactly a_i times. This implies that the character $(\lambda_i^M)_I$ does not involve λ_j for any $j \neq i$. Thus, $\lambda_i^M \neq \lambda_j^M$ for $i \neq j$. This proves the lemma. Q.E.D.

Hypotheses of Lemma 4.5 [FT] are $H \lhd X$, $\theta \in \mathrm{Irr}(H)$, $I = I(\theta)$, the inertia group of θ in X, and I/H is abelian. By the preceding lemma, we need only to prove the assertion for I.

Let λ be an irreducible component of θ^I and let $\{\mu_1, \dots, \mu_m\}$ be the set of all irreducible characters of I/H. Since I/H is abelian, μ_i are linear and $\{\mu_1, \dots, \mu_m\}$ is a multiplicative group of order $m = |I/H|$. Suppose that we take notation $\lambda\mu_i = \lambda$ if and only if $1 \leq i \leq n$. For every j, $(\lambda\mu_j)\mu_i = (\lambda\mu_j)$ for $i = 1, 2, \dots, n$.

We have $(\theta^I)_H = m\theta$ so $\lambda_H = a\theta$ for some positive integer a. Then,

$$\lambda(1_H)^I = (\lambda_H)^I = a\lambda^I.$$

Since $(1_H)^I = \sum \mu_j$, the irreducible components of θ^I are characters of the form $\lambda\mu_j$. This proves that all the irreducible components of θ^I are of the same degree. Also, the equality

$$\lambda(\sum \mu_j) = a\theta^I$$

yields that θ^I contains each irreducible component $\lambda\mu_j$ with the same multiplicity, say b. This proves the first assertion of Lemma 4.5 [FT]. We remark that $n = ab$.

The second part of the lemma asserts that if in addition H is a Hall subgroup of the inertia group I, then θ^X is a sum of exactly $|I : H|$ distinct irreducible characters of degree $|X : I|\theta(1)$. By the lemma, it suffices to prove the case $X = I$.

We can take an abelian complement A of H in I because H is a Hall subgroup of I and I/H is abelian. We will show by induction that if $H \subseteq K \subseteq I$, θ^K is a sum of exactly $|K : H|$ distinct irreducible characters of degree $\theta(1)$. The first part of Lemma yields that

$$\theta^K = b(\lambda_1 + \cdots + \lambda_s)$$

where $\lambda_1, \dots, \lambda_s$ are distinct irreducible characters of degree $a\theta(1)$.

Suppose that $|K : H| = p$ is a prime. By definition of the induced character, we have

$$(\theta^K)_H = p\theta.$$

Then, the orthogonality relations yield

$$b^2 s = (\theta^K, \theta^K) = (\theta, (\theta^K)_H) = p(\theta, \theta) = p.$$

Since p is a prime, we have $b = 1$ and $s = p$. Thus, $n = n_K = 1$.

Suppose that $H \subseteq K \subseteq L \subseteq I$ and $|L : K| = q$ is a prime. Suppose that $n_K = 1$. Take an irreducible component λ of θ^K and let $\{\mu_1, \dots, \mu_s\}$ be the set of irreducible characters of the abelian group K/H. Since $n_K = 1$, the characters $\lambda\mu_i$ are distinct. Therefore,

$$\theta^K = \sum \lambda\mu_i.$$

We claim that $L \subseteq I(\lambda)$. If $x \in L$, $(\theta^K)^x = (\theta^x)^K = \theta^K$ because $x \in L \subseteq I$. Thus, λ^x is an irreducible component of θ^K, i.e. $\lambda^x = \lambda\mu_i$ for some i. We need to show that μ_i is the principal character of K/H. We may assume that $x \in K \cap A$. If μ_i is nonprincipal, there is an element $y \in K \cap A$ such that $\mu_i(y) \neq 1$ and the order of y is a power of some prime r. Lemma 4.2 [FT] implies

$$\lambda(y) \equiv \lambda(1) \pmod{\mathfrak{r}}$$

where $\mathfrak{r}$ is a prime ideal dividing r in the ring of integers of a number field. Since $n_K = 1$, we have $\lambda(1) = \theta(1)$. Also, $\lambda(1)$ divides the order $|H|$. The group H is a Hall subgroup of I so r does not divide $\lambda(1)$. It follows from the above congruence that $\lambda(y) \neq 0$. Since A is abelian and $x, y \in A$, we have

$$\lambda(y) = \lambda^x(y) = \lambda(y)\mu_i(y).$$

Therefore, $\mu_i(y) = 1$ because $\lambda(y) \neq 0$. This contradiction proves that $\lambda^x = \lambda$ and $L \subseteq I(\lambda)$.

By the result proved earlier, the induced character λ^L is a sum of $|L : K|$ distinct irreducible characters. This holds for any irreducible component of θ^K. Thus, θ^L is a sum of exactly $|L : H|$ distinct irreducible characters of degree $\theta(1)$. In particular, $n_L = 1$. This completes the proof of Lemma 4.5 [FT]. Q.E.D.

We need some lemmas about the fusion of elements.

Lemma I. *Let $M \in \mathcal{M}$ and let X be an F-set of M. Every element of $X^\sharp$ is conjugate to an element of D^* in M.*

Proof. Let $x \in X^\sharp$. If $x \in D_0$, the assertion is trivial. If $x \notin D_0$, we have $x \in D$. By (Fii, e), there is a conjugate y of x such that $y \in D_i$. Since x and y are two elements of X which are conjugate, (Fi) yields that they are conjugate in M. Q.E.D.

Lemma J. (a) *Every element g of M_i is conjugate in M_i to an element of the form $xh = hx$ where $x \in M \cap M_i$ and $h \in H_i$.*

(b) *Suppose that g is an element of M_i with $C_{H_i}(g) \neq 1$. Assume that g is conjugate in M_i to an element of the form hx where $x \in M \cap M_i$ and $h \in C_{H_i}(x)$, and at the same time g is conjugate to an element of the annex $A(y)$ with $y \in D_j$. Then, $j = i$ and the element x is conjugate to y in M_i. In particular, $x \in D_i$ and $g \in A(M_i)$.*

Proof. (a) If $i = 0$, $M_i = M$ and (a) holds trivially. Assume $i > 0$. The subgroup H_i is a normal Hall subgroup of M_i with complement $M \cap M_i$ by (Fii, b). Let $g = uv = vu$ be the decomposition of the element g into the product of a $\pi(H_i)$-element u and a $\pi(H_i)'$-element v. Since H_i is nilpotent, we can apply the Schur-Zassenhaus Theorem to the subgroup $\langle H_i, g\rangle$. Then, $\langle v\rangle$ is conjugate in M_i to a subgroup of $M \cap M_i$. It follows that g is conjugate in M_i to an element of the form hx where $x \in M \cap M_i$ and $h \in C_{H_i}(x)$.

(b) Suppose that $C_{H_i}(g) \neq 1$ and that g is conjugate to an element ky of $A(y)$ with $y \in D_j$ and $k \in C_{H_j}(y)$. The first assumption implies that $i > 0$. We will prove that $j > 0$. If $j = 0$, we have $C_G(y) \subseteq M$. It follows that

$$C_G(ky) \subseteq C_G(y) \subseteq M.$$

Since $C_{H_i}(g) \neq 1$ for some $i > 0$, $(|C_G(g)|, |H_i|) \neq 1$. We have $|C_G(g)| = |C_G(ky)|$ because g is conjugate to ky. Therefore,

$$(|C_G(y)|, |H_i|) \neq 1.$$

This contradicts (Fii,c) as $|C_G(y)| = |C_M(y)|$. Hence, we have $j > 0$.

It follows that $C_G(y) \subseteq M_j$ and $C_G(y) = C_{H_j}(y)C_M(y)$. Suppose that $j \neq i$. Then, by (Fii) (a) and (c), $|C_G(y)|$ is prime to $|H_i|$. This is a contradiction because

$$|C_G(g)| = |C_G(ky)| \quad \text{and} \quad C_G(ky) \subseteq C_G(y).$$

Therefore, we have $j = i$. Since $y \in X^\sharp$, the order of y is prime to $|H_i|$ by (Fii,c). Hence, y is the $\pi(H_i)'$-part of the element ky. Similarly, the element x is the $\pi(H_i)'$-part of hx. Since hx is conjugate to ky, the element x is conjugate to y in G. By (Fii,e), the element y is in $A(M_i)$. Since hx is conjugate to g in M_i and $C_{H_i}(g) \neq 1$, we have $C_{H_i}(x) \neq 1$.

If M_i is of type I, then $x \in A(M_i)$. If M_i is of type II, $(M_i)'$ is a Hall subgroup of M_i by (T1), and $y \in A(M_i) \subseteq (M_i)'$. Since x is conjugate to y in G, we have

$$|\langle x \rangle| = |\langle y \rangle|.$$

Hence, $x \in (M_i)'$ and $x \in A(M_i)$. Clearly, $y \neq 1$ so $y \notin H_i$. Since H_i is a Hall subgroup of M_i, we have $x \notin H_i$. Thus, x and y are elements of $A_0(M_i) \setminus H_i$ that is a TI-subset in G with normalizer M_i. Since x is conjugate to y, they are conjugate in M_i. It follows that

$$C_G(x) \subseteq M_i \quad \text{and} \quad x \in D_i.$$

By (Fii,e), $hx \in A(M_i)$. Since g is conjugate to hx in M_i, we have $g \in A(M_i)$. Q.E.D.

We will define the fundamental mapping τ.

Definition K. Let $M \in \mathcal{M}$ and let X be an F-set of M. For

$$\alpha \in I_0(X) \quad \text{and} \quad 1 \leq i \leq n,$$

define

$$\alpha_i = \alpha_{M \cap M_i}.$$

Let α_{i1} be the virtual character of M_i/H_i that is the lift of α_i and let α_{i2} be the virtual character of M_i induced by α_i. We define

$$\alpha^\tau = \alpha^G + \sum_{i=1}^{n} (\alpha_{i1} - \alpha_{i2})^G.$$

Thus, α^τ is a virtual character of the group G that vanishes at the identity.

Lemma L. (a) *If $g \in G$ is not conjugate to any element of $X^\sharp$ in G, then $\alpha^G(g) = 0$. If $g \in X^\sharp$, then*

$$\alpha^G(g) = |C_G(g) : C_M(g)|\alpha(g).$$

(b) *Let i be one of the integers between 1 and n. If $g \in G$ is not conjugate to any element x of M_i with $C_{H_i}(x) \neq 1$, then $(\alpha_{i1} - \alpha_{i2})^G(g) = 0$.*

Proof. (a) The first statement is obvious from the definition of induced characters. Suppose $a \in X^\sharp$. By definition,

$$\alpha^G(g) = \sum \alpha_0(x_i^{-1} g x_i)$$

where α_0 is the function that agrees with α on M but vanishes outside M, and the sum is over a system $\{x_i\}$ of the representatives of the cosets of M. We need to count the number of x_i such that $x_i^{-1}gx_i \in X^\sharp$. If $x^{-1}gx \in X$, (Fi) yields

$$x^{-1}gx = m^{-1}gm$$

for some $m \in M$. Hence, $xm^{-1} = c \in C_G(g)$. We choose c as a representative of the coset xM. Then, $\alpha_0(x_i^{-1}gx_i) = \alpha(g)$. This yields the result.

(b) If $x \in M_i$ is not conjugate to any element of $M \cap M_i$, then it follows from the definition of the induced character that $\alpha_{i2}(x) = 0$. We may take the set H_i as a set of representatives from the cosets of $M \cap M_i$. If $x \in M \cap M_i$ and $h \in H_i$,

$$h^{-1}xh \in M \cap M_i$$

implies $[x,h] = x^{-1}h^{-1}xh \in (M \cap M_i) \cap H_i = 1$. Hence, if $x \in M \cap M_i$, then

$$\alpha_{i2}(x) = |C_{H_i}(x)|\alpha_i(x).$$

Thus, $(\alpha_{i1} - \alpha_{i2})(x) = 0$ if $x \in M_i$ satisfies $C_{H_i}(x) = 1$. This, together with Lemma J(a), proves (b). Q.E.D.

The following lemmas correspond to the lemmas in Section 9 of [FT].

Lemma 11.1. *Let $M \in \mathcal{M}$ and X an F-set of M. For $\alpha \in I_0(X)$, let α^τ be defined as in Definition K. Then, $\alpha^\tau(g) = 0$ if g is not conjugate to an element of $A(x)$ for any $x \in D^*$. If $g \in A(x)$ for $x \in D^*$, then*

$$\alpha^\tau(g) = \alpha(x).$$

In the other words, if $\alpha \in I_0(X)$, the support of the function α^τ is contained in the territory of X, and the function α^τ is well-behaved.

Proof. Suppose that $\alpha^\tau(g) \neq 0$. Then, clearly, g must be conjugate to some element of $M, M_1, \dots,$ or M_n. In order to have $\alpha^G(g) \neq 0$ or $\alpha_{i2}^G(g) \neq 0$, the element g must be conjugate to an element of $X^\sharp$. By Lemma J, if $g \in M_i$ for $i > 0$, g is conjugate to an element of the form hx such that $x \in M \cap M_i$ and $h \in C_{H_i}(x)$. In order to have $\alpha_{i1}^G(g) \neq 0$, g must be conjugate to an element ky such that $y \in X^\sharp$ and k is a $\pi(H_i)$-element commuting with y.

Every element of $X^\sharp$ is conjugate to an element of D^* by Lemma I. It follows that if g is not conjugate to an element of $A(x)$ for any $x \in D^*$, $\alpha^\tau(g) = 0$. This proves the first part.

Suppose that the element $g \in G$ is not conjugate to an element x of M_i with $C_{H_i}(x) \neq 1$ for any $i > 0$. Then, by Lemma L(b), $\sum(\alpha_{i1} - \alpha_{i2})^G(g) = 0$. Hence, we have

$$\alpha^\tau(g) = \alpha^G(g).$$

If g is not conjugate to any element of $X^\sharp$ then $\alpha^G(g) = 0$. Suppose that g is conjugate to an element $x \in X^\sharp$. If x is conjugate to an element y of D_i for some $i > 0$, then $C_G(y) \subseteq M_i$ and $C_{H_i}(y) \neq 1$. This contradicts the hypothesis. By Lemma I, g is conjugate to an element u of D_0. Then,

$$\alpha^\tau(g) = \alpha^G(u) = \alpha(u)$$

by Lemma L (a).

Suppose that $g \in M_i$ and $C_{H_i}(g) \neq 1$. By Lemma J (a), we may assume $g = hx$ with $x \in M \cap M_i$ and $h \in C_{H_i}(x)$. We may also assume that $\alpha^\tau(g) \neq 0$. By the first paragraph of the proof, g is conjugate to an element of $A(y)$ for some $y \in D_j \quad (j \geq 0)$. By Lemma J (b), $j = i$ and $x \in D_i$. Since x is a power of g,

$$C_G(g) \subseteq C_G(x) \subseteq M_i.$$

The conditions (Fii)(e), (a) and (c) yield that for $j \neq i$,

$$(|C_G(x)|, |H_j|) = 1.$$

Since $C_G(g) \subseteq C_G(x)$, g is not conjugate to any element u of M_j with $C_{H_j}(u) \neq 1$ and $j \neq i$. It follows from Lemma L that

$$\alpha^\tau(g) = \alpha^G(g) + (\alpha_{i1} - \alpha_{i2})^G(g).$$

Suppose that $h \neq 1$ in $g = hx$. Then, $\pi(\langle g \rangle) \cap \pi(H_i) \neq \emptyset$. Hence, by (Fii, c), g is not conjugate to any element of $X^\sharp$. Lemma L yields $\alpha^G(g) = 0$. Also, no conjugate of g lies in $M \cap M_i$ because $M \cap M_i$ is a $\pi(H_i)'$-subgroup. Thus, $\alpha_{i2}^G(g) = 0$. If $g_1 = v^{-1}gv$, $v \in G$, and $g_1 \in M_i$, then Lemma J (b) yields $g_1 \in A(M_i)$. Therefore, by (Fii,d), we have $v \in M_i$. This proves

$$\alpha^\tau(g) = \alpha_{i1}^G(g) = \alpha_{i1}(x).$$

Suppose that $h = 1$ in $g = hx$. All conjugates of g are contained in $A(M_i) \setminus H_i$. By (Fii, d),

$$(\alpha_{i1} - \alpha_{i2})^G(g) = (\alpha_{i1} - \alpha_{i2})(x).$$

Since $x \in M \cap M_i$, we have $\alpha_{i1}(x) = \alpha(x)$ and

$$\alpha_{i2}(x) = |C_{H_i}(x)|\alpha(x).$$

By (Fii, e), we have $|C_{H_i}(x)| = |C_G(x) : C_M(x)|$. Therefore, $\alpha^\tau(g) = \alpha(x)$ by Lemma L. Q.E.D.

Lemma 11.2. *Let $M \in \mathcal{M}$ and X an F-set of M. For $\alpha \in I_0(X)$, let α^τ be defined as in Definition K. Then, for $x \in A(M_i)$,*

$$\alpha^\tau(x) = \alpha_{i1}(x).$$

Furthermore, $(\alpha^\tau)_{M_i}$ is a linear combination of characters of M_i/H_i. If M_i is of type II, elements of $(M \cap M_i) \setminus (M_i)'$ are not contained in X and for $y \in M_i \setminus (M_i)'$

$$\alpha^\tau(y) = 0 = \alpha_{i1}(y).$$

Proof. By Lemma J, an element x of M_i is conjugate in M_i to an element of the form hu with $u \in M \cap M_i$ and $h \in C_{H_i}(u)$. Suppose $x \in A(M_i)$. Then $C_{H_i}(x) \neq 1$. Suppose that x is conjugate to an element of $A(y)$ for some $y \in D_j$ $(j \geq 0)$. By Lemma J (b), $u \in D_i$. Hence, by Lemma 11.1,

$$\alpha^\tau(x) = \alpha(u) = \alpha_{i1}(hu) = \alpha_{i1}(x)$$

because x is conjugate to hu in M_i. On the other hand, if x is not conjugate to any element of $A(y)$ for $y \in D^*$, then $u \notin X^\sharp$ and $\alpha^\tau(x) = 0$ by Lemma 11.1. Thus,

$$\alpha^\tau(x) = 0 = \alpha_{i1}(hu) = \alpha_{i1}(x)$$

because $\alpha_{i1}(hu) = \alpha_i(u) = \alpha(u) = 0$.

Suppose that M_i is of type II and $\alpha^\tau(y) \neq 0$ for some $y \in M_i \setminus (M_i)'$. Since M_i is of type II, $\kappa(M_i) = \{q\}$ and $q \in \pi(\langle y \rangle)$ for some prime q and $C_{H_i}(y) \neq 1$. The element y is conjugate to an element of the form hu with $u \in M \cap M_i$ and $h \in C_{H_i}(u)$. By Lemma 11.1, the assumptions of Lemma J (b) are satisfied. Thus, we have $u \in D_i$ and $y \in A(M_i)$ by Lemma J. This is a contradiction because $A(M_i) \subseteq (M_i)'$ in the group M_i of type II. Therefore, $\alpha^\tau(y) = 0$ for $y \in M_i \setminus (M_i)'$.

Since M_i is of type II, $M \cap M_i$ is a Frobenius group. Thus, if y is an element of $M \cap M_i$ outside $(M_i)'$, the order of y is q and $(|C_G(y)|, |H_i|) \neq 1$. Suppose that $y \in X^\sharp$. Then, y must be conjugate to an element $z \in D_i$. It follows that $z \in A(M_i)$ by (Fii, e). Since M_i is of type II, $A(M_i) \subseteq$

$(M_i)'$ and $(M_i)'$ is a Hall subgroup of M_i. This is a contradiction because both z and y have the same order. This proves

$$\alpha_{i1}(y) = \alpha(y) = 0.$$

It remains to prove that $(\alpha^\tau)_{M_i}$ is a linear combination of characters of M_i/H_i. Let θ be any irreducible character of M_i which does not have H_i in its kernel. By Lemma 4.3 [FT], θ vanishes on those elements x of M_i such that $C_{H_i}(x) = 1$. Compute $((\alpha^\tau)_{M_i}, \theta)$.

Suppose that M_i is of type I. Then, θ vanishes off $A(M_i)$ and $(\alpha^\tau)_{M_i}$ agrees with α_{i1} on $A(M_i)$. Hence,

$$((\alpha^\tau)_{M_i}, \theta) = (\alpha_{i1}, \theta) = 0.$$

This proves the assertion. If M_i is of type II, then both $(\alpha^\tau)_{M_i}$ and α_{i1} vanish outside $(M_i)'$. On $(M_i)'$, θ vanishes off $A(M_i)$ and $(\alpha^\tau)_{M_i} = \alpha_{i1}$ on $A(M_i)$. Therefore, we have

$$((\alpha^\tau)_{M_i}, \theta) = (\alpha_{i1}, \theta) = 0.$$

Lemma 11.3. *Let $M \in \mathcal{M}$ and X an F-set of M. For $\alpha \in I_0(X)$, let α^τ be defined as in Definition K. Then,*

$$(\alpha^\tau, 1_G)_G = (\alpha, 1_M)_M$$

where 1_G and 1_M are the principal characters of G and M, respectively.

Lemma 11.4. *Let $M \in \mathcal{M}$ and X an F-set of M. Let Θ be a virtual character of G that is well-behaved. If $\alpha, \beta \in I_0(X)$, then*

$$(\alpha^\tau, \Theta)_G = (\alpha, \Theta_M)_M, \quad (\alpha^\tau, \beta^\tau)_G = (\alpha, \beta)_M.$$

Lemma 11.5. *Let $M \in \mathcal{M}$ and X an F-set of M. Let Θ be a class function of G that is well-behaved. Let G_0 be the territory of the set X. Then, we have*

$$\frac{1}{|G|}\sum\nolimits_{x \in G_0} \Theta(x) = \frac{1}{|M|}\sum\nolimits_{x \in X^\sharp} \Theta(x).$$

The proof of each of the above three lemmas is similar to the corresponding proof of Lemmas 9.3, 9.4, and 9.5 in [FT]. We mention here that the assumption of Θ being well-behaved is essential in the proof.

§12. Coherent Set of Characters

Let $M \in \mathcal{M}$ and let $X$ be an F-set of $M$. In the preceding section, we defined a mapping from $I_0(X)$ to the set of virtual characters of the group $G$. We will denote this mapping $\tau = \tau_M$ in the remainder of this paper. Its main property is stated in Lemma 11.4: *the mapping $\tau$ is an isometry on $I_0(X)$*. It is useful to extend the domain of $\tau$ so as to include some characters. For this purpose, the concept of coherent subsets has emerged; its definition is in Section 10 of [FT]. For the purpose of reference we state the definition.

If $\mathcal{S}$ is a set of virtual characters, we denote by $I_0(\mathcal{S})$ the set of linear combinations of elements of $\mathcal{S}$ with integer coefficients which take the value zero at the identity.

Definition. A set $\mathcal{S}$ of virtual characters of $M$ is said to be coherent if and only if

(1) $I_0(\mathcal{S}) \neq \{0\}$ and $I_0(\mathcal{S}) \subseteq I_0(X)$, and
(2) It is possible to extend $\tau$ form $I_0(\mathcal{S})$ to a linear isometry mapping $\mathcal{S}$ into the set of virtual characters of $G$.

When $\mathcal{S}$ is a coherent set, an extension of $\tau$ to $I(\mathcal{S})$ will be denoted by the same letter $\tau$. The following lemma which corresponds to Lemma 10.4 of [FT] illustrates the usefulness of the concept of coherency and suggests a tight connection between $\lambda$ and λ^τ when λ^τ is defined.

Lemma 12.1. *Let $M \in \mathcal{M}$ and let $X$ be an F-set of $M$. Let $a$ be the least common multiple of all the orders of elements in $X$. Suppose that $\mathcal{S}$ is a coherent set of virtual characters of $M$ such that $\mathcal{S}$ contains at least two irreducible characters. If $\lambda$ is an irreducible character in $\mathcal{S}$, then the values assumed by λ^τ are contained in the field $\mathbb{Q}_a$ of the primitive $a$th roots of unity.*

Proof. Let $n = |G|$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}_a)$. By assumption, $\mathcal{S}$ contains another irreducible character $\mu$. Then,

$$\mu(1)\lambda - \lambda(1)\mu \in I_0(\mathcal{S})$$

and the values assumed by $(\mu(1)\lambda - \lambda(1)\mu)^\tau$ lie in $\mathbb{Q}_a$ by Lemma 11.1. Therefore,

$$\sigma(\mu(1)\lambda^\tau - \lambda(1)\mu^\tau) = \mu(1)\lambda^\tau - \lambda(1)\mu^\tau.$$

Since $\mathcal{S}$ is coherent, λ^τ and μ^τ are either irreducible characters or the negatives of irreducible characters of $G$. The same statement holds for $\sigma(\lambda^\tau)$ and $\sigma(\mu^\tau)$. It follows that $\sigma(\lambda^\tau) = \lambda^\tau$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}_a)$. Thus, the values assumed by λ^τ lie in $\mathbb{Q}_a$. Q.E.D.

It follows easily from the definition that a subset $\mathcal{T}$ of a coherent set $\mathcal{S}$ is coherent provided $I_0(\mathcal{T}) \neq 0$. It is more difficult to decide whether or not the union of two or more coherent sets is coherent. One of the useful necessary conditions is Theorem 10.1 [FT]. We will state the theorem for the purpose of reference and refer the proof as well as the definition of a subcoherent set to the original paper [FT]. The following set of conditions and definitions is used.

Hypothesis 12.2. (i) Let $M \in \mathcal{M}$ and let X be an F-set of M.

(ii) For $1 \leq i \leq k$, $\mathcal{S}_i = \{\lambda_{is} \mid 1 \leq s \leq n_i\} \subseteq I(X)$.

(iii) $\mathcal{S} = \bigcup \mathcal{S}_i$ consists of pairwise orthogonal characters.

(iv) For any i $(1 \leq i \leq k)$, $\mathcal{S}_i$ is coherent with isomrtry τ_i, $\mathcal{S}_i$ is partitioned into sets $\mathcal{S}_{ij}$ such that each $\mathcal{S}_{ij}$ either consists of irreducible characters of the same degree and $|\mathcal{S}_{ij}| \geq 2$ or $(\mathcal{S}_{ij}, \tau_{ij})$ is subcoherent in $\mathcal{S}$ where τ_{ij} is the restriction of τ_i on $\mathcal{S}_{ij}$.

(v) For $1 \leq i \leq k$, $1 \leq s \leq n_i$, there exist integers ℓ_{is} such that

$$1 = \ell_{11} \leq \ell_{21} \leq \cdots \leq \ell_{k1},$$
$$\lambda_{is}(1) = \ell_{is}\lambda_{11}(1), \quad \text{and} \quad \ell_{i1} \mid \ell_{is}.$$

(vi) λ_{11} is an irreducible character of M.

(vii) For any integer m with $1 < m \leq k$,

$$\sum\nolimits_{i=1}^{m-1} \sum\nolimits_{s=1}^{n_i} \frac{\ell_{is}^2}{\|\lambda_{is}\|^2} > 2\ell_{m1}.$$

Theorem 12.3. *Suppose that Hypothesis* 12.2 *is satisfied. Then,* $\mathcal{S}$ *is coherent.*

The isometry on $\mathcal{S}$ is an extension of τ_i and is essentially unique (cf. Theorem 10.1 [FT]). The most important condition is the inequality (vii); we refer it as "the inequality"of Hypothesis 12.2.

For applications in this paper it is convenient to have a specialized set of conditions adapted to our case. To state the results we need further definitions.

Let $\mathcal{S}$ be a set of pairwise orthogonal characters. Define an equivalence relation on $\mathcal{S}$ by the condition that two characters in $\mathcal{S}$ are equivalent if and only if they have the same degree and the same weight. For any normal subgroup A, let $\mathcal{S}(A)$ be the subset of $\mathcal{S}$ consisting of those characters which are equivalent to some character in $\mathcal{S}$ that has A in its kernel.

Consider the following set of conditions.

Hypothesis 12.4. (i) Let $M \in \mathcal{M}$ and let $X = A(M)$.

(ii) Let H be a nilpotent normal subgroup of M such that

$$M_F \subseteq H \subseteq X.$$

Define $K = M$ if M is of type I; otherwise, let $K = M'$.

(iii) $\mathcal{S}$ is a set of characters of M which are induced by nonprincipal irreducible characters of K, each of which vanishes outside X. Assume that $I_0(\mathcal{S}) \neq 0$ and $\mathcal{S}$ consists of pairwise orthogonal characters.

(iv) There exista an integer d such that $d|M : K|$ divides $\lambda(1)$ for every $\lambda \in \mathcal{S}$. Furthermore, $\mathcal{S}$ contains an irreducible character of degree $d|M : K|$.

(v) Define an equivalence relation as before. Then, eqch equivalence class of $\mathcal{S}$ is either subcoherent in $\mathcal{S}$, or consists of irreducible characters and contains at least two characters.

Theorem 12.5. *Suppose that Hypothesis* 12.4 *is satisfied. Let H_1 be a normal subgroup of M such that $H_1 \subseteq H$ and*

$$|H : H_1| > 4d^2|M : K|^2 + 1.$$

If $\mathcal{S}(H_1)$ is coherent and contains an irreducible character of degree $d|M : K|$, then $\mathcal{S}$ is coherent.

This is Theorem 11.1 [FT] of page 817 which is proved under more complex conditions. Actually, we need to consider the case when the group M/H is a Frobenius group with Frobenius kernel K/H and $\mathcal{S}$ is the set of all irreducible characters of M/H that do not contain K/H in their kernel. In this case we will state the following result.

Lemma 12.6. *Let M be of type III or IV and let $\mathcal{S}_0$ be the set of all irreducible characters of M/H that do not contain K/H in their kernel. Then, $\mathcal{S}_0$ is coherent except possibly if K/H is a nonabelian p-group for some prime p and*

$$|(K/H) : (K/H)'| \leq 4|M : K|^2 + 1.$$

In this case, we have $(K/H)' = \Phi(K/H)$.

This is Lemma 11.2 [FT].

Lemma 12.7. *Let $M \in \mathcal{M}$, $H \lhd M$, $H_1 \subseteq H$, $e = |M : H|$, and $h = |H : H_1|$. Let $\mathcal{S}$ be the set of characters of M which are induced by nonprincipal irreducible characters of H. Suppose that H is an F-set of*

M and $\mathcal{S}$ is coherent. Assume further that $H_1 \lhd M$, H/H_1 is abelian, M/H_1 is a Frobenius group with Frobenius kernel H/H_1, and

$$|H : H_1| > (|M : H| + 1)|M : H| + 1.$$

Let $\zeta = (1_H)^M$ and let λ be an irreducible character of M/H_1 with degree e. Then, $\{\mathcal{S}, \zeta\}$ is coherent if we define

$$\zeta^\tau = (\zeta - \lambda)^\tau + \lambda^\tau.$$

Proof. Since M/H_1 is a Frobenius group with Frobenius kernel H/H_1, there are irreducible characters of degree $|M : H| = e$. In fact, there are $n = (h-1)/e$ such characters. Let $\lambda_1 = \lambda, \lambda_2, \ldots, \lambda_n$ be those characters. Then, $\lambda_i - \lambda_j \in I_0(H)$. Thus, $\{\lambda_i^\tau\}$ are defined; they are virtual characters of G with weight one and satisfy

$$(\lambda_i - \lambda_j)^\tau = \lambda_i^\tau - \lambda_j^\tau.$$

Since $\alpha = \zeta - \lambda \in I_0(H)$, Lemma 11.4 yields $\|\alpha^\tau\|^2 = e + 1$,

$$(\alpha^\tau, (\lambda_i - \lambda_j)^\tau) = 0$$

and $(\alpha^\tau, (\lambda - \lambda_i)^\tau) = -1$ if $2 \leq i, j \leq n$. Write

$$\alpha^\tau = \varDelta - \lambda^\tau.$$

Then, if $a_i = (\varDelta, \lambda_i^\tau)$, then $a_1 = a_i$ for all i and

$$\varDelta = 1_G + \sum a_i \lambda_i^\tau + \varDelta_1$$

where $(\varDelta_1, 1_G) = (\varDelta_1, \lambda_i^\tau) = 0$. It follows that

$$1 + (a_1 - 1)^2 + (n-1)a_1^2 + \|\varDelta_1\|^2 = \|\alpha\|^2 = e + 1.$$

If $a_1 \neq 0$, then we have $n - 1 \leq e$. This contradicts the assumption. Thus, $\varDelta$ does not involve any λ_i^τ. Hence, we have

$$\|\varDelta\|^2 = e = \|\zeta\|^2.$$

Let σ be any character of $\mathcal{S}$. We want to prove $(\varDelta, \sigma^\tau) = 0$. By definition, $\sigma = \mu^M$ for some nonprincipal irreducible character μ of H. Since $H \lhd M$, we have $(\zeta, \sigma) = 0$. Suppose that $(\varDelta, \sigma^\tau) \neq 0$. Then, $\sigma \neq \lambda_i$. Choose $\lambda_2 \neq \lambda$ and consider

$$\beta = \mu(1)\lambda_2 - \sigma.$$

Then, $\beta \in I_0(H)$ and Lemma 11.4 yields $(\alpha^\tau, \beta^\tau) = (\alpha, \beta) = 0$ because $\lambda_2 \neq \lambda$ and $(\zeta, \sigma) = 0$. Since $\mathcal{S}$ is coherent,

$$\beta^\tau = \mu(1)\lambda_2^\tau - \sigma^\tau$$

and $(\lambda_1^\tau, \sigma^\tau) = 0$. Then,

$$0 = (\alpha^\tau, \beta^\tau) = (\Delta - \lambda^\tau, \mu(1)\lambda_2^\tau - \sigma^\tau) = -(\Delta, \sigma^\tau) \neq 0.$$

This contradiction proves $(\Delta, \sigma^\tau) = 0$ for every $\sigma \in \mathcal{S}$. Since $\|\Delta\|^2 - \|\zeta\|^2$, the set $\{\mathcal{S}, \zeta\}$ is coherent if we define $\zeta^\tau = \Delta$. Q.E.D.

§13. The Self Normalizing Cyclic Subgroup

Suppose that there is a subgroup in $\mathcal{M}$ that is not of type I. Then, by Theorem I, there is a cyclic subgroup $W = W_1 \times W_2$ such that $W_i \neq 1$ for $i = 1, 2$ and $N_G(W_0) = W$ for any nonempty subset W_0 of $\widehat{W} = W \setminus \{W_1, W_2\}$. Consequences of the existence of such a subgroup are very important. They are discussed in Section 13 of [FT]. We will briefly review them and introduce the notation.

Let ω_{10} and ω_{01} be faithful irreducible characters of W/W_2 and W/W_1, respectively. Define

$$\omega_{ij} = \omega_{10}^i \omega_{01}^j$$

for $0 \leq i < w_1 = |W_1|$ and $0 \leq j < w_2 = |W_2|$. Thus, ω_{00} is the principal character of W. The following lemma is the key to applications and serves as introduction of the family of virtual characters $\{\eta_{ij}\}$ of G.

Lemma 13.1. *The set $\widehat{W}$ is a TI-subset with normalizer W in G (in fact, in any subgroup that contains W). There exists an orthonormal set $\{\eta_{ij}\}$ of virtual characters of G such that for $0 \leq i < w_1$ and $0 \leq j < w_2$, the value assumed by η_{ij}, η_{i0}, η_{0j} lie in $\mathbb{Q}_w$, $\mathbb{Q}_{w_1}$, $\mathbb{Q}_{w_2}$, respectively. We have $\eta_{00} = 1_G$, $\eta_{ij}(x) = \omega_{ij}(x)$ for $x \in \widehat{W}$, and*

$$(\omega_{00} - \omega_{i0} - \omega_{0j} + \omega_{ij})^G = 1_G - \eta_{i0} - \eta_{0j} + \eta_{ij}$$

for $1 \leq i < w_1$ and $1 \leq j < w_2$. In particular, the right side of the above equality is a virtual character that vanishes outside $\mathcal{C}_G(\widehat{W})$. Furthermore, every irreducible character of G distinct from $\{\pm\eta_{ij}\}$ vanishes on $\widehat{W}$.

The proof is in Lemma 13.1 [FT]. The set $\{\eta_{ij}\}$ is orthonormal. Therefore, either η_{ij} or $-\eta_{ij}$ is an irreducible character of G and they are distinct.

Lemma 13.2. *Suppose that a virtual character $\alpha = \sum a_{ij}\omega_{ij}$ of W vanishes on $\widehat{W}$. Then, for all s and t, we have*

$$a_{00} - a_{s0} - a_{0t} + a_{st} = 0.$$

If in addition $\alpha = \beta_1 + \beta_2$ with $\|\beta_1\|^2 = \|\beta_2\|^2 = 2$, then $\alpha = 0$.

Proof. The first part is proved as in the proof of Lemma 13.2 [FT]. The second half follows by case-by-case analysis. Q.E.D.

Theorem I yields that the subgroup W is contained in two subgroups S and T of $\mathcal{M}$ such that neither S nor T is of type I,

$$S \cap T = W, \quad S'W_1 = S, \quad T'W_2 = T,$$

and $S' \cap W_1 = T' \cap W_2 = 1$. We can apply Lemma 13.1 to S and T. Thus, each subgroup has a family of orthonormal virtual characters corresponding to the family $\{\omega_{ij}\}$. The following lemma serves to define the notation.

Lemma 13.3. *Let $M = S$ and let $H = M_F$. Suppose that M is not of type I. Then, $W_2 \subseteq H \subseteq M'$ and $W \setminus W_2$ is a TI-subset of M. There is a complement V of H in M' that is normalized by W_1. The group VW_1 is a Frobenius group with Frobenius kernel V. The group V is nilpotent; if M is of type II, V is abelian.*

Proof. All the conditions follow from the conditions (T1)–(T7) in the definition of groups not of type I in [BG], page 128. Thus, (T1) yields $H \subseteq M'$, while (T4) yields $W_2 \subseteq H$ and $C_{M'}(x) = W_2$ for all $x \in {W_1}^\sharp$. It follows that $C_M(x) = W$ if $x \in W \setminus W_2$. Therefore, $W \setminus W_2$ is a TI-subset of M with normalizer W. The remaining conditions also follow from (T1)–(T7). Q.E.D.

Lemma 13.4. *Let $M \in \mathcal{M}$ be not of type I. Use the notation in Lemma 13.3. Then, M has a family of irreducible characters μ_{ij} $(0 \le i < w_1, 0 \le j < w_2)$ such that for some $\varepsilon_j = \pm 1$*

$$\mu_{ij}(x) = \varepsilon_j \omega_{ij}(x)$$

for all $x \in \widehat{W}$. The family of virtual characters $\{\varepsilon_j\mu_{ij}\}$ is the one corresponding to $\{\omega_{ij}\}$ in Lemma 13.1. For each k, $(\mu_{ik})_{M'} = (\mu_{jk})_{M'}$ and μ_k defined by $\mu_k = (\mu_{ik})_{M'}$ is an irreducible character of M'. Define $\xi_k = \sum_i \mu_{ik}$. Then

$$\xi_k = (\mu_k)^M = \sum\nolimits_i \mu_{ik}.$$

Proof. By Lemma 13.1, there is a family of irreducible characters $\{\mu_{ij}\}$ such that $\pm\mu_{ij}(x) = \omega_{ij}(x)$ for all $x \in \widehat{W}$. Set $q = |W_1|$. Then, M has exactly q linear characters because $M/M' \cong W_1$. Let ζ be the linear character such that $\zeta_W = \omega_{10}$. Then, $\{\zeta^i\}$ $(0 \leq i < w_1)$ is the set of linear characters of M and $(\zeta^i)_W = \omega_{i0}$. Let $\varepsilon_j = \pm 1$ so that

$$\mu_{0j}(x) = \varepsilon_j \omega_{0j}(x)$$

for $x \in \widehat{W}$. Since ζ^i is a linear character, $\zeta^i \mu_{0j}$ is an irreducible character of M. Consider the restriction of $\zeta^i \mu_{0j}$ on $\widehat{W}$. We have for $x \in \widehat{W}$

$$\zeta^i \mu_{0j}(x) = \zeta^i(x)\mu_{0j}(x) = \varepsilon_j \omega_{i0}(x)\omega_{0j}(x) = \varepsilon_j \omega_{ij}(x).$$

Since the characters ω_{ij} are distinct on $\widehat{W}$, Lemma 13.1 yields

$$\zeta^i \mu_{0j} = \mu_{ij}.$$

Thus, $\mu_{ij}(x) = \varepsilon_j \omega_{ij}(x)$ for $x \in \widehat{W}$. This proves that $\{\varepsilon_j \mu_{ij}\}$ is the family corresponding to $\{\omega_{ij}\}$ in M. Clearly, $\mu_k = (\mu_{ik})_{M'}$ is independent of i. By the tensor product formula, we have

$$\xi_k = (\mu_k)^M = \mu_{0k} \otimes (1_{M'})^M = \sum\nolimits_i \mu_{ik}.$$

Since $(\xi_k)_M = q\mu_k$, the orthogonality relations yield

$$q = (\xi_k, \xi_k) = (\mu_k^M, \xi_k) = (\mu_k, q\mu_k)_M = q\|\mu_k\|^2.$$

Therefore, μ_k is an irreducible character of M'. Q.E.D.

The set $W \setminus W_2$ is a TI-subset of M by Lemma 13.3. For each k $(0 \leq k < w_2)$, the set $\{\omega_{ik} \mid 0 \leq i < w_1\}$ is coherent and the characters $\{\omega_{ik}^\tau\}$ are $\{\varepsilon_k \mu_{ik}\}$ (cf. Lemma 13.3 of [FT]).

Lemma 13.5. *Let $M \in \mathcal{M}$ be not of type I and use the notation in Lemma* 13.3. *Then, an irreducible character of M' induces either an irreducible character of M or one of the characters ξ_j $(0 \leq j < w_2)$.*

The proof of Lemma 13.7 of [FT] gives the result.

Lemma 13.6. *Let M and $\{\mu_{ij} \mid 0 \leq i < w_1, 0 \leq j < w_2\}$ be as in Lemma* 13.4. *Suppose that for some i, j, k with $0 \leq i < w_1$, $1 \leq j, k < w_2$, we have $\mu_{ij}(1) = \mu_{ik}(1)$. Then, $\mu_{ij} - \mu_{ik} \in I_0(A_0(M))$ and*

$$(\mu_{ij} - \mu_{ik})^\tau = \pm(\eta_{ij} - \eta_{ik})$$

where η_{ij}, η_{ik} *are virtual characters of* $G$ *defined in Lemma* 13.1.

Proof. The factor group $M/H$ is isomorphic to the group VW_1 which is a Frobenius groupwith Frobenius kernel$V$. By 3.16 of [FT], every nonprincipal irreducible character of M'/H induces an irreducible character of $M$. Therefore, Lemma 13.5 yields that $\mu_{ij}$ with positive $j$ does not contain $H$ in its kernel. By Lemma 4.3 [FT], these $\mu_{ij}$ vanish on $M' \setminus A(M)$. Thus, if $j, k > 0$ and $\mu_{ij}(1) = \mu_{ik}(1)$, then for $X = A_0(M)$,

$$\mu_{ij} - \mu_{ik} \in I_0(X).$$

Since $\tau$ is an isometry on $I_0(X)$, $(\mu_{ij} - \mu_{ik})^\tau$ is the difference of two irreducible characters.

We have $\widehat{W} \subseteq X$. If $x \in \widehat{W}$, then $C_G(x) = W \subseteq M$. Thus, x is not conjugate to any element in $A(y)$ for $y \in D_t$ with $t > 0$. Hence, Lemma 11.1 yields that

$$(\mu_{ij} - \mu_{ik})^\tau(x) = (\mu_{ij} - \mu_{ik})(x)$$

for $x \in \widehat{W}$. It follows that $(\mu_{ij} - \mu_{ik})^\tau$ is the difference of two characters of the form $\pm\eta_{st}$. Since $\eta_{ij}(x) = \omega_{ij}(x)$ for $x \in \widehat{W}$, Lemma 13.2 yields that $(\mu_{ij} - \mu_{ik})^\tau = \pm(\eta_{ij} - \eta_{ik})$. Q.E.D.

Lemma 13.7. *Let* $M$, $\{\mu_{ij}\}$, *and*ξ_k *be as in Lemma* 13.4. *Choose* $k$ *with* $1 \leq k < w_2$. *Let* $\mathcal{S}_1 = \{\xi_j \mid 1 \leq j < w_2, \xi_j(1) = \xi_k(1)\}$. *Then,* $\mathcal{S}_1$ *is coherent and*

$$\xi_j^\tau = \varepsilon \sum\nolimits_i \eta_{ij}$$

for some $\varepsilon = \pm 1$. *Furthermore, if* $\mathcal{S}$ *is the set of characters of* $M$ *which are induced by the nonprincipal irreducible characters of* M' *that vanish outside* $A(M)$, *then* $(\mathcal{S}_1, \tau)$ *is subcoherent in* $\mathcal{S}$.

The proofs of Lemmas 13.9 and 13.10 in [FT] can be adapted to a proof of the above lemma by changing the references suitably (and correcting a misprint).

Lemma 13.8. *Let* $M \in \mathcal{M}$ *be of type II or III,* $H = M_F$, *and* $q = |W_1|$. *For positive integers* $r$ *and* $s$ *with* $r > 1$, *let* $A(r, s)$ *be the set of nonprincipal irreducible characters* $\alpha$ *of* $H$ *such that* $|I(\alpha) : H| = qr$ *and* $\alpha(1) = s$. *Let* $B(r, s)$ *be the set of characters of* $M$ *induced from the irreducible components of* $\alpha^{M'}$ *with* $\alpha \in A(r, s)$. *Then,* $B(r, s)$ *consists of characters of the same degree and* $B(r, s)$ *is coherent.*

Proof. Since $M$ is of type II or III, the factor group M'/H is abelian and $H$ is a Hall subgroup of $M$. We can apply Lemma 4.5 of [FT]. If

$\alpha \in A(r,s)$, then the inertia index of α in M' is r. So, by Lemma 4.5 of [FT], $\alpha^{M'}$ is a sum of exactly r distinct irreducible characters $\theta_1, \dots, \theta_r$ of M' of degree $|M' : H|s/r$.

Lemma 13.5 yields that elements of $B(r,s)$ are irreducible characters or one of the characters ξ_j. Let $\mathcal{S}_1$ be the set of irreducible characters in $B(r,s)$ and let $\mathcal{S}_2$ be the set of ξ_j which are in $B(r,s)$. The characters of $B(r,s)$ have the same degree. By Lemma 4.3 [FT], they vanish outside $A(M)$. If $\beta \in \mathcal{S}_i$ for $i = 1, 2$, then the complex conjugate $\overline{\beta} \in \mathcal{S}_i$. Thus, $I_0(\mathcal{S}_i) \neq \emptyset$. It follows that each subset $\mathcal{S}_i$ is coherent. We want to prove that the union $\mathcal{S}_1 \cup \mathcal{S}_2$ is coherent. Since $\mathcal{S}_1$ consists of irreducible characters of the same degree and $\mathcal{S}_2$ is subcoherent (by Lemma 13.7), Theorem 12.3 yields that $\mathcal{S}_1 \cup \mathcal{S}_2$ is coherent provided the inequality of Hypothesis 12.2 is satisfied. The condition becomes $|\mathcal{S}_1| > 2$ in this case. We need to examine the set of irreducible components $\{\theta_i\}$ of $\alpha^{M'}$. By assumption $|I(\alpha) : H| = qr$ with $r > 1$. We may assume that $Q = W_1 \subseteq I(\alpha)$ because Q is a Hall subgroup of M (by (T1)). Then, $I(\alpha) \cap VW_1 = RQ$ where $R = V \cap I(\alpha)$ is contained in the inertia group I of α in M' and $|R| = r$.

From the proof of Lemma 4.5 [FT] at the beginning of Section 11 of this paper, we have

$$\alpha^I = \gamma_1 + \gamma_2 + \cdots + \gamma_r$$

where γ_i are irreducible characters of I. Since α is Q-invariant, Q permutes these characters $\{\gamma_i\}$. Since $r \equiv 1 \pmod{q}$, one of them, say γ_1, is Q-invariant. We can write $\gamma_i = \gamma_1\mu_i$ where $\mu_1, \dots, \mu_r$ are the set of linear characters of I/H and μ_1 is the principal character. Since $I/H \cong R$, Q acts on the set of nonprincipal characters $\{\mu_2, \dots, \mu_r\}$ without fixed points. Thus, if the notation is such that $\gamma_i^{M'} = \theta_i$, then θ_1 is Q-invariant and all the other θ_i for $i > 1$ induce irreducible characters of $B(r,s)$. Therefore, each $\alpha \in A(r,s)$ contributes one character of $\mathcal{S}_2$ and $(r-1)/q$ characters of $\mathcal{S}_1$. Since $r > 1$ is odd, we have $(r-1)/q \geq 2$. If $\alpha \in A(r,s)$, then $\overline{\alpha} \in A(r,s)$ and $\overline{\alpha}$ is not conjugate to α in M. It follows that $|\mathcal{S}_1| \geq 4$. This proves that $B(r,s)$ is coherent. Q.E.D.

§14. Further Properties of Coherent Sets

In this section, we use the following notation. Let $M \in \mathcal{M}$ and let X be an F-set of M. Let H be one of the supporting subgroups for the set X with $N = N_G(H) \in \mathcal{M}$. Thus, H is N_F, i.e. the largest normal nilpotent Hall subgroup of N. Define N_0 as follows. If N is of type I, let $N_0 = N$, while if N is not of type I, then $N_0 = N'$. It follows from the definition that $A(N) \subseteq N_0$.

The following two lemmas correspond to Lemmas 10.2 and 10.3 of [FT].

Lemma 14.1. *Let M, X, H, N and N_0 be as above. For each nonprincipal irreducible character α of H, let $S(\alpha)$ be the set of irreducible characters of N_0 which are involved in α^{N_0}, and let $T(\alpha)$ be the set of the virtual characters of G of the form $(\theta_1 - \theta_2)^G$ with θ_1, $\theta_2 \in S(\alpha)$. If Θ is a virtual character of G which is orthogonal to the elements of $T(\alpha)$ for all $\alpha \neq 1_H$, then Θ is constant on the cosets of H which lie in $N_0 \setminus H$.*

Proof. The subgroup H is a Hall subgroup of N by definition of groups of type I or II. If N is of type I, then N satisfies the assumptions of Lemma 4.5 [FT]. If N is of type II, then $N_0 = N'$ and N_0/H is abelian by (IIiii). Lemma 4.5 [FT] is applicable to N_0. In all cases, α^{N_0} is a sum of irreducible characters of the same degree with multiplicity one.

Fix a nonprincipal irreducible character α of H. If θ_1, $\theta_2 \in A(\alpha)$.

$$(\Theta_{N_0}, \theta_1 - \theta_2) = (\Theta, (\theta_1 - \theta_2)^G) = 0.$$

Thus, Θ_{N_0} contains each $\theta \in S(\alpha)$ with the same multiplicity. Since the sum of all $\theta \in S(\alpha)$ is α^{N_0}, we have

$$\Theta_{N_0} = \Theta_1 + \beta^{N_0}$$

where Θ_1 is a virtual character of the group N_0/H and β is a virtual character of H. Since β^{N_0} vanishes outside H, Θ_{N_0} is constant on the cosets of H lying in $N_0 \setminus H$. Q.E.D.

Lemma 14.2. *Suppose that M, X, H and N_0 are as in Lemma 14.1. Let $\mathcal{S}$ be a coherent subset of $I(X)$ that contains at least two irreducible characters. For any $\lambda \in \mathcal{S}$, λ^τ is constant on the cosets of H that lie in $N_0 \setminus H$.*

Proof. Take any nonprincipal irreducible character α of H and let $S(\alpha)$ be the set of irreducible characters of N_0 defined in Lemma 14.1. We will show that for θ_1, $\theta_2 \in S(\alpha)$

$$((\lambda^\tau)_{N_0}, \theta_1 - \theta_2) = 0.$$

Assume that this does not hold. Let λ_1,$\lambda_2 \in \mathcal{S}$ be distinct irreducible characters. Then

$$\beta = \lambda_1(1)\lambda - \lambda(1)\lambda_1 \in I_0(X).$$

By Lemma 11.2, $(\beta^\tau)_N$ is a linear combination of characters of N/H. Hence,

$$((\beta^\tau)_{N_0}, \theta_1 - \theta_2) = 0.$$

It follows that

$$((\lambda_1^\tau)_{N_0}, \theta_1 - \theta_2) \neq 0.$$

Similarly, we have $((\lambda_2^\tau)_{N_0}, \theta_1 - \theta_2) \neq 0$.

Suppose that N is of type I so $N_0 = N$. By Lemma 4.3 of [FT], $\theta_i \in S(\alpha)$ vanishes outside $A(N)$. Since θ_1 and θ_2 are equal on H, $\theta_1 - \theta_2$ vanishes outside $A(N) \setminus H$. Since N is of type I, $A(N) = A_0(N)$ and (Fii,d) yields that $A_0(N) \setminus H$ is a TI-subset of G with normalizer N. Hence, $(\theta_1 - \theta_2)^G = \Theta_1 - \Theta_2$ where Θ_i are irreducible characters of G. We have

$$(\lambda_i^\tau, (\theta_1 - \theta_2)^G) = ((\lambda_i^\tau)_N, \theta_1 - \theta_2) \neq 0.$$

It follows that the irreducible character $\pm\lambda_i^\tau$ is either Θ_1 or Θ_2. We may assume that $\lambda_i^\tau = \varepsilon\Theta_i$ for $\varepsilon = 1$ or -1. It is crucial that

$$\lambda_1(1)\lambda_2^\tau - \lambda_2(1)\lambda_1^\tau$$

vanishes at the identity so both λ_1^τ and λ_2^τ are irreducible characters or both of them are not. Then, $\lambda_1(1) = \lambda_2(1)$ and

$$\lambda_1 - \lambda_2 \in I_0(X).$$

By Lemma 11.2, $((\lambda_1 - \lambda_2)^\tau)_N$ is orthogonal to $\theta_1 - \theta_2$. Thus,

$$\begin{aligned} 0 &= ((\lambda_1^\tau - \lambda_2^\tau)_N, \theta_1 - \theta_2) \\ &= (\lambda_1^\tau - \lambda_2^\tau, (\theta_1 - \theta_2)^G) \\ &= (\varepsilon(\Theta_1 - \Theta_2), (\Theta_1 - \Theta_2) = 2\varepsilon. \end{aligned}$$

This contradiction yields that λ^τ is orthogonal to every element in $T(\alpha)$ for any $\alpha \neq 1_H$. By Lemma 14.1, λ^τ is constant on a coset of H that lies in $N \setminus H$.

Assume that N is a group of type II. Suppose that

$$((\lambda^\tau)_{N_0}, \theta_1 - \theta_2) \neq 0$$

for some θ_1, $\theta_2 \in S(\alpha)$. Then, θ_1^N and θ_2^N are distinct characters of N. If they are irreducible, then the previous argument can be applied here. In this case, θ_1^N and θ_2^N vanish outside $A_0(N) \setminus H$, and $A_0(N) \setminus H$ is a TI-subset in G by (Fii,d). Hence, $(\theta_1 - \theta_2)^G$ is a difference of two irreducible characters. We obtain a contradiction as before.

Suppose that θ_1^N is not irreducible. In this case, we are in the situation of Lemma 13.8. The set $A(N)$ is an F-set of N. Let $\sigma = \tau_N$ be the isometry associated with N. Then, by Lemma 13.8, the set $S(\alpha) \cup S(\overline{\alpha})$ is coherent with respect to the isometry σ and for some j. We have

$$(\theta_1^N)^\sigma = \varepsilon \sum_i \eta_{ij}$$

where $\{\eta_{ij}\}$ is the family of characters defined in Lemma 13.1. Thus,

$$(\theta_1^N)^\sigma - (\theta_2^N)^\sigma = \varepsilon \sum_i \eta_{ij} - \Theta_2$$

where $\{\Theta_i\}$ is the family of virtual characters $\{\theta_i^N \mid i > 1\}$.

Since N is of type II, Theorem II (F*iii*) yields that M is a Frobenius group and $X = M_F$. Let $q = |M : M'|$. By Lemma 11.2, elements of N of order q are not contained in X. Since $X = M_F$ is a Hall subgroup of M, no element of X has order q. Lemma 12.1 yields that λ_1^τ as well as λ_2^τ is q-rational.

The virtual character $\theta_1 - \theta_2$ vanishes outside $A(N) \setminus H$. If $g \in A(N) \setminus H$ is conjugate to an element of the form hx where $x \in N \cap M$ and $h \in C_{H_i}(x)$, then Lemma J (b) yields that $x \in D_i$. By Theorem II, we have $N = \mathcal{M}(C_G(x))$. Since g is conjugate in N to an element having this property, $C_G(g) \subseteq N$. In other words, no suppoting subgroup contributes any to $(\theta_1^N - \theta_2^N)^\sigma(g)$. It follows that

$$(\theta_1 - \theta_2)^G = (\theta_1^N - \theta_2^N)^\sigma = \varepsilon \sum_i \eta_{ij} - \Theta_2$$

for some j. We have shown that λ_i^τ is not equal to $\pm\Theta_k$. Since both λ_1^τ and λ_2^τ are not orthogonal to $(\theta_1 - \theta_2)^G$, both λ_1^τ and θ_2^τ are one of $\pm\eta_{ij}$. However, at most one of the characters $\pm\eta_{ij}$ is q-rational for a given j. This contradiction proves that λ^τ is constant on the cosets of H that lie in $N_0 \setminus H$. Q.E.D.

Lemma 14.3. *Let $M \in \mathcal{M}$, X an F-set of M, and let $\mathcal{S}$ be a coherent subset of $I(X)$. If $\mathcal{S}$ contains at least two irreducible characters, every $\lambda \in \mathcal{S}$ satisfies the property that λ^τ is constant on the set of the form $A(x)$ for every $x \in D^*$.*

Proof. The sets $A(x)$ and D^* are defined at the beginning of Chapter II. If $x \in D_0$, then $C_G(x) \subseteq M$. In this case, $A(x) = \{x\}$ and the assertion is trivial. Suppose that $x \in D_i$ for some $i > 0$. Then, $C_G(x) \subseteq M_i$ for some supporting subgroup M_i. By (F*ii*, e), we have

$x \in A(M_i)$. It follows from the definition of the subgroup $(M_i)_0$ at the beginning of this section that $A(M_i) \subseteq (M_i)_0$. Since $A(x)$ is contained in a coset of H_i in $(M_i)_0 \setminus H_i$, Lemma 14.2 yields that λ^τ is constant on the set $A(x)$. Q.E.D.

For any virtual character λ, the set of irreducible characters ρ such that $(\lambda, \rho) \neq 0$ is called the *support* of λ.

The following lemma corresponds Lemma 10.5 of [FT].

Lemma 14.4. *Let X be an F-set of $M \in \mathcal{M}$. Let $\mathcal{S}$ be a coherent set consisting of characters of $I(X)$ with disjoint supports and let Θ be a virtual character of M that is well behaved. Suppose that there is a virtual character θ of M such that for every $\alpha \in I_0(\mathcal{S})$,*

$$(\alpha^\tau, \Theta) = (\alpha, \theta).$$

Then, there is a pair (r, β) of a rational number r and a virtual character β of M such that β is orthogonal to every element of $\mathcal{S}$ and

$$\Theta(g) = \theta(g) + r\beta(g) \quad \textit{for} \quad g \in X^\sharp.$$

Suppose that Θ_1 is a well behaved virtual character of G that is orthogonal to every element of $\mathcal{S}^\tau$, then there is a pair (r_1, β_1) of a rational number r_1 and a virtual character β_1 of M such that β_1 is orthogonal to every element of $\mathcal{S}$ and $\Theta_1(g) = r_1\beta_1(g)$ for $g \in X^\sharp$.

Suppose that $\mathcal{S}$ contains at least two irreducible characters of M. Then, for any $\lambda \in \mathcal{S}$, there is a pair (s, γ) of a rational number s and a virtual character γ of M, depending on λ, such that γ is orthogonal to every element of $\mathcal{S}$ and

$$\lambda^\tau(g) = \lambda(g) + s\gamma(g) \quad \textit{for} \quad g \in X^\sharp.$$

Proof. Since $\mathcal{S}$ is coherent, $I_0(\mathcal{S}) \neq 0$. Therefore, $\mathcal{S}$ contains at least two characters. Let λ, $\mu \in \mathcal{S}$. Then, $\alpha = \lambda(1)\mu - \mu(1)\lambda$ is an element of $I_0(X)$. Since Θ is well behaved, Lemma 11.4 yields

$$(\alpha^\tau, \Theta) = (\alpha, \Theta_M).$$

By assumption, there exists a virtual character θ such that $(\alpha, \Theta_M - \theta) = 0$. For each $\sigma \in \mathcal{S}$, let $\theta(\sigma)$ be the portion of $\Theta_M - \theta$ on the support of σ. Thus,

$$\Theta_M - \theta = \sum_{\sigma \in \mathcal{S}} \theta(\sigma) + \Delta_1$$

where Δ_1 is a linear combination of irreducible characters not involved in any $\sigma \in \mathcal{S}$. Since

$$0 = (\alpha, \Theta_M - \theta) = (\lambda(1)\mu - \mu(1)\lambda, \Theta_M - \theta),$$

the orthogonality relations yield

$$\mu(1)(\lambda, \theta(\lambda)) = \lambda(1)(\mu, \theta(\mu)).$$

Thus, for a rational number s,

$$(\lambda, \theta(\lambda)) = s\lambda(1) \text{ for every } \lambda \in \mathcal{S}.$$

Let $\rho(\sigma)$ be the portion of the regular representation ρ on the support of $\sigma \in \mathcal{S}$. If $\sigma = \sum_i a_i \xi_i$ is the decomposition of σ into the sum of irreducible characters ξ_i, then $\rho(\sigma) = \sum_i \xi_i(1)\xi_i$. Hence,

$$(\sigma, \rho(\sigma)) = \sum_i a_i \xi_i(1) = \sigma(1).$$

Let $\rho = \sum_\sigma \rho(\sigma) + \Delta_2$. Then, Δ_2 is a linear combination of irreducible characters not involved in any $\sigma \in \mathcal{S}$. Set $s = m/n$ with integers m, n and define

$$r = 1/n \quad\text{and}\quad \beta = \sum_{\sigma \in \mathcal{S}} (n\theta(\sigma) - m\rho(\sigma)) - m\Delta_2 + n\Delta_1.$$

Then, for $x \in X^\sharp$,

$$r\beta(x) = (\sum \theta(\sigma) + \Delta_1)(x) - s\rho(x) = \Theta_M(x) - \theta(x).$$

We compute (σ, β). Since the supports of elements of $\mathcal{S}$ are disjoint, we have

$$(\sigma, \beta) = n(\sigma, \theta(\sigma)) - m(\sigma, \rho(\sigma)) = 0.$$

This proves the first part.

For the second part, $\theta_1 = 0$ satisfies the assumption of the first part for Θ_1 since $(\alpha^\tau, \Theta) = 0$ for every $\alpha \in I_0(X)$. For the third part, Lemma 11.4 yields with $\Theta = \lambda^\tau$,

$$(\alpha^\tau, \Theta) = (\alpha^\tau, \lambda^\tau) = (\alpha, \lambda)$$

for all $\alpha \in I_0(X)$. The first part applies. Q.E.D.

§15. Characters of Subgroups of Type I

Let $M \in \mathcal{M}$ be a subgroup of type I. Let $H = M_F$, $X = A(M)$, and let $\mathcal{S}$ be the set of irreducible characters of M that do not have H in their kernel. Let E be a complement of H in M. By (I*iii*), E contains a subgroup E_0 of the same exponent as E such that HE_0 is a Frobenius group with Frobenius kernel H. With the notation introduced here we prove the following lemma.

Lemma 15.1. *Let $M \in \mathcal{M}$ be a subgroupof type I. Then the set $\mathcal{S}$ defined above satisfies Hypothesis* 12.4 *with $H = M_F$, $K = M$ and $d = |E_0|$.*

Proof. If $\lambda \in \mathcal{S}$, Lemma 4.3 of [FT] yields that λ vanishes outside X. If $\lambda \in \mathcal{S}$, then the complex conjugate character $\overline{\lambda}$ is different from λ and $\overline{\lambda} \in \mathcal{S}$. Thus, $I_0(\mathcal{S}) \neq 0$ and $\mathcal{S}$ satisfies (*iii*) of Hypothesis 12.4. Since $\mathcal{S}$ consists of irreducible characters, $\mathcal{S}$ satisfies (*v*).

The definition of groups of type I implies that elements of $A(M) \cap E$ are τ_2-elements in the notation of §6. Therefore, $E = AB$ with $(|A|, |B|) = 1$ such that A is abelian and B is a Z-group (cf. Hypothesis 28.1 [FT]). In fact, $E = E_1E_2E_3$, E_2 is abelian, and E_1 and E_3 are cyclic groups of relatively prime order by Lemmas 6.1 and 6.8, and Theorem 6.7. We may take $A = E_2$ and $B = E_1E_3$. Since E_0 has the same exponent as E, the order of B divides $|E_0|$. Conjugacy of Hall subgroups in a solvable group yields that we may assume $B \subseteq E_0$. Furthermore, we may assume that A contains a Hall $\pi(A)$-subgroup of E_0.

Since HE_0 is a Frobenius group with Frobenius kernel H, no element of E_0 stabilizes any nonprincipal irreducible character of H. Thus, for any $\lambda \in \mathcal{S}$, the number of conjugate characters $|M : I(\lambda)|$ is divisible by $|E_0|$. By (I*ii*), the normal closure of $I(\lambda)/H$ is abelian. Therfore, Lemma 4.5 [FT] yields that λ^M is a sum of irreducible characters of degree $|M : I(\lambda)|\lambda(1)$. Thus, $d = |E_0|$ divides $\lambda(1)$ for every $\lambda \in \mathcal{S}$.

It remains to prove that $\mathcal{S}$ contains an irreducible character of degree exactly $d = |E_0|$. This is proved as in Lemma 28.1 of [FT]. Let $E = AB$ as above. Since H is nilpotent, $H/\Phi(H)$ is elementary abelian. Let L be a maximal A-invariant subgroup such that $\Phi \subseteq L \subset H$, and let $A_1 = C_A(H/L)$. Then, A acts on H/L irreducibly and A/A_1 is cyclic. Since E_0 has the same exponent as E and $E_0 \cap A_1 = 1$, $|A/A_1|$ is equal to the exponent of A. This implies that $E_0A_1 = E$. Let λ be a nonprincipal linear character of H/L. Then, $HA_1 = I(\lambda)$. Therefore, Lemma 4.5 [FT] yields that λ^M is a sum of irreducible characters of degree exactly equal to $|E_0| = d$. Q.E.D.

Remark. At the final stage of proof, Lemma 4.5 [FT] yields that λ^M is a sum of exactly $|A_1|$ irreducible characters. We have

$$|A_1| = |E : E_0|.$$

Thus, M has at least $2|E : E_0|$ irreducible characters of degree d.

Theorem 15.2. *Let $M \in \mathcal{M}$ be a group of type I and let $\mathcal{S}$ be as in Lemma* 15.1. *If $H/\Phi(H)$ is not a chief factor of M, then $\mathcal{S}$ is coherent. The assumption on H is satisfied if $Z(E)$ contains an element x such that $C_H(x) \not\subseteq H'$ and $C_H(x) \neq H$.*

Proof. Let $d = |E_0|$. Since E_0 acts regularly on H, each chief factor of M in H has order at least $2d + 1$ It follows that $|H : H'| > 4d^2 + 1$. By Theorem 12.5, $\mathcal{S}$ is coherent if $\mathcal{S}(H')$ is coherent.

Let $\mathcal{S}_1, \dots, \mathcal{S}_k$ be the equivalence classes of characters in $\mathcal{S}(H')$. Each $\mathcal{S}_i$ is a set of irreducible characters of the same degree. If $\lambda \in \mathcal{S}_i$, then $\overline{\lambda} \in \mathcal{S}_i$. Thus, $|\mathcal{S}_i| \geq 2$. Hence, by Lemma 10.1 [FT], each $\mathcal{S}_i$ is coherent. Let $n_i = |\mathcal{S}_i|$ and let $d\ell_i$ be the common degree of the characters of $\mathcal{S}_i$. We may choose the notation so that

$$\ell_1 = 1 < \ell_2 < \cdots < \ell_k.$$

Lemma 4.5 [FT] yields that for any nonprincipal linear character α, the irreducible component of α^M has degree $|M : I(\alpha)|$. Since $d = |E_0|$, we get $\ell_i \leq |E : E_0|$.

If $\mathcal{S}(H')$ is not coherent, Theorem 12.3 yields that the inequality of Hypothesis 12.2 is violated, i.e. we have

$$\sum_{i=1}^{m-1} n_i \ell_i^2 \leq 2\ell_m \leq 2|E : E_0|$$

for some m.

We define $\overline{H} = H/\Phi(H)$ and use the *bar* convention. By assumption, we have a normal subgroup H_1 of H such that $\overline{H_1}$ is a nontrivial proper E-invariant subgroup. Since $(|E|, |H|) = 1$, there is a complementof $\overline{H_1}$ in $\overline{H}$. Thus, there is an E- invariant subgroup H_2 such that $H_1H_2 = H$ and $H_1 \cap H_2 = \Phi(H)$. Then, H_2 is a normal subgroup of M. We have remarked that there are at least $2|E : E_0|$ irreducible characters of degree d having H_1 in their kernel and at least $2|E : E_0|$ irreducible ones of degree d having H_2 in their kernel. It follows that $4|E : E_0| \leq n_1$. This contradicts the earlier inequality. Therefore, $\mathcal{S}$ is coherent.

Suppose that $Z(E)$ contains an element x such that $C_H(x) \not\subseteq H'$ and $C_H(x) \neq H$. Let $\overline{C} = C_{\overline{H}}(x)$. Then, $\overline{H} = \overline{C} \times [\overline{H}, x]$. If $\overline{C} = \overline{H}$, then $C_H(x)\Phi(H) = H$. This implies $C_H(x) = H$. Therefore, $\overline{C} \neq \overline{H}$. If $\overline{C} = 1$, then $C_H(x)(x) \subseteq \Phi(H)$. This is impossible as $C_H(x)H'$ corresponds to a direct factor of H/H'. Since $x \in Z(E)$, $\overline{C}$ is M-invariant. Hence, $\overline{H} = H/\Phi(H)$ is not a chief factor of M and the first part of Theorem 15.2 yields that $\mathcal{S}$ is coherent. Q.E.D.

§16. Characters of Subgroups of Type III and IV

The following notation is used as in §29 [FT]. Let $S = S'Q^*$ be a subgroup of type II, III, or IV where $q = |Q^*|$ is a prime and Q^* corresponds to the subgroup W_1 in the definition of the groups of type II, III, or IV. Let $H = S_F$ and let V be a Q^*-invariant complement of H in S. We have a subgroup T not of type I paired with S in Theorem I.

Let $\pi(H) = \{p_1, \ldots, p_t\}$ and for $1 \leq i \leq t$, let $P_i \in Syl_{p_i}(H)$, $C_i = C_V(P_i)$, and $C = \bigcap_{i=1}^t C_i$. Let $|H| = h$, $|V| = v$, $|Q^*| = q$, $|C_i| = c_i$ $(1 \leq i \leq t)$, and $|C| = c$.

Let $\mathcal{S}_0$ be the set of characters of S which are induced by non-principal irreducible characters of S'/H and $\mathcal{S}$ the set of characters of S induced by irreducible characters of S' that do not have H in their kernel.

Theorem 16.1. (a) *If S is of type III, then $\mathcal{S}_0 \cup \mathcal{S}$ is coherent except possibly if H is abelian with $|H| = p^q$ for some prime p, VQ^* acts irreducibly on H, and $C = 1$.* (b) *If S is of type IV, then $\mathcal{S}_0 \cup \mathcal{S}$ is coherent except possibly if H is abelian with $|H| = p^q$ for some prime p, VQ^* acts irreducibly on H, $C = V'$, and $\mathcal{S}_0$ is not coherent.*

This is Theorem 29.1 [FT]. We paraphrase a part of their proof.

Throughout this section we assume that S is of type III or IV. By Theorem I, T is of type II. Therefore W_2 is of prime order. Let $p = |W_2|$ and write $p = p_1$, $P = P_1$, and $P^* = W_2$. Since S is of type III or IV, we have $S'' \subseteq F(S) = HC_S(H) = HC \subseteq S'$ by (T3).

We will prove Theorem 16.1 in 6 steps.

Lemma 16.2. *Hypothesis* 12.4 *is satisfied for S, $F(S)$, and $\mathcal{S}_0 \cup \mathcal{S}$ in place of M, H, and $\mathcal{S}$, respectively, with $d = 1$.*

Proof. By the definition of groups of type III or IV, $H \subseteq F(S)$, $F(S) \neq S'$, and S/H is a Frobenius group with Frobenius kernel S'/H. Thus, $\mathcal{S}_0$ contains an irreducible character of degree $q = |S : S'|$. Every character of $\mathcal{S}_0 \cup \mathcal{S}$ is induced by an irreducible character of S'. So, the degree is a multiple of q. Thus, (iv) of Hypothesis 12.4 is satisfied.

By Lemmas 13.5 and 13.7, each equivalence class of $\mathcal{S}_0 \cup \mathcal{S}$ is either subcoherent or consists of irreducible characters. An equivalence class contains λ as well as $\overline{\lambda}$. Thus, the condition (v) is satisfied. Q.E.D.

Lemma 16.3. *Let $F = F(S)$ and let $\mathcal{S}(F')$ be the subset of $\mathcal{S}_0 \cup \mathcal{S}$ consisting of those characters which are equivalent to some character in $\mathcal{S}_0 \cup \mathcal{S}$ that has F' in its kernel. If $\mathcal{S}(F')$ is coherent, then $\mathcal{S}_0 \cup \mathcal{S}$ is coherent.*

Proof. Since $W_2 \subseteq P$, V does not centralize P. Then, the Frobenius group VQ^* acts nontrivially on $P/\Phi(P)$. This implies $|P\colon \Phi(P)| \geq p^q$. Thus,

$$|F\colon F'| \geq |P\colon \Phi(P)| \geq p^q > 4q^2 + 1$$

by (5.9) of [FT]. Theorem 12.5 yields Lemma 16.3. Q.E.D.

Lemma 16.4. *If $\mathcal{S}(F')$ is not coherent, then $S'' = F$.*

Proof. By Corollary 9.6, W_2 is a subgroup of S''. It follows that S/S'' is a Frobenius group with Frobenius kernel S'/S''. The proof of Lemma 29.3 [FT] proves Lemma 16.4. Q.E.D.

Lemma 16.5. *If $\mathcal{S}(F')$ is not coherent, then $H = P$, $P' = \Phi(P)$, $|P : P'| = p^q$, $P^* \cap \Phi(P) = 1$, and $C = V'$. Furthermore, VQ^* acts irreducibly on P.*

Proof. The proof is the same as that of Lemma 29.4 [FT]. Since $|P\colon \Phi(P)| = p^q$ and V does not act trivially, VQ^* acts irreducibly on $P/\Phi(P)$. Q.E.D.

Lemma 16.6. *If $\mathcal{S}(F')$ is not coherent, then P is an elementary abelian p-group of order p^q.*

Proof. See the proof of Lemma 29.5 [FT]. I will paraphrase the part of the proof concerning the linear characters s_i of V modulo p.

For $u, v \in V$, we have $s_i(uv) \equiv s_i(u)s_i(v) \pmod p$. Thus, s_i are indeed linear characters modulo p. None of these characters is trivial because $C_{P/P'}(V) = 1$. If we take the notation that a generator w of Q^* shifts the one-dimensional V-modules downwards $i \to i - 1$, then

$$s_{i+1}(v) \equiv s_i(w^{-1}vw) \quad \text{for all} \quad v \in V.$$

If $s_i s_j = 1$ for some $i < j = i + k$, then for $x = w^k$, $s_j(v) = s_i(x^{-1}vx)$ so $1 = s_i(v)s_j(v) = s_i(vx^{-1}vx)$ for all v. We claim that the mapping defined by $\theta : v \longrightarrow vx^{-1}vx$ induces an injection on the group V/V'. Suppose that $\theta(v) \equiv \theta(u) \pmod{V'}$. Then,

$$x^{-1}vu^{-1}x \equiv v^{-1}u \equiv uv^{-1}[v^{-1}, u] \equiv (vu^{-1})^{-1}$$

modulo V'. Since the group VQ^*/V' has odd order, this happens only when $vu^{-1} \equiv 1 \pmod{V'}$. Thus, θ induces an injection on a finite set. Therefore, θ induces a surjective map. Then, for every $v \in V$, there are elements $u \in V$ and $z \in V'$ such that $v = \theta(u)z$. Since $s_i(z) = 1$, we have $s_i(v) = s_i(\theta(u)) = 1$. This contradicts the statement that s_i is not trivial. Thus, $s_i s_j \neq 1$ for any i, j with $1 \leq i, j \leq q$.

The remaining proof is given in [FT]. Q.E.D.

Lemma 16.7. *If $\mathcal{S}(F')$ is not coherent and $C \neq 1$, then $\mathcal{S}_0$ is not coherent.*

Proof. This is a paraphrase of the proof of Lemma 29.6 [FT]. Assume that $\mathcal{S}_0$ is coherent. Note that S/H is a Frobenius group with Frobenius kernel S'/H that is a nonabelian group of order v. Thus, $\mathcal{S}_0$ is the set of all irreducible characters of S/H that do not have S' in their kernel.

Let $\mathcal{S}_1 = \mathcal{S}_0$ and let $\mathcal{S}_2, \dots, \mathcal{S}_k$ be the equivalence classes of $\mathcal{S}(F') - \mathcal{S}_0$ such that every character of $\mathcal{S}_m$ has degree $l_m q$ for $m \geq 2$ and $l_2 \leq l_3 \leq \cdots \leq l_k$. By assumption, $\mathcal{S}(F')$ is not coherent. We check the validity of Hypothesis 12.2. If $\lambda \in \mathcal{S}_i$, then $\overline{\lambda} \in \mathcal{S}_i$. Now, Lemmas 13.5 and 13.7 yield the condition (iv). Since $\mathcal{S}_0$ contains an irreducible character of degree d, all conditions of Hypothesis 12.2 except the inequality are satisfied. Since $\mathcal{S}(F')$ is not coherent, the inequality must be violated. If $\lambda \in \mathcal{S}_m$ for $m \geq 2$, then λ is equivalent to a constituent μ of a character induced by a linear character of F and $\lambda(1) = \mu(1)$. Since $V' = C$ by Lemma 6.5 and $F = HC$, the degree $l_m q$ of μ satisfies $l_m \leq v/c$.

Consider the contribution to the left side of the inequality from $\mathcal{S}_0$. A character λ_{1s} of $\mathcal{S}_0$ is irreducible of degree $l_{1s}q$. Since S/H is a Frobenius groupwith Frobenius kernelS'/H, $\mathcal{S}_0$ is the set of irreducible characters of S/H that do not have S' in their kernel. There are exactly q other characters of degree 1. Thus,

$$\sum_s (l_{1s}q)^2 + q = qv, \quad \text{or} \quad \sum_s \frac{l_{1s}^2}{\|\lambda_{1s}\|^2} = \frac{v-1}{q}.$$

Thus, we obtain $v - 1 \leq 2l_m q \leq 2qu/c$. Since $1 < c < u$ and $c \equiv 1 \pmod{2q}$, we get a contradiction. Q.E.D.

Suppose that S is of type III or IV. If $\mathcal{S}_0 \cup \mathcal{S}$ is not coherent, $\mathcal{S}(F')$ is not coherent by Lemma 16.3. Then, by Lemmas 16.5 and 16.6, $H = P$ is elementary abelian of order p^q and VQ^* acts irreducibly on P. If S is of type III, then V is abelian so $C = V' = 1$ by Lemma 16.5. If S is of type IV, then $C = V'$ and $\mathcal{S}_0$ is not coherent by Lemma 16.7. This proves Theorem 16.1. Q.E.D.

§17. Characters of Subgroups of Type II, III and IV

We will use the notation introduced at the beginning of §16. In addition, we denote $a = \exp V/V'$.

In the first part of this section, we assume that

(1) S is a subgroup of type II, III, or IV,
(2) $\mathcal{S}$ is not coherent if S is of type III or IV, and
(3) V/V' has exponent a.

In this section, we denote by $\mathcal{S}(A)$ the set of characters in $\mathcal{S}$ which have A in their kernel. This usage is different from the one used in §16. We follow the argument of §30 [FT].

Lemma 17.1. *The degree of every character in $\mathcal{S}$ is divisible by aq.*

Proof. Every character in $\mathcal{S}$ is a constituent of a character of S induced by a nonprincipal character θ of H. Let $V_1 = V \cap I(\theta)$ and let $b = |V : V_1|$. If S is of type II or III, V is abelian by (II*iii*) or (III*iii*). By Lemma 4.5 [FT], it suffices to show that a divides b.

The group V_1 centralizes a section of H. Then, $V_1 \subseteq A(S)$ as shown in the proof of Lemma 30.1 [FT]. Consider V^b and suppose that $V^b \neq 1$. Then, $V^b \subseteq V_1 \subseteq A(S)$. If S is of type II, the modified (II*v*) yields $N_G(V^b) \subseteq S$. Since V^b char V, we get $N_G(V) \subseteq N_G(V^b) \subseteq S$ in contradiction to (II*iv*). If S is of type III, $V^b \neq 1$ is a normal subgroup of the Frobenius group VQ^*. Since $\mathcal{S}$ is not coherent, Theorem 16.1 yields that VQ^* acts irreducibly on H. Then, the abelian group $V^b \neq 1$ acts semisimply and one component is trivial as $V^b \subseteq V_1$. It follows that V^b acts trivially on H. Therefore, $V^b \subseteq C$, contradicting Theorem 16.1.

Suppose that S is of type IV. Then, Theorem 16.1 yields that $\mathcal{S}_0$ is not coherent. By Lemma 12.6, $V(\cong S'/H)$ is a nonabelian r-group for some prime r and $V' = \Phi(V)$. In this case V/V' is an elementary abelian r-group, so $a = r$. Since VQ^* acts irreducibly on H, we have $C_H(V) = 1$. It follows that V does not stabilize any nonprincipal character of H. Hence, the degree of a character in $\mathcal{S}$ is divisible by r. This proves Lemma 17.1. Q.E.D.

Lemma 17.2. *For $1 \leq i \leq t$, $|P_i : \Phi(P_i)| = {p_i}^q$, VQ^* acts on $P_i/\Phi(P_i)$ irreducibly, and V/C_i has exponent a.*

The proof of Lemma 30.2 [FT] applies.

Lemma 17.3. *For $1 \leq i \leq t$, either $a \mid (p_i - 1)$ or $a \mid ({p_i}^q - 1)$ and $(a, p_i - 1) = 1$. In the second case, V/C_i is a cyclic group of order a and acts irreducibly on $P_i/\Phi(P_i)$.*

Cf. Lemma 30.3 [FT].

We prove two (known) properties of finite abelian p-groups for some prime p.

Lemma O. (1) *Let A be a finite abelian p-group such that $\Phi(A)$ is a maximal characteristic subgroup of A. Then, A is a direct product of cyclic groups of the same order.*

(2) *Suppose that an abelian group U acts on a finite abelian p-group A. Assume that the exponent of U divides $p - 1$. Then, A is a direct product of U-invariant cyclic subgroups.*

Lemma 17.4. *Suppose $(a, p_i - 1) = 1$ for some i, $1 \leq i \leq t$. Let $H_1 = P_i' \Pi_{j \neq i} P_j$. Then, $|H : H_1| = |P_i : P_i'| = p^{qm_i}$ for some integer m_i. Furthermore, $\mathcal{S}(H_1)$ contains at least*

$$\frac{1}{q}\{\frac{(p_i^{qm_i} - 1)c_i}{a} - (p_i^{m_i} - 1)\}$$

irreducible characters of degree aq and at least $p_i^{m_i} - 1$ characters of weight q and degree aq.

Proof. I will paraphrase the proof of Lemma 30.4 [FT]. Lemma 17.3 yields that V/C_i is cyclic. Suppose that S is of type IV. Then, by Theorem 16.1, $\mathcal{S}_0$ is not coherent. We showed in the proof of Lemma 17.1 that $V' = \Phi(V) = C = C_i$. Then, $V/\Phi(V)$ is cyclic. Hence, V is cyclic. This is a contradiction because V is nonabelian for type IV. Therefore, S is of type II or III, and V is abelian. Lemma 17.3 yields that V acts irreducibly on $P_i/\Phi(P_i)$. It follows from Lemma M that $H/H_1 (\cong P_i/P_i')$ is a direct product of q cyclic groups of order $p_i^{m_i}$. On each chief factor in H/H_1, Q^* centralizes a subgroup of order p_i. Since $C_H(Q^*)$ is cyclic by Theorem C (2), we have $|C_{H/H'}(Q^*)| = p_i^{m_i}$.

The group HC_i/H_1 is the direct product of H/H_1 and H_1C_i/H_1. Both factors are abelian. Since V/C_i acts regularly on H/H_1, every linear character α of HC_i/H_1 that does not have H/H_1 in its kernel has exactly $a = |V : C_i|$ conjugates. Hence, α induces an irreducible character of degree a. There are at least $(p_i^{m_i q} - 1)c_i/a$ distinct irreducible characters of degree a. Among them, precisely $p_i^{m_i}-1$ are Q^*-invariant. The assertions of Lemma 17.4 follow from Lemma 13.5. Q.E.D.

Lemma 17.5. *Suppose that $a \mid (p_i - 1)$ for some i with $1 \leq i \leq t$. Let H_1 be as in Lemma 17.4. Then, $|H : H_1| = |P_i : P_i'| = p_i^{m_i q}$ for some integer m_i and $\mathcal{S}(H_1)$ contains at least*

$$\frac{(p_i^{m_i}-1)}{a}\frac{v}{av'}$$

irreducible characters of degree aq where $|V'| = v'$.

Proof. The Frattini factor group of H/H_1 is isomorphic to $P_i/\Phi(P_i)$. By Lemma 17.2, VQ^* acts irreducibly on $P_i/\Phi(P_i)$. Since $a \mid (p_i - 1)$, H/H_1 is a direct product of V-invariant cyclic groups of the same order. There are V-invariant subgroups K_1 and K_2 such that H/K_2 is a cyclic group of order p^{m_i}, $K_1K_2 = H$, and $K_1 \cap K_2 = H_1$. Let $V_1 = C_V(H/K_2)$. Then, V/V_1 is a subgroup of $\mathrm{Aut}(H/K_2)$. Hence, V/V_1 is cyclic, so $|V : V_1| \leq a$.

Consider the factor group $L = HV_1/K_2V'$. Since $V_1 \supseteq V'$ and V_1 centralizes H/K_2, L is abelian. Let $\mathcal{L}$ be the set of linear characters of L which do not contain H in their kernel. If $\lambda \in \mathcal{L}$, λ induces an irreducible character θ of degree $|V : V_1|$ in $\mathcal{S}$. By Lemma 17.1, $|V : V_1| \geq a$. Hence, $|V : V_1| = a$. Suppose that $\theta^S = \lambda^S$ is not irreducible or for $\lambda, \mu \in \mathcal{L}$, they induce the same irreducible character of $\mathcal{S}$. In the first case, λ is Q^*-invariant, so $H \cap \ker\lambda$ is Q^*-invariant. In the second case, λ and μ are Q^*-conjugate so $H \cap \ker\lambda$ and $H \cap \ker\mu$ are Q^*-conjugate. However, $H \cap \ker\lambda$ and $H \cap \ker\mu$ have the same index and both contain K_2. Since H/K_2 is a cyclic group of order $p_i^{m_i}$, there is a unique subgroup of each index. It follows that $H \cap \ker\lambda$ is Q^*- invariant. Since every subgroup of H that contains K_2 is V-invariant, H contains a subgroup of index p_i that is VQ^*-invariant. This contradicts Lemma 17.2.

We have $|\mathcal{L}| = l = (p^{m_i} - 1)v/av'$ and the characters of $\mathcal{L}$ produce exactly l/a distinct irreducible characters of degree aq in $\mathcal{S}(H_1)$.

Q.E.D.

Lemma 17.6. *If $\mathcal{S}(H')$ contains no irreducible character of degree aq, then $t = 1$, $P_1' = \Phi(P_1)$, $a = u = (p_1{}^q - 1)/(p_1 - 1)$, and $c = c_1 = 1$. Furthermore, $\mathcal{S}(H')$ is coherent and S is not of type IV.*

Proof. See the proof of Lemma 30.6 [FT]. We note that in the following equation $a = (p_i{}^q - 1)/(p_i - 1)$, p_i is determined by a. This remark yields $t = 1$. Since $c = 1$, $V' = C = 1$, and S is not of type IV. Since $\mathcal{S}(H')$ contains all the characters of degree aq and weight q,

$\mathcal{S}(H')$ consists of characters ξ_j, $0 \leq j < p$. By Lemma 13.7, $\mathcal{S}(H')$ is coherent. Q.E.D.

In the remainder of this section we assume that

(2)$'$ $\mathcal{S}$ is not coherent

in place of the condition (2). Note that $S'' \subseteq F(S) = HC \subseteq S'$ by Theorem A (7). Define $F = F(S)$.

Lemma 17.7. *If $\mathcal{S}(H')$ is not coherent, then $H = P_1$, $C_1 = 1$, $a = (p-1)/2$, $p = p_1$, $v \neq a$, and $\Phi(P_1) = P_1'$. The degree of every character in $\mathcal{S}(H')$ is either aq or vq/c, and $\mathcal{S}(H')$ contains exactly $2v/a$ irreducible characters of degree aq. Furthermore, S is not of type IV.*

Proof. The proof of Lemma 30.7 [FT] shows that if $\mathcal{S}(F')$ is not coherent, the degree of any character in $\mathcal{S}(F')$ is either aq or uq where $u = v/c$, and the other conditions in Lemma 17.7 are satisfied. If S is of type II or III, then V is abelian. Hence, $F' = H'$ because $F = H \times C$ with C abelian. Thus, the result is proved if S is of type II or III.

It remains to show that if $\mathcal{S}(H')$ is not coherent, then S is not of type IV. Suppose that S is of type IV. Since $\mathcal{S}(H')$ is not coherent, $\mathcal{S}_0 \cup \mathcal{S}$ is not coherent. Theorem 16.1 (b) yields that $H = P$ is elementary abelian, VQ^* acts irreducibly on P, and $\mathcal{S}_0$ is not coherent. Since $S/H \cong VQ^*$ is a Frobenius group, Lemma 12.6 implies that V is an r-group for some prime r and $V' = \Phi(V)$. It follows that V/V' is an elementary abelian group of order r^n. Thus, the exponent of V/V' is r; we have $r = a$. We claim that $n \leq 2$. Suppose that $n > 2$. Since $H = P$ is elementary abelian, so is F/C. Let θ_1 and θ_2 be linear characters of F/C with exactly a conjugates in S', so each induces an irreducible character of degree a. Suppose that $\theta_1\theta_2$ is not the principal character. Then, $I(\theta_1\theta_2) \supseteq I(\theta_1) \cap I(\theta_2)$. Since both $I(\theta_1)$ and $I(\theta_2)$ have index r, the index of $I(\theta_1\theta_2)$ in S' is at most r^2. Since the index of the inertia group of a nonprincipal character is either r or r^n, $|S' : I(\theta_1\theta_2)| = r$. Thus, the set of linear characters with at most r conjugates forms a VQ^*-invariant subgroup of the character group of F/C. Since VQ^* acts irreducibly on F/C, every nonprincipal character of F/C has exactly r conjugates. It follows from the permutation lemma that the number of orbits on the character group by the action of V is the same as the number of orbits on $P^\sharp$. Since each orbit has at least r elements, every element of $P^\sharp$ has exactly r conjugates. Take an element $x \neq 1$ in P^*. Then, $C_V(x) = X$ is a maximal subgroup of V. Since x is Q^*-invariant, so is X. Hence, $C_P(X)$ is VQ^*-invariant. Since VQ^* acts on P irreducibly, we have $C_P(X) = P$. This contradicts Theorem 16.1

because $C = C_V(P) = V'$. Therefore, we have $n \leq 2$. If $n = 1$, $V/\Phi(V)$ is cyclic. This implies that V is cyclic. This contradicts the definition of a group of type IV (IV*iii*). If $n = 2$, Lemma 11.3 [FT] yields that $\mathcal{S}_0$ is coherent. This final contradiction shows that S is not of type IV if $\mathcal{S}(H')$ is not coherent. Q.E.D.

Lemma 17.8. *The family $\mathcal{S}(H')$ is coherent.*

Proof. Suppose that $\mathcal{S}(H')$ is not coherent. Lemma 17.7 yields that $H = P_1$, $C_1 = 1$, $a = (p-1)/2$, $p = p_1$, $v \neq a$, $P_1' = \Phi(P_1)$, and S is of type II or III. The last condition implies that the subgroup V is abelian. Let $\mathcal{S}_1$ be the set of irreducible characters in $\mathcal{S}(H')$ of degree aq. By Lemma 17.7, the degree of every character in $\mathcal{S}(H')$ is either aq or vq, and $|\mathcal{S}_1| = 2v/a$. We will prove some properties of characters of $P = P_1$ having exactly a conjugates. Note that there is such a character because $\mathcal{S}_1 \neq \emptyset$.

We prove a lemma. *Let θ be a nonprincipal character of P/P' with exactly a conjugates. Then, $V_1 = V \cap I(\theta)$ contains no Q^*-invariant subgroup different from* 1.

Proof. Suppose $1 \neq U \subseteq V_1$ and U is Q^*-invariant. Then, V_1 centralizes$P/\ker\theta$. Since V is a p'-group, $C_{P/P'}(V) \neq 1$. Hence, $C_{P/P'}(U) \neq 1$, and it is a direct factor of P/P' because U is a p'-group. Since U is Q^*-invariant and V is abelian, $C_{P/P'}(U)$ is VQ^*-invariant. By Lemma 17.2, VQ^* acts irreducibly on $P/\Phi(P)$. It follows that $C_{P/P'}(U) = P/P'$, and hence $U \subseteq C_V(P) = C_1 = 1$. This contradiction proves the lemma. Q.E.D.

We claim that there is a pair of characters θ_1 and θ_2 of P/P' having exactly a conjugates such that $\theta_1\theta_2$ has v conjugates. Suppose that this does not hold. Then, the characters having at most a conjugates form a subgroup of the character group of P/P' that is VQ^*-invariant. Then, Lemma 17.2 yields that every character of P/P' has at most a conjugates. This gives a contradiction as follows. There is a Q^*-invariant nonprincipal character θ of P/P'. Then, $I(\theta) \cap V$ is Q^*-invariant, contradicting the lemma.

Choose a pair of characters θ_1 and θ_2 each having exactly a conjugates such that $\theta_1\theta_2$ has v conjugates. Then, $|S' \colon I(\theta_i)| = a$ for $i = 1, 2$, and $I(\theta_1) \cap I(\theta_2) = P$. Thus, v divides a^2; in particular, $v \leq a^2$. We will prove that $r(V) \leq 2$. Take an arbitrary prime $r \in \pi(V)$. We will show that V has a Sylow r-subgroup generated by at most two elements. Let x be an element of order a in V, and let w be a generator of Q^*. If $\langle x\rangle \cap \langle x\rangle^w$ is an r'-group, $\langle x, x^w\rangle$ contains a Sylow r-subgroup of V

that is generated by two elements. Suppose that $\langle x\rangle \cap \langle x\rangle^w$ contains a subgroup R of order r. Then, R is the unique subgroup of order r in $\langle x\rangle$ as well as in $\langle x\rangle^w$. Thus, R is Q^*-invariant. By the lemma, $I(\theta_i)$ does not contain R. Let $V_i = I(\theta_i) \cap V$. Then, $V_1 \cap V_2 = 1$. Since $V_i \cap R = 1$, V/V_i has a cyclic Sylow r-subgroup. The Second Isomorphism Theorem yields that V_1 also has a cyclic Sylow r-subgroup. Thus, a Sylow r-subgroup of V is generated by at most two elements. Since V is abelian, we have $r(V) \leq 2$. If $r(V) = 1$, V would be cyclic. Then, $a = v$, contrary to $a \neq v$. Thus, $r(V) = 2$.

We prove that if θ has exactly a conjugates, then $V_1 = I(\theta) \cap V$ is cyclic and $V_1 \cap V_1{}^w = 1$ for any $w \in Q^*$. If V_1 is not cyclic, V_1 contains an elementary abelian group E of order r^2 for some $r \in \pi(V)$. Since $r(V) = 2$, E is a characteristic subgroup of V. Thus, E is Q^*-invariant, contradicting the lemma. Therefore, V_1 is cyclic. If $V_1 \cap V_1{}^w \neq 1$ for some $w \neq 1$ in Q^*, then take a subgroup R of prime order in $V_1 \cap V_1{}^w$. Since V_1 is cyclic, R is the unique subgroup of its order. The same holds for $V_1{}^w$. Then, R is a Q^*-invariant subgroup of V_1. The lemma yields that this is not possible. Thus, $V_1 \cap V_1{}^w = 1$.

The proof of Lemma 30.8 [FT] can be carried over. The Q^*-invariant nonprincipal characters of P have exactly v conjugates as seen from the third paragraph of the present proof. Thus, $\mathcal{S}(H')$ contains $p-1$ characters of weight q and of degree qv.

Let λ be an irreducible character of degree aq in $\mathcal{S}_1$. Then Lemma 4.5 [FT] yields that λ is induced by a linear character of some subgroup U of index a in S'. Define $\alpha = 1_U{}^S - \lambda$. Since $U \lhd S'$ (as $S'/H \cong V$ is abelian), $1_U{}^{S'}$ is the regular representation of the group S'/U. Since $U = I(\theta)$ for some nonprincipal character θ with exactly a conjugates, $U \cap U^w = H$ for all $w \in Q^{*\sharp}$. If $|U : H| = b$, then $U/H \cong V_1 = I(\theta) \cap V$ is cyclic. Thus, UU^w/H is the set S_b/H of elements of order dividing b. It follows that S is Q^*-invariant. If a linear character ξ of S' has U in its kernel, $\ker \xi^w \supseteq U^w$. Thus, ξ^w has U in the kernel if and only if $\ker \xi \supseteq S_b$. Therefore, we can compute $(1_U)^S$. It is the sum of $\rho_{S/S'}$, irreducible characters induced by nonprincipal characters of S'/S_b with multiplicity q and $(a - a/b)$ other irreducible characters with multiplicity 1. Thus, it follows that $\|\alpha\|^2 = q+q^2((a/b)-1)/q+a-(a/b)+1 = a+1+(q-1)a/b$.

The remaining portion of the proof is the same as that of Lemma 30.8 [FT]. Q.E.D.

Lemma 17.9. *S is of type II.*

Lemma 17.10. *If $\mathcal{S}$ contains an irreducible character of degree aq, then Hypothesis* 12.4 *is satisfied with $M = S$, $X = A(S)$, $H = S_F = P$,* *and $d = a$.*

Lemma 17.11. *If $\mathcal{S}$ contains an irreducible character of degree $aq$, then $|H\colon H'| \leq 4a^2q^2 + 1$.*

Proof. We need only to check that the present $\mathcal{S}(H')$ is the same as $\mathcal{S}(H')$ in Theorem 12.5. Suppose that $\lambda \in \mathcal{S}(H')$ in the sense of Theorem 12.5. Then, $\lambda$ has the same degree as the character $\mu$ in $\mathcal{S}$ that has H' in the kernel. By the definition of $\mathcal{S}$, $\lambda$ is induced by an irreducible character λ_1 of S'. Similarly, $\mu$ is induced by an irreducible character μ_1 of S'. Since $H' \subseteq \ker \mu$, the restriction of μ_1 on $H$ is a direct sum of irreducible characters of degree 1. Since S'/H is abelian, Lemma 4.5 [FT] yields that $\mu_1(1)$ is prime to $|H|$. Note that $H$ is a Hall subgroup of $S$. Since $\lambda_1(1) = \mu_1(1)$, the degree of λ_1 is prime to $|H|$. Therefore, the irreducible constituents of the restriction of λ_1 to $H$ are linear. It follows that $H' \subseteq \ker \lambda$. Now, Theorem 12.5 yields Lemma 17.11 because $\mathcal{S}$ is not coherent. Q.E.D.

Lemma 17.12. *For $1 \leq i \leq t$, $(a, p_i - 1) = 1$ and P_iV/C_i is a Frobenius group.*

Lemma 17.13. *The group $H$ is a nonabelian 3-group with $H' = \Phi(H)$. There is an irreducible character of degree $aq$ in $\mathcal{S}$ and $a < 3^{q/2}$.*

Proof. By Lemma 17.8, $H' \neq 1$ so $H$ is nonabelian. Choose the notation that $P_1' \neq 1$. Let

$$P_1 = P_{11} \supset P_{12} \supset \cdots \supset P_{1n} = P' \supset P_{1\ n+1} = P_0$$

be a part of a chief series of $S$. Then, P_1/P_o is a nilpotent group of class 2. Lemma 17.9 yields that $S$ is of type II. Hence, by (IIv), $C_H(V) = 1$. It follows from Theorem 3.10 [BG] that Q^* centralizes some nonidentity in each chief factor. Since $C_H(Q^*)$ is cyclic, P_1/P_0 has exponent p^n. The mapping $y \to y^{p^{n-1}}$ induces a $V$-homomorphism of $P_1/\Phi(P_1)$ into P_1'/P_0. Therefore, the minimal polynomial of the generator $x$ of U/C_1 on $P_1/\Phi(P_1)$ is the same as that on P_1'/P_0. By Lemma 6.2 [FT], we have $q > 3$ and $a < 3^{q/2}$.

If $\mathcal{S}$ contains no irreducible character of degree $aq$, Lemma 17.6 yields $H = P_1$ and $a = ({p_1}^q - 1)/(p_1 - 1)$. Hence,

$$3^{q-1} \leq {p_1}^{q-1} < a < 3^{q/2}.$$

This contradiction proves that there is an irreducible character of degree $aq$ in $\mathcal{S}$.

Let $|P_1 : P_1'| = {p_1}^{mq}$. Then, by Lemma 17.11,

$${p_1}^{mq}\Pi_{i>1}{p_i}^q \leq |H\colon H'| \leq 4a^2q^2 + 1 < 4 \cdot 3^q q^2 + 1.$$

By (5.9) [FT], we have $m = 1$, $t = 1$, and ${p_1}^q < 4 \cdot 3^q q^2 + 1$. Thus, p_1 is small. Eventually, we have $p_1 = 3$ (cf. page 960 [FT]). Hence, H is a 3-group because $t = 1$. Since $m = 1$, we have $\Phi(H) = H'$. Q.E.D.

Theorem 17.14. *Let S be a subgroup of type II, III, or IV. Let a be the exponent of the group V/V', and let T be the element of $\mathcal{M}$ paired with S in Theorem I. Then, the family $\mathcal{S}$ of characters is coherent except possibly if S is of type II, H is a nonabelian 3-group, HV/C is a Frobenius group with Frobenius kernel HC/C, $a < 3^{q/2}$, $|H\colon H'| = 3^q$, and T is of type V.*

§18. Characters of Subgroups of Type V

In this section let $T = T'W_2$ be a subgroup of type V. Let S be the subgroup in $\mathcal{M}$ which satisfies the conditions of Theorem I. By (d), S is of type II. We use the notation introduced at the beginning of §16.

Let $\mathcal{T}$ be the set of all characters of T which are induced by nonprincipal irreducible characters of T'. For $0 \leq i \leq q-1$, $0 \leq j \leq w_2 - 1$, let η_{ij} be the generalized characters of G associated with ω_{ij} of W and let ν_{ij} be the characters of T defined in Lemma 13.4. By Lemma 13.5, T' has exactly q irreducible characters which induce characters of weight w_2. Denote them $\nu_0 = 1_{T'}, \nu_1, \ldots, \nu_{q-1}$. Then, $\zeta_i = {\nu_i}^T$ has weight w_2. Since q is a prime, the characters $\nu_1, \ldots, \nu_{q-1}$ are algebraically conjugate. Therefore, $\nu_i(1) = \nu_1(1)$ for $1 \leq i \leq q-1$.

We prove a lemma.

Lemma P. *If λ is an irreducible character of $\mathcal{T}$, then λ^τ is defined and λ^τ is not equal to $\pm\eta_{st}$ for any s and t.*

Proof. If $\lambda \in \mathcal{T}$, then $\overline{\lambda}$ is an irreducible character in $\mathcal{T}$ and $\overline{\lambda} \neq \lambda$. Then, $\{\lambda, \overline{\lambda}\}$ is coherent and λ^τ is (not uniquely) defined by $(\lambda - \overline{\lambda})^\tau = \lambda^\tau - \overline{\lambda}^\tau$. Suppose that $\lambda^\tau = \pm\eta_{st}$. Then, for an element $x \in \widehat{W}$, we have

$$\lambda^\tau(x) = \pm\eta_{st}(x) = \pm\omega_{st}(x).$$

Since λ vanishes on $\widehat{W}$, $\lambda^\tau - \overline{\lambda}^\tau = (\lambda - \overline{\lambda})^\tau$ vanishes on x. Thus, we get that $\overline{\lambda}^\tau(x) = \pm\omega_{st}(x) \neq 0$. By Lemma 13.1, $\overline{\lambda}^\tau$ is one of $\pm\eta_{ij}$; in fact, $\omega_{st}(x) = \omega_{ij}(x)$ on $x \in \widehat{W}$ implies that $\overline{\lambda}^\tau = \pm\eta_{st} = \lambda^\tau$. This contradicts the inequality $\lambda \neq \overline{\lambda}$. Q.E.D.

Lemma 18.1. *The family $\mathcal{S}(H')$ contains an irreducible character of S except possibly if w_2 is a prime and $S' = HV$ is a Frobenius group with Frobenius kernel H.*

Proof. We can apply Lemma 17.6. If $\mathcal{S}(H')$ contains no irreducible character, then $H = P_1$ is a p_1-group, $H' = \Phi(H)$, $v = a = ({p_1}^q - 1)/(p_1 - 1)$ and $c_1 = c = 1$. Suppose that H is nonabelian. Choose a chief factor P_1'/P_0 of S. Then, $P_1'/P_0 \subseteq Z(P_1/P_0)$ and it is an elementary abelian. As in the proof of Lemma 17.13, Lemma 6.2 [FT] yields $a < 3^{q/2}$. Since $a = ({p_1}^q - 1)/(p_1 - 1)$, we have a contradiction $3^{q-1} < 3^{q/2}$. Therefore, H is abelian. It follows from $H' = \Phi(H)$ that H is elementary abelian. On each chief factor in H, Q^* has a nontrivial centralizer. Since $C_H(Q^*) = W_2$ is cyclic, $w_2 = |W_2|$ is a prime and VQ^* acts irreducibly on H. Thus, HV is a Frobenius group with Frobenius kernel H.

Q.E.D.

Lemma 18.2. *Let $a_{ij} = ((\nu_1(1)\zeta_0 - \zeta_i)^\tau, \eta_{0j})$. Then $a_{ij} \neq 0$ for $1 \leq i \leq q-1$, $0 \leq j \leq w_2 - 1$.*

Proof. Let $M \in \mathcal{M}$ be a supporting subgroup of T and let $N = M_F$. By (F*iii*), M is a group of type I. Let $E = M \cap T$. Then (F*ii*)(b) yields that E is a complement of N in M. We prove the following lemma.

The elements of $A(M)$ are $\pi(W_2)'$-elements.

Proof. Since T is of type V, we have $A(T) = T'$. Take an element $x \neq 1$ of $C_{T'}(W_2) = Q^*$. Then, by (F*ii*)(c), we have $(|N|, |C_T(x)|) = 1$. It follows that $(|N|, |W_2|) = 1$. Suppose that there is an element of $A(M)$ of order r for some prime r in $\pi(W_2)$. Since N is an r'-group, there is a subgroup R of order r in E with $C_N(R) \neq 1$. By replacing M by conjugate, we may assume $R \subseteq W_2$ because W_2 is a cyclic Hall subgroup of T. By Theorem 8.7 (d), $N_T(R) = Q^* \times W_2$ and it is cyclic. By Lemma 6.1 (d) and Theorem 6.5 (b), E has abelian Sylow subgroups. It follows that E has cyclic Sylow r-subgroups. Then, $r \in \tau_1(M) \cup \tau_3(M)$. Since M is a ϖ-subgroup by (F*ii*), $C_N(R) \neq 1$ implies that $r \in \kappa(M)$. This contradicts Proposition 10.1 (a). Q.E.D.

We claim that $\Theta = \eta_{0j}$ satisfies the property that Θ is constant on the cosets of N which lie in $M - N$. By Lemma 14.1, we need to check that Θ is orthogonal to the elements of $T(\alpha)$ for every nonprincipal irreducible character α of N. Take $\theta_1, \theta_2 \in S(\alpha)$. Since M is of type I, θ_i are irreducible characters of M which vanish outside $A(M)$ and $\theta_1 = \theta_2$ on N by Lemmas 4.3 and 4.5 [FT]. Thus, $\theta_1 - \theta_2$ vanishes outside $A(M) - N$. Since M is of type I, $A(M) = A_0(M)$ and $A(M) - N$ is a TI-set of G with normalizer M by (F*ii*)(d).

Thus, $(\theta_1 - \theta_2)^G$ is the difference of two irreducible characters of G. Suppose that $(\Theta, (\theta_1 - \theta_2)^G) \neq 0$. Then, $\Theta = \eta_{0j}$ is involved in $\Psi = (\theta_1 - \theta_2)^G$. The virtual character Ψ vanishes outside $\mathcal{C}_G(A(M))$. Since elements of $A(M)$ are $\pi(W_2)'$- elements by the lemma, there is a Galois automorphism of $\mathbb{Q}_{|G|}$ that leaves $(\theta_1 - \theta_2)^G$ invariant but moves η_{0j} to η_{0k} with $k \neq j$. Then, η_{0k} is involved in Ψ with the same multiplicity. This is a contradiction because Ψ is the difference of two characters. Hence, η_{0j} is constant on the sets of the form $A(x)$ for $x \in D^*$.

Lemma 11.4 yields now

$$(\nu_1(1)\zeta_0 - \zeta_i, (\eta_{0j})_T) = ((\nu_1(1)\zeta_0 - \zeta_i)^\tau, \eta_{0j}) = a_{ij}.$$

The rest of the proof is the same as that of Lemma 31.2 [FT]. Q.E.D.

From now on, the lemmas of this section will be proved under the assumption that $\mathcal{T}$ is not coherent, and we will derive a contradiction from this hypothesis.

By Corollary 9.6, we have $Q^* \subseteq T''$. Then, T/T'' is a Frobenius group with Frobenius kernel T'/T''. We check that Hypothesis 12.4 is satisfied for S, S', $\mathcal{T}$ in place of M, H, $\mathcal{S}$ with $d = 1$. Since T/T'' is a Frobenius group, there is an irreducible character of degree $w_2 = |T:T'|$. The last condition of Hypothesis 12.4 holds by Lemmas 13.5 and 13.7. If $H_1 = T''$, then $\mathcal{S}(H_1)$ in Theorem 12.5 is the set of irreducible characters of T/T'' which do not have T'/T'' in their kernel. Since T'/T'' is abelian, this family is coherent. Then, Theorem 12.5 yields that $\mathcal{T}$ is coherent if

$$|T' : T''| > 4|T : T'|^2 + 1.$$

Since we are assuming that $\mathcal{T}$ is not coherent, we have

$$|T' : T''| \leq 4w_2^2 + 1.$$

This implies that W_2 acts on T'/T'' irreducibly. It follows that $T' = Q$ is a q-group for the prime $q = |Q^*|$. Define

$$|Q : Q'| = q^b \quad \text{and} \quad |T : Q| = w_2 = e.$$

Lemma 18.3. *Suppose that $\mathcal{T}$ is not coherent and $|Q : Q'| = q^b$ with $b = 2c$ an even number. Then, $|T : Q| = e$ is not a power of any prime.*

Proof. This is Lemma 31.3 [FT]. We will paraphrase a part of their proof. Suppose that $e = p^h$ for some prime p. Since $\mathcal{T}$ is not coherent, Lemma 11.5 [FT] yields that $q^c+1=2p^h$, q^c is the degree of any nonlinear irreducible characters of $Q/[Q,Q']$, and if Q_1 is a normal subgroup of T such that $Q_1 \subseteq Q'$ and $Q_1 \neq Q'$, then T/Q_1 is not a Frobenius group. Note that $Q'/[Q,Q']$ is contained in the center of $Q/[Q,Q']$. Therefore, Lemma 4.1 [FT] yields that the degree of any irreducible character of $Q/[Q,Q']$ is at most q^c.

Since $\mathcal{T}$ is not coherent, Q is nonabelian. So, $Q' \neq 1$. Let Q_1 be a normal subgroup of T such that $Q_1 \subseteq Q'$ and Q'/Q_1 is a chief factor of T. Then, $[Q,Q'] \subseteq Q_1$. Since $Q_1 \neq Q'$, the group T/Q_1 is not a Frobenius group. Then, some nonidentity element of W_2 has a nontrivial centralizer in Q_1. By Proposition 8.2, W_2 acts in a prime manner on Q. Thus, we have $Q^* \not\subseteq Q_1$. Since $[Q,Q'] \subseteq Q_1$, Q^*Q_1 is a normal subgroup of Q. Clearly, W_2 normalizes Q^*Q_1. Therefore, Q^*Q_1 is a normal subgroup of T. Since Q'/Q_1 is a chief factor of T, we have $Q^*Q_1 = Q'$. Then, $|Q' : Q_1| = |Q^*| = q$. Any nonlinear irreducible representation of Q/Q_1 has degree q^c because $Q_1 \supseteq [Q,Q']$, and it represents the subgroup Q'/Q_1 (in the center of Q/Q_1) by scalar matrices. Since each coset of Q_1 in Q' contains an element of Q^*, any nonlinear irreducible character of Q/Q_1 is W_2-invariant. Thus, there are $q-1$ nonlinear irreducible characters $\nu_1,\dots,\nu_{q-1}$ that induce reducible characters of T. Let $\zeta_i = {\nu_i}^T$ for $1 \leq i \leq q-1$. These characters are algebraically conjugate.

Since $|Q:Q'| = q^b$ with $b=2c$, $\mathcal{T}$ contains $(q^b-1)/e = 2(q^c-1)$ irreducible characters of degree e. Let $\{\lambda_i\}$ be these irreducible characters of degree e. Since $Q=A(T)$, $\{\lambda_i\}$ is coherent. Thus, the set of virtual characters $\{{\lambda_i}^\tau\}$ of weight one is defined by Lemma 10.1 [FT]. None of these ${\lambda_i}^\tau$ is equal to $\pm\eta_{st}$.

Define $\alpha = \zeta_0 - \lambda_1$ and $\beta = q^c\lambda_1 - \zeta_1$. Consider the decomposition of α^τ and β^τ as in the proof of Lemma 31.3 [FT]. Then,

$$\beta^\tau = q^c{\lambda_1}^\tau - x\sum_i {\lambda_i}^\tau + \varDelta$$

for some integer x and $({\lambda_i}^\tau, \varDelta) = 0$ for all i. If we write

$$\varDelta = \sum a_{ij}\eta_{ij} + \varDelta_0$$

where $\varDelta_0$ does not involve any η_{ij}, Lemma 13.2 yields

$$a_{00} - a_{i0} - a_{0j} + a_{ij} = 0$$

because β^τ vanishes on $\widehat{W}$. By Lemma 11.3, $(\beta^\tau, 1_G) = (\beta, 1_T) = 0$ so $a_{00} = 0$.

The set $\{\zeta_s\}$, $1 \leq s \leq q-1$, is coherent by Lemma 13.7 with ${\zeta_s}^\tau = \varepsilon \sum_j \eta_{sj}$. Then, by Lemma 11.4,

$$(\Delta, {\zeta_s}^\tau - {\zeta_1}^\tau) = (\beta^\tau, {\zeta_s}^\tau - {\zeta_1}^\tau) = (\beta, \zeta_s - \zeta_1) = e.$$

It follows that $a_{s0} - a_{10} = \pm 1$ with the sign independent of s. With $a = a_{20}$, we have
(18.1)

$$(a \pm 1)^2 + (q-2)a^2 + \sum_j {a_{0j}}^2 + \sum_j \{(a \pm 1 + a_{0j})^2 + (q-2)(a + a_{0j})^2\} \leq \|\Delta\|^2.$$

Let k be the contribution from the third term. Since each pair of complex conjugate characters contributes an even integer to the sum, k is even. The terms in the last sum and the first two terms contribute at least one, so

$$k + e \leq \|\Delta\|^2.$$

By definition, $(q^c\zeta_0 - \zeta_1)^\tau = q^c\alpha^\tau + \beta^\tau$. Lemma 18.2 implies that for any value of j $(1 \leq j \leq e-1)$

$$(\alpha^\tau, \eta_{oj}) \neq 0 \quad \text{or} \quad (\beta^\tau, \eta_{0j}) \neq 0.$$

Since $\|\beta^\tau\|^2 = q^{2c} + e$ by Lemma 11.4, we have

$$(q^c - x)^2 + x^2(2q^c - 3) + k + e \leq q^{2c} + e, \quad x^2(q^c - 1) - xq^c \leq 0.$$

Therefore, $0 \leq x \leq q^c/(q^c - 1) < 2$. Thus, $x = 0$ or $x = 1$. Suppose that $x \neq 0$. Then, $x = 1$ and $\|\Delta\|^2 = e + 2$. It follows that $k \leq 2$. If $k = 0$, we get a contradiction as in [FT]. Assume that $k = 2$. Then, $a_{0r} = a_{0s} = \pm 1$ for exactly two r, s and the remaining a_{0j} are zero. The values taken by β^τ are in the field $\mathbb{Q}_{|Q|}$ by Lemma 11.1, while the values taken by η_{0j} are in the field $\mathbb{Q}_e$ by Lemma 13.1. Then, η_{0r} has at least $p-1$ algebraic conjugates η_{0j} with $a_{0j} = a_{0r}$. It follows that $p - 1 = 2$. Thus, $p = 3$ and $q \neq 3$.

Since $\|\Delta\|^2 = e + 2 = e + k$, the contribution from each term of the last sum in (18.1) is exactly one. Since $q - 2 > 1$, we have $a + a_{0j} = 0$ for each j with $1 \leq j \leq e-1$. Since the first two terms of (18.1) also contribute 1, we have $a = 0$. This contradicts $a_{0r} = a_{0s} = \pm 1$.

Therefore, $x = 0$ and we have

$$\beta^\tau = q^c{\lambda_1}^\tau + \Delta$$

with $\|\Delta\|^2 = e$. It follows that $k = 0$ and $a_{0j} = 0$ for $1 \leq j \leq e-1$. Then, (18.1) reads

$$e((a \pm 1)^2 + (q-2)a^2) \leq e.$$

Hence, $a = 0$ or $a \pm 1 = 0$ and $q = 3$. If $a = 0$, then $a_{ij} = 0$ for all $i \geq 2$ and $a_{1j} = a_{10} = \pm 1$. Thus,

$$\beta^\tau = q^c {\lambda_1}^\tau \pm {\zeta_1}^\tau.$$

If $a \pm 1 = 0$ and $q = 3$, $a_{10} = 0$ and $a_{20} = \pm 1$. Hence, $a_{1j} = 0$ and $a_{2j} = a_{20} = \pm 1$. Thus, $\beta^\tau = q^c {\lambda_1}^\tau \pm {\zeta_2}^\tau$. Since $q = 3$, we have only two characters ζ_1 and ζ_2. We see that the union of characters $\{\lambda_i\}$ and $\{\zeta_s\}$ is coherent. This set is precisely $\mathcal{T}(Q_1)$, the set of characters of $\mathcal{T}$ which are induced by characters of Q/Q_1. Thus, $\mathcal{T}(Q_1)$ is coherent. The index $|Q : Q_1|$ is q^{2c+1} and $q^{2c+1} > 4e^2 + 1$ because $e = (q^c + 1)/2 \geq 2$.

We check that Hypothesis 12.4 is satisfied with $d = 1$. We wish to apply Theorem 12.5. The only point we need to worry about is the definition of $\mathcal{T}(Q_1)$. Thus, suppose that μ is a character of $\mathcal{T}$ that is equivalent to $\tau \in \mathcal{T}$ that has Q_1 in its kernel. Then, τ is either an irreducible character of degree e or a character of degree q^c and of weight e. Our set $\mathcal{T}(Q_1)$ contains all the irreducible characters of degree e and all the reducible ones of degree $q^c e$ because there are only $q - 1$ such characters. Thus, $\mu \in \mathcal{T}(Q_1)$. Theorem 12.5 yields that $\mathcal{T}$ is coherent, contrary to the assumption. Q.E.D.

Lemma 18.4. *The family $\mathcal{S}$ for the group S is coherent.*

This follows from Theorem 17.14, Lemma 18.3, and Lemma 11.6 [FT] as shown in [FT]. Q.E.D.

We use the following notation. Let

$$1 = q^{f_0} < q^{f_1} < \cdots$$

be the set of degrees of irreducible characters of Q and

$$\nu_1(1) = q^{f_n}.$$

Since $Q^* \subseteq Q'$ by Theorem C(3), the principal character of Q is the only linear character of Q that is W_2-invariant. Thus, $\nu_1(1) > 1$, i.e. $n > 0$. For $0 \leq i \leq n - 1$, let λ_i be an irreducible character of T with $\lambda_i(1) = eq^{f_i}$. Let $\mathcal{S}_i$ be the set of irreducible characters of T which are induced by irreducible characters of Q with degree q^{f_i}. Define j_s inductively as follows. Let $j_0 = 0$. Define j_s to be the largest integer not exceeding $n + 1$ such that

$$\mathcal{T}_{s-1} = \bigcup_{i=j_{s-1}}^{j_s - 1} \mathcal{S}_i$$

is coherent. Let Q_0 be the normal closure of Q^* in T. Let

$$1 = q^{g_0} < q^{g_1} < \cdots < q^{g_m}$$

be all the degrees of irreducible characters of Q/Q_0. For any j with $0 \leq j \leq m$, let θ_j be an irreducible character of T/Q_0 of degree eq^{g_j}. Since T/Q_0 is a Frobenius group, any nonprincipal irreducible character of Q/Q_0 induces an irreducible character of T/Q_0. Define

$$\begin{aligned} \alpha &= \zeta_0 - \lambda_0, \\ \beta_i &= q^{f_i - f_{i-1}}\lambda_{i-1} - \lambda_i \qquad (1 \leq i \leq n-1), \\ \gamma_j &= q^{g_j - g_{j-1}}\theta_{j-1} - \theta_j \qquad (1 \leq j \leq m). \end{aligned}$$

Lemma 18.5. *With the notation introduced above, we have*

$$\begin{aligned} &({\beta_i}^\tau, \eta_{0t}) = 0 \quad \textit{for} \quad 0 \leq t \leq e-1, 1 \leq i \leq n-1 \\ &({\gamma_j}^\tau, \eta_{0t}) = 0 \quad \textit{for} \quad 0 \leq t \leq e-1, 1 \leq j \leq m. \end{aligned}$$

Furthermore, if e is a prime, then one of the following possibilities occurs:

$$\alpha^\tau = 1_G - {\lambda_0}^\tau + \sum_{t=1}^{e-1} \eta_{0t},$$

$$\alpha^\tau = 1_G + \overline{\lambda_0}^\tau + \sum_{t=1}^{e-1} \eta_{0t} \quad \textit{and} \quad 2e+1 = |Q : Q'|,$$

$$\alpha^\tau = 1_G + \sum_{s=1}^{q-1} \eta_{s0} + \Gamma$$

with $(\Gamma, \eta_{st}) = 0$ *for* $0 \leq s \leq q-1$, $0 \leq t \leq e-1$.

Proof. Write

$$\alpha^\tau = \Gamma_{00} + \Delta_{00}, \quad {\beta_i}^\tau = \Gamma_{i0} + \Delta_{i0}, \quad {\gamma_j}^\tau = \Gamma_{0j} + \Delta_{0j}$$

where Δ_{ij} is a linear combination of the generalized characters η_{st} and Γ_{ij} is orthogonal to each of these η_{st}. Since α^τ, ${\beta_i}^\tau$, and ${\gamma_j}^\tau$ vanish on $\widehat{W}$, Lemma 13.2 yields that $\Delta_{ij} = \sum a_{st}\eta_{st}$ with a_{st} (depending on i and j) satisfying

$$a_{00} - a_{s0} - a_{0t} + a_{st} = 0$$

for all s and t. For $1 \leq s \leq q-1$, $(\zeta_s - \zeta_1)^\tau$ is orthogonal to α^τ, β^τ, and γ^τ. Since ${\zeta_s}^\tau = \varepsilon \sum_j \eta_{sj}$ for $s > 1$, we have

$$a_{s0} = a_{10} \quad \text{for} \quad 1 \leq s \leq q-1.$$

Consider β_i. Suppose that $\lambda_{i-1} \in \mathcal{T}_s$ and write

$$\beta_i{}^\tau = \Delta + \Delta_1$$

where $\Delta_1 \in I(\mathcal{T}_s{}^\tau)$ and Δ is orthogonal to $I(\mathcal{T}_s{}^\tau)$. The Lemma at the beginning of Section 18 yields $\{\pm\eta_{st}\} \cap \mathcal{T}_s{}^\tau = \emptyset$. Thus, Δ_{i0} is a partial sum of Δ. By Theorem 12.1 [FT],

$$\|\Delta\|^2 \leq e + 1.$$

Since $(\beta_i{}^\tau, (\lambda_i - \overline{\lambda}_i)^\tau) \neq 0$, $\beta_i{}^\tau$ involves either $\lambda_i{}^\tau$ or $\overline{\lambda}_i{}^\tau$. If $\lambda_i \in \mathcal{T}_s$, the coherence of $\mathcal{T}_s$ yields that $\Delta = 0$. If $\lambda_i \notin \mathcal{T}_s$, then $\lambda_i{}^\tau$ (or $\overline{\lambda}_i{}^\tau$) is involved in Δ. Since $\lambda_i{}^\tau \neq \pm\eta_{st}$, we have

$$\|\Delta_{i0}\|^2 \leq e.$$

We can prove $a = 0$ as in Lemma 31.5 [FT]. Hence,

$$\Delta_{i0} = \sum_{t=1}^{e-1} a_{0t} \sum_{s=0}^{q-1} \eta_{st}.$$

By Lemma 11.1, the virtual characters of $I_0(\mathcal{T})^\tau$ take nonzero values only at q-singular elements. On the other hand, the virtual characters of $I_0(\mathcal{S})^\tau$ vanish on q-singular elements by Lemma 11.1 and (F*ii*)(c). Thus, $I_0(\mathcal{T})^\tau$ is orthogonal to $I_0(\mathcal{S})^\tau$. Since $\mathcal{S}$ is coherent by Lemma 18.4, we have $(\xi_k(1)\xi_r{}^\tau - \xi_r(1)\xi_k{}^\tau, \Delta_{i0}) = (\xi_k(1)\xi_r{}^\tau - \xi_r(1)\xi_k{}^\tau, \beta_i{}^\tau) = 0$. On the other hand, $(\xi_k{}^\tau, \Delta_{i0}) = \pm a_{0k}q$. Hence,

$$\xi_k(1)a_{0r} = \xi_r(1)a_{0k}.$$

Suppose that $a_{0t} \neq 0$ for some t. Then, $a_{0k} \neq 0$ for all k. Hence, $\|\Delta_{i0}\|^2 \geq q(e-1)$. This contradicts $\|\Delta_{i0}\|^2 \leq e$. Therefore, $\Delta_{i0} = 0$. The case for γ_j is similar.

The remainder of the proof is the same as the proof of Lemma 31.5 [FT]. Q.E.D.

We continue to use the notation introduced just before Lemma 18.5.

Lemma 18.6. *With the notation of the preceding lemma, let* $\lambda = \lambda_{n-1}$ *and* $\beta = q^{f_n - f_{n-1}}\lambda - \zeta_1$. *Then* $(\beta^\tau, \eta_{0t}) = 0$ *for* $0 \leq t \leq e-1$.

Proof. Let $\mathcal{T}_b$ be the coherent set that contains $\mathcal{S}_{n-1}$. If $\zeta_1 \in \mathcal{T}_b$, then $\beta^\tau \in I(\mathcal{T}_b{}^\tau)$ and $(\beta^\tau, \eta_{0t}) = 0$. If $\zeta_1 \notin \mathcal{T}_b$, we apply Theorem 12.1 [FT]. The proof is the same as that of Lemma 31.6 [FT]. Q.E.D.

Theorem 18.7. *The set $\mathcal{T}$ is coherent.*

Proof. Suppose that $\mathcal{T}$ is not coherent and use the notation introduced in Lemmas 18.5 and 18.6. In particular, α, β_i, γ_j, λ_i, and θ_j have the same meaning as in Lemmas 18.5 and 18.6. We may choose the notation $\lambda_0 = \theta_0$. We have

$$(q^{f_n}\zeta_0 - \zeta_1)^\tau = q^{f_n}\alpha^\tau + \sum_i q^{f_n - f_i}\beta_i{}^\tau.$$

By Lemma 18.2, $((q^{f_n}\zeta_0 - \zeta_1)^\tau, \eta_{0j}) \neq 0$. Since Lemmas 18.5 and 18.6 yield $(\beta_i{}^\tau, \eta_{0t}) = 0$ for all i with $1 \leq i \leq n$, we have $(\alpha^\tau, \eta_{0t}) \neq 0$ for $0 \leq t \leq e-1$. Thus, if $(\alpha^\tau, \eta_{0t}) = a_t$, then $a_t \neq 0$ and $\sum a_t{}^2 \leq \|\alpha^\tau\|^2 = e+1$. Therefore, $a_t = 1$ or -1, and α^τ involves exactly one more irreducible character with multiplicity 1 or -1. Since

$$(\alpha^\tau, (\lambda_0 - \overline{\lambda}_0)^\tau) = -1,$$

the extra character is either $\pm\lambda_0{}^\tau$ or $\pm\overline{\lambda}_0{}^\tau$. In the latter case, we have $|Q : Q'| = 2e+1$ and there are exactly 2 irreducible characters of T with degree e. We may choose the notation that

$$\alpha^\tau = 1_G - \lambda_0{}^\tau + \sum a_t\eta_{0t} \qquad (a_t = 1 \text{ or } -1). \tag{18.2}$$

Lemma 18.5 yields $(\gamma_s{}^\tau, \eta_{0t}) = 0$ for $1 \leq s \leq m$, $0 \leq t \leq e-1$. Since

$$(q^{g_j}\theta_0 - \theta_j)^\tau = \sum_{s=1}^{j} q^{g_j - g_s}\gamma_s,$$

we have

$$((q^{g_j}\theta_0 - \theta_j)^\tau, \alpha^\tau) = ((q^{g_j}\theta_0 - \theta_j)^\tau, -\lambda_0{}^\tau).$$

The left side is equal to $(q^{g_j}\theta_0 - \theta_j, \alpha) = -q^{g_j}$ by Lemma 11.4 (and the choice $\theta_0 = \lambda_0$). Since $\|(q^{g_j}\theta_0 - \theta_j)^\tau\|^2 = q^{2g_j} + 1$ and $((q^{g_j}\theta_0 - \theta_j)^\tau, (\theta_j - \overline{\theta}_j)^\tau) = -1$, we have

$$(q^{g_j}\theta_0 - \theta_j)^\tau = q^{g_j}\theta_0{}^\tau - \theta_j{}^\tau. \tag{18.3}$$

If there are only two irreducible characters of degree eq^{g_j}, there is an ambiguity in the definition of $\theta_j{}^\tau$. But, we can take a consistent notation. Let Q_0 be the normal closure of Q^* in T as defined before Lemma 18.5. Let $\mathcal{T}(Q_0)$ be the set of irreducible characters of $\mathcal{T}$ having the degrees eq^{g_j} with $0 \leq j \leq m$. Then, (18.3) implies that $\mathcal{T}(Q_0)$ is coherent.

Consider $(q^{f_n}\lambda_0 - \zeta_1)^\tau = \sum_{i=1}^{n} q^{f_n - f_i}\beta_i$. By (18.2) together with Lemmas 18.5 and 18.6,

$$((q^{f_n}\lambda_0 - \zeta_1)^\tau, \alpha^\tau) = ((q^{f_n}\lambda_0 - \zeta_1)^\tau, -\lambda_0{}^\tau).$$

Lemma 11.4 yields that the left side is equal to $-q^{2f_n}$. Since $\|(q^{f_n}\lambda_0 - \zeta_1)^\tau\|^2 = q^{2f_n} + e$, we have

$$(q^{f_n}\lambda_0 - \zeta_1)^\tau = q^{f_n}\lambda_0{}^\tau + \Delta$$

with $\|\Delta\|^2 = e$. The set $\{\zeta_s\}$ of virtual characters ζ_s is subcoherent by Lemma 13.7. Hence, the definition of subcoherent set yields that $\Delta = \pm\zeta_s{}^\tau$. In fact, $\Delta = -\zeta_1{}^\tau$ except possibly when $q - 1 = 2$. In the exceptional case, there are exactly two virtual characters of weight e. We can choose the notation

$$(q^{f_n}\lambda_0 - \zeta_1)^\tau = q^{f_n}\lambda_0{}^\tau - \zeta_1{}^\tau. \tag{18.4}$$

Let Q_1 be a normal subgroup of T such that $Q_1 \subseteq Q_0$ and Q_0/Q_1 is a chief factor of T. It follows from the definition of Q_0 that $Q^* \not\subseteq Q_1$. Then, Q^*Q_1 is a normal subgroup of T and $Q^*Q_1 = Q_0$ (cf. the second paragraph of the proof of Lemma 18.3). Thus, $|Q_0 : Q_1| = q$.

Since $\mathfrak{T}$ is not coherent and $\mathfrak{T}(Q_0)$ is coherent, Theorem 12.5 yields that

$$|Q : Q_0| \le 4e^2 + 1.$$

Hence, Q/Q_0 has no proper W_2-invariant subgroup. Since T/Q_0 is a Frobenius group, this implies that $\Phi(Q) \subseteq Q_0$. On the other hand, $Q^* \subseteq Q'$ by Theorem C (3). Therefore, $Q_0 \subseteq Q'$. Thus, $\Phi(Q) = Q_0 = Q'$. The subgroup Q_1 satisfies $|Q_0 \colon Q_1| = q$. Hence, $Z(Q/Q_1) = Q_0/Q_1$ and Q/Q_1 is an extraspecial q-group. Thus, $|Q : Q'| = q^{2c}$ for some integer c. Define

$$\mathfrak{T}(Q_1) = \mathfrak{T}(Q_0) \cup \{\zeta_i \mid 1 \le i \le q-1\}.$$

Then, $\mathfrak{T}(Q_1)$ consists of all characters in $\mathfrak{T}$ having the same weight and degree as some character in $\mathfrak{T}$ which has Q_1 in its kernel. By (18.4), $\mathfrak{T}(Q_1)$ is coherent. Since $\mathfrak{T}$ is not coherent, Theorem 12.5 yields

$$q^{2c+1} = |Q : Q_1| \le 4e^2 + 1.$$

By Theorem 2.5 [BG], e divides $q^c + 1$ or $q^c - 1$. Since e is odd, we have $2e \le q^c + 1$. Then,

$$q^{2c+1} \le 4e^2 + 1 \le (q^c + 1)^2 + 1 < 2q^{2c}.$$

This contradiction proves Theorem 18.7. Q.E.D.

Corollary 18.8. $\alpha^\tau = 1_G - {\lambda_0}^\tau + \sum_{t=1}^{e-1} \eta_{0t}$.

Proof. Let $a_t = (\alpha^\tau, \eta_{0t})$. Since $\mathcal{T}$ is coherent by Theorem 18.7, we have

$$(18.5) \qquad \begin{aligned}(\nu_1(1)\zeta_0 - \zeta_1)^\tau &= \nu_1(1)\alpha^\tau + (\nu_1(1)\lambda_0 - \zeta_1)^\tau \\ &= \nu_1(1)\alpha^\tau + \nu_1(1){\lambda_0}^\tau - {\zeta_1}^\tau.\end{aligned}$$

By the Lemma at the beginning of this section, $({\lambda_0}^\tau, \eta_{0t}) = 0$. Also, $({\zeta_1}^\tau, \eta_{0t}) = 0$. This follows from Lemma 13.1 if $q > 3$ because ${\zeta_1}^\tau = \pm\sum_j \eta_{1j}$. If $q = 3$, ${\zeta_1}^\tau$ is not uniquely determined; however, ${\zeta_1}^\tau$ is either $\pm\sum_j \eta_{1j}$ or $\pm\sum_j \eta_{2j}$. Thus, we have $({\zeta_1}^\tau, \eta_{0t}) = 0$. Lemma 18.2 and (18.5) yield

$$0 \neq ((\nu_1(1)\zeta_0 - \zeta_1)^\tau, \eta_{0t}) = \nu_1(1)a_t.$$

Since $|\mathcal{T}| > 2$, α^τ involves $-{\lambda_0}^\tau$. Since ${\lambda_0}^\tau$ is not one of $\pm\eta_{st}$, we have

$$\alpha^\tau = 1_G - {\lambda_0}^\tau + \sum a_t \eta_{0t}.$$

It follows from $\|\alpha^\tau\|^2 = e + 1$ that $a_t = 1$ or -1 for each t. By Lemma 13.1, ${\lambda_0}^\tau$ vanishes on $\widehat{W}$. The same holds for α^τ. By Lemmas 13.1 and 13.2, we have $a_t = 1$ for $0 \leq t \leq e - 1$. Q.E.D.

Corollary 18.9. *The group S' is a Frobenius group and the number w_2 is prime.*

Proof. Suppose that Corollary 18.9 is false. By Lemma 31.1, $\mathcal{S}(H')$ contains an irreducible character θ. Consider the group S/H'. Let $E = Q^*V$ be a complement of H in S. Since S is of type II, E is a Frobenius group with Frobenius kernel V and $C_H(V) = 1$ (cf. (II*iv*) and the modified (II*v*)). By Theorem 3.10 [BG], Q^* centralizes a nonidentity element of H/H'. Thus, $\mathcal{S}(H')$ contains one of the reducible characters. Hence, we can take $\xi_i \in \mathcal{S}(H')$. Note that $\mathcal{S}(H')$ is coherent. This is clear if $\mathcal{S}$ is coherent. If $\mathcal{S}$ is not coherent, Lemma 17.8 yields that $\mathcal{S}(H')$ is coherent. Hence, $\mathcal{S}(H')$ is coherent always. If we define $\beta = \theta(1)\xi_1 - \xi_1(1)\theta$, $\beta \in I_0(\mathcal{S}(H'))$ and $\beta^\tau = \theta(1){\xi_1}^\tau - \xi_1(1)\theta^\tau$.

Let α be the element of $I_0(\mathcal{T})$ defined in Corollary 18.8. We prove that α^τ is orthogonal to β^τ. By Lemma 11.1, α^τ vanishes on elements not conjugate to an element of $A(x)$ for any $x \in T'^\sharp$. Suppose that $g = xy = yx \in A(x)$ and $\alpha^\tau(g) \neq 0$. We claim that $\beta^\tau(g) = 0$. Suppose $\beta^\tau(g) \neq 0$. By Lemma 11.1 applied to S, g is conjugate to an element of S or one of the supporting subgroups of S. Since T is of type V, T is not conjugate to any supporting subgroup by (F*ii*). If M is a supporting subgroup of S, then $\sigma(M) \cap \sigma(T) = \sigma(S) \cap \sigma(T) = \emptyset$ by Theorem 7.9. Since $g = xy$ is conjugate to an element of S or a supporting subgroup, the element x is conjugate to an element of S. Since $\beta^\tau(g) \neq 0$, x is conjugate to an element of $A(S) - H$. It follows that $(|C_G(x)|, |H|) \neq 1$. This implies that S is conjugate to a supporting subgroup of T. Let S^h be a conjugate of S that contains $C_G(x)$. Then, by (F*ii*), $S^h \cap T$ is a complement of H^h that contains $C_T(x)$. Since x is conjugate to an element of $A(S)$, the order of x is prime to q. On the other hand, $Q^* \subseteq C_T(x)$ because T' is nilpotent. This contradicts the structure of $S^h \cap T$ being a Frobenius group with Frobenius complement of order q. Thus, $(\alpha^\tau, \beta^\tau) = 0$. In fact, the above argument proves that any element of $I_0(\mathfrak{T})$ is orthogonal to every element of $I_0(\mathfrak{S})$. We compute $(\alpha^\tau, \beta^\tau)$ using Corollary 18.8. We have

$$(\alpha^\tau, \beta^\tau) = (1_G - \lambda_0{}^\tau + \sum \eta_{0t}, \theta(1)\xi_1{}^\tau - \xi_1(1)\theta^\tau).$$

Note that $\lambda_0{}^\tau \neq \theta^\tau$. This follows from $((\lambda_0 - \overline{\lambda}_0)^\tau, (\theta - \overline{\theta})^\tau) = 0$. Since $\xi_1{}^\tau = \varepsilon \sum_i \eta_{i1}$ (or $\pm \sum_i \eta_{i2}$), we have

$$(\alpha^\tau, \beta^\tau) = (\sum \eta_{0t}, \theta(1)\varepsilon \sum \eta_{i1}) = \varepsilon\theta(1).$$

This contradicts $(\alpha^\tau, \beta^\tau) = 0$. Q.E.D.

Theorem 18.10. *No element of* $\mathcal{M}$ *is of type V.*

Proof. We will paraphrase the proof of Theorem 32.1 [FT]. Suppose that $\mathcal{M}$ contains a subgroup T of type V. For $M = T$, we use the notation introduced at the beginning of Chapter II. Thus, D^* and $A(x)$ for $x \in D^*$ have the same meaning as defined there. We denote by S the subgroup of type II defined in Theorem I. The subgroup $H = S_F$ is a TI-set by (T7). In addition, the following notation is used: $T = T'W_2$, $S = S'Q^*$, $W = Q^* \times W_2$, $|W_2| = w_2 = e$, $|Q^*| = q$ and $|S' \colon H| = v$. Let $\mathfrak{T}$ be the set of characters of T introduced at the beginning of this section. Then, by Theorem 18.7, $\mathfrak{T}$ is coherent. Let

$$\mathfrak{T}^* = \{\mathfrak{T}, \zeta_0\}.$$

Corollary 18.8 yields that $\mathfrak{T}^*$ is coherent if we define

$$\zeta_0{}^\tau = 1_G + \sum_{t=1}^{e-1} \eta_{0t}.$$

The family $\mathcal{T}^*$ consists of irreducible characters of T and q reducible characters $\zeta_0, \zeta_1, \ldots, \zeta_{q-1}$ of weight e. There are irreducible characters ν_{ij} of T such that

$$\xi_i = \sum_{j=0}^{e-1} \nu_{ij} \quad \text{with} \quad (\nu_{ij})_{T'} = (\nu_{i0})_{T'}.$$

There is an irreducible character λ of degree e in $\mathcal{T}$. Lemma 14.4 applied with T and $\mathcal{T}^*$ in place of M and $\mathcal{S}$ yields

$$\lambda^\tau(x) = \lambda(x) + s\gamma(x) \quad \text{for } x \in T'^\sharp$$

where γ is orthogonal to every element of $\mathcal{T}^*$. Since the irreducible characters of T are $\{\nu_{ij}\}$ and the characters in $\mathcal{T}$, we have

$$\gamma = \sum a_{ij}\nu_{ij}.$$

Since $(\gamma, \zeta_i) = 0$ for $0 \leq i \leq q-1$, we have $\sum_j a_{ij} = 0$ for $0 \leq i \leq q-1$. It follows that

$$\gamma_{T'} = \sum_{i,j} a_{ij}(\nu_{ij})_{T'} = \sum_i \left(\sum_j a_{ij} \right) (\nu_{i0})_{T'} = 0.$$

This proves that $\lambda^\tau(x) = \lambda(x)$ for $x \in T'^\sharp$. By Lemma 14.3, λ^τ is constant on the set of the form $A(x)$ for $x \in D^*$. Hence, Lemma 11.5 yields

$$(18.6) \qquad \frac{1}{|G|} \sum_{x \in G_1} |\lambda^\tau(x)|^2 = \frac{1}{|T|} \sum_{x \in T'^\sharp} |\lambda(x)|^2 = 1 - \frac{e}{|T'|}.$$

Let G_1 be the set of elements of G which are conjugate to some element of $A(x)$ for $x \in D^*$. By Lemma 11.5 with Θ replaced by 1_G, we have

$$\frac{|G_1|}{|G|} = \frac{1}{e}\left(1 - \frac{1}{|T'|}\right).$$

Define $G_2 = \mathcal{C}_G(\widehat{W})$. By Theorem 8.7 (e),

$$\frac{|G_2|}{|G|} = 1 - \frac{1}{e} - \frac{1}{q} + \frac{1}{eq}.$$

Let G_3 be the set of elements of G which are conjugate to some elements of $H^\sharp$. Since H is a TI-set, we have

$$\frac{|G_3|}{|G|} = \frac{1}{qv|H|}(|H| - 1).$$

These sets G_1, G_2, and G_3 are disjoint. Let G_0 be the complement of the union $G_1 \cup G_2 \cup G_3$. Then,

$$\begin{aligned} \frac{|G_0|}{|G|} &= 1 - \frac{1}{e}\left(1 - \frac{1}{|T'|}\right) - \left(1 - \frac{1}{e} - \frac{1}{q} + \frac{1}{eq}\right) - \frac{1}{qv} + \frac{1}{qv|H|} \\ &> \frac{1}{q} - \frac{1}{eq} - \frac{1}{qv} \geq \frac{1}{3q} \end{aligned} \tag{18.7}$$

because $e \geq 3$ and $v \geq 3$. By (18.6), we have

$$\frac{1}{|G|}\sum_{x \in G_0} |\lambda^\tau(x)|^2 \leq 1 - (1 - \frac{e}{|T'|}) = \frac{e}{|T'|}.$$

By Corollary 18.9, e is a prime and S' is a Frobenius group. Hence, $\eta_{01}, \ldots, \eta_{0e-1}$ are algebraically conjugate characters with values in $\mathbb{Q}_e$. Since S' is a Frobenius group, every element whose order is divisible by e lies in $G_2 \cup G_3$. Thus, η_{0t} take the same integral value on G_0. Since $(\zeta_0 - \lambda)^\tau$ vanishes off G_1,

$$\lambda^\tau(x) = 1 + (q-1)\eta_{01}(x) \quad \text{for} \quad x \in G_0.$$

In particular, $\lambda^\tau(x)$ is an odd integer so

$$|\lambda^\tau(x)|^2 \geq 1 \quad \text{for} \quad x \in G_0.$$

Thus,

$$\frac{|G_0|}{|G|} \leq \frac{1}{|G|}\sum_{x \in G_0} |\lambda^\tau(x)|^2 \leq \frac{e}{|T'|}.$$

Therefore, $|T'| < 3qe$ by (18.7). Theorem C (3) implies $Q^* \subseteq T''$. Hence, we get $|T' \colon T''| < 3e$. Since T/T'' is a Frobenius group, $|T' \colon T''| \geq 2e+1$. Thus,

$$|T''|(2e+1) \leq |T'| < 3qe, \quad q \leq |T''| < 3eq/(2e+1) < 2q.$$

It follows that $|T''| = q$ and W_2 acts irreducibly on T'/T''. This implies that T' is an extraspecial q-group. If $|T'/T''| = q^{2c}$, then Theorem 2.5 [BG] yields that e divides $q^c + 1$ or $q^c - 1$. Hence, $e \leq (q^c + 1)/2$ and

$$q^{2c} = |T' \colon T''| < 3e \leq 3(q^c + 1)/2 \leq 2q^c.$$

This contradiction proves Theorem 18.10.

Corollary 18.11. *Let S be a subgroup of type II, III, or IV in $\mathcal{M}$. Then, the family $\mathcal{S}$ is coherent.*

This follows from Theorems 17.14 and 18.10.

§19. Subgroups of Type I

We remark that a subgroup $M \in \mathcal{M}$ of type I is a Frobenius group if and only if $\tau_2(M)$ is empty. This is easy to see. If $\tau_2(M) = \emptyset$, then the complement E in (I*iii*) is a Z-group and the only subgroup of E with the same exponent as E is E. Thus, $E_0 = E$ and by (I*iii*), M is a Frobenius group. Suppose conversely that M is a Frobenius group. Then, $H = M_F$ is the nilpotent normal subgroup of maximal order in M. Then, H is the Frobenius kernel of the Frobenius group M. It follows from the property of a Frobenius complement that all Sylow subgroups of M/H are cyclic. This implies $\tau_2(M) = \emptyset$ (cf. the notation of §6).

Theorem 19.1. *Every subgroup of type I is a Frobenius group.*

The proof is by contradiction. Suppose that $\mathcal{M}$ has a subgroup of type I that is not a Frobenius group. The following notation will be used. Let ρ be the set of primes defined as follows: $p_i \in \rho$ if and only if $\mathcal{M}$ has a subgroup M_i of type I such that $p_i \in \tau_2(M_i)$. By Lemma H, the groups M_i are ϖ-groups; in particular, $p_i \in \varpi$. (The set ρ is denoted σ in [FT]; I have chosen this notation because σ has a different meaning in [BG] and we have been using σ in the sense of [BG].) The smallest prime in ρ will be denoted $p = p_k$. Let $M = M_k$, $K = M_F$, $P_0 \in Syl_p(M)$, $P \in Syl_p(G)$ such that $P_0 \subseteq P$, $A = \Omega_1(P_0)$, and

$$L \in \mathcal{M}(N_G(A)).$$

If L is of type I, let $U = L_F$ and choose a complement E of U in L. If L is not of type I, then L is of type II, III, or IV by Theorem 18.10. In this case, let $H = L_F$, U a complement of H in L', and W_1 a complement of L' in L with $W_1 \subseteq N_L(\mathsf{U})$. The order $|W_1|$ is a prime by (T7). Note the particular usage of the symbol U.

Let $\mathcal{L}$ be the set of characters of L defined as follows: If L is of type I, $\mathcal{L}$ is the set of all irreducible characters of L which do not have U in their kernel. If L is of type II, III, or IV, then $\mathcal{L}$ is the set of characters of L each of which is induced by a nonprincipal irreducible character of L' that vanishes outside $A(L)$. Thus, if L is of type I, $\mathcal{L}$ is the set of characters studied in §15. If L is of type III or IV, then $\mathcal{L}$ corresponds to the set $\mathcal{S}_0 \cup \mathcal{S}$ in §16.

Lemma 19.2. *The subgroup L is not of type II; it is either a Frobenius group with cyclic Frobenius complement or of type III or IV. There is no subset of L that is a TI-set of G and contains A. The group P is either an abelian group of rank 2 or the center $Z(P)$ is cyclic, and we can take $P \subseteq U$. Furthermore, L is the unique subgroup of $\mathcal{M}$ that contains $N_G(A)$.*

Proof. Since $p \in \tau_2(M)$, $A \in \mathcal{E}_p^2(M)$ and P_0 is an abelian group of rank 2 by Theorem 6.5 (b). We have $C_G(A) \subseteq M$ by Proposition 6.4 (a). It follows that either $P = P_0$ or $Z(P)$ is cyclic.

By Lemma 6.2 applied with A and L in place of X and M^*, we have that $p \in \sigma(L) \cup \tau_2(L)$. If $p \in \tau_2(L)$, Theorem 6.5 (b) applied with L in place of M yields $N_G(A) \not\subseteq L$, contradicting the definition of L. Thus, $p \in \sigma(L)$ and $A \subseteq L_\sigma$. In fact, $p \in \sigma_0(L)$ as $p \in \varpi$.

We have $A \in \mathcal{E}_p^2(M)$ by Theorem 6.5 (b). Since A normalizes K, some element $a \neq 1$ of A commutes with some element $y \neq 1$ of K by Proposition 1.16 [BG]. But, $K \cap L = 1$ by Theorem 6.5 (e). Thus, A is not contained in any subset of L that is a TI-set in G.

Suppose that L is of type II. Then, by Theorem 9.7 (a) with L in place of M, $L_\sigma = H \subseteq F(L)$ and $F(L)$ is a TI-set of G. Since $A \subseteq L_\sigma$, this contradicts what we proved in the preceding paragraph. Thus, L is not of type II.

If L is of type III or IV, $F(L)$ is a TI-set in G by (T7). Therefore, $A \not\subseteq F(L)$ but $A \subseteq L_\sigma = L'$. Thus, $p \in \pi(U)$. Since U is a Hall subgroup of L_σ, U contains a Sylow p-subgroup of G. We can choose $P \subseteq \text{U}$.

Suppose that L is of type I. Then, $L_{\sigma_0} = U$. Since U is a Hall subgroup of G, we have $P \subseteq \text{U}$. In fact, since U is nilpotent, P is a normal subgroup of L. We will prove that L is a Frobenius group. Suppose that L is not a Frobenius group. Then, $\tau_2(L)$ is not empty. Let $q \in \tau_2(L)$ and take $Q \in \mathcal{E}_q^2(L)$. Then, $q \in \rho$. It follows that $p < q$. By Theorem 6.5 (d), we have $C_U(Q) = 1$. Thus, Q acts on $\Omega_1(Z(P))$ nontrivially. Since $r(Z(P)) \leq 2$, we have $q < p$, contradicting the minimal nature of p. This proves that L is a Frobenius group.

The subgroup E is a Frobenius complement of L. Hence, E acts on $\Omega_1(Z(P))$ faithfully. If $Z(P)$ is cyclic, E is abelian. If P is abelian, $\Omega_1(P) = A$. Theorem 2.6 [BG] yields that E is abelian. A Frobenius complement is cyclic if it is abelian. Therefore, E is cyclic.

It remains to prove that $\mathcal{M}(N_G(A)) = \{L\}$. Suppose that P is nonabelian. Choose a subgroup P_1 such that $P_0 \subseteq P_1 \subseteq P$ with $|P_1 : P_0| = p$. Since $C_G(A) \subseteq M$ by Proposition 6.4 (a), P_1 is nonabelian. We have $P_1 \subseteq N_G(A)$ as $A = \Omega_1(P_0)$. By Theorem 6.13, $P_1 \in \mathcal{U}$. Hence, $N_G(A) \in \mathcal{U}$. Assume that P is abelian. Then, $P_0 = P$ and

$N_G(P) \subseteq N_G(A)$. Suppose that $L_0 \in \mathcal{M}(N_G(A))$. Then, $p \in \sigma(L_0) \cap \sigma(L)$. Theorem 7.9 yields that L_0 is conjugate to L: $L_0 = g^{-1}Lg$ for some $g \in G$. Then, $P, g^{-1}Pg \in Syl_p(L_0)$; hence, $P = h^{-1}g^{-1}Pgh$ for some $h \in L_0$. Thus, $L_0 = x^{-1}Lx$ with $x = gh \in N_G(P) \subseteq N_G(A) \subseteq L$. Therefore, $L_0 = L$. This proves the uniqueness of L. Q.E.D.

Lemma 19.3. *There exists an irreducible character $\lambda \in \mathcal{L}$ that does not have P in its kernel such that $\lambda(1)$ divides $p-1$ or $p+1$. The group L/L' is a cyclic group of order e with e dividing $p-1$ or $p+1$.*

Proof. Suppose that L is of type III or IV. Then, L/H is a Frobenius group with Frobenius kernel isomorphic to U. Since $P \subseteq U$, L/H has an irreducible character λ of degree w_1 that does not have P in its kernel. Since L/H is a Frobenius group, W_1 acts faithfully on $\Omega_1(Z(P))$. It follows that $w_1 \mid p^2-1$. Since w_1 is a prime by (T7), $\lambda(1) = w_1$ divides $p-1$ or $p+1$.

Suppose that L is of type I. Then, by Lemma 19.2, L is a Frobenius group with Frobenius kernel U and Frobenius complement E that is cyclic. Thus, there is an irreducible character λ of L of degree $e = |E|$ that does not have P in its kernel. We need to prove that e divides either $p-1$ or $p+1$. As before, E acts faithfully on $\Omega_1(Z(P))$. Thus, if $Z(P)$ is cyclic, e divides $p-1$. If P is abelian, $e \mid p^2-1$. Suppose that e has prime divisors q_1 and q_2 such that

$$q_1 \mid p-1 \quad \text{and} \quad q_2 \mid p+1.$$

We will derive a contradiction. Let Q_i be a subgroup of E of order q_i. Then, Q_2 acts regularly on $\mathcal{E}_p^1(A)$, while Q_1 has at least two fixed points on $\mathcal{E}_p^1(A)$. Since Q_1Q_2 is abelian, Q_2 moves a Q_1-invariant subgroup to a Q_1-invariant subgroup. Thus, there are at least 3 Q_1-invariant subgroups of order p in A. It follows that Q_1 acts on A as a scalar, i.e. Q_1 does not centralize A but every subgroup of order p in A is Q_1-invariant. By Proposition 6.4 (b), there is $A_0 \in \mathcal{E}^1(A)$ such that $N_G(A_0) \subseteq M$. This implies that $Q_1 \subseteq M$. Then, $Q_1 \subseteq N_M(A)$. By Corollary 6.6 (b), $C = N_M(A)$ is a complement of K in M. The structure of M as a group of type I yields that there is a subgroup C_0 of C with the same exponent as C such that C_0 is a Frobenius complement of the Frobenius group KC_0. We are in the situation that $P = P_0$ is abelian. Then, Lemma 6.8 (a) yields that $q_1 \notin \tau_2(M)$ so C has a cyclic Sylow q_1-subgroup. We may take C_0 such that $Q_1 \subseteq C_0$. Then, $AQ_1 \cap C_0$ has order pq_1 and it is not cyclic. This contradicts the structure of a Frobenius complement. Thus, we have $e \mid p-1$ or $e \mid p+1$. Q.E.D.

Lemma 19.4. *The family $\mathfrak{L}$ is coherent. Let $\lambda$ be the character defined in Lemma* 19.3. *Then, $\lambda^\tau(x) = \lambda(x)$ for $x \in A(L)^\sharp$.*

Proof. Let $e = |L : L'|$. We prove that the set $\mathfrak{L}$ of characters is coherent. Suppose that $L$ is of type I. By Lemma 19.2, $L$ is a Frobenius group with Frobenius kernel U and $L/U$ is a cyclic group of order $e$. By (Iv) for the group of type I, $L$ satisfies one of the three conditions (a), (b), or (c) (cf. [BG], p.128). Since $P \subseteq U$, $U$ is not a TI-set of $L$. Thus, the condition (a) does not nold. If $L$ satisfies (b), $U$ is abelian and $\mathfrak{L}$ is coherent. If $L$ satisfies (c), then the exponent of $L/U$ divides $p-1$. Hence, $e$ divides $p-1$ and

$$|U : U'| \geq p^2 > 4e^2 + 1.$$

Since $\mathfrak{L}(U')$ is coherent, Theorem 12.5 yields that $\mathfrak{L}$ is coherent.

Suppose that $L$ is of type III or IV. Then, $L/H$ is a Frobenius group with Frobenius kernel $UH/H \cong$ U. If $\mathfrak{L}(H)$ is not coherent, Lemma 12.6 yields that $U$ is a nonabelian $p$-group with

$$|U : U'| \leq 4e^2 + 1.$$

Thus, $P = U$ is nonabelian. By Lemma 19.2, the center of $P$ is cyclic. Then, Lemma 19.3 yields $e \mid p-1$. This is a contradiction because

$$p^2 \leq |U : U'| \leq (p-1)^2 + 1 < p^2.$$

It follows that $\mathfrak{L}(H)$ is coherent. By Theorem 16.1 (b), $\mathfrak{L}$ is coherent if $L$ is of type IV.

Suppose that $L$ is of type III and $\mathfrak{L}$ is not coherent. Then, $L/H$ is a Frobenius group with abelian Frobenius kernel which is isomorphic to $U$. Let $\mathfrak{L}_0$ be the set of characters of $L$ which are induced by nonprincipal irreducible characters of L'/H. Then, $\mathfrak{L}_0$ is coherent and $|\mathfrak{L}_0| = (u-1)/e$. If $\mathfrak{L}_1 = \mathfrak{L} - \mathfrak{L}_0$, then by Corollary 18.11, $\mathfrak{L}_1$ is coherent. Since we assumed that $\mathfrak{L}$ is not coherent, Theorem 16.1 (a) yields that $H$ is an elementary abelian group of order r^e for some prime r, $C_U(H) = 1$, and UW_1 acts irreducibly on $H$. Since $A \subseteq \mathcal{E}_p^2(U)$, some nonidentity element of $A$ lies in the inertia group of a nonprincipal linear character of $H$. As we can see from the proof of Lemma 13.8, there is an irreducible character $\mu \in \mathfrak{L}_1$ of degree de with $d \leq (u/p)$ where $u = |U|$. Let $\lambda$ be a character of $\mathfrak{L}_0$. Then, $\lambda$ is an irreducible character of degree $e$. Consider

$$\alpha = \xi_0 - \lambda \quad \text{and} \quad \beta = d\lambda - \mu,$$

where $\xi_0 = (1_{L'})^L$. If $\lambda_1, \lambda_2 \in \mathfrak{L}_0$ are distinct from $\lambda$,

$$(\beta^\tau, (\lambda_1 - \lambda_2)^\tau) = 0 \quad \text{and} \quad (\beta^\tau, (\lambda - \lambda_2)^\tau) = d$$

by Lemma 11.4. Therefore, we have

$$(19.1) \qquad \beta^{\tau} = d\lambda^{\tau} - x \sum_{\nu \in \mathcal{L}_0} \nu^{\tau} - \mu^{\tau} + \Delta_1$$

where $(\Delta_1, \nu^{\tau}) = 0$ for every $\nu \in \mathcal{L}_0$. Lemma 11.4 yields

$$\|\beta^{\tau}\|^2 = \|\beta\|^2 = d^2 + 1.$$

Hence, we have $(d - x)^2 + x^2(((u-1)/e) - 1) + 1 \leq d^2 + 1$, or

$$(19.2) \qquad x^2(u-1)/e \leq 2dx.$$

By Lemma 19.3, e divides $p-1$ or $p+1$. If $2e \neq p+1$, then $2e \leq p-1$. It follows from (19.2) that

$$0 \leq x \leq 2ed/(u-1) \leq (p-1)d/(u-1) < 1$$

because $pd \leq u$ and $d > 1$. The above inequality yields $x = 0$ and $\mathcal{L}$ is coherent. Therefore, we have $2e = p+1$. Since $2ed/(u-1) < 2$, we have $x = 1$.

Consider $\alpha^{\tau} = (\xi_0 - \lambda)^{\tau}$. If we define $\alpha^{\tau} = 1_G + \Delta - \lambda^{\tau}$, then $(\Delta, \nu^{\tau}) = 0$ for every $\nu \in \mathcal{L}_0$, and $\|\Delta\|^2 = e - 1$ (cf. the proof of Lemma 12.7). We will show that

$$\Delta = \sum_{i=1}^{e-1} \eta_{i0}.$$

There is a long detour. The set $\mathcal{L}_1$ contains $|W_2| = r$ reducible characters $\xi_1, \ldots, \xi_{r-1}$. We will show that $\xi_k(1) = ue$ for $k > 0$. Let θ be an irreducible character of minimal degree in $\mathcal{L}_1$ with $\theta(1) = d_1 e$. Then, θ_H contains a nonprincipal linear character η of H and $I(\eta) \cap U \neq 1$. Take a prime $q \in \pi(I(\eta) \cap U)$. Since U is abelian and $A \subseteq \mathsf{U}$, we have $U \subseteq C_G(A) \subseteq M$ by Proposition 6.4 (a). In fact, U is contained in the complement $N_M(A)$ of K in M (Corollary 6.6 (b)). Suppose that $q \neq p$. If $q \in \tau_2(M)$, then $q > p$ by the minimal choice of p in the set ρ. If $q \notin \tau_2(M)$, then U has a cyclic Sylow q-subgroup. Since W_1 acts regularly on U, we have $q \equiv 1 \pmod{e}$. Since $e = (p+1)/2$, we have $q \geq p+2$. If $\beta_1 = d_1\lambda - \theta$,

$$\beta_1{}^{\tau} = d_1\lambda^{\tau} - x_1 \sum \nu^{\tau} - \theta^{\tau} + \Delta_2$$

with $x_1^2(u-1) \leq 2ed_1x_1$. Since $d_1 \leq u/q$, the inequality $x_1 \neq 0$ yields $q(u-1) \leq (p+1)u$. Since $q \geq p+2$,

$$\frac{p+2}{p+1} \leq \frac{u}{u-1}.$$

This implies $p+1 \geq u-1 \geq p^2-1$. This contradiction proves that $x_1 = 0$ and $\mathfrak{L}$ is coherent. Thus,

$$\pi(I(\eta) \cap U) = \{p\}.$$

If $|I(\eta) \cap U| > p$, then we have an irreducible character of degree $d_2 e$ with $d_2 \leq u/p^2$. Then, a similar argument yields

$$p(u-1) \leq (p+1)u/p < 2u.$$

This is impossible. Thus, the degree of an irreducible character in $\mathfrak{L}_1$ is either ue/p or ue. For a nonprincipal linear character η of H, the index $|I(\eta) : H|$ cannot be equal to pe because W_1 does not normalize any subgroup of order p as $|W_1| = e = (p+1)/2$. Hence, the degree $\xi_k(1)$ of the reducible character ξ_k $(k > 0)$ is ue.

As remarked before, H is an abelian r-group for some prime r. We will show that $r \geq 2e$. We have seen that there is a subgroup B of order p in A such that $C_H(B) \neq 1$. Let $H_1 = C_H(B)$. Then, $H = H_1 \times H_2$ with $H_2 = [H, B]$ by Proposition 1.6 [BG]. Since U normalizes B, U acts on H_1 and H_2. If η is a nonprincipal linear character of H/H_2, then $I(\eta) \cap U = B$ as we have shown. It follows that the group U/B acts regularly on H_1. This implies that U/B is cyclic. Hence, $U = B \times C$ with C being cyclic. We will show that C can be chosen in such a way that C acts regularly on H.

The group UW_1 acts on H irreducibly by Theorem 16.1 (a). Since $N_H(A) = C_H(A)$ is W_1-invariant, we have

$$N_L(A) \cap H = N_H(A) = 1.$$

Note that $C_U(H) = 1$ by Theorem 16.1(a). It follows that $N_G(A) = N_L(A) = UW_1$. Since $U \subseteq C_G(A) \subseteq M$ but $N_G(A) \not\subseteq M$, we have $M \cap L = U$. The elementary abelian group A acts on K. Therefore, $C_K(A_1) \neq 1$ for some $A_1 \in \mathcal{E}^1(A)$. Since $C_K(A_1) \not\subseteq L$, M is one of the supporting subgroups of the F-set $A(L) = L'$. By (F*ii*), $C_G(A_1) \subseteq M$. Since $H \cap M = H \cap U = 1$, we have

$$C_H(A_1) = 1.$$

We can take $C \supseteq A_1$. Then, for any subgroup C_1 of prime order in C, $C_H(C_1) = 1$. Therefore, C acts regularly on H. It follows that $r^e \equiv 1 \pmod{u/p}$. If $|H_1| = r^m$, then $m < e$ and $r^m \equiv 1 \pmod{u/p}$. Since e is a prime, we have $r \equiv 1 \pmod{u/p}$. The prime p divides u/p. This implies

$$r-1 \geq p \quad \text{or} \quad r \geq p+1 = 2e.$$

Lemma 13.4 yields that $\xi_k = \sum \mu_{ik}$ where $\{\mu_{ik}\}$ is the set of irreducible characters associated with the selfnormalizing cyclic subgroup $W = W_1 \times W_2$. By the definition of the characters μ_{ik}, there is a sign ε that is independent of i such that $\mu_{ik}(x) = \varepsilon\omega_{ik}(x)$ for all $x \in W - W_2$. We claim that $\varepsilon = 1$. Consider the restriction $(\mu_{0k})_{W_1}$. Then, $(\mu_{0k})_{W_1} - \varepsilon 1_{W_1}$ vanishes on $W_1^\sharp$, so it is a multiple of the regular representation of W_1. Therefore, $\mu_{0k}(1) \equiv \varepsilon \pmod e$. Since $\mu_{0k}(1) = u$, we have $\varepsilon = 1$.

The group W_2 is of order r. Since r is a prime, the characters $\mu_{i1}, \mu_{i2}, \dots, \mu_{ir-1}$ are r-conjugate; so are $\eta_{i1}, \dots, \eta_{ir-1}$. Recall the definition of Δ. It is defined

$$(\xi_0 - \lambda)^\tau = 1_G + \Delta - \lambda^\tau.$$

The weight of Δ is $e-1$ and $(1_G, \Delta) = (\nu^\tau, \Delta) = 0$ for every $\nu \in \mathfrak{L}_0$. We claim that Δ is r-rational and $(\Delta, \eta_{ik}) = 0$ if $k > 0$. Let ν be an irreducible character of $\mathfrak{L}_0$ different from λ. Then, α^τ as well as $(\lambda - \nu)^\tau$ are r-rational by Lemma 11.1. The proof of Lemma 12.1 shows that λ^τ is r-rational. Therefore, Δ is r-rational. Suppose that $(\Delta, \eta_{ik}) = a_k \neq 0$ for some i and $k > 0$. Since $\eta_{i1}, \dots, \eta_{ir-1}$ are r-conjugate, we have $(\Delta, \eta_{it}) = a_k \neq 0$ for every $t > 0$. Thus, Δ involves $a_k \sum_t \eta_{it}$ and

$$\|\Delta\|^2 \geq r - 1.$$

Since $r - 1 \geq 2e - 1$, we have a contradiction that

$$e - 1 = \|\Delta\|^2 \geq 2e - 1.$$

Thus, $(\Delta, \eta_{ik}) = 0$ if $k > 0$.

Finally, we will prove that $\Delta = \sum_i \eta_{i0}$. For a fixed $k > 0$, consider

$$\gamma_i = \mu_{i0} - \mu_{ik} + \Sigma_0$$

where Σ_0 is the sum of irreducible characters of $\mathfrak{L}_0$. There are $(u-1)/e$ characters of degree e in $\mathfrak{L}_0$ and for $x \in {W_1}^\sharp$,

$$\mu_{ik}(x) = \omega_{ik}(x) = \omega_{i0}(x) = \mu_{i0}(x).$$

Since $\mu_{ik}(1) = u$ and $\mu_{i0}(1) = 1$, we have $\gamma_i \in I_0(A_0(L))$. Since

$$(\gamma_0 - \gamma_i)^\tau = (1_L - \mu_{0k} - \mu_{i0} + \mu_{ik})^\tau = 1_G - \eta_{0k} - \eta_{i0} + \eta_{ik},$$

we have ${\gamma_i}^\tau = \eta_{i0} - \eta_{ik} + \Gamma$ where Γ is independent of i. We will compute $({\gamma_0}^\tau, \alpha^\tau)$ using Lemma 11.4. Here, $\alpha = \xi_0 - \lambda$, so $\alpha^\tau = 1_G + \Delta - \lambda^\tau$. Since $\xi_0 = \sum_i \mu_{i0}$, we have

$$({\gamma_0}^\tau, \alpha^\tau) = (\gamma_0, \alpha) = 0.$$

Similarly, $({\gamma_i}^\tau, \alpha^\tau) = (\gamma_i, \alpha) = 0$. Thus, if $i > 0$,

$$\begin{aligned} 0 &= ({\gamma_0}^\tau, \alpha^\tau) = 1 + (\Gamma, \varDelta) - (\Gamma, \lambda^\tau) \\ &= ({\gamma_i}^\tau, \alpha^\tau) = (\eta_{i0}, \varDelta) + (\Gamma, \varDelta) - (\Gamma, \lambda^\tau). \end{aligned}$$

Therefore, $(\eta_{i0}, \varDelta) = 1$. We have used the lemma that $\lambda^\tau \neq \pm\eta_{st}$ for any s and t. We have

$$\varDelta = \sum_{i=0}^{e-1} \eta_{i0}. \tag{19.3}$$

Clearly, $\varDelta$ is a real-valued character. By the definition of β, we have $\overline{\beta} = d\overline{\lambda} - \overline{\mu}$. Then,

$$\beta - \overline{\beta} = d(\lambda - \overline{\lambda}) - (\mu - \overline{\mu}).$$

Since $\beta - \overline{\beta}$, $\lambda - \overline{\lambda}$, and $\mu - \overline{\mu} \in I_0(A(L))$, we have

$$(\beta - \overline{\beta})^\tau = d(\lambda - \overline{\lambda})^\tau - (\mu - \overline{\mu})^\tau = d(\lambda^\tau - \overline{\lambda}^\tau) - (\mu^\tau - \overline{\mu}^\tau).$$

On the other hand, we can compute $(\beta - \overline{\beta})^\tau = \beta^\tau - \overline{\beta}^\tau$ using (19.1). Since $\sum \nu^\tau$ is real, we have

$$\beta^\tau - \overline{\beta}^\tau = d(\lambda^\tau - \overline{\lambda}^\tau) - (\mu^\tau - \overline{\mu}^\tau) + \varDelta_1 - \overline{\varDelta}_1.$$

Therefore, $\varDelta_1 = \overline{\varDelta}_1$ is a real-valued virtual character. It follows from (19.3) that $(\varDelta, \varDelta_1)$ is an even integer. We will contradict this by showing $(\varDelta, \varDelta_1) = -1$.

Compute $(\alpha^\tau, \beta^\tau)$ in two ways. Lemma 11.4 yields

$$(\alpha^\tau, \beta^\tau) = (\alpha, \beta) = -d.$$

By (19.1), we have

$$(\alpha^\tau, \beta^\tau) = (\varDelta, \varDelta_1) - (d-1) = (\varDelta, \varDelta_1) - d + 1.$$

Thus, $(\varDelta, \varDelta_1) = -1$. This contradiction proves that $\mathfrak{L}$ is coherent in all cases.

We can apply Lemma 12.7 for M, H, H_1, h and $\mathfrak{S}$ replaced by L, L', L'', p^2 and $\mathfrak{L}$. Since $P \subseteq U$ and U is nilpotent, we have $|L' : L''| \geq p^2$. By Lemma 19.3, $e \leq (p+1)/2$. This implies $p^2 - 1 > e(e+1)$. If we define $\varDelta$ by $(\xi_0 - \lambda)^\tau = 1_G + \varDelta - \lambda^\tau$ and

$${\xi_0}^\tau = 1 + \varDelta,$$

the set $\{\mathcal{L}, \xi_0\}$ is coherent by Lemma 12.7.

For $x \in A(L)^\sharp$, Lemma 14.4 yields that

$$\lambda^\tau(x) = \lambda(x) + s\gamma(x)$$

where s is a rational number and γ is a virtual character that is orthogonal to every element of $\mathcal{L}^* = \{\mathcal{L}, \xi_0\}$. If L is of type I, $\mathcal{L}$ consists of all nonlinear irreducible characters of L. Thus, $\gamma = \sum a_i\lambda_i$ where λ_i are linear characters of L/L'. Since $\xi_0 = \sum \lambda_i$, $(\gamma, \xi_0) = 0$ means $\sum a_i = 0$. Thus, for an element x of L', we have $\gamma(x) = 0$. This proves $\lambda^\tau(x) = \lambda(x)$ in this case.

If L is not of type I, then $\mathcal{L}^*$ consists of irreducible characters induced by characters of L' and ξ_k for $0 \leq k \leq w_2 - 1$. Thus, $\gamma = \sum a_{st}\mu_{st}$ with $(\gamma, \xi_k) = 0$ for all k. Then, for each k, $\sum_s a_{sk} = 0$. Since $(\mu_{sk})_{L'} = (\mu_{tk})_{L'}$ by Lemma 13.4, $\gamma(x) = 0$ for $x \in L'$. This proves that $\lambda^\tau(x) = \lambda(x)$ for $x \in A(L)^\sharp$. Q.E.D.

The next lemma is stated in [FT], p. 980, without proof.

Lemma P. *Let $M, L \in \mathcal{M}$. If M and L are not conjugate, no subgroup of $\mathcal{M}$ can serve as a supporting subgroup of $A(M)$ and at the same time of $A(L)$.*

Proof. Suppose that $N \in \mathcal{M}$ is a supporting subgroup of $A(M)$. Then, there is an element $x \in A(M)$ such that $C_G(x) \not\subseteq M$ and $C_G(x) \subseteq N$. By Theorem II, $x \in {M_{\sigma_0}}^\sharp$ and $M \cap N$ is a complement of N_σ in N. By Theorem 8.4, $\pi(\langle x\rangle) \subseteq \tau_2(N)$. Similarly, if N is a supporting subgroup of $A(L)$, there is an element $y \in {L_{\sigma_0}}^\sharp$ such that $C_G(y) \not\subseteq L$, $C_G(y) \subseteq N$, $\pi(\langle y\rangle) \subseteq \tau_2(N)$, and $L \cap N$ is a complement of N_σ in N. Since N_σ is a Hall normal subgroup of N, $L \cap N$ is conjugate to $M \cap N$ in N. Let $M \cap N = (L \cap N)^g$ for $g \in N$ and let $x' = y^g$. Then, $x, x' \in M \cap N$.

Take $p \in \tau_2(N)$ and suppose that G has a nonabelian Sylow p-subgroup. Then, by Theorem 6.7 (a), $\tau_2(N) = \{p\}$. Therefore, both x and y are p-elements and $\sigma(M) \cap \sigma(L) \neq \emptyset$. Since M is not conjugate to L, this contradicts Theorem 7.9. Hence, G has an abelian Sylow subgroup for every prime in $\tau_2(N)$. By Lemma 6.8 (a), a Hall $\tau_2(N)$-subgroup E_2 of $M \cap N$ is a normal abelian subgroup of $M \cap N$. Since $x, x' \in E_2$, they commute. The element x' is a $\sigma_0(L)$-element. Hence, x' is a $\sigma(M)'$-element by Theorem 7.9. By Corollary 8.3, we have either (1) $\pi(\langle x'\rangle) \subseteq \kappa(M)$ and $C_G(x) \subseteq M$, or (2) $\pi(\langle x'\rangle) \subseteq \tau_2(M)$ and $\mathcal{M}(C_G(x')) = \{M\}$. Since $C_G(x) \not\subseteq M$ and $C_G(x') \subseteq N$, neither case holds. This contradiction proves Lemma P. Q.E.D.

Lemma Q. *For each $M \in \mathcal{M}$, let $G_0(M)$ be the territory of M. Let $L \in \mathcal{M}$ and assume that L is not conjugate to M. Then,*

$$G_0(M) \cap G_0(L) = \emptyset$$

unless either M is conjugate to a supporting subgroup for $A(L)$ or L is conjugate to a supporting subgroup for $A(M)$.

Proof. The elements of $A(x)$ are of the form hx where $h \in C_H(x)$ and the order of x is prime to the order of h. The subgroup H is a supporting subgroup for $A(M)$; thus, $H = H_i = (M_i)_\sigma = (M_i)_F$ for some $M_i \in \mathcal{M}$. Suppose that $G_0(M) \cap G_0(L) \neq \emptyset$ and

$$g^{-1}(hx)g = ky$$

where k is an element of a supporting subgroup K of $A(L)$ and $ky = yk$ for some $y \in A(L)$.

Suppose that $h \neq 1$. Then, $C_G(x) \not\subseteq M$ and $C_G(x) \subseteq M_i$. By Theorem II, this implies $x \in {M_{\sigma_0}}^\sharp$ and $y \in {N_\sigma}^\sharp$. Note that any supporting subgroup is a ϖ-group. If $k \neq 1$, we have $y \in {L_{\sigma_0}}^\sharp$. Since $\pi(\langle y \rangle) \subseteq \pi(\langle h \rangle) \cup \pi(\langle x \rangle)$,

$$\sigma(L) \cap \sigma(M_i) \neq \emptyset \quad \text{or} \quad \sigma(L) \cap \sigma(M) \neq \emptyset.$$

By Theorem 7.9, L is conjugate to M_i that is a supporting subgroup for $A(M)$. Suppose that $k = 1$. If $\pi(\langle y \rangle) \cap \sigma(L) \neq \emptyset$, then the preceding argument shows that L is conjugate to M_i. Assume that $\pi(\langle y \rangle) \cap \sigma(L) = \emptyset$. Then, y is an $\sigma(L)'$-element of $A(L)$. Theorem II yields that $C_G(y) \subseteq L$. Since $g^{-1}(hx)g = y$, we have

$$C_G(y) \subseteq C_G(g^{-1}xg) = g^{-1}C_G(x)g \subseteq (M_i)^g.$$

By the definition of $A(L)$, y commutes with an element z of ${L_\sigma}^\sharp$. Since y is a ϖ-element, we have $z \in {L_{\sigma_0}}^\sharp$. Corollary 8.3 yields that either $\pi(\langle y \rangle) \subseteq \kappa(L)$ or $\mathcal{M}(C_G(y)) = \{L\}$. The definition of $A(L)$ yields that nonidentity elements of Hall $\kappa(L)$-subgroups are excluded from $A(L)$. Thus, the first possibility does not occur.

Therefore, we have $\mathcal{M}(C_G(y)) = \{L\}$. It follows from $C_G(y) \subseteq (M_i)^g$ that $L = {M_i}^g$.

If $k \neq 1$, a similar proof shows that M is conjugate to a supporting subgroup for $A(L)$. Suppose that $h = 1 = k$. Suppose that $\pi(\langle x \rangle) \subseteq \sigma_0(M)$. Then, $C_G(x)$ is contained in either M or a conjugate of a supporting subgroup. Since L is not conjugate to M, Theorem 7.9 yields that $\pi(\langle y \rangle) \cap \sigma(L) = \emptyset$. The argument of the preceding paragraph proves that $\mathcal{M}(C_G(y)) = \{L\}$. Since y is conjugate to x, we conclude that L is conjugate to a supporting subgroup of $A(M)$.

Suppose that $\pi(\langle x\rangle) \not\subseteq \sigma_0(M)$. Note that x centralizes some nonidentity element of M_F. Since M_F is a ϖ-group, x is a ϖ-element. Since $\pi(\langle x\rangle) \not\subseteq \sigma_0(M)$, there is a Hall subgroup $\langle x'\rangle$ of $\langle x\rangle$ such that x' is a $\sigma(M)'$-element and x' commutes with an element u of ${M_{\sigma_0}}^\sharp$. As before, Corollary 8.3 yields that $\mathcal{M}(C_G(x')) = \{M\}$. Since $x^g = y$, the element $(x')^g = y'$ is a power of y. Thus, $y' \in A(L)$. It follows that $C_G(y')$ is contained in either L or a conjugate of a supporting subgroup of $A(L)$. Since

$$\mathcal{M}(C_G(y')) = \mathcal{M}(C_G(x'))^g = \{M^g\},$$

M is conjugate to a supporting subgroup for $A(L)$. Q.E.D.

Lemma 19.5. *Let λ be the irreducible character in $\mathcal{L}$ defined in Lemma* 19.3. *Then, λ^τ is conformal relative to $A(M)$ and*

$$\frac{1}{|M|}\sum_{x\in K^\sharp} |\lambda^\tau(x)|^2 < \frac{\lambda(1)^2}{|L|}.$$

Proof. We will prove that λ^τ is conformal relative to M. Let N be a supporting subgroup of $A(M)$. Since M is of type I but not a Frobenius group, Theorem II yields that N is of type I. Let $\Theta = \lambda^\tau$.

By Lemma 14.1, it suffices to check that Θ is orthogonal to every virtual character of the form $(\theta_1 - \theta_2)^G$ with $\theta_1, \theta_2 \in S(\alpha)$ for $\alpha \neq 1_H$, $\alpha \in \mathrm{Irr}(H)$. For the notation, see Lemma 14.1. Since N is of type I, θ_1 and θ_2 are irreducible characters of N and $\theta_1 - \theta_2$ vanishes outside $A(N)-H$. By (F*ii*)(d), $A(N)-H$ is a TI-set. This implies that $(\theta_1-\theta_2)^G$ is a difference of two irreducible characters of G. Let

$$(\theta_1 - \theta_2)^G = \Theta_1 - \Theta_2.$$

If $\lambda^\tau = \Theta$ is not orthogonal to $(\theta_1 - \theta_2)^G$, then Θ must be either Θ_1 or Θ_2. The virtual character $\Theta_1 - \Theta_2$ vanishes outside the territory $G_0(N)$ of N. Lemma 19.2 yields that L is either a Frobenius group or of type III or IV. Thus, by (F*ii*)(d) or (F*iii*), L is not conjugate to any supporting subgroup for A(N). Since N is not a Frobenius group by (F*ii*)(d), N is not conjugate to L. By definition, N is a supporting subgroup for $A(M)$. Hence, by Lemma P, N is not conjugate to any supporting subgroup for $A(L)$. By Lemma Q, the territory of L is disjoint from that of N. Since $\mathcal{L}$ is coherent by Lemma 19.4, $\Theta - \overline{\Theta}$ vanishes outside of $G_0(L)$. Then, we have

$$((\theta_1 - \theta_2)^G, \Theta - \overline{\Theta}) = 0$$

because $G_0(N) \cap G_0(L) = \emptyset$. Thus, $(\theta_1 - \theta_2)^G$ contains Θ and $\overline{\Theta}$ with the same multiplicity. Since $\Theta \neq \overline{\Theta}$, this is a contradiction and proves that λ^τ is conformal relative to M.

We can apply Lemmas 12.5 and 12.6 to $\Theta(x) = |\lambda^\tau(x)|^2$. Let $G_1(M)$ be the proper territory of M. Then, $G_1(M)$ is the set of elements of G which are conjugate to some element of $A(x)$ with $x \in K^\sharp$. Since L is not conjugate to M, $\sigma(L) \cap \sigma(M) = \emptyset$ by Theorem 7.9. It follows that $G_1(M)$ is disjoint from $G_0(L)$. Lemma 12.6 yields

$$\frac{1}{|M|} \sum_{x \in K^\sharp} |\lambda^\tau(x)|^2 = \frac{1}{|G|} \sum_{x \in G_1(M)} |\lambda^\tau(x)|^2.$$

Since $G_1(M) \cap G_0(L) = \emptyset$, the orthogonality relation yields

$$\frac{1}{|G|} \sum_{x \in G_1(M)} |\lambda^\tau(x)|^2 < 1 - \frac{1}{|G|} \sum_{x \in G_0(L)} |\lambda^\tau(x)|^2.$$

Then, Lemmas 12.5 and 19.4 yield

$$\frac{1}{|M|} \sum_{x \in K^\sharp} |\lambda^\tau(x)|^2 < 1 - \frac{1}{|L|} \sum_{x \in (L')^\sharp} |\lambda(x)|^2.$$

The right side is equal to $\lambda(1)^2/|L|$ because λ vanishes outside L'.

Q.E.D.

Lemma 19.6. *Let $F = M \cap L$. Then, F is a complement of K in M. There is an element z of $A \cap Z(F)^\sharp$ such that $C_K(z) \not\subseteq K'$.*

Proof. We have $A \subseteq M \cap L$ and some nonidentity element of A has a nontrivial centralizer in K. Thus, M is a supporting subgroup for $A(L)$. By (F*ii*), $M \cap L = F$ is a complement of K in M.

Since M is of type I, F contains a subgroup F_0 of the same exponent as F that acts regularly on K. It follows that any subgroup of $\mathcal{E}^1(F_0)$ lies in the center $Z(F_0)$. Therefore, there is no Frobenius group that contains A. Note that A is the set of elements of order p in F by Corollary 6.6 (a) and Theorem 6.5 (b).

If L is of type I, L is a Frobenius group by Lemma 19.2. Since F is not a Frobenius group as shown in the preceding paragraph, we have $F \subseteq U$. Therefore, F is nilpotent. By (I*iv*) for M, every Sylow subgroup of F is abelian. Hence, F is abelian. The group $A \in \mathcal{E}_p^2(F)$ acts on K/K'. By Proposition 1.16 [BG], there is an element $z \in A^\sharp$ such that $C_{K/K'}(z) \neq 1$. Proposition 1.5 [BG] shows that $C_K(z) \not\subseteq K'$. This proves Lemma 19.6 if L is of type I.

Suppose that L is of type III or IV. We may assume $P \subseteq U$. If $F \not\subseteq L'$, we may choose $W_1 \subseteq F$. Then, $\langle A, W_1\rangle$ is a Frobenius group in F. This does not occur. Therefore, $F \subseteq L'$. Let $F_1 = F \cap H$. Then, F_1 is a normal subgroup of F. We may assume that $F = F_1(F \cap U)$ by replacing U by a conjugate if necessary. Since U is nilpotent by (T2), $F \cap U$ is abelian. The subgroup A lies in $F \cap U$ and $A \lhd F$ by Corollary 6.6 (a). Therefore, $[F_1, A] = 1$ and $A \subseteq Z(F)$. Then, Lemma 19.6 holds as before. Q.E.D.

Lemma 19.7. *Let* M *be the set of all irreducible characters of* M *which do not have* K *in their kernel. Let* λ *be the character defined in Lemma* 19.3. *If* M *is coherent, then* λ^τ *is constant on* $K^\sharp$.

Proof. Let a be the least common multiple of the orders of all the elements of $A(L)$. By Lemma 19.2, we have $A(L) = L' = L_\sigma$. Since M is not conjugate to L, Theorem 7.9 yields that $\sigma(L) \cap \sigma(M) = \emptyset$. Thus, $(a, |K|) = 1$. Since $\mathfrak{L}$ is coherent by Lemma 19.4, we can apply Lemma 12.1 to conclude that the values taken by λ^τ lie in the field $\mathbb{Q}_a$. Lemma 19.5 yields that λ^τ is conformal relative to $A(M)$. Assume that M is coherent. We will show that λ^τ is orthogonal to every element of M^τ. Let α be a character of M. Then, α_K is not rational as $\overline{\alpha}_K \neq \alpha_K$. Since $(a, |K|) = 1$, there is a Galois automorphism that sends α_K to $\overline{\alpha}_K$ and induces the identity on $\mathbb{Q}_a$. This yields that $\lambda^\tau \neq \alpha^\tau$. Lemma 14.4 yields that there is a pair (r, β) of a rational number r and a virtual character β of M such that β is orthogonal to every element of M and $\lambda^\tau(x) = r\beta(x)$ for $x \in A(M)^\sharp$. Then, β is a linear combination of irreducible characters of M/K. Thus, $\lambda^\tau(x) = r\beta(x)$ for $x \in K^\sharp$ and λ^τ is constant on $K^\sharp$. Q.E.D.

Proof of Theorem 19.1. For some element x of $A^\sharp$, $C_K(x) \neq 1$. Take $y \in C_K(x)^\sharp$. Since M is a supporting subgroup for $A(L)$, Lemma 14.3 yields that λ^τ is conformal relative to $A(L)$. Thus, λ^τ is constant on the annex $A(x)$. It follows that

$$\lambda^\tau(xy) = \lambda^\tau(x) = \lambda(x).$$

The last equality comes from Lemma 19.4. Let $\mathbb{Q}_0$ be the field of primitive $|G|$th roots of unity and let $\mathfrak{P}$ be the prime ideal dividing p in the ring of integers in $\mathbb{Q}_0$. By Lemma 4.2 [FT], we have

$$\lambda^\tau(y) \equiv \lambda^\tau(xy) = \lambda(x) \equiv \lambda(1) \pmod{\mathfrak{P}}.$$

The values taken by λ^τ lie in $\mathbb{Q}_a$ where a is the exponent of L'. Therefore,

$\lambda^\tau(y)$ is a rational number, so we have

$$\lambda^\tau(y) \equiv \lambda(1) \pmod{p}.$$

By Lemma 19.3, $\lambda(1)$ divides $p+1$ or $p-1$. This yields that $\lambda(1) \leq (p+1)/2$ and

$$|\lambda^\tau(y)| \geq p - \lambda(1) \geq \lambda(1) - 1. \tag{19.4}$$

This inequality holds whenever $y \neq 1$ commutes with an element $x \in A^\sharp$. As before, let F be a complement of K in M. Lemma 19.6 yields that there is an element $z \in A^\sharp \cap Z(F)$ such that $C_K(z) \not\subseteq K'$. If $C_K(z) = K$, then (19.4) holds for every $y \in K^\sharp$. If $C_K(z) \neq K$, then Theorem 15.2 yields that M is coherent. By Lemma 19.7, λ^τ is constant on $K^\sharp$. Since (19.4) holds for at least one element of $K^\sharp$, it holds for every $y \in K^\sharp$ because λ^τ is constant on $K^\sharp$.

Let $e = \lambda(1)$. Then, Lemma 19.5 yields that

$$\frac{1}{|M|}(|K|-1)(e-1)^2 \leq \frac{1}{|M|}\sum_{x \in K^\sharp} |\lambda^\tau(x)|^2 < \frac{e^2}{|L|}.$$

Since $|M| = |K||M \cap L|$, we have

$$\frac{(|K|-1)}{|K|}\left(\frac{e-1}{e}\right)^2 < \frac{|M \cap L|}{|L|} \leq \frac{1}{3}.$$

Since $(e-1)/e \geq 2/3$, $|K| < 4$ and $|K| = 3$. The subgroup K is a Hall subgroup of G with $|N_G(K)|$ odd. Then, G is not simple. This contradicts the assumption. Thus, Theorem 19.1 holds. Q.E.D.

Theorem 19.8. *If there is no subgroup of type II, then G contains a nilpotent Hall ϖ-subgroup that is isolated.*

Proof. By Theorem I, all $M \in \mathcal{M}$ are of type I. By Theorem 19.1, they are Frobenius groups. It follows from (F*ii*)(d) that no supporting subgroup of type I is a Frobenius group. Thus, if $M \in \mathcal{M}$, there is no supporting subgroup for $A(M)$. Therefore, if $H = M_F$, then $H = M_{\sigma_0}$ and, for every $x \in H^\sharp$, $C_G(x) \subseteq M$. Since M is a Frobenius group, we have $C_G(x) \subseteq H$.

Take a prime $p \in \varpi$, $P \in Syl_p(G)$, and $M \in \mathcal{M}(N_G(P))$. Then, M is of type I. Therefore, M is a Frobenius group with Frobenius kernel $H = M_{\sigma_0} = M_F$ and $P \subseteq H$. Thus, H is a nilpotent ϖ-subgroup having the property that $C_G(x) \subseteq H$ for every $x \in H^\sharp$. We will show that H is a Hall ϖ-subgroup of G that is isolated.

Take a prime q in ϖ and suppose that pq is an edge of the prime graph of G. Then, there is a pair (x, y) of elements x and y such that $x \in P^\sharp$ and y is an element of $C_G(x)^\sharp$ of order q. Let $Q \in Sy\ell_q(G)$ such that $y \in Q$ and let $z \in Z(Q)^\sharp$. Then, starting from $x \in P^\sharp$ we have in succession $y \in H$, $z \in H$, and $Q \subseteq H$. Repeating this argument, we conclude that if $r \in \varpi$, then H contains a Sylow r-subgroup of G. Therefore, H is a Hall ϖ-subgroup of G. It is nilpotent and isolated.

Q.E.D.

§20. The Pair of Subgroups S and T

In this section, we will assume that there is a subgroup in $\mathcal{M}$ that is not of type I. Theorem I yields that there is a pair of subgroups S and T which satisfy the conditions (a)—(e) of Theorem I. By Theorem 18.10, each of them is of type II, III, or IV. Throughout this section, we follow the notation of Section 34 of [FT]. Thus, p and q are distinct primes in ϖ such that

$$W = P^*Q^*, \ S = S'Q^*, \ T = T'P^*, \ |P^*| = p, \quad \text{and} \quad |Q^*| = q.$$

Let $P \in Sy\ell_p(S)$ and $Q \in Sy\ell_q(T)$. By Theorem C(2), $P^* \subseteq S_F$. Therefore, $P \subseteq S_F$ and P is a normal subgroup of S. It follows that $P^* \subseteq P$. Similarly, $Q^* \subseteq Q \lhd T$.

Let U be a Q^*-invariant complement of P in S'. Then, UQ^* is a complement of P in S. Let

$$C = C_{\mathsf{U}}(P).$$

Then, $C \lhd U$. Since $P^* \subseteq P$, we have $P^* \cap U = 1$. Proposition 8.2 (b) yields that Q^* acts regularly on U. Thus, the group UQ^* is a Frobenius group with Frobenius kernel U. Then, the prime q does not divide the order of U. Thus,

$$Q^* \in Sy\ell_q(S).$$

Also, U is nilpotent. Since $C \subseteq U$, C is nilpotent; so is $PC = P \times C$. It follows that $PC \subseteq F(S)$. Clearly, we have $F(S) = P \times (F(S) \cap U) \subseteq PC$. Therefore,

$$F(S) = P \times C = PC.$$

By (T3), $S'' \subseteq F(S) \subseteq S'$. It follows that $S'/PC \cong U/C$ is abelian.

Similarly, let V be a P^*-invariant complement of Q in S'. Then, VP^* is a complement of Q in T and VP^* is a Frobenius group with Frobenius kernel V. Also, $P^* \in Sy\ell_p(T)$. Let

$$D = C_V(Q).$$

Then, $D \lhd V$, $QD = F(T)$ and $T'/QD \cong V/D$ is abelian. Note that $A(S)$ is a TI-set of G with normalizer S. This is proved as follows. If $A(S)$ is not a TI-set, there is an element $x \in A(S)^\sharp$ such that $C_G(x) \not\subseteq S$. Then, $C_G(x)$ is contained in a conjugate of a supporting subgroup M_i by (F*ii*)(e). Since S is not of type I, M_i is of type I by (F*iii*). Then, by Theorem 19.1, M_i is a Frobenius group. But, none of the supporting subgroups can be a Frobenius group by (F*ii*)(d). Thus, $A(S)$ is a TI-set of G.

Similarly, $A(T)$ is a TI-set.

Let $\mathcal{S}$ be the set of characters of S which are induced by irreducible characters of S' not having P in their kernel. Since $P \subseteq S_F$, this set $\mathcal{S}$ is a part of the set of characters considered in §16 for subgroups of type II, III, or IV. Hence, Corollary 18.11 yields that the set $\mathcal{S}$ defined here is coherent. Let $\mathcal{T}$ be the set of characters of T induced by irreducible characters of T' which do not have Q in their kernel. Then, $\mathcal{T}$ is also coherent.

Let η_{ij} be the virtual characters of weight 1 associated with the self-normalizing cyclic group $W = P^*Q^*$. We use the notation of §13 and

$$\eta_{ij}(x) = \omega_{ij}(x) \quad \text{for} \quad x \in \widehat{W}.$$

Let μ_{ij} be the set of irreducible characters of S defined in Lemma 13.4. Then, $\mu_{ij}(x) = \varepsilon_j \omega_{ij}(x)$ for $x \in \widehat{W}$ with $\varepsilon_j = 1$ or -1. Let

$$\xi_k = \sum_{i=0}^{q-1} \mu_{ik}.$$

Similarly, let ν_{ij} be the set of irreducible characters of T defined in Lemma 13.4. Thus, $\nu_{ij}(x) = \pm\omega_{ij}(x)$ for $x \in \widehat{W}$, where the sign is independent of j. Let

$$\zeta_i = \sum_{j=0}^{p-1} \nu_{ij}.$$

By Lemma 13.5, characters of $\mathcal{S}$ (or $\mathcal{T}$) are either irreducible or one of the characters ξ_j $(0 \le j \le p-1)$ (or ζ_i $(0 \le i \le q-1)$).

We use the following notation:

$$|C| = c, \ |D| = d, \ |U\!:\!C| = u, \ |V\!:\!D| = v, \ \text{ and } \ |G| = g.$$

For the following lemmas in this section, we maintain the symmetry between S and T. So, the results proved for S hold for T as well.

Lemma 20.1. *There is a normal subgroup P_0 of S such that $P_0 \subseteq P$, P/P_0 is an elementary abelian group of order p^q, and the group UQ^* acts irreducibly on P/P_0. Either U/C is a cyclic group with u dividing $(p^q-1)/(p-1)$ that acts irreducibly and regularly on P/P_0, or U/C is a product of at most $q-1$ cyclic groups with u dividing $(p-1)^{q-1}$. For $1 \le j \le p-1$, ξ_j is induced by a linear character of PC and $\xi_j(1) = uq$. Either PU is a Frobenius group with Frobenius kernel P such that $|P| = p^q$ and $u = (p^q-1)/(p-1)$, or $\mathcal{S}$ contains an irreducible character of degree uq that is induced by a linear character of PC.*

This is Lemma 34.1 [FT]. Some additional remarks included in Lemma 20.1 are really proved there. Q.E.D.

Lemma 20.2. *Either PU is a Frobenius group with Frobenius kernel P with $|P| = p^q$ and $u = (p^q-1)/(p-1)$, or QV is a Frobenius group with Frobenius kernel Q with $|Q| = q^p$ and $v = (q^p-1)/(q-1)$.*

Proof. This is Lemma 34.2 [FT]. We paraphrase their proof. Suppose that the result is false. Then, Lemma 20.1 yields that $\mathcal{S}$ contains an irreducible character λ of degree uq that is induced by a linear character of PC and $\mathcal{T}$ contains an irreducible character θ of degree vp that is induced by a linear character of QD. Define

$$\alpha = \lambda - \xi_1 \quad \text{and} \quad \beta = \theta - \zeta_1.$$

Then, α^τ takes nonzero values only on conjugates of $(PC)^\sharp$. Since $PC = F(S)$, α^τ is nonzero only at $\sigma(S)$-elements. Similarly, β^τ is nonzero only at $\sigma(T)$-elements. Since S is not conjugate to T, Theorem 7.9 yields that $\sigma(S) \cap \sigma(T) = \emptyset$; hence, $(\alpha^\tau, \beta^\tau) = 0$. Similarly,

$$((\lambda - \overline{\lambda})^\tau, (\beta - \overline{\beta})^\tau) = 0.$$

This implies $\lambda^\tau \neq \theta^\tau$ since $\lambda \neq \overline{\lambda}$.

By Lemma 13.7, $\xi_1^\tau = \pm\sum_{i=0}^{q-1} \eta_{i1}$ and $\zeta_1^\tau = \pm\sum_j \eta_{1j}$. By Lemma O, we have $\lambda^\tau \neq \pm\eta_{st} \neq \theta^\tau$. Thus,

$$(\alpha^\tau, \beta^\tau) = (\lambda^\tau - \xi_1^\tau, \theta^\tau - \zeta_1^\tau) = (\pm\sum_i \eta_{i1}, \pm\sum_j \eta_{1j}) = \pm 1.$$

This contradicts $(\alpha^\tau, \beta^\tau) = 0$. Q.E.D.

Lemma 20.3. *For $1 \le j \le p-1$,*

$$\sum_{x \in (PC)^\sharp} |\eta_{0j}(x)|^2 \ge uc|P| - u^2.$$

Proof. We paraphrase the proof of Lemma 34.3 [FT]. The set of irreducible characters of S consists of $\{\mu_{ij}\}$, $0 \leq i \leq q-1$, $0 \leq j \leq p-1$, the set $\operatorname{Irr} \mathcal{S}$ of irreducible characters in $\mathcal{S}$, and the set $\operatorname{Irr}(S/P)$. By Lemma 13.7, ${\xi_t}^\tau = \varepsilon_t \sum_i \eta_{it}$. Write the restriction $(\eta_{0t})_S$ as a linear combination of irreducible characters of S as follows:

$$(20.1) \qquad (\eta_{0t})_S = \varepsilon\mu_{0t} + \sum_{s,t>0} c_{st}\mu_{st} + \sum_{\lambda \in \operatorname{Irr}\mathcal{S}} a_\lambda \lambda + \Delta$$

where $\varepsilon = \varepsilon_j$ and Δ is a character of S/P. Since $\mathcal{S}$ is coherent, Lemmas M and 11.4 yield

$$(20.2) \qquad (\alpha^\tau, \eta_{0j}) = (\alpha, (\eta_{0j})_S)$$

for every $\alpha \in I_0(\mathcal{S})$. Take j and k with $1 \leq j, k \leq p-1$ and let $\alpha = \xi_j - \xi_k$. Note that $\xi_j(1) = uq = \xi_k(1)$, so $\alpha \in I_0(\mathcal{S})$. Then, (20.1) and (20.2) yield

$$\sum_{s=0}^{q-1} c_{sj} = \sum_{s=0}^{q-1} c_{sk}$$

including $k = t$. For each k, $(\mu_{ik})_{S'}$ is independent of i by Lemma 13.4 and $(\mu_{ik})_{S'} = \psi_k$ is an irreducible character of degree u of S'. Then, we have

$$\left(\sum_{s,t>0} c_{st}\mu_{st}\right)_{S'} = a\sum_{k=1}^{p-1} \psi_k(1)\psi_k$$

with $a\psi_k(1) = au = \sum_{s=0}^{q-1} c_{sk}$. Thus, a is a rational number such that au is an integer. If $\operatorname{Irr}\mathcal{S}$ is not empty, take $\lambda \in \operatorname{Irr}\mathcal{S}$. Then, $\lambda(1)$ is divisible by q because λ is induced by an irreducible character θ of S'. Let $\alpha = \theta(1)\xi_k - u\lambda$. Since $\xi_k(1) = uq$, we have $\alpha \in I_0(\mathcal{S})$. Then, (20.1) and (20.2), together with Lemma N, yield

$$\theta(1)\sum_{s=0}^{q-1} c_{sk} = ua_\lambda \quad \text{or} \quad a_\lambda = a\theta(1).$$

Therefore,

$$\left(\sum_\lambda a_\lambda \lambda\right)_{S'} = a\sum_\lambda \theta(1)(\theta_1 + \cdots + \theta_q)$$

where $\theta_1, \ldots, \theta_q$ are components of $\lambda_{S'}$. It follows that

$$\left(\sum_{s,t>0} c_{st}\mu_{st} + \sum_\lambda a_\lambda \lambda\right)_{S'} = a\rho_1$$

where ρ_1 is the portion of the regular representation of S' on the set of irreducible characters which do not have P in their kernel. Let ρ be the regular representation of S' and write $\rho = \rho_1 + \rho_2$. Then, ρ_2 is the regular representation of S'/P. If x is a nonidentity element of S', then

$$0 = \rho(x) = \rho_1(x) + \rho_2(x).$$

Let $\beta = -a\rho_2 + \Delta_{S'}$. Then, β is a linear combination of irreducible characters of S'/P with rational coefficients. It follows that for $x \in (S')^\sharp$,

$$\eta_{0t}(x) = \varepsilon\psi_t(x) + \beta(x).$$

Since $\rho_2(1) = |S'/P| = cu$, $\beta(1) = -acu + \Delta_{S'}(1)$ is an integer because $\Delta_{S'}$ is a character and au is an integer. The remainder of the proof is the same as the proof of Lemma 34.3 [FT]. We have

$$\begin{aligned}\sum_{x\in(PC)^\sharp} |\eta_{0t}(x)|^2 &= \sum(\varepsilon\psi_t(x) + \beta(x))(\varepsilon\overline{\psi}_t(x) + \overline{\beta}(x)) \\ &= \sum |\psi_t(x)|^2 + \varepsilon\sum(\psi_t(x)\overline{\beta}(x) \\ &\qquad + \overline{\psi}_t(x)\beta(x)) + \sum|\beta(x)|^2.\end{aligned}$$

Since ψ_t is an irreducible character that vanishes outside PC, the first term is $uc|P| - u^2$. Since β is a sum of irreducible characters of S'/P, the second sum is equal to $-2\varepsilon u\beta(1)$. The values of β are constant on each coset of P. Thus, the third sum is

$$|P|\sum_{x\in U} |\beta(x)|^2 - \beta(1)^2.$$

Lemma 20.1 yields that u divides either $(p^q - 1)/(p-1)$ or $(p-1)^{q-1}$, and $|P| \geq p^q$. Hence, we have

$$|P| \geq 2u + 1$$

and $|P|\beta(1)^2 - \beta(1)^2 - 2eu\beta(1) \geq 2u(\beta(1)^2 - \varepsilon\beta(1)) \geq 0$ because $\beta(1)$ is an integer. This proves Lemma 20.3. Q.E.D.

Lemma 20.4. *For* $1 \leq i \leq q-1$,

$$\sum_{x\in PC-C} |\eta_{i0}(x)|^2 \geq (|P|-1)c.$$

Proof. We use the same method as in the proof of Lemma 20.3. Since η_{i0} is orthogonal to every character of $\mathcal{S}^\tau$, we have

$$(\eta_{i0})_{S'} = a\rho_1 + \gamma$$

where au is an integer, ρ_1 is the portion of the regular representation ρ with $\rho - \rho_1$ the regular representation of S'/P, and γ is a character of S'/P. Then, ρ_1 vanishes outside P, ρ_1 takes the value $-uc$ on $P-1$, and $\rho_1(1) = (|P|-1)uc$. Let $\delta = (\eta_{i0})_U$ and $y \in P^{*\sharp}$. Since γ is a character of S'/P, $(\eta_{i0})_{S'}$ takes a constant value on each coset of P except at the identity. Thus,

(20.3)

$$\begin{aligned}\sum_{x\in PC-C} |\eta_{i0}(x)|^2 &= (|P|-1)\left(\sum_{x\in U^\sharp} |\delta(x)|^2 + |\eta_{i0}(y)|^2\right)\\ &= (|P|-1)(c\|\delta\|^2 - |\delta(1)|^2 + |\eta_{i0}(y)|^2).\end{aligned}$$

Clearly, $\|\delta\|^2$ is a nonzero integer. Let $z \in Q^{*\sharp}$, and let $\mathfrak{Q}$ be a prime ideal dividing q in the ring of algebraic integers of $\mathbb{Q}_{pq}$. Then, $\eta_{i0}(y) \equiv \eta_{i0}(yz) = \omega_{i0}(yz) \equiv \omega_{i0}(y) = 1 \pmod{\mathfrak{Q}}$. Thus, the left side of (20.3) is positive. It suffices to show that $|\delta(1)|^2 - |\eta_{i0}(y)|^2$ is an integral multiple of c. We have

$$\eta_{i0}(y) = a\rho_1(y) + \gamma(y) = -auc + \gamma(1),$$

$$\delta(1) = a\rho_1(1) + \gamma(1) = a(|P|-1)uc + \gamma(1).$$

Hence,

$$|\delta(1)|^2 - |\eta_{i0}(y)|^2 = (a(|P|-2)uc + 2\gamma(1))a|P|uc.$$

Since au is an integer, this is an integral multiple of c. Q.E.D.

Lemma 20.5. *Suppose that $\mathcal{S}$ contains an irreducible character λ of degree uq which is induced by a character of PC. Then,*

$$\sum_{x\in(PC)^\sharp} |\lambda^\tau(x)|^2 > uqc|P| - (uq)^2 - 2uq^2.$$

Proof. We have

$$(\lambda^\tau)_{S'} = \lambda_{S'} + a\rho_1 + \alpha$$

where au is an integer, ρ_1 is the portion of the regular representation ρ of S', $\rho = \rho_1 + \rho_2$ with ρ_2 the regular representation of S'/P, and α is a character of S'/P. Let

$$\beta = -a\rho_2 + \alpha.$$

Then for $x \in (S')^\sharp$, $\lambda^\tau(x) = \lambda(x) + \beta(x)$. The value of $\beta(x)$ is constant on each coset of P except at the identity. The proof of Lemma 34.5 [FT] may be applied. We have

(20.4)
$$\begin{aligned}\sum_{x\in(PC)^\sharp} |\lambda^\tau(x)|^2 &= \sum(\lambda(x)+\beta(x))(\overline{\lambda}(x)+\overline{\beta}(x))\\ &= \sum|\lambda(x)|^2 + \sum(\lambda(x)\overline{\beta}(x)+\beta(x)\overline{\lambda}(x)) + \sum|\beta(x)|^2.\end{aligned}$$

Since $\lambda \in \operatorname{Irr} S$ with $\lambda(1) = uq$, the first sum is $uqc|P| - (uq)^2$. None of the irreducible components of $\lambda_{S'}$ has P in its kernel. Hence, the second sum is $-2\lambda(1)\beta(1)$. Since β is constant on each coset of P,

$$\sum|\beta(x)|^2 = |P|\sum_{x\in U}|\beta(x)|^2 - |\beta(1)|^2.$$

Suppose $|\beta(1)| < q$. Then, $2\lambda(1)|\beta(1)| < 2uq^2$. The result follows from (20.4). On the other hand, if $|\beta(1)| \geq q$, then $2\lambda(1)|\beta(1)| \leq 2u|\beta(1)|^2 \leq (|P|-1)|\beta(1)|^2$. The result follows from (20.4) again. Q.E.D.

Lemma 20.6. *Let G_0 be the set of elements of G which are not conjugate to any element of PC, Q, or $\widehat{W}$. Suppose that $\mathcal{S}$ contains an irreducible character λ of degree uq. Define*

$$\begin{aligned}A_1 &= \{x \in G_0 \mid \lambda^\tau(x) \neq 0\},\\ A_2 &= \{x \in G_0 \mid \eta_{10}(x) \neq 0\}, \text{ and}\\ A_3 &= \{x \in G_0 \mid \eta_{01}(x) \neq 0 \text{ and } \eta_{01}(x) \equiv 0 \pmod{(q-1)}\}.\end{aligned}$$

Then, $G_0 = A_1 \cup A_2 \cup A_3$.

Lemma 20.7. *The following statements hold.*

(*i*) *If $q \geq 5$, then P is an elementary abelian group of order p^q and $u/c > 9p^{q-1}/20q$.*
(*ii*) *If $p, q \geq 5$, then $c = 1$ and $u > (13/20)p^{q-1}/q$.*
(*iii*) *If $p = 3$ and $c \neq 1$, then $u = 121$, $q = 5$, and $c = 11$.*
(*iv*) *If $q = 3$, then $c = 1$ or $c = 7$. Furthermore $u > (p^2+p+1)/13$.*

(v) *If $q = 3$, then P is an elementary abelian p-group and $|P| = p^q$ or $p = 7$, $c = 1$, and $|P| = 7^4$.*

(vi) *If $q = 3$ and $c = 7$, then $u > (p^2 + p + 1)/2$.*

Lemma 20.8. *If $q \geq 5$, then PU/C is a Frobenius group and we also have that u divides $(p^q - 1)/(p - 1)$.*

Lemma 20.9. *If $p, q \geq 5$, then $c = 1$, $|P| = p^q$, and either $u = (p^q - 1)/(p - 1)$ or $p \equiv 1 \pmod{q}$ and $uq = (p^q - 1)/(p - 1)$.*

These lemmas are proved as in [FT], §34. In the proof the references to Lemma 34.n [FT] should be to Lemma 20.n of this paper.

§21. Four Propositions

We continue to use the notation introduced at the beginning of §20. Thus, S and T are subgroups in $\mathcal{M}$, and p and q are distinct primes such that $|W| = pq$. The purpose of this section is to prove that $c = d = 1$, $|P| = p^q$, $|Q| = q^p$, PU is a Frobenius group, and QV is a Frobenius group.

Suppose that both p and q are greater than 3. Then, Lemma 20.7 (i) and (ii) yield that P is an elementary abelian group of order p^q and $c = 1$. By symmetry, Q is an elementary abelian group of order q^p and $d = 1$. By Lemma 20.8, PU is a Frobenius group and u divides $(p^q - 1)/(p - 1)$. By symmetry, QV is a Frobenius group. Thus, the result holds if $p, q \geq 5$. We may assume that $q = 3$ from now on. We prove four propositions.

Proposition 21.1. *If $q = 3$, then $c = 1$.*

Proof. Suppose that $q = 3$ and $c \neq 1$. By Lemma 20.7 (iv) and (vi), we have $c = 7$ and

$$u > (p^2 + p + 1)/2.$$

By Lemma 20.1, u divides either $p^2 + p + 1$ or $(p - 1)^2$. It follows from the inequality that $u = p^2 + p + 1$. Lemma 20.7 (v) yields that P is an elementary abelian group of order p^3. Then, by Lemma 20.1, U/C is a cyclic group that acts irreducibly and regularly on P. Hence, the group S'/C is a Frobenius group with Frobenius kernel PC/C. The group PC is nilpotent; so is $\mathfrak{U}$. Since U/C is cyclic, $\mathfrak{U}$ is abelian. Since $p \in \varpi$, we have $7 \in \varpi$ and $\mathfrak{U}$ is a ϖ-group. Therefore, S is a ϖ-group of type II or III.

Suppose that $S$ is of type II. Then, $S_\sigma = S_F$ (Proposition 10.1); it is either $P$ or $PC$. Suppose that $S_\sigma = PC$. Then, $(u, 7) = 1$. Let $U = C \times R$ with a $7'$-group $R$ and let $M \in \mathcal{M}(N_G(R))$. Then, by (II$iv$), $N_G(R) \nsubseteq S$. Hence, $M$ is not conjugate to $S$. Since $UQ^* \subseteq M$, $M$ is not $q$-closed. Hence, $M$ is not conjugate to $T$ either. By Theorem I, $M$ is of type I. Then, by Theorem 19.1, $M$ is a Frobenius group with Frobenius kernel M_σ. It follows that $U \subseteq M_\sigma \cap S_\sigma$. This contradicts Theorem 7.9. Therefore, we have $S_\sigma = P$.

Let $M \in \mathcal{M}(N_G(U))$. As before, $M$ is a Frobenius group with Frobenius kernel M_σ. Let $H = M_\sigma$. Then, $M = N_G(H)$ and $Q^* \subseteq M$. It follows from the structure of a Frobenius complement that $|M : H| = 3$ or $3p$. By (IIv), $N_G(C) \subseteq S$. Then, $C_G(C)$ is of rank at most 2. Therefore, $H$ contains a characteristic subgroup of order 7 or 7^2. Thus, if $|M : H| = 3p$, then $p$ divides $7-1$ or $(7^2-1)(7^2-7)$. This is impossible as $p \neq 3, 7$. Hence, we have $|M : H| = 3$.

Let M be the set of irreducible characters of $M$ that do not have $H$ in their kernel. Since $M$ is a Frobenius group with $H$ as the Frobenius kernel, M is the set of nonlinear irreducible characters of $M$. If M is not coherent, then $H$ is a nonabelian group of prime power order (a power of 7) such that $|H : H'| \leq 4|M : H|^2 + 1 = 37$. This implies that $H$ is cyclic and $H \subseteq N_G(C) \subseteq S$. This is not the case. Hence, M is coherent. Let $\theta$ be the character of $M$ induced by the principal character of $H$. Then, by Lemma 12.7, $\mathsf{M}^* = \mathsf{M} \cup \{\theta\}$ is coherent. We can determine θ^τ as follows. Take an irreducible character $\lambda$ of $M$ with $\lambda(1) = 3$. Then, $(\theta - \lambda)^\tau$ vanishes outside the territory $G_0(M)$. We check that $S$ and some of its conjugates are the only supporting subgroups for $A(M)$. We remarked that no group of type I can be a supporting subgroup because it is a Frobenius group. A similar reasoning applies to the group $T$ because $QV$ is a Frobenius group by Lemma 20.2. Thus, the territory $G_0(M)$ consists of elements conjugate to some element of $H^\sharp$ or $PC - P$. In particular, $(\theta - \lambda)^\tau$ vanishes on $\widehat{W}$. Therefore, by Lemma 13.1, we have

$$(\theta^\tau - \lambda^\tau, \eta_{00} - \eta_{i0} - \eta_{0j} + \eta_{ij}) = 0.$$

It follows that θ^τ is a virtual character of weight 3 that involves η_{00} and one of $\eta_{i0}$, $\eta_{0j}$, or $\eta_{ij}$. Clearly, θ^τ is rational. Since $\eta_{0j}$ or $\eta_{ij}$ $(j \neq 0)$ has $p-1$ algebraic conjugates, θ^τ does not involve $\eta_{0j}$ or $\eta_{ij}$. Hence, $\theta^\tau = 1 + \eta_{10} + \eta_{20}$.

Let $\lambda \in \mathsf{M}$ be the irreducible character of degree 3 as above. We claim that $\lambda^\tau(x) = \lambda(x)$ for $x \in H^\sharp$. Note that λ^τ is well-behaved relative to $A(M)$ by Lemma 14.3. Then, by Lemma 14.4, there is a virtual character γ of M such that γ is orthogonal to every $\mu \in \mathrm{M}^*$ and

$$\lambda^\tau(x) = \lambda(x) + r\gamma(x) \qquad (x \in H^\sharp)$$

with some rational number r. If μ is a nonlinear irreducible character of M, then $\mu \in \mathcal{M}^*$. Hence, $(\gamma, \mu) = 0$ by the property of γ. Thus, γ does not involve μ. Hence, γ is a sum of linear characters. Then, $(\gamma, \theta) = 0$ implies that γ vanishes on $H^\sharp$. Hence, $\lambda^\tau(x) = \lambda(x)$ for $x \in H^\sharp$.

Let $G_0 = G_0(M)$. Then, Lemma 11.5 applied to $|\lambda^\tau(x)|^2$ and 1_G yield (with $h = |H|$)

$$\frac{1}{g}\sum_{x\in G_0} |\lambda^\tau(x)|^2 = \frac{1}{|M|}\sum_{x\in H^\sharp} |\lambda^\tau(x)|^2 = \frac{1}{|M|}\sum_{x\in H^\sharp} |\lambda(x)|^2 = 1 - \frac{3}{h},$$

$$\frac{1}{g}|G_0| = \frac{1}{|M|}\sum_{x\in H^\sharp} 1 = \frac{h-1}{3h}.$$

Let G_1 be the set of elements of $G - G_0$ which are not conjugate to any element of $\widehat{W}$, $P^\sharp$, or $Q^\sharp$. On G_1, $(\theta - \lambda)^\tau$ vanishes. The virtual characters η_{10} and η_{20} are 3-conjugate. Therefore, they take the same value on G_1. Thus,

$$1 + 2\eta_{10}(x) - \lambda^\tau(x) = 0$$

for $x \in G_1$. This implies that $\lambda^\tau(x) \neq 0$ on G_1. Hence,

$$\begin{aligned}\frac{3}{h} &\geq \frac{1}{g}\sum_{x\in G_1} |\lambda^\tau(x)|^2 \geq \frac{1}{g}|G_1| \\ &\geq 1 - \frac{h-1}{3h} - (1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq}) - \frac{|P|-1}{|S|} - \frac{|Q|-1}{|T|},\end{aligned}$$

$$\frac{8}{3h} + \frac{1}{3cu} + \frac{1}{pv} \geq \frac{2}{3p} + \frac{1}{|S|} + \frac{1}{|T|} > \frac{2}{3p}.$$

We have $u = p^2 + p + 1 \geq 3p$, $v = (3^p - 1)/2 \geq 63$, and $h \geq cu$. Hence, the left side of the above inequality is at most $(8+1+1)/63p = 10/63p < 1/6p$. This is a contradiction.

Suppose that S is of type III. Then, $S' = S_\sigma = A(S)$. Since there is no supporting subgroup for $A(S)$, S_σ is a TI-set of G with normalizer S. Let $\mathcal{S}_1 = \mathcal{S}_0 \cup \mathcal{S}$ in the notation of §16. Then, $\mathcal{S}_1$ is the set of characters of S which are induced by nonprincipal irreducible characters of S'. Let ξ_0 be the character of S induced by the principal character of S'. By

Theorem 16.1 (a), $\mathcal{S}_1$ is coherent. As before, $\mathcal{S}_2 = \mathcal{S}_1 \cup \{\xi_0\}$ is coherent and

$$\xi_0{}^\tau = 1 + \eta_{10} + \eta_{20}.$$

Let λ be an irreducible character of degree 3 lying in $\mathcal{S}_0$. By Lemma 13.5, the characters of $\mathcal{S}_2$ are either irreducible or one of ξ_j for $0 \leq j \leq p-1$. Then, any virtual character of S that is orthogonal to all $\mu \in \mathcal{S}_2$ vanishes on $(S')^\sharp$. It follows from Lemma 14.4 that $\lambda^\tau(x) = \lambda(x)$ for $x \in (S')^\sharp$. Let G_0 be the set of elements of G which are conjugate to some element of $(S')^\sharp$. Since S' is a TI-set in G, we have

$$\frac{1}{g}\sum_{x\in G_0}|\lambda^\tau(x)|^2 = \frac{1}{|S|}\sum_{x\in(S')^\sharp}|\lambda^\tau(x)|^2 = \frac{1}{|S|}\sum|\lambda(x)|^2 = 1-\frac{3}{|S'|}$$

and $|G_0|/g = (|S'|-1)/|S|$. Let G_1 be the set of elements of $G - G_0$ which are not conjugate to any element of $\widehat{W}$ or $Q^\sharp$. Since $(\xi_0 - \lambda)^\tau$ vanishes on G_1 and $\eta_{10} = \eta_{20}$ on G_1, we see that λ^τ does not vanish on G_1. Thus,

$$\frac{3}{|S'|} \geq \frac{1}{g}\sum_{x\in G_1}|\lambda^\tau(x)|^2 \geq \frac{1}{g}|G_1| \geq 1-(1-\frac{1}{p}-\frac{1}{q}+\frac{1}{pq})-\frac{|S'|-1}{|S|}-\frac{|T'|-1}{|T|}.$$

Hence,

$$\frac{3}{|S'|}+\frac{1}{p|V|} \geq \frac{2}{3p}+\frac{1}{|S|}+\frac{1}{|T|} > \frac{2}{3p}.$$

This is a contradiction. Q.E.D.

Proposition 21.2. *Suppose that $q = 3$. Then $d = 1$.*

Proof. Suppose that $q = 3$ and $d \neq 1$. Then, by Lemma 20.7 (*iii*) with q, c, and S replaced by p, d, and T, we have $p = 5$, $d = 11$, and $v = 121 = (11)^2$. Since $v = (3^5-1)/2$, V/D is cyclic by Lemma 20.1. It follows that V is abelian. Thus, T is of type II or III.

Suppose that T is of type III. Let $\mathcal{V}$ be the set of characters of T which are induced by nonprincipal irreducible characters of T'. By Theorem 16.1, $\mathcal{V}$ is coherent. Let ζ_0 be the character induced by the principal character of T'. By Lemma 12.7, $\mathcal{V}^* = \mathcal{V} \cup \{\zeta_0\}$ is coherent. We will see what $\zeta_0{}^\tau$ is. Let $\lambda \in \mathcal{V}$ be a character of degree p and let

$$\alpha = \zeta_0 - \lambda.$$

We use the same method as in the proof of Lemma 19.4. The characters ν_{ij} associated to the cyclic subgroup W satisfy $\nu_{ij}(1) = v$ for $i > 0$

(Lemma 20.1). Since $v \equiv 1 \pmod p$, all signs attached to ν_{ij} are 1. For a fixed $i \neq 0$, let

$$\gamma_j = \nu_{0j} - \nu_{ij} + \delta \qquad (0 \leq j \leq 4)$$

where δ is a sum of characters of degree p in $\mathcal{V}$ such that $\delta(1) = v - 1$. For example, let δ be the sum of distinct characters of degree 5 which have QD in their kernel. (There are exactly $(v-1)/5$ such characters.) We have $\gamma_j \in I_0(A_0(T))$. Thus, $\gamma_j{}^\tau$ are defined. Since

$$(\gamma_0 - \gamma_j)^\tau = \eta_{00} - \eta_{i0} - \eta_{0j} + \eta_{ij},$$

we have $\gamma_j{}^\tau = \eta_{0j} - \eta_{ij} + \Delta$ with Δ independent of j. For each j with $0 \leq j \leq 4$, $(\gamma_j{}^\tau, \zeta_0{}^\tau) = (\gamma_j, \zeta_0) = 1$. We have

$$5 = \sum_j (\eta_{0j}, \zeta_0{}^\tau) + (\sum_j \eta_{ij}, \zeta_0{}^\tau) + 5(\Delta, \zeta_0{}^\tau).$$

Since $\zeta_i{}^\tau = \pm \sum_j \eta_{ij}$ and $(\zeta_i{}^\tau, \zeta_0{}^\tau) = 0$, we get

$$5 = 1 + \sum_{j>o} (\eta_{0j}, \zeta_0{}^\tau) + 5(\Delta, \zeta_0{}^\tau).$$

Therefore, $(\eta_{0j}, \zeta_0{}^\tau) \neq 0$ for some $j > 0$. The characters $\eta_{01}, \ldots, \eta_{04}$ are p-conjugate, while $\zeta_0{}^\tau$ is p-rational. Hence, $(\eta_{0j}, \zeta_0{}^\tau)$ is independent of j. Since $\zeta_0{}^\tau$ is of weight 5, we have $\zeta_0{}^\tau = 1_G \pm \sum_{j>0} \eta_{0j}$. Since $(\gamma_j{}^\tau, \zeta_0{}^\tau) = 1$,

$$\zeta_0{}^\tau = 1_G + \sum_{j>0} \eta_{0j}.$$

Since $\mathcal{V}^*$ consists of all the characters of T which are induced by irreducible characters of T', Lemma 14.4 yields that

$$\lambda^\tau(x) = \lambda(x) \quad \text{for} \quad x \in (T')^\sharp.$$

Since there is no supporting subgroup, $A(T) = T'$ is a TI-set of G. Let G_0 be the set of elements of G which are conjugate to some element of $(T')^\sharp$. Then,

$$\begin{aligned} \frac{1}{g} \sum_{x \in G_0} |\lambda^\tau(x)|^2 &= \frac{1}{|T|} \sum_{x \in (T')^\sharp} |\lambda^\tau(x)|^2 \\ &= \frac{1}{|T|} \sum_{x \in (T')^\sharp} |\lambda(x)|^2 = 1 - \frac{5}{|T'|} \end{aligned}$$

because $\lambda$ vanishes on $T - T'$. We have $|G_0|/g = (|T'| - 1)/|T|$. Let G_1 be the set of elements of $G - G_0$ which are not conjugate to any element of $\widehat{W}$ or $P^\sharp$. Then if $y \in G_1$, then $\alpha^\tau(y) = 0$ and $\eta_{01}(y) = \eta_{0j}(y)$ for all $j > 0$. It follows that

$$1 + 4\eta_{01}(y) - \lambda^\tau(y) = 0.$$

This implies $\lambda^\tau(y) \neq 0$. Then,

$$\begin{aligned}\frac{5}{|T'|} &\geq \frac{1}{g}\sum_{x \in G_1} |\lambda^\tau(x)|^2 \geq \frac{1}{g}|G_1| \\ &\geq 1 - \frac{|G_0|}{g} - (1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq}) - \frac{|P| - 1}{|S|}.\end{aligned}$$

Thus,

$$\frac{5}{|T'|} + \frac{1}{3u} \geq \frac{4}{15} + \frac{1}{|S|} + \frac{1}{|T|} > \frac{4}{15}.$$

This is not the case. Therefore, $T$ is not of type III.

Suppose that $T$ is of type II. In this case, $11 \in \varpi$ so $T$ is a $\varpi$-group. Take $M \in \mathcal{M}(N_G(V))$. Since $M$ contains VP^* which is not $p$-closed, $M$ is not conjugate to $P$. The prime 11 lies in $\sigma(T)'$. In fact, $D$ centralizes $Q$; hence, $N_G(D) \subseteq T$ by (IIv). Since $N_G(V) \not\subseteq T$ by (IIiv), $V$ is not cyclic. Thus, $11 \in \tau_2(T) \cap \sigma(M)$ by Lemma 6.11. It follows that $M$ is not conjugate to $S$. By Theorem I, $M$ is of type I. Hence, by Theorem 19.1, $M$ is a Frobenius group with Frobenius kernel M_σ. Let $H = M_\sigma$. Then, $M = N_G(H)$. Since $N_G(D) \subseteq T$, we have $N_H(D) = T \cap H = V$. It follows that $|H|$ is a power of the prime 11 and $Z(H)$ is cyclic. Therefore, $|M/H| = e$ divides $11 - 1 = 10$. Since P^* is contained in $N_G(V)$, we have $e = 5$.

Let $\mathcal{V}$ be the set of irreducible characters of $M$ which do not have $H$ in their kernel. If $\mathcal{V}$ is not coherent, then $|H : H'| \leq 4e^2 + 1 = 101$. This implies that $H$ is cyclic. Therefore, $\mathcal{V}$ is coherent. Let ζ_0 be the character of $M$ induced by the principal character of $H$. As before, $\mathcal{V}^* = \mathcal{V} \cup \{\zeta_0\}$ is coherent. Let $\lambda$ be an irreducible character of $M$ of degree 5, and let

$$\alpha = \zeta_0 - \lambda.$$

Then, $\alpha \in I_0(A(M))$ and $\alpha$ vanishes on the conjugates of $\widehat{W}$. (The group $T$ is a supporting subgroup of $A(M)$. But, the territory of $A(M)$ does not intersect with $\widehat{W}$.) It follows that

$$(\alpha^\tau, \eta_{00} - \eta_{i0} - \eta_{0j} + \eta_{ij}) = 0.$$

Since $\lambda^\tau \neq \pm\eta_{st}$ for any s, t by Lemma N, we have

$$({\zeta_0}^\tau, \eta_{00} - \eta_{i0} - \eta_{0j} + \eta_{ij}) = 0.$$

Since $\alpha^\tau = {\zeta_0}^\tau - \lambda^\tau$ involves the principal character of G, $({\zeta_0}^\tau, \eta_{00}) = 1$. We will show that $({\zeta_0}^\tau, \eta_{0j}) \neq 0$. Suppose that $({\zeta_0}^\tau, \eta_{0j}) = 0$. If $({\zeta_0}^\tau, \eta_{ij}) \neq 0$, then

$${\zeta_0}^\tau = 1_G + a \sum_{j>0} \eta_{ij}$$

because η_{ij} for $1 \leq j \leq 4$ are p-conjugate. Then,

$$5 = \|{\zeta_0}^\tau\|^2 = 1 + 4a^2.$$

On the other hand, we have $({\zeta_0}^\tau, {\zeta_i}^\tau) = (\zeta_0, \zeta_i) = 0$ for $i > 0$. Since ${\zeta_i}^\tau = \pm\sum_j \eta_{ij}$, $({\zeta_0}^\tau, {\zeta_i}^\tau) = \pm 4a$. This is a contradiction. Hence, $({\zeta_0}^\tau, \eta_{ij}) = 0$ for $i, j > 0$. Then, $({\zeta_0}^\tau, {\zeta_i}^\tau) = 0$ implies $({\zeta_0}^\tau, \eta_{i0}) = 0$. This contradiction finally proves $({\zeta_0}^\tau, \eta_{0j}) \neq 0$. Then,

$${\zeta_0}^\tau = 1 + \sum_{j>0} \eta_{0j}.$$

Lemma 14.4 yields that

$$\lambda^\tau(x) = \lambda(x) \quad \text{for} \quad x \in H^\sharp.$$

By Lemma 14.3, λ^τ is well-behaved relative to $A(M)$. Hence, we can apply Lemma 11.5. Let G_0 be the territory of $A(M)$. Then,

$$\frac{1}{g} \sum_{x \in G_0} |\lambda^\tau(x)|^2 = \frac{1}{|M|} \sum_{x \in H^\sharp} |\lambda^\tau(x)|^2 = \frac{1}{|M|} \sum_{x \in M^\sharp} |\lambda(x)|^2 = 1 - \frac{e}{|H|}.$$

And

$$\frac{1}{g}|G_0| = \frac{1}{g} \sum_{x \in G_0} 1 = \frac{1}{|M|} \sum_{x \in H^\sharp} 1 = \frac{|H| - 1}{|M|}.$$

Let G_1 be the set of elements of $G - G_0$ which are not conjugate to any element of $\widehat{W}$, $P^\sharp$, or $Q^\sharp$. Then, $\alpha^\tau(x) = 0$ for $x \in G_1$. Also, we have $\eta_{01}(x) = \eta_{0j}(x)$ for $j > 0$ and $x \in G_1$. It follows that

$$1 + 4\eta_{01}(x) - \lambda^\tau(x) = 0 \quad \text{for} \quad x \in G_1.$$

This implies that $\lambda^\tau(x) \neq 0$ on G_1. Therefore, we have

$$\begin{aligned}\frac{e}{|H|} &\geq \frac{1}{g}\sum_{x \in G_1} |\alpha(x)|^2 \geq \frac{1}{g}|G_1| \\ &\geq 1 - \frac{|H|-1}{|M|} - (1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq}) - \frac{|P|-1}{|S|} - \frac{|Q|-1}{|T|},\end{aligned}$$

$$\frac{e}{|H|} + \frac{1}{3u} + \frac{1}{5 \cdot 11^3} \geq \frac{4}{15} + \frac{1}{|M|} + \frac{1}{|S|} + \frac{1}{|T|} > \frac{4}{15}.$$

Since $u = 31$ and $|H| \geq 11^3$, this is a contradiction. Q.E.D.

Proposition 21.3. *Suppose that $q = 3$. Then, P is an elementary abelian group of order p^3.*

Proof. Suppose that Proposition 21.3 fails. Then, by Lemma 20.7 (v), we have $p = 7$ and $|P| = p^4$. The group P is elementary abelian. The group U is abelian and its order u divides either $(p^3-1)/(p-1)$ or $(p-1)^{q-1}$. Since $p = 7$ and $(u, 6) = 1$, Lemma 20.1 yields that U is a cyclic group of order dividing $p^2 + p + 1 = 57 = 3 \cdot 19$. Since $(u, 3) = 1$, we must have $u = 19$.

Lemma 20.1 yields a normal subgroup P_0 such that UQ^* acts irreducibly on P/P_0. Then, $|P_0| = 7$ and U centralizes P_0. There is a subgroup P_1 of order p^3 such that UQ^* acts irreducibly on P_1. Then,

$$P = P_0 \times P_1$$

and $P_0 = C_P(U)$. Since $C_P(U) \neq 1$, S is not of type II. Therefore, S is of type III. Since there is no supporting subgroup, $S' = A(S)$ is a TI-set.

Let $\mathcal{U}$ be the set of characters of S which are induced by nonprincipal irreducible characters of S'. By Theorem 16.1 (a), $\mathcal{U}$ is coherent. Let ξ_0 be the character of S that is induced by the principal character of S'. Then, by Lemma 12.7, $\mathcal{U}^* = \mathcal{U} \cup \{\xi_0\}$ is coherent. Let λ be an irreducible character of degree 3 lying in $\mathcal{U}$, and let

$$\alpha = \xi_0 - \lambda.$$

Then, α^τ vanishes on any conjugate of $\widehat{W}$. It follows that

$$(\alpha^\tau, 1_G - \eta_{i0} - \eta_{0j} + \eta_{ij}) = 0 \quad \text{for} \quad i, j > 0.$$

By Lemma N, λ^τ is orthogonal to every η_{st}. Hence,

$$({\xi_0}^\tau, 1_G - \eta_{i0} - \eta_{0j} + \eta_{ij}) = 0.$$

The virtual characters η_{0j} $(1 \leq j \leq 6)$ are p-conjugate, while $\xi_0{}^\tau$ is p-rational. Since $\|\xi_0{}^\tau\|^2 = 3$, $\xi_0{}^\tau$ does not involve η_{0j}. By the same reasoning, $\xi_0{}^\tau$ does not involve η_{ij}. It follows that

$$\xi_0{}^\tau = 1_G + \eta_{10} + \eta_{20}.$$

We can argue as in the previous propositions. We have

$$\lambda^\tau(x) = \lambda(x) \quad \text{for} \quad x \in (S')^\sharp.$$

Let G_0 be the set of elements of G which are conjugate to some element of $(S')^\sharp$. Since S' is a TI-set,

$$\begin{aligned}\frac{1}{g}\sum_{x\in G_0} |\lambda^\tau(x)|^2 &= \frac{1}{|S|}\sum_{x\in(S')^\sharp} |\lambda^\tau(x)|^2 \\ &= \frac{1}{|S|}\sum_{x\in(S')^\sharp} |\lambda(x)|^2 = 1 - \frac{3}{|S'|}\end{aligned}$$

because λ vanishes on $S - S'$. Similarly,

$$|G_0|/g = (|S'| - 1)/|S|.$$

Let G_1 be the set of elements of $G - G_0$ which are not conjugate to any element of $\widehat{W}$ or $Q^\sharp$. Then, α^τ vanishes on G_1, and $\eta_{10}(y) = \eta_{20}(y)$ for $y \in G_1$. Thus,

$$1 + 2\eta_{10}(y) - \lambda^\tau(y) = 0 \quad \text{for} \quad y \in G_1.$$

This implies $\lambda^\tau(y) \neq 0$ for $y \in G_1$. Then,

$$\begin{aligned}\frac{3}{|S'|} &\geq \frac{1}{g}\sum_{x\in G_1} |\lambda^\tau(x)|^2 \geq \frac{1}{g}|G_1| \\ &\geq 1 - \frac{|S'|-1}{|S|} - (1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq}) - \frac{|Q|-1}{|T|}.\end{aligned}$$

Then,

$$\frac{3}{|S'|} + \frac{1}{7\cdot v} \geq \frac{1}{p} - \frac{1}{pq} + \frac{1}{|S|} + \frac{1}{|T|} > \frac{2}{21}.$$

Since $|S'| = 7^4 \cdot 19$ and $v = 1093$, this is a contradiction. Q.E.D.

Proposition 21.4. *Suppose that $q = 3$. Then, U is a cyclic group of order dividing p^2+p+1 that acts on P irreducibly and regularly. The group PU is a Frobenius group. The group Q is also an elementary abelian group of order 3^p and QV is a Frobenius group with Frobenius kernel Q. The group V is a cyclic group of order dividing $(3^p-1)/2$.*

Proof. Since $q = 3$, we have $p \geq 5$. By Lemma 20.7 (i) with q and P replaced by p and Q, Q is an elementary abelian group of order 3^p. By Proposition 21.2, we have $d = 1$ and $D = 1$. Lemma 20.8 with q and P replaced by p and Q yields that QV is a Frobenius group with Frobenius kernel Q and $v = |V|$ divides $(3^p-1)/2$. By Lemma 20.1 for T, V is a cyclic group.

Suppose that Proposition 21.4 fails. Then, by Lemma 20.1, the group U is a product of at most 2 cyclic groups and u divides $[(p-1)/2]^2$. Since U is abelian, S is either of type II or type III.

Suppose that S is of type III. Let $\mathfrak{U}$ be the set of characters of S which are induced by nonprincipal irreducible characters of S'. If $\mathfrak{U}$ is coherent, we can apply the same argument as the one in the proof of Proposition 21.3. At the end, we get

$$\frac{3}{|S'|} + \frac{|Q|}{|T|} \geq \frac{2}{3p}.$$

Since $|S'| = p^3u > 15p$ and $|T| = v|Q|$ with

$$v = (3^p-1)/2 \geq 5p,$$

we have a contradiction

$$\frac{2}{5p} > \frac{3}{|S'|} + \frac{|Q|}{|T|} \geq \frac{2}{3p}.$$

We will prove that $\mathfrak{U}$ is coherent. Since $U \cong S'/P$ is abelian, $\mathfrak{U}$ contains $(u-1)/3$ irreducible characters of degree 3. By assumption, U is an abelian group of exponent dividing $(p-1)/2$. Therefore, there is a U-invariant subgroup P_1 of P with index $|P : P_1| = p$. Then, $U/C_U(P/P_1)$ is cyclic. Since $C_U(P/P_1)$ is contained in the inertia group of any linear character of P/P_1, there is a linear character θ of P such that $|S' : I(\theta)| \leq \exp U \leq (p-1)/2$. It follows that there is an irreducible character μ of $\mathfrak{U}$ having the degree $3d$ with $1 < d \leq (p-1)/2$ (cf. §11, the proof of Lemma 4.5 [FT]). Let λ be an irreducible character of degree 3 lying in $\mathfrak{U}$. Let

$$\alpha = \xi - \lambda \quad \text{and} \quad \beta = d\lambda - \mu$$

where ξ is the character of S induced by the principal character of S'. Then, $\alpha, \beta \in I_0(A(S))$ and α^τ, β^τ are defined. Since S is of type III, we have $A(S) = S'$. Then, for characters ν, ν' of degree 3 in $\mathfrak{U}$,

$$(\beta^\tau, (\nu - \nu')^\tau) = 0$$

if $\nu \neq \lambda \neq \nu'$; while $(\beta^\tau, (\nu - \lambda)^\tau) = -d$. It follows that

$$\beta^\tau = d\lambda^\tau - x\sum \nu^\tau - \mu^\tau + \varDelta$$

for some integer x where the sum is over all irreducible characters ν of degree 3. If $x = 0$, $\mathfrak{U}$ is coherent. Suppose that $x \neq 0$. We have $\|\beta^\tau\|^2 = d^2 + 1$. It follows from this

$$x^2(u-1)/3 \leq 2dx. \tag{21.1}$$

Note that $\mathfrak{U}$ contains exactly $(u-1)/3$ irreducible characters of degree 3. The above inequality implies $x > 0$. Lemma 20.7(*iv*) yields $u > (p^2+p+1)/13$. Since $d \leq (p-1)/2$, (21.1) yields $p \leq 37$. By Lemma 20.1, u divides $(p-1)^2/4$. Thus,

$$\frac{p^2+p+1}{13} < u \leq \frac{(p-1)^2}{4}.$$

If $p-1$ is divisible by 4 or 3, we can replace $(p-1)^2/4$ by $(p-1)^2/16$ to get a contradiction. Thus, $p \equiv -1 \pmod{12}$ and $p = 11$ or 23. If $p = 23$, u divides 11^2. If $u = 11$, then $u \not\equiv 1 \pmod 3$. This contradicts the fact that UQ^* is a Frobenius group. Thus, $u = 121$ and (21.1) yields $x < 1$. Therefore, we have $p = 11$, $u = 25$, $d = 5$, and (21.1) yields $0 < x < 2$. Hence, $x = 1$ and

$$\beta^\tau = d\lambda^\tau - \sum \nu^\tau - \mu^\tau + \varDelta.$$

As before, $\varDelta$ is a real-valued virtual character such that $(1_G, \varDelta) = (\nu^\tau, \varDelta) = 0$ for every $\nu \in \mathfrak{U}$ with $\nu(1) = 3$. We check that

$$\alpha^\tau = 1_G + \eta_{10} + \eta_{20} - \lambda^\tau.$$

Since $\overline{\eta_{20}} = \eta_{10}$, $(\alpha^\tau, \varDelta)$ is an even integer. But, $(\alpha^\tau, \beta^\tau) = (\alpha, \beta) = -d$ by Lemma 11.4. Thus, we have

$$(\alpha^\tau, \beta^\tau) = -(d-1) + (\alpha^\tau, \varDelta)$$

which implies $(\alpha^\tau, \varDelta) = -1$. This contradiction proves that $\mathfrak{U}$ is coherent. Thus, Proposition 21.4 is proved if S is of type III.

Suppose that $S$ is of type II. Let $M \in \mathcal{M}(N_G(U))$. Then, $M$ is not conjugate to $S$ or $T$. Therefore, by Theorem I, $M$ is of type I. By Theorem 19.1, $M$ is a Frobenius group with Frobenius kernel M_σ. We have

$$U \subseteq M_\sigma.$$

The group Q^* is contained in $M$. Hence, $|M\colon M_\sigma| = 3$ or $3p$.

By Lemma 20.1, $u$ divides $(p-1)^2/4$. As before, $p-1$ is not divisible by 4 or 3. Hence, if $u \neq (p-1)^2/4$, then

$$\frac{p^2+p+1}{13} < u \leq \frac{(p-1)^2}{20}$$

which is a contradiction. It follows that $u = (p-1)^2/4$ and U is the direct product of two cyclic groups of order $(p-1)/2$. Thus, all Sylow subgroups of U are abelian of rank 2. Hence, we have $\pi(\mathsf{U}) = \tau_2(S)$. Take $r \in \pi(U)$ and let $A \in \mathcal{E}_p^2(\mathsf{U})$. Then, for some $B \in \mathcal{E}^1(A)$, $C_P(B) \neq 1$ by Proposition 1.16 [BG]. For $B$, $C_G(B) \subseteq S$ by (IIv). This implies that

$$Z(M_\sigma) \subseteq S \cap M_\sigma = \mathsf{U}.$$

Since M_σ is nilpotent, $\pi(Z(M_\sigma)) = \pi(M_\sigma)$. Thus,

$$\pi(U) \subseteq \pi(M_\sigma) = \pi(Z(M_\sigma)) \subseteq \pi(U).$$

Therefore, $\pi(U) = \pi(M_\sigma)$. Suppose that $|\pi(U)| > 1$ or some Sylow subgroup of $U$ is a Sylow subgroup of $G$. Then, by Theorem 6.7, $G$ has abelian Sylow $r$-subgroups for each $r \in \pi(U)$. By Lemma 6.8(b), U is a Hall $\tau_2(S)$-subgroup of $G$. It follows that $U = M_\sigma$. Since $N_G(U) \nsubseteq S$, we have $|M\colon M_\sigma| = 3p$. Since $M$ is a Frobenius group,

$$|A| \equiv 1 \pmod{3p}$$

for each $A \in \mathcal{E}^2(U)$. Since $u = |U| = (p-1)^2/4$, we have $U = A$ and $u \equiv 1 \pmod{3p}$. (If $A \neq U$, $|U| \geq (3p+1)^2$ which is impossible.) Thus,

$$(p-1)^2 - 4 = 12kp$$

for some integer $k$. Hence, $p$ divides 3. This contradicts the assumption $p > q = 3$. Therefore, $\pi(U) = \{r\}$ for a single prime $r$ and $G$ has a nonabelian Sylow $r$-subgroup. It follows from the structure of $S$ that $P = S_\sigma$. Then, Theorem 6.7 yields that $C = C_A(P)$ has order $p$. This contradicts Proposition 21.2. Q.E.D.

Theorem. *Let G be a finite simple group and let ϖ be a connected component of the prime graph $\Gamma(G)$ such that $2 \notin \pi$. Then, we have one of the two cases*:

(1) *G contains a nilpotent Hall ϖ-subgroup H that is isolated in G, or*

(2) *$\varpi = \{p, q\}$ and there is a self-normalizing cyclic group W of order pq.*

References

[BG] H. Bender and G. Glauberman, "Local Analysis for the Odd Order Theorem, London Math. Soc. Lecture Note Series 188", Cambridge University Press, 1995, pp. 1–174.

[FT] W. Feit and J. G. Thompson, Solvability of groups of odd order, Pacific J. Math., **13** (1963), 775–1029.

[GK] K. W. Gruenberg and O. Kegel, Unpublished manuscript.

[GR] K. W. Gruenberg and K. W. Roggenkamp, Decomposition of the augmentation ideal and of relation modules of a finite group, Proc. London Math. Soc., **(3)31** (1975), 149–166.

[W] J. S. Williams, Prime Graph Components of Finite Groups, J. Algebra, **69** (1981), 487–513.

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 209–244

A characterization of ${}^2\mathbf{E}_6(2)$

Michael Aschbacher

§1. Introduction

This paper is part of a program to provide a uniform, self-contained treatment of part of the foundations of the theory of the sporadic finite simple groups. More precisely our eventual aim is to provide complete proofs of the existence and uniqueness of the twenty-six sporadic groups and to derive the basic structure of each sporadic. The two books [SG] and [3T] make a beginning on that program.

In this paper we provide a uniqueness proof for the group ${}^2E_6(2)$. Of course ${}^2E_6(2)$ is a group of Lie type, not a sporadic group, but in order to treat the Monster and the Baby Monster, one first needs to treat ${}^2E_6(2)$. Thus this paper begins that part of the program dealing with the large sporadics.

Suzuki was one of the pioneers in identifying finite groups from information on subgroup structure. His characterization of $L_3(2^n)$ in [S] identifies those groups by producing a BN-pair. That approach is not so different from the one adopted in our program. Indeed in the work of S. Smith and the author on quasithin groups, the groups $L_3(2^n)$, $n$ even, can not quite be handled using our standard methods, so we appropriate a clever counting argument of Suzuki's from [S] to fill the gap. Hopefully Suzuki would regard this paper as continuing a tradition which he pioneered.

Define a finite group $G$ to be of *type* ${}^2E_6(2)$ if $G$ possesses an involution $z$ such that $F^*(C_G(z)) = O_2(C_G(z))$ is extraspecial of width 10, $C_G(z)/O_2(C_G(z)) \cong U_6(2)$, and $z$ not weakly closed in $O_2(C_G(z))$ with respect to $G$.

Define $G$ to be of *type* $\mathbf{Z}_2/{}^2E_6(2)$ if $G$ possesses an involution $z$ such that $F^*(C_G(z)) = O_2(C_G(z))$ is extraspecial of width 10 and $C_G(z)$ has a subgroup $H$ of index 2 such that $H/O_2(C_G(z)) \cong U_6(2)$, and $z$ is not weakly closed in $O_2(C_G(z))$ with respect to $G$.

This work was partially supported by NSF-9622843
Received March 18, 1999.

Our main theorems are:

Theorem 1. *Each group of type* $^2E_6(2)$ *is isomorphic to* $^2E_6(2)$.

Theorem 2. *If* G *is of type* $\mathbf{Z}_2/^2E_6(2)$ *then* $F^*(G)$ *is of index* 2 *in* G *and* $F^*(G) \cong {}^2E_6(2)$.

Theorems 1 and 2 are proved in sections 8 and 9, respectively, where they appear as Theorems 8.7 and 9.1. Many lemmas are included in the paper which are not used in the proof of the main theorems. They will be used later in the program and appear here because it is convenient to provide an exposition of related results in one place. Similarly the proof of the following two lemmas will appear in later papers in this series for the same reason, as will the proof of the third part of lemma 5.8.

(1.1) *Let* Γ *be a building of type* F_4 *and* Δ *the collinearity graph of* Γ. *Then* Δ *is simply connected.*

(1.2) *Let* G *be a group and* V *a faithful finite dimensional* $\mathbf{F}_2G$-*module. Assume* $u \in V^{\#}$ *such that the full group* T *of transvections on* V *with center* u *is contained in* G. *Let* $U = \langle u^G \rangle$ *and* $L = \langle T^G \rangle$. *Then* $Aut_L(U) = GL(U)$.

§2. Presentations for modules

In this section Ω is a graph with vertex set Ω and $\Omega(x)$ denotes the set of vertices adjacent to a vertex x of Ω. Assume G is a group of automorphism of Ω transitive on the vertices of the graph and let V be the permutation module for G on Ω over $\mathbf{F}_2$. Thus Ω is a basis for the $\mathbf{F}_2$-space V and $G \leq GL(V)$ is transitive on the basis Ω.

Define a bilinear form β on V by

$$\beta(x,y) = 0 \text{ if and only if } y \in \Omega(x) \cup \{x\} \text{ for } x,y \in \Omega.$$

As the relation defining the graph Ω is symmetric, the bilinear form β is symmetric.

Let $R = \mathrm{Rad}(\beta)$ be the radical of the bilinear form β; that is

$$R = \{v \in V : \beta(u,v) = 0 \text{ for all } u \in V\}.$$

Finally let $\bar{V} = V/R$ and write $\bar{\beta}$ for the bilinear form induced by β on $\bar{V}$. That is

$$\bar{\beta}(\bar{v},\bar{u}) = \beta(u,v)$$

which is well defined as R is the radical of β. Further as R is the radical of β, the induced form $\bar{\beta}$ is nondegenerate, so $\bar{\beta}$ is a symplectic form on $\bar{V}$. As G is a group of automorphisms of the graph Ω, G preserves the form β, and hence also the induced form $\bar{\beta}$. We summarize all this as:

(2.1) *$(\bar{V}, \bar{\beta})$ is a symplectic space over $\mathbf{F}_2$ and $G \leq Sp(\bar{V})$ is a group of isometries of this symplectic space transitive on the generating set $\bar{\Omega}$ of $\bar{V}$.*

(2.2) *Assume U is an $\mathbf{F}_2G$-module and $\rho : \Omega \to U$ is a map such that $U = \langle \rho(\Omega) \rangle$ and $\rho : \Omega \to \rho(\Omega)$ is an equivalence of G-sets. Assume further that γ is a symplectic form on U with*

$$\beta(x,y) = \gamma(\rho(x), \rho(y)) \textit{ for all } x, y \in \Omega.$$

Then ρ extends to an $\mathbf{F}_2G$-isometry $\bar{\rho} : (\bar{V}, \bar{\beta}) \to (U, \gamma)$.

Proof. As $U = \langle \rho(\Omega) \rangle$, the map ρ extends to a surjective $\mathbf{F}_2G$-homomorphism $\rho : V \to U$. Let $v \in V$; then $v = \sum_{y \in S(v)} y$, where $S(v)$ is the support of v with respect to the basis Ω. Further for $x \in \Omega$, $\beta(v,x) = |\Gamma(x) \cap S(v)| \mod 2$, where $\Gamma(x) = \Omega - x^{\perp}$. Now $\rho(v) = \sum_{y \in S(v)} \rho(y)$ and

$$\gamma(\rho(v), \rho(x)) = \sum_{y \in S(v)} \gamma(\rho(y), \rho(x)) = |\Gamma(x) \cap S(v)| \mod 2 = \beta(v,x)$$

as $\beta(x,y) = \gamma(\rho(x), \rho(y))$ for all $x, y \in \Omega$. Therefore $v \in R$ if and only if $\beta(v,x) = 0$ for all $x \in \Omega$ if and only if $\gamma(\rho(v), \rho(x)) = 0$ for all $x \in \Omega$ if and only if $\rho(v) \in U^{\perp} = 0$, since $U = \langle \rho(\Omega) \rangle$. Therefore $R = \ker(\rho)$, so ρ induces the isometry $\bar{\rho} : (\bar{V}, \bar{\beta}) \to (U, \gamma)$. Q.E.D.

(2.3) *Assume (U,q) and (W,Q) are orthogonal spaces over $\mathbf{F}_2$ with G irreducible on U, $G \leq O(U,q)$, and $G \leq O(W,Q)$. Let γ and α be the bilinear forms of q and Q, respectively, and assume $\rho : (U,\gamma) \to (W,\alpha)$ is an $\mathbf{F}_2G$-isometry. Then $\rho : (U,q) \to (W,Q)$ is also a $\mathbf{F}_2G$-isometry.*

Proof. As G is irreducible on U, there is at most one quadratic form on U preserved by G with bilinear form γ. (cf. 4.9 in [A]; the argument is easy.) Therefore q is that unique form. Similarly as $\rho : U \to W$ is an equivalence of $\mathbf{F}_2G$-representations, G is irreducible on W, so Q is the unique quadratic form on W preserved by G with bilinear form α, so that ρ is also an isometry of the corresponding orthogonal spaces.

Q.E.D.

(2.4) *Assume (U,q) and (W,Q) are orthogonal spaces over $\mathbf{F}_2$ with G irreducible on U, $G \leq O(U,q)$, and $G \leq O(W,Q)$. Assume further that $u \in U$, $w \in W$, with $G_u = G_w$, $U = \langle uG \rangle$, $W = \langle wG \rangle$, and $\gamma(u,ug) = \alpha(w,wg)$ for all $g \in G$, where γ and α are the bilinear forms of q and Q, respectively. Then there exists an $\mathbf{F}_2G$-isometry $\rho : (U,q) \to (W,Q)$ with $\rho(u) = w$.*

Proof. As $G_u = G_w$, the map $\rho : uG \to wG$ defined by $\rho(ug) = wg$ is a well defined equivalence of permutation representations. Now take Ω_U to be the graph on uG with $\Omega_U(u) = \Omega_U \cap u^\perp$. As $\gamma(u,ug) = \alpha(w,wg)$, ρ defines a G-equivariant isomorphism of Ω_U with the corresponding graph Ω_W on wG. Now apply 2.2 to get $\mathbf{F}_2G$-sometries $\rho_U : (U,q) \to (\bar{V}_U, \bar{q})$ and $\rho_W : (W,Q) \to (\bar{V}_W, \bar{Q})$, where $\bar{V}_U$ and $\bar{V}_W$ are modules of the graphs Ω_U and Ω_W, respectively, and $\bar{q}$ and $\bar{Q}$ are the transfer of the forms q and Q via ρ_U and ρ_W. As $\rho : \Omega_U \to \Omega_W$ is a G-isomorphism, ρ induces an $\mathbf{F}_2G$-isometry $\bar{\rho} : (\bar{V}_U, \bar{\beta}_U) \to (\bar{V}_W, \bar{\beta}_W)$, and hence also an $\mathbf{F}_2G$-isometry $\bar{\rho} : (\bar{V}_U, \bar{q}) \to (\bar{V}_W, \bar{Q})$ by 2.3. Then the composition $\rho_W^{-1} \circ \bar{\rho} \circ \rho_U$ agrees with ρ on uG and is the required extension. Q.E.D.

§3. Some central extensions

We adopt the notation of section 33 of [FGT] and section 23 of [3T] in discussing central extensions. In particular if G is a perfect finite group then $\mathrm{Cov}(G)$ is the universal covering group of G and $\mathrm{Schur}(G)$ is the Schur multiplier of G. In particular $\mathrm{Schur}(G) \leq Z(\mathrm{Cov}(G))$ with $\mathrm{Cov}(G)/\mathrm{Schur}(G) \cong G$. In addition if p is a prime define

$$\mathrm{Cov}_p(G) = \mathrm{Cov}(G)/O^p(\mathrm{Schur}(G))\Phi(O_p(\mathrm{Schur}(G)))$$

and

$$\mathrm{Schur}_p(G) = \mathrm{Schur}(G)/O^p(\mathrm{Schur}(G))\Phi(O_p(\mathrm{Schur}(G)))$$

That is $\mathrm{Cov}_p(G)$ is the largest perfect central extension of an elementary abelian p-subgroup by G.

Let $\mathcal{H}$ be the class of finite groups H such that $F^*(H)$ is an extraspecial 2-group and $H/O_2(H))$ is irreducible on $F^*(H)/Z(F^*(H))$. Our notational convention will be to write $Q = F^*(H)$, $\tilde{H} = H/Z(Q)$, and $H^* = H/Q$. We recall from section 8 of [SG] that the commutator map and power map define a nondegenerate bilinear form and quadratic form on $\tilde{Q}$ preserved by H^*. By Exercise 8.5 in [FGT], $\mathrm{Out}(Q) = O(\tilde{Q})$ is the isometry group of this quadratic form.

(3.1) *Let* $H_i \in \mathcal{H}$, $i = 1, 2$, *with* $Q_1 \cong Q_2$ *and assume* $\tilde{Q}_i$ *is absolutely irreducible as an* $\mathbf{F}_2H_i^*$*-module. Then* $\tilde{H}_1 \cong \tilde{H}_2$ *if and only if the induced representations of* H_i^* *on* $\tilde{Q}_i$ *are quasiequivalent for* $i = 1, 2$.

Proof. Identifying Q_1 and Q_2 via our isomorphism, we may take $Q_1 = Q_2 = Q$. Then identifying $\tilde{H}_i$ with $\mathrm{Aut}_{H_i}(Q)$, we have $\tilde{H}_i \leq \mathrm{Aut}(Q) = A$ and $H_i^* \leq A/\tilde{Q} = Out(Q) \cong O(\tilde{Q})$.

The representations of H_1^* and H_2^* on $\tilde{Q}$ are quasiequivalent if and only if H_1^* and H_2^* are conjugate in $GL(\tilde{Q})$. Further as $\tilde{Q}$ is an absolutely irreducible $\mathbf{F}_2H_i^*$-module, the quadratic form on $\tilde{Q}$ is the unique one preserved by $\tilde{H}_i$, (cf. 4.9 in [A]), so H_1^* is conjugate to H_2^* in $GL(\tilde{Q})$ if and only if the groups are conjugate in $O(\tilde{Q})$. Thus the representations are quasiequivalent if and only if $\tilde{H}_1$ is conjugate to $\tilde{H}_2$ in A, establishing the lemma. Q.E.D.

(3.2) *Let* $H \in \mathcal{H}$ *be perfect and let* $\hat{H} = \mathrm{Cov}_2(H)$, $\hat{Q} = O_2(\hat{H})$, *and* $P = [\hat{Q}, \hat{H}]$. *Then*

(1) $\hat{H}/P \cong \mathrm{Cov}_2(H^*)$ *and* $\hat{Q}/P \cong \mathrm{Schur}_2(H^*)$.

(2) $P \cong Q \times H^1(H^*, \tilde{Q})$.

(3) *If* H_1 *is a perfect central extension of* $\tilde{H}$ *then the representation of* $\mathrm{Aut}(H_1)$ *on* H_1 *by conjugation factors through* $\mathrm{Aut}(\hat{H})$.

(4) $D = C_{\mathrm{Aut}(\hat{H})}(P/Z(P))$ *is elementary abelian and centralizes* $P/\Phi(P)$, *and* $D/\mathrm{Aut}_P(\hat{H})$ *acts faithfully as the full group of transvections on* $Z(P)$ *with center* $\Phi(P)$.

(5) $D/\mathrm{Aut}_P(\hat{H})$ *is regular on the complements to* $\Phi(P)$ *in* $Z(P)$, *so if* U *is such a complement then* $\mathrm{Aut}(\hat{H}) = DN_{\mathrm{Aut}(\hat{H})}(U)$ *with* $\mathrm{Aut}_P(\hat{H}) = N_D(U)$.

(6) *If* $H_0 \in \mathcal{H}$ *with* $F^*(H_0) \cong F^*(H)$ *then* $H_0/Z(H_0) \cong H/Z(H)$ *if and only if* $H_0 \cong \hat{H}/V$ *for some complement* V *to* $\Phi(P)$ *in* $Z(\hat{H})$ *containing* U.

Proof. This is an extension of 8.17 in [SG], where the result is essentially proved under the extra hypotheses that $H^1(H^*, \tilde{Q}) = 0$ and H^* is absolutely irreducible on $\tilde{Q}$. Much of the same proof works. In particular if $\rho : \hat{H} \to H$ is the universal covering of H and $\hat{Z} = \ker(\rho)$ then $\hat{Q} = \rho^{-1}(Q)$ is of class 2 with center $Z = \rho^{-1}(Z(Q))$, $Z = Z(\hat{H})$, and $|Z : \hat{Z}| = 2$. As $\hat{Z} = \mathrm{Shur}_2(H)$, $\hat{Z}$ is elementary abelian. Arguing as in the proof of 8.17 of [SG], $\Phi(P)$ is elementary abelian, so as $Z = \Phi(P)\hat{Z}$, Z is elementary abelian. Similarly the proof of 8.17 in [SG] shows that (1) holds. Part (3) follows from the universal property of ρ; cf. 33.7 and 33.8 in [FGT].

Let $x \in \hat{Q}$ with $x\rho$ of order 4 in Q. Then $x^2 \in Z = Z(\hat{H})$, so $(x^g)^2 = x^2$ for all $g \in \hat{H}$. But as H^* is irreducible on $\tilde{Q}$, $\tilde{Q} = \langle \tilde{x}^{H^*} \rangle$, so $\hat{Q} = \langle x^{\hat{H}}, \hat{Z} \rangle$ and then as $\Phi(Q) = \langle x^2\rho \rangle$, $\Phi(\hat{Q}) = \langle x^2 \rangle$ is of order 2. Therefore $\hat{Q} \cong Q \times E_{2^m}$ as Z is elementary abelian. Then as $\hat{Q} = P\hat{Z}$, $\Phi(\hat{Q}) = \Phi(P)$ and $P \cong Q \times E_{2^n}$.

As $H^* \leq O(\tilde{Q})$, $\tilde{Q}$ is self dual as an H^*-module. Therefore as $P = [P, \hat{H}]$ and $H^* \cong \hat{H}/\hat{Q} = \hat{H}/C_{\hat{H}}(P/\Phi(P))$ with $P/Z(P) \cong \tilde{Q}$ self dual as an H^*-module, $n \leq \dim_{\mathbf{F}_2}(H^1(H^*, \tilde{Q})) = k$. (cf. 17.12 in [FGT].) So (2) will be established once we show $n \geq k$.

Let $A = \mathrm{Aut}(\hat{H})$ and $D = C_A(P/Z(P))$. Then $[\hat{H}, D] \leq C_{\hat{H}}(P/Z(P$ $)) = \hat{Q}$, so as $\hat{Q}/Z$ is of exponent 2, so is D. Suppose $d \in D - \hat{Q}/Z$ and let $\tilde{P} = \hat{P}/\Phi(P)$, and form the product $E = \tilde{P}\langle d \rangle$. As d centralizes $\hat{H}/\hat{Q}$ and $\hat{H}/P$ is perfect, d centralizes $\hat{H}/P$, so $\hat{H}$ acts on E. Claim E is abelian. If not, as $\tilde{P}$ is abelian, $C_{\tilde{P}}(d) = Z(E)$ is $\hat{H}$ invariant, so as H^* is irreducible on $\tilde{Q} = \tilde{P}/\tilde{Z}(P)$ and $\tilde{P} = [\tilde{P}, \hat{H}]$, either $Z(E) \leq \tilde{Z}(P)$ or $\tilde{P} = Z(E)$, with the latter impossible as E is nonabelian. So $C_{\tilde{P}}(d) \leq \tilde{Z}(P)$. Let $x \in P - Z(P)$, $U = \langle [x, d] \rangle$, and $\bar{E} = E/\tilde{U}$. Then $\bar{x} \in C_{\bar{P}}(d) - \bar{Z}(P)$, so the argument above shows $\bar{E}$ is abelian, and hence $\tilde{U} = [\tilde{P}, d]$. Therefore $|\tilde{P} : C_{\tilde{P}}(d)| = |\tilde{U}| = 2$, so as $C_{\tilde{P}}(d) \leq \tilde{Z}(P)$, $\tilde{Q}$ is of order 2, a contradiction.

We have shown that E is abelian and hence that D centralizes $P/\Phi(P)$. On the other hand $[C_A(P), \hat{H}] \leq C_{\hat{H}}(P) = Z$, so as $\hat{H}$ is perfect, $C_A(P) = 1$. Thus D is faithful on P. But $P = P_0Z(P)$ with $P_0 \cong Q$ and as D centralizes $P/\Phi(P)$, D centralizes $P_0/\Phi(P_0)$. Hence as $\mathrm{Inn}(P_0) = C_{\mathrm{Aut}(P_0)}(P_0/\Phi(P_0))$, $D/\mathrm{Inn}(P)$ is faithful on $Z(P)$. That is $D/\mathrm{Inn}(P)$ acts faithfully as a group of transvections on $Z(P)$ with center $\Phi(P)$. So to complete the proof of (2) and (4), it remains to show $m(D/\mathrm{Inn}(P)) \geq k$.

Let W be the largest $\mathbf{F}_2H^*$-module with $C_W(H^*) = 0$ and $V = [W, H^*] \cong \tilde{Q}$.(cf. section 17 in [FGT].) Let $x \mapsto \dot{x}$ be an H^*-isomorphism of $\tilde{Q}$ with V. The representation of H^* on W induces a representation $\pi : \tilde{H} \to GL(W)$ of $\tilde{H}$ on W. Form the semidirect product $G = \tilde{H}W$ of W by $\tilde{H}$ with respect to the representation π and let $V_0 = \{x\dot{x} : x \in \tilde{Q}\} \leq G$. As $\tilde{Q}$ centralizes W, V_0 is a normal subgroup of G and in G/V_0, $x \in \tilde{Q}$ is identified with $\dot{x}$, so G/V_0 has normal subgroups $\tilde{H}V_0/V_0 \cong \tilde{H}$ and $WV_0/V_0 \cong W$ with $(\tilde{H}V_0/V_0) \cap (WV_0/V_0) = \tilde{Q}V_0/V_0 \cong \tilde{Q}$. Hence

W induces a faithful group of automorphism on $\tilde{H}$ centralizing $\tilde{Q}$ and by part (3), W factors through D, so $m(D/\mathrm{Inn}(P)) \geq m(W/V) = k$, completing the proof of (2) and (4).

Notice that (4) implies (5). Finally (5) and the argument in the penultimate paragraph of the proof of 8.17 in [SG] establishes (6).

Q.E.D.

(3.3) *Let $H \in \mathcal{H}$ be perfect with* $\mathrm{Schur}_2(H^*) = 1$. *Then each $H_0 \in \mathcal{H}$ with $F^*(H_0) \cong F^*(H)$ and $H_0/Z(F^*(H_0)) \cong H/Z(F^*(H))$ is isomorphic to H.*

Proof. Adopt the notation of 3.2. As $\mathrm{Schur}_2(H^*) = 1$, $P = \hat{Q}$ by 3.2.1. Then by 3.2.6, $H \cong \hat{H}/U \cong H_0$ for some fixed complement U to $\Phi(P)$ in $Z(P)$. Q.E.D.

§4. Large extraspecial 2-subgroups

In this section we assume the following hypotheses:

Hypothesis 4.1. G is a finite group, z is an involution in G, $H = C_G(z)$, and $Q = F^*(H)$ is an extraspecial 2-group.

In addition we adopt the following notational conventions: Let $\tilde{H} = H/\langle z\rangle$ and $H^* = H/Q$. From section 8 in [SG], $\tilde{Q}$ has the structure of an orthogonal space over $\mathbf{F}_2$ when we identify $\mathbf{F}_2$ with $\{1, z\}$ and take $q(\tilde{u}) = u^2$ and $(\tilde{u}, \tilde{v}) = [u, v]$ for $u, v \in Q$. Of course H^* is embedded into $O(\tilde{Q})$ via its action by conjugation.

The *width* of an extraspecial 2-group Q is the integer w such that $|Q| = 2^{2w+1}$.

Example 4.2. Let w be a positive integer and L a finite group. A pair (G, z) satisfies Hypothesis $\mathcal{H}(w, L)$ if (G, z) satisfies Hypothesis 4.1 with Q of width w, $H^* \cong L$, and z not weakly closed in Q with respect to G. In [SG] the Monster and Baby Monster are constructed as groups satisfying Hypotheses $\mathcal{H}(12, Co_1)$ and $\mathcal{H}(11, Co_2)$, respectively.

(4.3) *Assume no element of H induces a transvection on $\tilde{Q}$, and let x be an involution in Q with $x \notin z^G$ and $T \in Syl_2(C_H(x))$. Then*

(1) $\langle x, z\rangle = Z(T) = C_G(C_Q(x))$, *$z$ is weakly closed in $Z(T)$ with respect to G, and $T \in Syl_2(C_G(x))$.*

(2) $x^G \cap Q = x^H$.

Proof. Let $X = \langle z, x\rangle$. Then $Z(T)^* \leq C_H(C_Q(x))^* = Y^*$, and Y^* centralizes the hyperplane $\widetilde{C_Q(x)})$ of $\tilde{Q}$, so as no element of H induces a transvection on $\tilde{Q}$, $Y \leq Q$. Then as $X = Z(C_Q(x))$, $X = Y = Z(T)$. As $xz \in x^Q$, z is weakly closed in X with respect to G. Hence $T \in Syl_2(C_G(x))$, establishing (1).

Let $x^g \in Q$ and $S \in Syl_2(C_H(x^g))$. Then by (1), $T, S^{g^{-1}}$ are Sylow in $C_G(x)$, so there is $c \in C_G(x)$ with $T^c = S^{g^{-1}}$. Then $z^{cg} = z$ as z is weakly closed in $Z(S)$, so $h = cg \in H$ with $Z(T)^h = Z(S)$, and hence replacing h by kh with $k \in Q - C_Q(x)$ if necessary, $x^h = x^g$, establishing (2). Q.E.D.

In the remainder of this section we assume the following hypothesis:

Hypothesis 4.4. Hypothesis 4.1 holds with z not weakly closed in Q with respect to G. In addition $T \in Syl_2(H)$ and $J(T^*) \cong E_{2^{w-1}}$, where $w > 2$ is the width of Q.

We adopt the following notational conventions: Let $g \in G - H$ with $s = z^g \in Q$, $E = Q \cap Q^g$, and $R = (Q^g \cap H)(Q \cap H^g) \leq T$.

Remark. Note that by Hypothesis 4.1, hypotheses (L1)-(L3) of section 8 of [SG] are satisfied by Q. Further as $w \geq 2$ and z is not weakly closed in Q with respect to G, the hypotheses of 8.7.3 in [SG] are satisfied, so by that result, Q is a large extraspecial subgroup of G, as defined in section 8 of [SG]. In particular we can appeal to the lemmas in that section.

(4.5) (1) $E \cong E_{2^{w+1}}$.

(2) $C_{H^*}(\tilde{s}) = N_{H^*}(R^*)$.

(3) $R^* = J(T^*)$.

(4) *Let* $X_2 = \langle Q, Q^g\rangle$ *and* $V = \langle z, s\rangle$. *Then* $P_2 = {}'N_G(V) = X_2C_H(V)$ *with* $R = C_{X_2}(V)$, $P_2/R = X_2/R \times C_G(V)/R$, $X_2/R \cong S_3$, *and* $C_G(V)/R \cong N_{H^*}(R^*)/R^*$.

(5) $E/V \leq Z_2(R)$ *is centralized by* X_2 *and is isomorphic to the dual of* R^* *as a module for* $C_G(V)/R$.

(6) $R/E \cong E_{2^{2w-2}}$ *is the tensor product of the natural module for* X_2/R *and the module* R^* *for* $C_G(V)/R$. *In particular* $C_Q(s)/E$ *is isomorphic to* R^* *as a* $C_H(V)$*-module.*

(7) R^* *induces the full group of transvections with center* $\tilde{s}$ *on* $\tilde{E}$ *and the full group of transvections with axis* $C_Q(s)/E$ *on* Q/E.

(8) *If* $N_{H^*}(R^*)$ *is irreducible on* R^* *then* $N_{H^*}(E) = C_{H^*}(\tilde{s})$ *and* H^* *is absolutely irreducible on* $\tilde{Q}$.

Proof. By 8.15 in [SG], $m_2(E) = m + 1$ with $m \leq w$ and R^* is elementary abelian of rank $2w - m - 1$. Let $R \leq T \in Syl_2(H)$. By Hypothesis 4.4, $J(T^*) \cong E_{2^{w-1}}$, so $2w - m - 1 = m(R^*) \leq m(T^*) = w - 1$, and hence $w \leq m$. We conclude $m = w$ and $R^* = J(T^*)$. In particular (1) and (3) hold.

Next by (1) and 8.15 in [SG], (4) and (5) hold, and R/E is the tensor product of the natural module for $X_2/R \cong L_2(2)$ with the $C_G(V)/R$-module isomorphic to R^*, E/V is dual to R^* as a $C_G(V)/R$-module, and R^* induces the full group of transvections on $\tilde{E}$ with center $\tilde{s}$. Then as Q/E is dual to $\tilde{E}$ as a $N_{H^*}(E)$-module, R^* induces the full group of transvections with axis $C_Q(s)/E$ on Q/E, establishing (7).

For $e \in E$, $[RQ, \tilde{e}] \leq \langle \tilde{s} \rangle$ and for $q \in C_Q(s) - E$, $[RQ, \tilde{q}] \leq \tilde{E}$. Finally for $u \in Q - C_Q(s)$, $C_Q(s) \leq [RQ, u]E$, so $qe \in [RQ, u]$ for some $e \in E$. Then $[RQ, qe] \leq [RQ, u]$ and as RQ centralizes E/V, $m([RQ, \tilde{q}\tilde{e}]) \geq m([RQ, \tilde{q}]) - 1$, so

$$m([RQ, \tilde{u}]) \geq w - 1 + m([RQ, \tilde{q}]) - 1 > m([RQ, \tilde{q}]).$$

Therefore $m([RQ, \tilde{u}]) \geq m([RQ, \tilde{y}])$ for all $y \in R \cap Q$, so $R \cap Q \trianglelefteq N_H(RQ)$. Hence $V = Z(R \cap Q) \trianglelefteq N_H(RQ)$, so $N_H(RQ) = QC_H(s)$. This completes the proof of (2).

Finally assume $N_{H^*}(R^*)$ is irreducible on R^*. Then by (4)-(7), $C_H(V)/R \cong N_{H^*}(R^*)/R^*$ has chief series

$$0 < \tilde{V} < \tilde{E} < C_Q(t)/\langle z \rangle < Q$$

and the stabilizers in H^* of each of the nontrivial members of this series, other than $\tilde{E}$, also stabilizes V. Further as $F^*(H) = Q$ and $1 \neq R^* \trianglelefteq N_{H^*}(R^*) = C_{H^*}(\tilde{V})$, $C_{H^*}(\tilde{V})$ is proper in H^*, so either H^* is irreducible on $\tilde{Q}$ or $C_{H^*}(\tilde{s}) < N_{H^*}(E)$. Indeed in the former case as $\tilde{V}$ is of order 2 and $C_{GL(\tilde{Q})}(H^*)$-invariant, the representation is even absolutely irreducible.

So we may assume $C_{H^*}(\tilde{s}) < N_{H^*}(E)$, and it remains to derive a contradiction. Then $N_{H^*}(E)$ is irreducible on $\tilde{E}$, so by 1.2, $N_{H^*}(E)$ induces $GL(\tilde{E})$ on $\tilde{E}$. Further as R^* is faithful on $\tilde{E}$ and normal in $N_{H^*}(V) = C_{H^*}(\tilde{s})$ and $R^* = J(T^*)$, $N_{H^*}(E)$ is faithful on $\tilde{E}$. Then as $E_{2^{w-1}} \cong R^* = J(T^*)$ while $N_{H^*}(E) \cong GL(\tilde{E}) \cong GL_w(2)$, it follows that $w \leq 2$, contrary to Hypothesis 4.4. Namely $m_2(GL_w(2)) > w - 1$ for $w > 3$ and $J(T^*) = T^* \cong D_8$ when $N_{H^*}(E) \cong GL_3(2)$. Q.E.D.

(4.6) *If $C_{R^*}(N_{H^*}(R^*) = 1$ then*
(1) $\langle\tilde{s}\rangle = C_{\tilde{Q}}(N_{H^*}(R^*))$, and
(2) $z^G \cap Q = \{z\} \cup s^H$.

Proof. By 4.5.2 and 4.5.6, $C_Q(s)/E$ is isomorphic to R^* as a $N_{H^*}(R^*)$-module, while by hypothesis, $C_{R^*}(N_{H^*}(R^*)) = 1$, so $N_{H^*}(R^*)$ has no fixed points on $C_Q(s)/E$. Hence (1) follows from 4.5.2 and 4.5.7.

Let $y \in G - H$ and $t = z^y \in Q$. By (1), 4.5.3, and symmetry between s and t, $\langle\tilde{t}\rangle = C_{\tilde{Q}}(N_{H^*}(J(S^*)))$ for some $S^* \in Syl_2(H^*)$. Then by Sylow's Theorem, $J(S^*)$ is H^*-conjugate to $J(T^*)$, so t is H-conjugate to s. Q.E.D.

(4.7) *Assume $R^* = C_{H^*}(R^*)$. Then*
(1) No element of H^* induces a transvection on $\tilde{Q}$.
(2) If in addition $C_{R^*}(N_{H^*}(R^*)) = 1$, then $x^G \cap Q = x^H$ for each involution $x \in Q$ with $x \notin \{z\} \cup s^H$.

Proof. Part (2) follows from (1), 4.3, and 4.6. If $h^* \in H^*$ induces a transvection on $\tilde{Q}$ then h^* is an involution, to we may take $h \in T$. By 4.5.5, E/V is dual to $R^* \cong C_Q(s)/E$ as a T^*-module and $C_Q(s)/E$ is isomorphic to R^* by 4.5.6, so if $[R^*, h^*] \neq 1$ then $m([\tilde{Q}, h^*]) \geq 2m([R^*, h^*]) > 1$, a contradiction. Hence $h^* \in C_{H^*}(R^*) = R^*$. Then by 4.5.7, $m([\tilde{Q}, h^*]) > 1$. Q.E.D.

(4.8) *Assume H^* is irreducible on $\tilde{Q}$. Then*
(1) The regular orbits of R^* on $\tilde{Q}/\langle\tilde{s}\rangle$ are those in $\tilde{Q}/\langle\tilde{s}\rangle - \widetilde{C_Q(s)}/\langle\tilde{s}\rangle$.
(2) If (G_1, z_1) satisfies Hypothesis $\mathcal{H}(w, H^*)$ and $C_{R^*}(N_{H^*}(R^*)) = 1$ then $\tilde{H}_1 \cong \tilde{H}$.

Proof. Let $V = \langle s, z\rangle$ and $\bar{Q} = Q/V$. By 4.5.7, R^* induces the group of transvections with axis $C_Q(s)/E$ on Q/E, so all orbits of R^* on $\bar{Q} - \overline{C_Q(s)}$ are regular. Hence to prove (1) it suffices to show $C_{R^*}(\bar{u}) \neq 1$ for each $u \in C_Q(s)$. If $u \in E$ this follows from 4.5.7, so assume $u \in C_Q(s) - E$ with $C_{R^*}(\bar{u}) = 1$. Then $m([R^*, \bar{u}]) = m(R^*) = w - 1 = m(\bar{E})$, while by 4.5.7, $[R, u] \leq E$, so $[R^*, \bar{u}] = \bar{E}$. By symmetry between z and s, we may assume there is $v \in Q^g \cap H - E$ with $[v, Q \cap H^g]V = E$. But as v^* induces an involutory automorphism on $\tilde{Q}$, $[\tilde{Q}, v^*] \leq C_{\tilde{Q}}(v^*)$, so v^* centralizes $\tilde{E}$, contrary to 4.5.7. This completes the proof of (1).

Let $K^* = N_{H^*}(R^*)$ and Ω the graph on H^*/K^* with K^* adjacent to K^*h^* if $K^*h^*R^*$ is not a regular orbit for R^*. Let β be the bilinear form on $\tilde{Q}$. By (1), $\beta(\tilde{s}, \tilde{s}^h) = 0$ if and only if $K^*h^* \in \Omega(K^*)$.

Assume the hypotheses of (2) and let γ be the bilinear form on $\tilde{Q}_1$. Then there is an isomorphism $H^* \cong H_1^*$ which induces a representation of H^* on $\tilde{Q}_1$. By 4.5.2, $K^* = C_{H^*}(\tilde{s}_1)$ for some $s_1 = z_1^{g_1} \in Q_1$ and by (1) applied to G_1, $\gamma(\tilde{s}_1, \tilde{s}_1^h) = 0$ if and only if $K^*h^* \in \Omega(K^*)$. Therefore by 2.4, the representations of H^* on $\tilde{Q}$ and $\tilde{Q}_1$ are equivalent and $\tilde{Q}$ is isometric to $\tilde{Q}_1$. As $\tilde{Q}$ and $\tilde{Q}_1$ are isometric, $Q \cong Q_1$. As H^* is irreducible on $\tilde{Q}$ and $C_{\tilde{Q}}(K^*) = \langle \tilde{s} \rangle$ is 1-dimensional by 4.6.1, $\tilde{Q}$ is an absolutely irreducible $\mathbf{F}_2H^*$-module. Hence by 3.1, $\tilde{H} \cong \tilde{H}_1$. Q.E.D.

(4.9) *Assume $N_{H^*}(R^*)$ is irreducible on R^* and (G_1, z_1) satisfies Hypothesis $\mathcal{H}(w, H^*)$. Then $\tilde{H}_1 \cong \tilde{H}$.*

Proof. As $N_{H^*}(R^*)$ is irreducible on R^*, H^* is irreducible on $\tilde{Q}$ by 4.5.8, and $C_{R^*}(N_{H^*}(R^*)) = 1$. Hence the lemma follows from 4.8.2.

Q.E.D.

§5. $Sp_6(2)$ and $U_6(2)$

(5.1) *Let V be a $2m$-dimensional symplectic space over a perfect field F of characteristic 2 and $G = Sp(V)$. The the conjugacy classes of involutions of G are a_k, b_k, and c_k, $1 \le k \le m$, where for $d = a, b, c$ and $t \in d_k$, $m([V,t]) = k$, k is odd if and only if $d = b$, and $V(t) = \{v \in V : (v, v^t) = 0\} = V$ if $d = a$, while $V(t)$ is a hyperplane of V if $d = b$ or c.*

Proof. This is contained in section 7 of [ASe], but we repeat the proof here for completeness. Let t be an involution in G. For $u, v \in V$, $(v, u^t) = (u, v^t)$, so the map $v \mapsto (v, v^t)$ is a linear map from V into F with kernel $V(t)$. In particular $\dim(V/V(t)) \le 1$.

Suppose $V = V(t)$. Pick $y_1 \in V - C_V(t)$, $x_1 \in (y_1^t)^\perp - y_1^\perp$, and let $V_1 = \langle y_1, y_1^t, x_1, x_1^t \rangle$. Multiplying x_1 by a suitable scalar, we may take $(y_1, x_1) = 1$. Then $\{y_1, x_1, y_1^t, x_1^t\}$ is a hyperbolic basis for V_1. (cf. section 19 in [FGT]) In particular V_1 is nondegenerate so $V = V_1 \oplus V_1^\perp$, and proceeding by induction on m,

$$V = V_1 \perp \cdots V_r \perp W$$

where $W \le C_V(t)$ and V_i has a hyperbolic basis $\{y_i, x_i, y_i^t, x_i^t\}$. Notice $[V,t]$ has basis $\{y_i + y_i^t, x_i + x_i^t : 1 \le i \le r\}$, so $\dim([V,t]) = 2r$ and G is transitive on the set a_{2r} of involutions t with $V = V(t)$ and $\dim([V,t]) = 2r$ by Witt's Lemma.

So assume $V \ne V(t)$. Then $V(t)$ is a hyperplane of V, so $V(t) = V_0^\perp$ for the point $V_0 = V(t)^\perp$. Pick $u \in V - V(t)$, $a \in F$ with $a^2 = (u, u^t)^{-1}$, and let $x_1 = au$. Then $\{x_1, x_1^t\}$ is a hyperbolic basis for $V_1 = \langle x_1, x_1^t\rangle$ and $V = V_1 \oplus V_1^{\perp}$. Continuing in this fashion we write

$$V = V_1 \perp \cdots \perp V_s \perp W$$

where V_i has hyperbolic basis $\{x_i, x_i^t\}$ and $W \leq V(t)$. Then $V_0 = \langle v_0\rangle$, where $v_0 = \sum_{i=1}^{s} x_i + x_i^t$. If s is odd let $x = \sum_{i=1}^{s} x_i$ and observe $\{x, x^t\}$ is a hyperbolic basis for $U = \langle x, x^t\rangle$ with $U^{\perp} = V(t) \cap x^{\perp} \leq V(t)$, so by the a_{2r} case, the restriction of t to $U^{\perp}$ is of type a_{2r} and G is transitive on the set b_{2r+1} of involutions t with $m([V,t]) = 2r+1$.

Finally if s is even let $x = x_s$ and $y = \sum_{i<s} x_i$. Then $\{x, x^t, y, y^t\}$ is a hyperbolic basis for $U = \langle x, x^t, y, y^t\rangle$ with $V_0 \leq U$, so again $U^{\perp} \leq V(t)$ and by the a_{2r} case, G is transitive on the set c_{2r} of involutions with $V \neq V(t)$ and $m([V,t]) = 2r$. Q.E.D.

As an immediate corollary to 5.1 we have:

(5.2) *$Sp_6(2)$ has four classes b_1, a_2, c_2, and b_3 of involutions.*

(5.3) *Let $G = Sp_6(2)$. Then* $\mathrm{Schur}_2(G) \cong \mathbf{Z}_2$ *and involutions of type b_1 and c_2 in G lift to elements of order* 4 *in* $\mathrm{Cov}_2(G)$.

Proof. The centralizer of an involution in Co_3 is a covering of $Sp_6(2)$ over $\mathbf{Z}_2$, so it remains to show $|\mathrm{Schur}_2(G)| \leq 2$ and to establish the statement about lifts of involutions. Let b be a transvection in G, $H = C_G(b)$, and $A = O_2(H)$. Then b is of type b_1 and A is the core of the permutation module for the Levi factor $L \cong S_6$ for H, with each coset of $\langle b\rangle$ in A containing one involution of type a_2 and one of type c_2.

Let $\hat{G}$ be a covering of G over a center $Z = \langle z\rangle$ of order 2 and for $B \leq G$ write $\hat{B}$ for the preimage of B in $\hat{G}$. From the representation of L on A, either $\Phi(\hat{A}) = 1$ or $\hat{A} \cong \mathbf{Z}_4 * 2^{1+4}$. Assume the former. Then as $H^1(L, A/\langle b\rangle) \cong \mathbf{Z}_2$, $\hat{A}$ splits over Z. Further all involutions in L are of type b_1, a_2, or c_2, and hence lift to involutions as $\Phi(\hat{A}) = 1$. Therefore $\hat{L} = Z \times \hat{L}_0$ and then $\hat{H} = \hat{L}_0[\hat{A}, \hat{L}_0] \times Z$ splits over Z. But then as H contains a Sylow 2-subgroup of G, $\hat{G}$ splits over Z, a contradiction.

So $\hat{A} = \mathbf{Z}_4 * 2^{1+4}$ and in particular $\langle\hat{b}\rangle = \langle\beta\rangle$ so that involutions of type b_1 lift to element of order 4. Next G has a parabolic P with $P/O_2(P) \cong L_3(2)$ and possessing a P-submodule R of $O_2(P)$ which is the natural module for $P/O_2(P)$ with each involution in R of type a_2. As P is transitive on $R^{\#}$, $\Phi(\hat{R}) = 1$, so elements of type a_2 lift to involutions. Thus if $\sigma \in \hat{A}$ is the lift of an involution of type a_2 then $\sigma$ is an involution, so the lift $z\sigma$ of an involution of type c_2 is of order 4.

Now let $\tilde{G} = \mathrm{Cov}_2(G)$. Then $\hat{G} = \tilde{G}/U$ for some hyperplane $U$ of $V = Z(\tilde{G})$. Further if $\alpha \in \tilde{G}$ with $\alpha$ of type b_1 then $\alpha^2 \in V - U$. But if $U \neq 1$ there is a hyperplane $W$ of $V$ with $\alpha^2 \in W$, so that $\tilde{G}/W$ is a covering of $G$ over $\mathbf{Z}_2$ in which transvections lift to involutions, a contradiction. Q.E.D.

(5.4) *Up to isomorphism the spin module for* $Sp_6(2)$ *is the unique* 8*-dimensional irreducible* $\mathbf{F}_2Sp_6(2)$*-module.*

Proof. Let $G = Sp_6(2)$ and $0 \neq M$ an irreducible $\mathbf{F}_2G$-module. As $\mathbf{F}_2$ is a splitting field for $G$, $M = M(\lambda)$ for some restricted dominant weight $\lambda \neq 0$. Next the Weyl group $W$ for $G$ is of type C_3, so the orbit $\lambda W$ of $\lambda$ under $W$ is of length $|W : W_\lambda|$ where W_λ is the parabolic stabilizing $\lambda$, so either $|\lambda W| > 8$ or $\lambda = \lambda_1$ or λ_3 and $|\lambda W| = 6$ or 8, respectively, where λ_i is the ith fundamental dominant weight. As $M(\lambda_1)$ is the natural module of dimension 6 and $M(\lambda_3)$ the spin module of dimension 8, the lemma follows. Q.E.D.

(5.5) *Let* $G \cong U_6(2)$ *and* $V$ *an absolutely irreducible* 20*-dimensional* $\mathbf{F}_2G$*-module such that* $G_v \cong L_3(4)/E_{2^9}$ *for some* $v \in V$*. Let* $M = V \otimes_{\mathbf{F}_2} \mathbf{F}_4$ *regarded as a* $\mathbf{F}_4G$*-module. Then* $M = \bigwedge^3(N)$*, where* $N$ *is the natural module of dimension* 6 *for the covering* $\hat{G} \cong SU_6(2)$ *of* $G$*. In particular the* $\mathbf{F}_2G$*-module* $V$ *is determined up to equivalence.*

Proof. As $V$ is an absolutely irreducible $\mathbf{F}_2G$-module of dimension 20, $M$ is an irreducible $\mathbf{F}_4G$-module of dimension 20. Next $\hat{G} \leq S \leq GL(M)$ with $S \cong SL_6(4)$ and if $\sigma$ is the graph-field automorphism of $S$ with $C_S(\sigma) = \hat{G}$ then $\sigma$ acts on $M$ too. As $v$ is fixed by the maximal parabolic G_v of $G$, $v$ is a high weight vector for $M$ as an $\mathbf{F}_4S$-module, so $\mathbf{F}_4v$ is stabilized by a parabolic $P$ of $S$ containing $\hat{G}_v$ and invariant under $\sigma$. It follows that $P$ is the parabolic of $S$ corresponding to the middle node of the Dynkin diagram of $S$. Thus if $\lambda$ is the high weight vector of $M$ and $W$ is the Weyl group of $S$ then W_λ is the parabolic of $W$ corresponding to the middle node, so $W_\lambda \cong S_3 \times S_3$ and $\lambda W$ is of length $|W : W_\lambda| = 20$. Hence as $20 = \dim_{\mathbf{F}_4}(M)$, $\lambda$ is the unique dominant weight of $M$, so $\lambda = \lambda_3$ is the third fundamental dominant weight for $S$ and $M = M(\lambda_3)$ is the corresponding high weight module. Hence $M = \bigwedge^3(N)$. Q.E.D.

In the next three lemmas in this section let $G \cong U_6(2)$, $V$, $M$, $S$, and $N$ be as in Lemma 5.5. We discover in section 7 that a module satisfying the hypothesis of V admits the structure of an orthogonal space over $\mathbf{F}_2$ preserved by G, so as V is determined up to equivalence, V has that structure and $G \leq O(V)$.

(5.6) *Let $G_0 = G_1 \times G_2$ be the stabilizer in G of a nondegenerate 2-dimensional subspace of the natural module N for $\hat{G}$, with $G_1 \cong U_2(2)$ and $G_2 \cong U_4(2)$. Then as an orthogonal space over $\mathbf{F}_2$, $V = (V_1 \oplus V_2) \perp V_3$, where V_1 and V_2 are copies of the $O_6^-(2)$-module for G_2, $V_1 = [V, j]$ for some involution $j \in G_1$, and V_3 is isomorphic to the $U_4(2)$-module for G_2.*

Proof. Let G_0 be the stabilizer of a nondegenerate 2-subspace N_0 of N. Pick an orthonormal basis $\{x_1, \ldots, x_6\}$ for N with $x_1, x_2 \in N_0$. By 5.5 we may regard M as $\bigwedge^3(N)$. Let M_3 be the subspace of M spanned by $m_i = x_1 \wedge x_2 \wedge x_i$, $3 \leq i \leq 6$. Then G_1 centralizes M_3 and the map $m_i \mapsto x_i$ induces an isomorphism of M_3 with $N_0^\perp$ as an $\mathbf{F}_4G_2$-module, so M_3 is the natural module for $G_2 \cong U_4(2)$.

Next we can choose j to interchange x_1 and x_2, so $[M, j] = M_1$ is spanned by $m_{r,s} = (x_1 + x_2) \wedge x_r \wedge x_s$, $3 \leq r < s \leq 6$, and the map $m_{r,s} \mapsto x_r \wedge x_s$ is an isomorphism of M_1 with $\bigwedge^2(N_0^\perp)$ as an $\mathbf{F}_4G_2$-module. Therefore as $\bigwedge^2(N_0^\perp)$ is the $O_6^-(2)$-module for G_2 tensored up to $\mathbf{F}_4$, M_1 is that module. Similarly $G_1 = \langle j, i \rangle$ for i a conjugate of j and $M_2 = [M, i]$ is isomorphic to M_1 as an $\mathbf{F}_4G_2$-module and $M = M_1 \oplus M_2 \oplus M_3$. Recall $G = C_S(\sigma)$ with σ acting on M_i, so $M_i = V_i \otimes_{\mathbf{F}_2} \mathbf{F}_4$ for some $\mathbf{F}_2G_0$-submodule V_i of V satisfying the conclusions of this lemma. Q.E.D.

(5.7) *Let z be a long root element of G, $L \cong U_4(2)$ a Levi factor of $C_G(z)$, and W a $\mathbf{F}_2G$-module with $C_W(G) = 0$ and $[W, G] = V$. Then $W = W_1 \oplus W_2 \oplus W_3$ as a $\mathbf{F}_2L$-module, with $W_i \leq V$ of dimension 6 for $i = 1, 2$, $V_3 = V \cap W$ of dimension 8, and $C_W(L) = 0$.*

Proof. First $K = C_G(L) \cong S_3$ with KL the stabilizer in G of a nondegenerate 2-subspace N_0 of N. Thus by the previous lemma, $V = V_1 \oplus V_2 \oplus V_3$ with $V_1 + V_2 = [V, K]$, $\dim(V_1) = \dim(V_2) = 6$, and $V_3 = C_V(K)$ of dimension 8. Let Y be of order 3 in K. Then $V_1 + V_2 = [W, K]$. Let $W_3 = C_V(Y)$. Then $V_3 = V \cap W_3$ and it remains to show $C_W(L) = 0$. Assume not and let U be a point in $C_W(L)$. Replacing W by $V + U$ we may assume V is a hyperplane of W. Now $C_W(L) = C_{W_3}(L) = C_W(LK) = U$.

Let $E_{27} \cong E \leq L$ and $A = EY$. Then $A = J(T)$ for $T \in Syl_3(G)$ and $N_G(A)/A \cong S_6$. As V_3 is the $U_4(2)$-module for L, $V_3 = [V_3, E]$, so as $V_1 + V_2 = [W, Y]$, $V = [W, A]$ and $U = C_W(A)$. Therefore $X = \langle N_G(A), LK\rangle$ centralizes U, so to derive a contradiction, it remains to prove $X = G$.

Now X is a group generated by the class $D = z^X$ of 3-transpositions. Further as $C_G(z)$ is a maximal parabolic of G with L irreducible on $O_2(C_G(z))/\langle z\rangle$, $C_X(z) = \langle z\rangle \times L$. By Exercise 3.3 in [3T], $O_3(X) \leq Z(X) \geq O_2(X)$. Let $B = N_G(A)$; then $B = \langle C_B(z), C_B(d)\rangle$ for $d \in z^B - K$, so $X = \langle L, B\rangle = \langle C_X(z), C_B(d)\rangle$, and hence the commuting graph on D is connected. Therefore by 9.4.4 in [3T], X is primitive on D. Then by Theorem 9.5.4, X is rank 3 on D, and hence $C_X(z)$ is maximal in X, contradicting $C_X(z) < KL$. This completes the proof of the lemma. Q.E.D.

(5.8) (1) $\dim_{\mathbf{F}_2} H^1(G, V) = 2$.

(2) *Let* $L \cong U_4(2)$ *and* U *the natural module for* L *regarded as an* 8-*dimensional* $\mathbf{F}_2$-*module. Then* $\dim_{\mathbf{F}_2} H^1(L, U) = 2$.

(3) *Let* D *be the largest* $\mathbf{F}_2G$-*module such that* $D = [D, G]$ *and* $D/C_D(G) = V$, G_v *a* $L_3(4)/E_{2^9}$ *parabolic of* G, *and* $E/C_D(G)$ *the* 10-*dimensional* G_v-*submodule of* V. *Then* $C_D(G) \leq [E, G_v]$.

Proof. By 5.7, $\dim_{\mathbf{F}_2} H^1(G, V) \leq \dim_{\mathbf{F}_2} H^1(L, U)$. Further we find in a later paper in this series that $\dim_{\mathbf{F}_2} H^1(G, V) \geq 2$ and that (3) holds, so it remains to show $\dim_{\mathbf{F}_2} H^1(L, U) \leq 2$. Let W be the largest $\mathbf{F}_2L$-module with $[W, L] = U$ and $C_W(L) = 0$. (cf. 17.11 of [FGT]) As U is a $\mathbf{F}_4L$-module, so is W by the universal property of W, and it remains to show $\dim_{\mathbf{F}_4}(W/U) \leq 1$. Let $S \in Syl_3(L)$. Then $A = J(S) \cong E_{27}$ and $Z = Z(S)$ is of order 3 with $O_3(C_L(Z)) = P \cong 3^{1+2}$ and $C_G(Z)/P \cong SL_2(3)$. Now $U = [U, A]$ so $W = U \oplus C_W(A)$ and $N_L(A)$ centralizes $C_W(A)$. On the other hand $C_U(Z)$ is a point centralized by $O^3(C_L(Z))$, so the involution t inverting P/Z acts on S and hence centralizes $C_W(A)$ and then also $C_W(Z) = C_U(Z) + C_W(A)$. Then if x is of order 4 in $C_L(Z)$ with $x^2 = t$, x induces a $\mathbf{F}_4$-transvection on $C_W(Z)$ with center $C_U(Z)$, so if $\dim_{\mathbf{F}_4}(W/U) > 1$, then the hyperplanes $C_W(Z\langle x\rangle)$ and $C_W(A)$ of $C_W(Z)$ intersect nontrivial, so $C_W(X) \neq 0$, where $X = \langle N_L(A), x\rangle$. Finally as $N_L(A)$ is a maximal parabolic of $L \cong PSp_4(3)$ and $x \notin N_L(A)$, $X = L$, contradicting $C_W(L) = 0$.
Q.E.D.

(5.9) *Let* V *be a* 6-*dimensional unitary space over* $\mathbf{F}_4$ *and* Δ *the graph on the totally singular* 3-*subspaces of* V *with distinct* $x, y \in \Delta$ *adjacent if* $x \cap y \neq 0$. *Then* $Aut(\Delta) = P\Gamma(V) \cong Aut(U_6(2))$ *is the group of projective semilinear unitary maps on* V.

Proof. Let $G = P\Gamma(V)$ and $A = Aut(\Delta)$, so that $G \leq A$. For $x \in \Delta$, $G_x = LR$, where $R \cong E_{2^9}$ is the radical of G_x and L is a Levi factor isomorphic to $PGL_3(4)$ extended by a field automorphism. Further $\Delta(x) = \Delta_1(x) \cup \Delta_2(x)$ where

$$\Delta_i(x) = \{y \in \Delta : \dim(x \cap y) = i\}$$

with $|\Delta_1(x)| = 336$ and $|\Delta_2(x)| = 42$. Also $\Delta - x^\perp = \Gamma(x)$ is of order 512 with R regular on $\Gamma(x)$ and $L = G_{x,z}$ for suitable $z \in \Gamma(x)$.

For $y \in \Delta(x)$, let

$$\theta(y) = \{u \in \Delta(x) : x \cap y = x \cap u\}$$

and let $\theta = \{\theta(y) : y \in \Delta(x)\}$ and $\theta_i = \{\theta(y) : y \in \Delta_i(x)\}$. Notice $u \in \Delta(x,z)$ if and only if $u = (u \cap x) + (u \cap z)$ with $u \cap z = (u \cap x)^\perp \cap z$, so $|\Delta(x,z) \cap T| = 1$ for each $T \in \theta$. Thus if $m_i = |\Delta(y) \cap \Gamma(x)|$ for $y \in \Delta_i(x)$, then

$$m_i \cdot |\Delta_i(x)| = 512 \cdot 21$$

so $m_1 = 2^5$ and $m_2 = 2^8$. Therefore A_x acts on $\Delta_i(x)$ for $i = 1, 2$. Also for $y \in \Delta_2(x)$, $21 \cdot |\theta(y)| = |\Delta_2(x)| = 42$, so $\theta(y)$ is of order 2.

As R is regular on $\Gamma(x)$, $A_x = RA_{x,z}$. Now for $u \in \Delta_1(x,z)$ and $v \in \Delta_2(x,z)$, $u \in \Delta(v)$ if and only if $u \cap x \leq v \cap x$, so $\Delta(x,z)$ has the structure of the projective plane π on x, and that structure is preserved by $A_{x,z}$. Let B be the kernel of the action of $A_{x,z}$ on $\Delta(x,z)$. As $Aut(\pi) \cong L$ and L is faithful on $\Delta(x,z)$, $A_{x,z} = LB$. Further for $T \in \theta_2$, $|\Delta(x,z) \cap T| = 1$ and $|T| = 2$, so B fixes both points of T. Therefore B is trivial on $\Delta_2(x)$. However as L is irreducible on R, L is maximal in $G_x = LR$, so as R is regular on $\Gamma(x)$, G_x is primitive on $\Gamma(x)$, and hence for $z \neq w \in \Gamma(x)$, $\Delta_2(x,z) \neq \Delta_2(x,w)$. Therefore as B is trivial on $\Delta_2(x)$, B is also trivial on $\Gamma(x)$. Hence B fixes $\Delta(x,w) \cap T$ for each $T \in \theta_1$, so B is trivial on $\Delta_1(x)$, and therefore $B = 1$.

We have shown $A_{x,z} = LB = L$, so $A_x = RA_{x,z} = RL = G_x$. Then as G is transitive on Δ, $A = GA_x = G$, completing the proof. Q.E.D.

§6. Groups of type ${}^2E_6(2)$

Define a group G to be of *type* ${}^2E_6(2)$ if G possesses an involution z such that (G,z) satisfies Hypothesis $\mathcal{H}(10, U_6(2))$, in the language of Example 4.2. Throughout this short section, assume G is of type ${}^2E_6(2)$ and let z be an involution in G such that $H = C_G(z)$ and $Q = F^*(H)$ satisfy our hypotheses. Therefore Hypothesis 4.1 is satisfied, and indeed in a moment we see that Hypothesis 4.4 is also satisfied. Thus we adopt the notation of section 4, except that we write $t = z^g$ for our distinguished element of $z^G \cap Q - \{z\}$. In particular $H = C_G(z)$ satisfies $Q = F^*(H) \cong 2^{1+20}$, $H^* = H/Q \cong U_6(2)$, and z is not weakly closed in Q with respect to G. Recall also that $E = Q \cap Q^g$ and $R = (Q^g \cap H)(Q \cap H^g)$.

(6.1) (1) $E \cong E_{2^{11}}$.

(2) $N_{H^*}(E) = C_{H^*}(\tilde{t}) = N_{H^*}(R^*)$ *is the parabolic of* H^* *which is the split extension of* $R^* \cong E_{2^9}$ *by* $L_3(4)$ *with* R^* *the Todd module for* $L_3(4)$.

(3) $R^* = J(T^*)$ *for* $T \in Syl_2(H)$.

(4) *Let* $X_2 = \langle Q, Q^g \rangle$ *and* $V = \langle z, t \rangle$. *Then* $P_2 = N_G(V) = X_2 C_H(V)$ *with*

$$R = O_2(P_2) = C_{X_2}(V),$$

$P_2/R = X_2/R \times C_G(V)/R$, $X_2/R \cong S_3$, *and* $C_G(V)/R \cong L_3(4)$.

(5) $E/V = Z_2(R)$ *is centralized by* X_2 *and is the dual of the Todd module for* $C_G(V)/R$.

(6) $R/E \cong E_{2^{18}}$ *is the tensor product of the natural module for* X_2/R *and the Todd module for* $C_G(V)/R$.

(7) H^* *is absolutely irreducible on* $\tilde{Q}$.

Proof. Let $R \leq T \in Syl_2(H)$. By 23.4 in [3T], $J(T^*) \cong E_{2^9}$, so Hypothesis 4.4 is satisfied. Indeed $N_{H^*}(J^*)$ is the parabolic of $H^* \cong U_6(2)$ which is the split extension of $J(T^*)$ by $L_3(4)$ with $J(T^*)$ the Todd module. Therefore the lemma follows from 4.5. Q.E.D.

(6.2) $\tilde{Q} \otimes_{\mathbf{F}_2} \mathbf{F}_4$ *is isomorphic as a* $\mathbf{F}_4 H^*$*-module to* $\bigwedge^3(N)$, *where* N *is the natural module of dimension* 6 *for the covering* $\hat{H}^* \cong SU_6(2)$ *of* H^*. *In particular the representation of* H^* *on* $\tilde{Q}$ *is determined up to equivalence.*

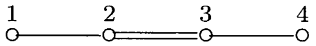
Proof. By 6.1.7, $\tilde{Q}$ is an absolutely irreducible $\mathbf{F}_2 H^*$-module of dimension 20, while by 6.1.2, $H^*_{\tilde{t}} \cong L_3(4)/E_{2^9}$. So as $H^* \cong U_6(2)$, the lemma follows from 5.5. Q.E.D.

§7. ${}^2E_6(2)$

In this section $G = {}^2E_6(2)$ and z is a long root involution in G. It is well known that:

(7.1) *The group* G *is of type* ${}^2E_6(2)$ *with* z *2-central in* G.

Thus we adopt the notation of section 6. In particular $H = C_G(z)$, $Q = O_2(H)$, and $T \in Syl_2(H)$ with $R \leq T$. Let $\Delta = z^G$, and let $P_1 = H$, P_2, P_3, P_4 be the four maximal parabolics of G containing T ordered so that we have the diagram



For $J \subseteq \{1,2,3,4\}$ let L_J be the standard Levi factor in the parabolic $P_J = \bigcap_{j \in J} P_j$ and $R_J = O_2(P_J)$ the unipotent radical of P_J. In particular $R = R_2$. Let W be the Weyl group of G.

(7.2) *H has the following 5 orbits on Δ:*
(1) $\Delta^0(z) = \{z\}$.
(2) $\Delta^1(z) = Q \cap \Delta - \{z\}$.
(3) $\Delta^2_1(z) = \Delta \cap H - Q$.
(4) $\Delta^2_2(z) = \{d \in \Delta : [z,d] \in \Delta\}$.
(5) $\Delta^3(z) = \{d \in \Delta : |zd| = 3\}$.

Proof. We sketch the proof in section 12 of [ASe] for completeness. The subgroup $W_1 = W \cap P_1$ has 5 orbits on W/W_1 so $H = P_1$ has 5 orbits on $G/H \cong \Delta$; cf. Exercise 14.6.1 in [FGT]. Now $z = U_\alpha(1)$, where α is the highest root in the root system Φ determining T. There is a long root $\beta \neq \alpha$ with $t = U_\beta(1) \in Q$; then $t \in \Delta^1(z)$. Similarly there is a long root γ such that $U_\gamma(1) \in L_1$, long roots ϵ_i, $i = 1,2$ with $U_{\epsilon_i}(1) \in L_1$, and $h \in H$ with $t^h \in C_Q(t)$, so that

$$[t, t^h] = z \quad \text{and } |U_{\epsilon_1}(1)U_{\epsilon_2}(1)| = 3$$

so $U_\gamma(1) \in \Delta^2_1(z)$ and $\Delta^2_2(z) \neq \varnothing \neq \Delta^3(z)$. Q.E.D.

(7.3) (1) *$L_1 \cong U_6(2)$ is a complement to Q in H.*

(2) *L_1 has 3 classes of involutions with representatives j_1, j_2, j_3, where j_i is the product of i transvections in $U_6(2)$. In particular j_1 is a long root involution of L_1 and j_2 is a short root involution.*

(3) *$A = J(T \cap L_1) \cong E_{2^9}$ is the unipotent radical of the parabolic $P_2 \cap L_1$ of L_1, $P_2 \cap L_1 = L_{1,2}A$ with $L_{12} \cong L_3(4)$, and A is the 9-dimensional Todd module for $L_{1,2}$.*

(4) *All involutions in L_1 are fused into A and if $a \in A \cap j_3^{L_1}$ then $C_{L_{1,2}}(a) \cong U_3(2)$.*

Proof. As L_1 is the standard Levi factor for P_1, L_1 is a complement to $R_1 = Q$ in $P_1 = H$. By 7.1, $L_1 \cong U_6(2)$. Then 23.2 in [3T] implies (2), 6.1 implies (3), and 23.3, and 22.2 in [3T] imply (4). Q.E.D.

(7.4) (1) $\dim([\tilde{Q}, j_i]) = 6, 8, 10$ *for* $i = 1, 2, 3$, *respectively.*

(2) Q *is transitive on the involutions in* j_3Q.

Proof. Let $M = N_{L_1}(L_{1,4})$. Then M is the stabilizer in L_1 of a nondegenerate 2-dimensional subspace of the natural module for $L_1 \cong U_6(2)$, so by 5.6, $M = M_1 \times M_2$ with $M_2 = L_{1,4} \cong U_4(2)$ and $M_1 = C_{L_1}(M_2) \cong L_2(2)$ with $j_1 \in M_1$. Further (again by 5.6) as an orthogonal space over $\mathbf{F}_2$, $\tilde{Q} = (\tilde{Q}_1 \oplus \tilde{Q}_2) \perp \tilde{Q}_3$, where $\tilde{Q}_1$ and $\tilde{Q}_2$ are copies of the $O_6^-(2)$-module for M_2, $\tilde{Q}_1 = [\tilde{Q}, j_1]$, and $\tilde{Q}_3$ is isomorphic to the $U_4(2)$-module for M_2. Thus $6 = \dim(\tilde{Q}_1) = \dim([\tilde{Q}, j_1])$. Next we can take $j_2 = ab$, where a, b are L_1 conjugates of j_1 in M_2, so $\dim([\tilde{Q}_3, j_2]) = 4$ and $\dim([\tilde{Q}_i, j_2]) = 2$ for $i = 1, 2$, and hence $\dim([\tilde{Q}, j_2]) = 8$. Finally we can take $j_3 = j_1j_2$. Then j_3 interchanges two of the three M_2-irreducibles on $\tilde{Q}_1 \oplus \tilde{Q}_2$, so $\dim([\tilde{Q}_1 \oplus \tilde{Q}_2, j_3]) = 6$ and $\dim([\tilde{Q}_3, j_3]) = \dim([\tilde{Q}_3, j_2]) = 4$. That is (1) holds.

As $\dim([\tilde{Q}_3, j_3]) = 10 = \dim(\tilde{Q})/2$, $C_{\tilde{Q}}(j_3) = [\tilde{Q}, j_3]$, so $\tilde{Q}$ is transitive on the involutions in $\tilde{j_3}\tilde{Q}$; cf. Exercise 2.8.1 in [SG]. Hence all involutions in j_3Q are conjugate to j_3 or j_3z. Next we have a symplectic form α on $\tilde{Q}_2$ defined by $\alpha(\tilde{u}, \tilde{v}) = (\tilde{u}, \tilde{v}j_1)$ and there exists $\tilde{u} \in \tilde{Q}_2$ with $\alpha(\tilde{u}, \tilde{u}j_2) \neq 0$ as j_2 is of type c_2 in M_2 and $\tilde{Q}_2$ is the $O_6^-(2)$-module for M_2. Therefore $(\tilde{u}, \tilde{u}j_3) = (\tilde{u}, \tilde{u}j_2j_1) = \alpha(\tilde{u}, \tilde{u}j_2) \neq 0$, and hence $\tilde{u} + \tilde{u}j_3 \in C_{\tilde{Q}}(j_3)$ is nonsingular, so $j_3^u = j_3z$, establishing (2). Q.E.D.

(7.5) (1) $j_1 \in \Delta$ *is a long root involution so* $j_1 \in z^G$ *and* $H = C_G(z) \cong C_G(j_1)$.

(2) j_2 *is a short root involution, there is* $x \in j_2^G \cap Q \cap Z(R_4)$, *and* $C_G(x) \leq P_4$, $C_G(x) = R_4C_{L_4}(x)$, *where* $C_{P_4}(x) \cong Sp_6(2)$ *is the stabilizer in* $L_4 \cong \Omega_8^-(2)$ *of* x *regarded as a nonsingular point of the* 8-*dimensional orthogonal space* $Z(R_4)$ *for* L_4, *with* $Q \cap Z(R_4)$ *the subspace orthogonal to* z.

(3) *There is* $y \in j_3^G \cap Q \cap Q^g$ *for* $g \in P_2 - H$, $C_G(y) \leq P_2$ *with* $|R_2 : C_{R_2}(y)| = 4$ *and* $C_{L_2}(y) \cong L_2(2) \times U_3(2)$.

(4) $z, t = z^g, x, y$ *are representatives for the orbits of* H *on involutions of* Q, *with* $C_{L_1}(\tilde{t}) \cong L_3(4)/E_{2^9}$, $C_{L_1}(\tilde{x}) \cong Sp_4(2)/2^9$, *and* $C_{L_1}(\tilde{y}) \cong U_3(2)/2^8$.

Proof. First j_1 is a long root involution of L_1 by 7.3.2, so $j_1 \in \Delta$ and (1) holds.

Similarly by 7.3.2, j_2 is a short root involution of L_1 and hence of G. Let $Z_4 = Z(R_4)$; it is well known (cf. [CKS]) that Z_4 is the natural module for $L_4 \cong \Omega_8^-(2)$ with long root involutions in Z_4 the singular points and short root involutions in Z_4 the nonsingular points. Further $Q \cap Z_4$ is the subspace of Z_4 orthogonal to z. So if $x \in Q \cap Z_4$ is a short root involution then $C_{L_4}(x) \cong Sp_6(2)$. Now $C_G(x) \leq P$ for some parabolic P by Borel-Tits; cf. 47.8.2 in [FGT]. But the only parabolics of G containing subgroups of the form $C_{L_4}(x)R_4 = Sp_6(2)/2^{24}$ are conjugates of P_4, so $P = P_4^h$ for some $h \in G$. Then $O_2(P) = O_2(C_{P_4}(x)) = R_4$, so $P = P_4$ and (2) is established.

Let $g \in P_2 - H$, $t = z^g$, and $E = Q \cap Q^g$. By 7.3, $A = J(T \cap L_1) = R_{1,2} \cap L_1 \cong E_{2^9}$ contains a conjugate of j_3. Further from 6.1.6, $L_{1,2}$ has three irreducibles on R_2/E, all fused under P_2, so AE/E is one of those irreducibles and $(Q \cap R_2)/E$ is another, and A is fused to $A^w \leq Q \cap R_2$ under P_2. Next A^w and $[E, L_{1,2}]$ are dual irreducibles for $L_{1,2}$ and there is $l \in N_{L_1}(L_{1,2})$ inducing a graph automorphism on $L_{1,2}$, so $A^{wl} = [E, L_{1,2}]$, and hence there is $y \in j_3^G \cap E$. Next $C_{P_2}(y) = C_{L_2}(y)C_{R_2}(y)$ with $C_{L_2}(y) = L_{2,3,4} \times C_{L_{1,2}}(y)$ and by 7.3.4 and 6.1.5, $C_{L_{1,2}}(y) \cong U_3(2)$ with $C_A(y)$ a hyperplane of A and $|R_2 : C_{R_2}(y)| = 4$. Thus to complete the proof of (3) it remains to show $C_G(y) \leq P_2$. Again by Borel-Tits, $C_G(y) \leq P$ for some parabolic P of G and by 4.3, z is weakly closed in the center of a Sylow 2-subgroup of $C_G(y)$, so $P \cap H$ is a parabolic of G. Then $C_H(y) \leq P \cap H$.

Let $B = C_A(y)$. Observe first that $C_{\tilde{Q}}(B) = \langle \tilde{t}, \tilde{y} \rangle$. For $C_{L_{1,2}}(y)$ is irreducible on the hyperplane $[Q/E, B]$ of Q/E and as $L_{1,2}$ is irreducible on A, B contains a conjugate b of j_3. By 7.4.1, $C_{\tilde{Q}}(b)E/E = [\tilde{Q}, b]E/E \leq [Q/E, B]$, so as $C_{L_{1,2}}(y)$ is irreducible on $[Q/E, B]$, so $C_{\tilde{Q}}(B) \leq E$, and then by 4.5.7 completes the proof of the observation.

Next as $|R_2 : C_{R_2}(y)| = 4$, R_2 is transitive on $\langle z, t, y \rangle - \langle z, t \rangle$, so $\tilde{t}$ is weakly closed in $C_{\tilde{Q}}(B) = \langle \tilde{t}, \tilde{y} \rangle$, and therefore $N_{L_1}(S) \leq L_1 \cap P_2 = N_{L_1}(A)$, for each 2-subgroup S of L_1 containing B. Hence $P_2 \cap P \cap L_1$ contains a Sylow 2-subgroup of $P \cap L_1$, so as $A = J(T \cap L_1)$, $A \leq P \cap H$. Then as $A = O_2(A(C_{L_1}(y) \cap N_{L_1}(A)))$ and $C_{L_1}(y)$ is irreducible on B, $B \leq O_2(P \cap L_1) \leq A$, so that $P \cap L_1 = P_2 \cap L_1$ and then $P \cap H = P_{1,2}$. Therefore $P_2 = \langle P_{1,2}, P_{2,3,4} \rangle \leq P$, so $P = P_2$ and (3) holds.

Now $|L_1| = 2^{15} \cdot 3^6 \cdot 5 \cdot 7 \cdot 11$ and $|C_{H^*}(\tilde{y})| = 2^{11} \cdot 3^2$, so $|\tilde{y}^H| = 2^4 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11$. Similarly $|C_H(\tilde{t})| = 2^{15} \cdot 3^2 \cdot 5 \cdot 7$, so $|\tilde{t}^H| = 3^4 \cdot 11$. Finally

$$C_H(x) = C_{P_4}(z) \cap C_{P_4}(x) = R_4 C_{L_4}(\langle z, x \rangle)$$

with $C_{L_4}(\langle z, x \rangle) \cong Sp_4(2)/2^5$, so $|C_H(x)| = 2^{33} \cdot 3^2 \cdot 5$. Then as $|C_Q(x)| = 2^{20}$, $|C_{L_1}(\tilde{x})| = 2^{13} \cdot 3^2 \cdot 5$, so $|\tilde{x}^H| = 2^2 \cdot 3^4 \cdot 7 \cdot 11$. Now the sum of the lengths of these three orbits is

$$3^4 \cdot 11 \cdot (1 + 2^2 \cdot 7 + 2^4 \cdot 5 \cdot 7) = 3^4 \cdot 11 \cdot 588 = 3^4 \cdot 11 \cdot 19 \cdot 31 = (2^9 + 1)(2^{10} - 1).$$

But $(2^9+1)(2^{10}-1)$ is the number of singular points in a 20-dimensional orthogonal space of maximal Witt index over $\mathbf{F}_2$, so (4) is established. Q.E.D.

(7.6) *Q is regular on $\Delta^3(z)$ and for $d \in \Delta^3(z)$, $C_G(\langle z, d\rangle)$ is conjugate under Q to L_1.*

Proof. By 7.2, we may take $z = U_\alpha(1)$ and $d = U_{-\alpha}(1)$. Then $C_G(\langle z, d\rangle) = H \cap H^{w_0} = P_1 \cap P_1^{w_0} = L_1$, where w_0 is the long word in W, as $\alpha W_0 = -\alpha$, so $z^{w_0} = d$. Thus as L_1 is a complement to Q, Q is regular on $\Delta^3(z)$. Q.E.D.

(7.7) *j_1, j_2, and j_3 are representatives for the three conjugacy classes of involutions in G.*

Proof. We first observe that if j is an involution in G then $z^i \in \Delta^3(z)$ for some $i \in j^G$. This is Lemma 12.2 in [ASe], but we sketch a proof for completeness. Without loss, $j \in H$. By 7.5, each involution in Q is fused into L_2, so we may assume $j \notin Q$. Let $H^* = H/Q$. It is easy to check that $|k^* k^{*j}| = 3$ for some root involution $k \in L_1$, so by 7.2, $k^j \in \Delta^3(k)$, completing the proof of the observation.

So each involution in G is fused to $s \in L_1 \cup L_1 z$, so s is fused to j_i or $j_i z$. Finally zj_i centralizes a conjugate of $\langle z, d\rangle$ in L_1 unless $i = 3$, so it remains to observe that zj_3 is conjugate to j_3 by 7.4.2.

We have shown each involution in G is conjugate to j_i for $i = 1$, 2, or 3. But by 7.5.4 and 4.7.2, these involutions are not fused in G. Q.E.D.

(7.8) *Let $g \in P_2 - H$, $t = z^g$, and $E = Q \cap Q^g$. Then*

(1) *For $h \in P_{1,3,4} - P_2$, $t^h \in E$.*

(2) *$U_3 = Q \cap Q^g \cap Q^{gh} \cong E_{2^7}$.*

(3) *Let $V_3 = \langle z, t, t^h\rangle$. Then $C_H(V_3)/O_2(C_H(V_3)) \cong L_2(4)$ has chief series*

$$0 < \tilde{V} < \tilde{V}_3 < \tilde{U}_3 < \tilde{E}$$

on $\tilde{E}$ with E/U_3 the $\Omega_4^-(2)$-module and U_3/V_3 the $L_2(4)$-module. Further $C_H(V_3)$ has four $L_2(4)$-sections and three $\Omega_4^-(2)$-sections on R_3.

Proof. First by 7.5.2, $Z_4 = Z(R_4)$ is the orthogonal space for $L_4 \cong \Omega_8^-(2)$ with $Q \cap Z_4$ the hyperplane orthogonal to z. Further the parabolic $P_{3,4}$ is the stabilizer in P_4 of the totally singular 3-subspace $V_3 = \langle z, t, t^h\rangle$. Thus $t^h \in E$ and indeed $V_3 = Z(P_3)$ with $C_H(V_3) = L_{1,2,3}R_3$ and $L_{1,2,3} \cong L_2(4)$ has chief series on $\tilde{E}$ has described in (3), except we have not shown that $U_3 = E_3$, where E_3 is the penultimate term in the series. But as U_3 is $C_H(V_3)$-invariant, $U_3 = E_3$ or V_3, and the latter is impossible as $U_3 \cap Z_4$ is of dimension 5.

Finally the chief sections can be retrieved as follows. Let $A = R_2 \cap L_1$ be as in 7.3. The nontrivial chief sections of $L_{1,2,3}$ on R_4 are those in $(R_{1,2,3} \cap L_1)/A$, A, E/V, and $C_Q(t)/E$, and by 6.1, A is isomorphic to $C_Q(t)/E$ and to the dual of E/V as an $L_{1,2,3}$-module. Finally $(R_{1,2,3} \cap L_1)/A$ is the $L_2(4)$-module, while A has one $L_2(4)$ chief section and one $\Omega_4^-(2)$-chief section. Q.E.D.

(7.9) *Let Δ be the graph with vertex z^G and z adjacent to t if $z \neq t \in Q$. Then Δ is simply connected.*

Proof. This follows from 1.1, since the building for G is of type F_4 and Δ is the collinearity graph of the building. Q.E.D.

(7.10) (1) *G has an involutory outer automorphism σ with $C_G(\sigma) \cong F_4(2)$, and we may choose σ so that:*

(2) *$C_{L_1}(\sigma) \cong Sp_6(2)$ and $C_Q(\sigma) = D_1D_2$ where $D_1 \cap D_2 = \langle z \rangle$, $[D_1, D_2] = 1$, $\tilde{D}_1 = [\tilde{Q}, \sigma]$, D_1 is isomorphic to the stabilizer of a nonsingular point in an 8-dimensional orthogonal space over $\mathbf{F}_2$ as a $C_{L_1}(\sigma)$-module, with singular points in j_2^G, and $D_2 \cong 2^{1+8}$ with $C_Q(\sigma)/D_1$ the spin module for $C_{L_1}(\sigma)$.*

(3) *$C_{L_2}(\sigma) \cong S_3 \times L_3(2)$ and σ centralizes $Z(R_2)$.*

(4) *For $S \in Syl_2(C_G(\sigma))$, $Z(S) = Z(S) \cap Q \cong E_4$.*

(5) *σ and σz are representatives for the orbits of G on involutions in σG and $C_G(\sigma z) = C_H(\sigma)$.*

(6) *Let Y be a diagonal group of outer automorphisms of G of order 3. Then $C_G(Y)$ is of even order and if all involutions in $C_G(Y)$ are in j_3^G then $N_{Aut(G)}(Y)/Y \cong Aut(U_3(8))$.*

Proof. This is well known; indeed σ is a graph-field automorphism of G. See for example section 4 of [CKS] for parts (1)-(5). Part (6) can be retrieved from the Springer-Steinberg theory of semisimple elements of finite groups of Lie type. Q.E.D.

(7.11) (1) $|\mathrm{Schur}_2(G)| = 4$.

(2) *The outer automorphism group of G is faithful on* $\mathrm{Schur}_2(G)$.

Proof. Let $\hat{G} = Cov_2(G)$ and $Z = Z(\hat{G})$. For $Y \leq G$, write $\hat{Y}$ for the preimage of Y in $\hat{G}$.

As $T \leq H$, $\hat{H}$ is a covering of H, and hence an image of $\mathrm{Cov}_2(H)$, described in 3.2. In particular $\hat{Q} \cong Q \times Z$ by 3.2, so $[\hat{Q}, \hat{E}] = \Phi(\hat{Q}) \cong \mathbf{Z}_2$. Then as $\hat{X}_2 = \langle \hat{Q}, \hat{Q}^g \rangle$, $[\hat{X}_2, \hat{E}] = \Phi(\hat{Q})\Phi(\hat{Q})^g \cong E_4$.

Next $L_2 = L_{234} \times L_{12}$ with $L_{234} = X \cap L_2 \cong S_3$ and $L_{12} \cong L_3(4)$. Let $\hat{Y}$ be of order 3 in $\hat{L}_{234}$. Then $\hat{V}_Y = [\hat{V}_2, \hat{Y}] = [\hat{X}_2, \hat{E}]$ is a complement to Z in $\hat{V}_2$ and $[\hat{R}_2, \hat{E}] = \hat{V}_Y$ as $R_2 = O_2(X_2)$. Therefore $\hat{R}_2$ centralizes $\hat{E}/\hat{V}_Y$, so setting $\hat{E}_Y = [\hat{E}, \hat{P}_2]$, it follows that $\hat{E}_Y = [\hat{E}, \hat{L}_{1,2}]\hat{V}_Y$.

Next $\hat{E}/\hat{V}_2 \cong E/V$ is quasiequivalent to the Todd module for L_{12} by 6.1.5. Therefore

$$|(\hat{V}_2 \cap \hat{E}_Y)/\hat{V}_Y| \leq |H^1(L_{12}, E/V)| = 4$$

with the last equality following from 23.6 in [3T]. Hence $U = Z \cap \hat{E}_Y$ is of order at most 4 and as $Out(G)$ induces a group of outer automorphisms on L_{12}, $Out(G)$ is faithful on U if $U \neq 1$ by 23.6 in [3T]. So it remains to show $U = Z$, since we will find in a later paper in this series that $\mathrm{Schur}_2(G) \neq 1$.

Let $G^* = \hat{G}/U$; it remains to show $Z^* = 1$. Now $R_2 = [R_2, Y]$ so $\hat{R}_2^*/\hat{E}_Y^* = [\hat{R}_2^*/\hat{E}_Y^*, \hat{Y}^*] \times Z^*$. Therefore $\hat{P}_2^*/[\hat{R}_2^*, \hat{Y}^*] \cong \hat{L}_{234}^* \times \hat{L}_{12}^*$ with $\hat{L}_{12}^*$ quasisimple with center Z^*. Next $Q \leq L_{234}R$ by 6.1, so $Q \cong \hat{Q}^*$ and $\hat{H}^*/\hat{Q}^*$ is quasi simple with center Z^*. Indeed

$$\hat{R}_2^*\hat{Q}^*/\hat{Q}^* = [\hat{R}_2^*, \hat{Y}^*]\hat{Q}^*/\hat{Q}^* \times Z^*$$

so by 23.5.5 in [3T], $Z^* = 1$, completing the proof. Q.E.D.

(7.12) *Assume $M(22) \cong M \leq G$ such that the set D of* 3-*transpositions of M is contained in Δ. Then $C_D(a) \neq \varnothing$ for each $a \in \Delta$, and indeed M has the following four orbits, Δ_i, $1 \leq i \leq 4$, on Δ:*

(1) $\Delta_1 = D$ *of order* 3, 510.

(2) $\Delta_2 = \{a \in \Delta : C_D(a) \subseteq O_2(C_G(a))\}$ *of order* 142, 155, *with $C_M(a) \cong M_{22}/E_{2^{10}}$ and $C_D(a)$ of order* 22 *generating $O_2(C_M(a))$.*

(3) $\Delta_3 = \{a \in \Delta - D : |D \cap O_2(C_G(a))| = 1\}$ *of order* 3, 127, 410, *with $C_M(a) \cong L_3(4)/E_{2^{10}}$ and $C_D(a)$ of order* 22 *generating $O_2(C_M(a))$.*

(4) $\Delta_4 = \{a \in \Delta : D \cap O_2(C_G(a)) = \varnothing\}$ *of order* 694, 980, *with $C_M(a) = \langle C_D(a) \rangle \cong Sp_6(2)/E_{64}$.*

Proof. First $\Delta_1 = D$ is an orbit of M on Δ of length 3, 510 by 16.7 in [3T].

As $D \subseteq \Delta$, we may take $z \in D$. Then $K = C_M(d)$ is quasisimple with $K/\langle d \rangle \cong U_6(2)$, so $H = KQ$ with $K \cap Q = \langle z \rangle$. Claim

(5) K has the following six orbits on $\Delta \cap H$:

(i) $\{z\}$.

(ii) $D_z = H \cap D - \{z\}$.

(iii) $\Delta_i(z)$, $i = 1, 2$ with $\Delta_1(z) \cup \Delta_2(z) = \Delta(z) = \Delta \cap Q - \{z\}$,

$$\Delta_2(z) = \{za : a \in \Delta_1(z)\},$$

and $C_K(a) \cong L_3(4)/E_{2^{10}}$ for $a \in \Delta(z)$.

(iv) $\Delta_3(z)$ with $C_K(a) \cong A_5/E_{16}/E_{2^{10}}$ for $a \in \Delta_3(z)$.

(v) $\Delta_4(z)$ with $C_K(a) \cong Sp_4(2)/2^{1+8}/\mathbf{Z}_2$ for $a \in \Delta_4(z)$.

Namely by 7.2, H has three orbits on $\Delta \cap H$: $\{z\}$, $\Delta(z) = H \cap Q - \{z\}$, and $\Delta_1^2(z) = H \cap \Delta - Q$. As $H = KQ$ with $K \cap Q = \langle z \rangle$, K has two orbits $\Delta_i(z)$, $i = 1, 2$ on $\Delta(z)$, with $\Delta_2(z) = \{za : a \in \Delta_1(z)\}$, and by 6.1.2 and 23.5 in [3T], $C_K(a) \cong L_3(4)/E_{2^{10}}$ for $a \in \Delta(z)$.

Next let $b \in D_z$. Then $b \in \Delta_1^2(z)$ and each member of $\Delta_1^2(z)$ is K-conjugate to bu for some $u \in [Q, b]$. Now $[\tilde{Q}, b]$ is the natural module for $C_K(b)/O_2(C_K(b)) \cong \Omega_6^-(2)$ with $O_2(C_K(b)) \cong 2^{1+8}/\mathbf{Z}_2$, (cf. 7.3 and the proof of 7.4) so K has two orbits $\Delta_3(z)$ and $\Delta_4(z)$ on $\Delta_1^2(z) - D_z$, with representatives bu and bv, where $u, v \in [\tilde{Q}, b]$ with $\tilde{u}$ a singular point of the orthogonal space $[\tilde{Q}, b]$ and $\tilde{v}$ a nonsingular point. Then $C_K(bu) = C_K(b) \cap C_K(u) \cong A_5/E_{16}/2^{1+8}/\mathbf{Z}_2$ and $C_K(bv) = C_K(b) \cap C_K(v) \cong Sp_4(2)/2^{1+8}/\mathbf{Z}_2$. Indeed $C_K(u)$ is the parabolic $N_K(T \cap D) \cong L_3(4)/E_{2^{10}}$ with $O_2(C_K(u)) = \langle T \cap D \rangle$, so $C_K(bu) \cong A_5/E_{16}/E_{2^{10}}$, completing the proof of the claim.

Let $z^\perp = \{z\} \cup D_z$. If $a \in \Delta(z)$ or $\Delta_3(z)$ then $z^\perp \cap C_G(a) = T \cap D$ is of order 22 and hence is of the form $S \cap D$ for some $S \in Syl_2(M)$, with $A = \langle S \cap D \rangle \cong E_{2^{10}}$. Further if $a \in \Delta(z)$ then by 6.1, $C_K(a)$ has 3 irreducibles on $(Q \cap H_a)(Q_a \cap H)/(Q \cap Q_a)$, and one of them is $A(Q \cap Q_a)/(Q \cap Q_a)$, so $A(Q \cap Q_a) = Q_a \cap H$ or $Q_{az} \cap H$. In the first case, $A \leq Q_a$. Therefore for each $b \in A \cap D$, $a \in \Delta(b)$, so $A \cap D = b^\perp \cap C_G(a)$ and $C_M(\langle a, b \rangle)$ acts 2-transitively as $L_3(4)$ on $A \cap D - \{b\}$. Therefore $N_M(A) \leq C_M(a)$ with $N_M(A)/A \cong M_{22}$ by 25.7 in [3T]. As $A \cap D$ is a connected component of $C_D(a)$, it follows (cf. 24.3 in [3T] and its proof) that $A \cap D = C_D(a)$, so that $N_M(a) = C_M(a)$. That is $a \in \Delta_2$.

In the second case, $za \in \Delta_2$ and $A \cap Q_a = \langle z \rangle$, so for $b \in A \cap D - \{z\}$, $b \notin Q_a$, and hence $a \notin Q_b$, so $a \in \Delta_i(b)$ for $i = 3$ or 4. As $C_K(\langle a, b \rangle) \cong A_5/E_{16}/E_{2^{10}}$, and $C_M(\langle a, b \rangle)$ contains no such subgroup if $a \in \Delta_4(b)$, we conclude $a \in \Delta_3(b)$. Therefore $S \cap D = b^\perp \cap C_G(a)$ for each $b \in S \cap D$, so as above, $S \cap D = C_D(a)$ and $\{z\} = D \cap Q_a$. Hence $C_M(a) = C_K(a)$ and $a \in \Delta_3$ in this case.

So Δ_2 and Δ_3 are the orbits of M on $\Delta - D$ consisting of elements

a with $D \cap Q_a \neq \varnothing$. This leaves

$$\Delta_4' = \{a \in \Delta : C_D(a) \neq \varnothing = D \cap Q_a\} = \bigcup_{d \in D} \Delta_4(d)$$

as an orbit under M.

Pick $a \in \Delta_4(z)$ and let $D(a) = C_D(a)$. Then $D(a)$ is a set of 3-transpositions of $M_a = \langle D(a) \rangle$. Now $C_K(a) \cong Sp_4(2)/2^{2+8}$ and $C_K(a) = \langle z^\perp \cap D(a) \rangle$. Indeed for each $b \in D(a)$, $a \in \Delta_4(b)$ as $a \notin \Delta_3 \cup \Delta_4$, so by 8.2.2 in [3T], M_a is transitive on $D(a)$. Then by a Frattini argument, $C_M(a) = M_a C_K(a) = M_a$. Also in the language of [3T], $V_z = \{z, d\}$, where d is the unique member of $D \cap aQ$, so by 9.2 in [3T], $\{z, d\} = z^{O_2(M_a)}$, so $[z, O_2(M_a)] = \langle zd \rangle \leq Z(O_2(M_a))$. Therefore $U = \langle (zd)^{M_a} \rangle$ is elementary abelian and z induces a transvection on U. Let $\bar{M}_a = M_a/U$. As $O_2(C_K(a))/\langle zd \rangle \cong 2^{1+8}$ and $O_2(C_K(a))/\langle z, d \rangle$ is the sum of two 4-dimensional irreducibles for $C_K(a)$, $m(C_U(z)) = 5$, $m(U) = 6$, and $C_{\bar{M}_a}(\bar{z}) \cong C_K(a)/C_U(z) \cong Sp_4(2)/E_{32}$. As $O_2(C_{\bar{M}_a}(\bar{z})) \not\leq Z(C_{\bar{M}_a}(\bar{z}))$, $O_3(\bar{M}_a) \leq Z(\bar{M}_a)$ by Exercise 3.2 in [3T], while as $[z, O_2(M_a)] \leq U$, $O_2(\bar{M}_a) \leq Z(\bar{M}_a)$. Then by Theorem Q in section 14 of [3T], $\bar{M}_a \cong Sp_6(2)$.

To complete the proof we calculate the order of $\mathcal{O} = \Delta_2$, Δ_3 and Δ_4' via $|\mathcal{O}| = |M : C_M(a)|$, for $a \in \mathcal{O}$, and determine they are as indicated in the statement of the lemma. Then we calculate that

$$|\Delta_1| + |\Delta_2| + |\Delta_3| + |\Delta_4'| = 3,968,055 = |\Delta|$$

so $\Delta_4' = \Delta_4$ and the proof of the lemma is complete. Q.E.D.

(7.13) *Let* $\hat{H} = \mathrm{Cov}_2(H)$, $\rho : \hat{H} \to H$ *the universal covering,* $V = \ker(\rho)$, $\hat{Q} = O_2(\hat{H})$ *and* $P = [\hat{Q}, \hat{H}]$. *Let* H_+ *be a group with* $Q_+ \cong F^*(H_+) \cong Q$ *and* $H_+/Z(H_+) \cong \tilde{H}$. *Then*

(1) $\hat{H} = \hat{L}P$ *with* $P \cap \hat{L} = 1$, $\hat{L} \cong Cov_2(L_1)$ *and* $\rho(\hat{L}) = L_1$.

(2) $P \cong E_4 \times Q$, $Z(\hat{L}) \cong E_4$, $\hat{Q} = Z(\hat{L}) \times P$ *and* $Z(\hat{H}) = Z(\hat{L}) \times Z(P)$.

(3) $Z(\hat{L}) \leq V$ *and* $V = [\tau, Z(\hat{H})]$ *is a complement to* $\Phi(P)$ *for some automorphism* τ *of order* 3 *inducing an outer automorphism on* $\hat{L}$.

(4) $H_+ \cong H$ *if and only if* H_+ *possesses a complement* L_+ *to* Q_+ *such that* $E_+/\langle t_+ \rangle$ *splits over* $\langle z_+, t_+ \rangle / \langle t_+ \rangle$ *as a* J_+*-module, where* x_+ *is the image of* $x = z, t, E$ *under the isomorphism* $Q \cong Q_+$, *and* $J_+ = C_{L_+}(t_+)$.

(5) *If* $H_+ = C_{G_+}(z_+)$ *for some group* G_+ *of type* ${}^2E_6(2)$ *and* H_+ *splits over* Q_+ *then* $H_+ \cong H$.

Proof. By 6.2, $\tilde{Q} \otimes_{\mathbf{F}_2} \mathbf{F}_4 \cong \bigwedge^3(N)$ as a $\mathbf{F}_4 L_1$-module. Then by 5.8, $H^1(L_1, \tilde{Q}) \cong E_4$. By 23.7 in [3T], $\mathrm{Schur}_2(L_1) \cong E_4$. Therefore (1) and (2) follow from 3.2.

Let $D = C_{Aut(\hat{H})}(P/\Phi(P))$ and $\hat{H}D$ the semidirect product of $\hat{H}$ by D. By 3.2, V is a complement to $\Phi(P)$ in $Z(\hat{H})$ and $D/Inn(P) \cong H^1(L_1, \tilde{Q}) \cong E_4$ is regular on complements to $\Phi(P)$ in $Z(P)$. Indeed by 3.2.6, $H_+ \cong \hat{H}/V_+$ for some complement V_+ to $\Phi(P)$ in $Z(\hat{H})$.

As $\tilde{Q} \otimes_{\mathbf{F}_2} \mathbf{F}_4 \cong \bigwedge^3(N)$ and the representation of L_1 on $\bigwedge^3(N)$ extends to $PGU_6(2) = L_1\langle\tau\rangle$ for some τ of order 3, the representation of L_1 on $\tilde{Q}$ extends to $L_1\langle\tau\rangle$. Thus τ is an automorphism of $\hat{H}$ by 3.2.3, so as τ is faithful on $\mathrm{Schur}_2(L_1)$ and $H^1(L_1, \tilde{Q})$, τ is faithful on $Z(\hat{H})/Z(P)$ and $Z(P)/\Phi(P)$. As some outer automorphism of G of order 3 acts on Q and L_1 and induces an outer automorphism of L_1, we may take τ to act on $\hat{L}$, τ induces an outer automorphism on $\hat{L}$, and $V = [Z(\hat{H}), \tau]$ is the unique τ-invariant complement to $\Phi(P)$, so that (3) holds.

Notice that D is transitive on the complements to $\hat{Q}/Z(\hat{H})$ in $\hat{H}/Z(\hat{H})$.

Let $L_+ = \hat{L}V_+/V_+$ be the image of $\hat{L}$ in H_+. We next prove

(6) Under the hypothesis of (5), we can pick L_+ with $O_2(J_+) \leq Q_{t_+} = O_2(C_{G_+}(t_+))$.

To simplify notation we argue in G. Now J has three 9-dimensional irreducibles on $O_2(J)Q/E$: $C_Q(t)/E$, $(Q_t \cap H)/E$, and $(Q_{tz} \cap H)/E$, so as $O_2(J)E/E$ is one of these irreducibles, conjugating L_+ by an element of $Q - C_Q(t)$ if necessary, we may take $O_2(J)E = Q_t \cap H$, establishing (6). We also prove

(7) Under the hypothesis of (5), there is a complement I_+ to $O_2(J_+)$ in J_+ such that E_+ splits over $\langle z_+, t_+\rangle$ as an I_+-module.

First if $G_+ = G$ then $I = L_{12}$ works as L_{12} acts on the complement $C_E(L_{234})$ to $\langle z, t\rangle$ in E. Moreover $\tilde{Q}$ is a semisimple L_{12}-module and $L_{12} = N_{L_1}([\tilde{E}, L_{12}])$.

In the general case $\tilde{H}_+ \cong \tilde{H}$ (cf. 8.1) so the preimage I_+ in L_+ of the image of $\tilde{L}_{12}$ in $\tilde{H}_+$ under this isomorphism acts semisimply on $\tilde{Q}_+$ as L_{12} is semisimple on $\tilde{Q}$. In particular $C_{Q_+}(I_+) \cong D_8$. Similarly as the image F of $[E_+, I_+]$ in $\tilde{Q}_{t_+}$ is a simple I_+-module, and as $\tilde{H}_{t_+}$ is isomorphic to $\tilde{H}_t$, $I_+Q_{t_+} = N_{H_{t_+}}(F)$ and then $\tilde{Q}_{t_+}$ is a semisimple I_+-module and $C_{Q_{t_+}}(I_+) \cong D_8$. Therefore $\langle C_{Q_+}(I_+), C_{Q_{t_+}}(I_+)\rangle$ contains an element X_+ of order 3 such that $C_{E_+}(X_+)$ is an I_+-invariant complement to $\langle z_+, t_+\rangle$ in E_+, completing the proof of (7).

Observe next that

(8) L_+ is a complement to Q_+ in H_+ if and only if $Z(\hat{L}) \leq V_+$.

We also claim

(9) If L_+ is a complement to Q_+ then $V_+ = V$ if and only if the following splitting property holds: $E_+/\langle t_+\rangle$ splits over $E_+/\langle z_+, t_+\rangle$ as a J_+-module.

If $V_+ = V$ this follows from (6) and (7). Namely by (6), we may choose L_1 so that $O_2(J) \leq Q_t$, where $J = C_{L_1}(t)$. Therefore $O_2(J)$ centralizes $E/\langle t\rangle$ as $E \leq Q_t$. Further by (7), E splits over $\langle z, t\rangle$ as an I-module, so as $J = O_2(J)I$, we have the splitting property.

Notice this argument only depended upon the hypothesis of (5). Thus (9) will imply (5), since under the hypothesis of (5), as D is transitive on complements to $\hat{Q}/Z(\hat{Q})$, we may assume the complement to Q_+ is the image of $\hat{L}$. Thus, as we just observed, H_+ has the splitting property, so $H \cong H_+$ by (9). Similarly (8) and (9) imply (4), so it remains to assume the splitting property and show $V_+ = V$. Let $\hat{E} = \rho^{-1}(E) \cap P$ and $\hat{J} = \rho^{-1}(C_{L_1}(t))$. We show $Z(P) \leq [\hat{E}, \hat{J}]\Phi(P)$, so that as H_+ has the splitting property,

$$V_+ \cap Z(P) = [\hat{E}, \hat{J}] = V \cap Z(P)$$

and then

$$V_+ = Z(\hat{L}) + (V_+ \cap Z(P) = Z(\hat{L}) + (V \cap Z(P) = V$$

as desired.

Now $P/\Phi(P)$ is the largest module $M = [M, L_1]$ for L_1 such that $M/C_M(L_1) \cong \tilde{Q}$. Further $J = C_{L_1}(\tilde{t})$ and $\tilde{E}$ is the unique 10-dimensional L_1-submodule of $P/Z(P)$, so $Z(P) \leq [\hat{E}/\Phi(P), J]$ by 5.8.3, completing the proof of the lemma. Q.E.D.

(7.14) *Let $\check{G}$ be the extension of G by the graph-field automorphism σ of 7.10 and $\check{H} = C_{\check{G}}(z)$. Assume $\check{H}_1$ is a group with $F^*(\check{H}_1) = Q_1 \cong Q$ and with a subgroup H_1 of index 2 containing Q_1 such that $H_1/Z(H_1) \cong \tilde{H}$. Then $\check{H}/\langle z\rangle \cong \check{H}_1/Z(H_1)$.*

Proof. As $F^*(\check{H}_1) = Q_1$ and H_1 is of index 2 in $\check{H}_1$ with $H_1/Z(H_1) \cong \tilde{H}$, $F^*(\check{H}_1/Q_1) = H_1/Q_1 \cong H^* \cong U_6(2)$. Therefore as $Out(U_6(2)) \cong S_3$, $\check{H}_1/Q_1 \cong \check{H}/Q$. As $H_1/Z(H_1) \cong \tilde{H}$, the representation of H_1/Q_1 on $\tilde{Q}_1 = Q_1/Z(Q_1)$ is quasiequivalent to that of H^* on $\tilde{Q}$ by 3.1. By 6.1.7, H^* is absolutely irreducible on $\tilde{Q}$, so $N_{GL(\tilde{Q})}(H^*) \cong Aut(U_6(2))$, and hence as $\check{H}_1/Q_1 \cong \check{H}/Q$, the representation of $\check{H}_1/Q_1$ on $\tilde{Q}_1$ is quasiequivalent to that of $\check{H}/Q$ on $\tilde{Q}$, so 3.1 completes the proof of the lemma. Q.E.D.

(7.15) (1) *For $p \neq 2$ or 11, p prime, and $P \in Syl_p(G)$, $C_G(P) \leq P$ and if $p = 3$ then $N_G(P)$ is a $\{2,3\}$-group.*

(2) *If $Y \leq G$ is of order 11 then $C_G(Y) \cong \mathbf{Z}_{11} \times S_3$.*

(3) *If $Y \leq G$ is of order 7 then $C_G(Y) = Y \times E(C_G(Y))$ with $E(C_G(Y)) \cong L_3(2)$ or $L_3(4)$.*

(4) *If $Y \leq G$ is of order 5 then $C_G(Y) \cong \mathbf{Z}_5 \times A_5$.*

(5) *If Y is a 3-central subgroup of G of order 3 then $C_G(Y)$ is a $\{2,3\}$-group.*

(6) *If $S \in Syl_3(G)$ then $J(S) \cong E_{3^5}$ and $N_G(J(S))/J(S) \cong O_6^-(2)$.*

Proof. This is well known and follows from the Springer-Steinberg theory of semisimple elements of finite groups of Lie type. Q.E.D.

(7.16) *If $M \leq G$ is of odd order then $|M| < 10^5$.*

Proof. Let $F = F(M)$. As M is of odd order, M is solvable, so $C_M(F) \leq F$. (cf 31.10 in [FGT]) Let p be a prime divisor of $|F|$ and $P = O_p(M)$. If $p \neq 3$ or 11 and $P \in Syl_p(G)$, then by 7.15.1, $O^p(F) \leq C_G(P) \leq P$, so $P = F$. Thus $|M| \leq n_p|P|$, where n_p is the maximal order of a subgroup X of $GL(P/\Phi(P))$ of odd order with $O_p(X) = 1$. In each case $n_p|P| < 10^5$.

Further if $p = 11$ then $F \leq O^2(C_G(P)) \cong \mathbf{Z}_{33}$ by 7.15.2, so

$$|M| \leq |F| \cdot |O(Aut(\mathbf{Z}_{11}))| \leq 33 \cdot 5 < 10^5$$

Similar arguments work if P is of order 5 or 7, using 7.15.3 and 7.15.4.

Therefore we may assume $F = O_3(M)$. Now if $P \in Syl_3(FC_G(F))$ then by a Frattini argument, $M \leq N_G(F) = C_G(F)(N_G(P) \cap N_G(F)$, so as $C_M(F) \leq F$, $N_G(P) \cap N_G(F)$ contains a subgroup M_0 of odd order with $|M_0| \geq |M|$. Hence replacing M by M_0 if necessary, we may assume $P = F$. In particular taking $F \leq S \in Syl_3(G)$, $Z = Z(S) \leq F$. Let $U = \langle Z^M \rangle$, so that $Z \cong E_{3^n}$ for some n. Then $C_M(U) \leq C_M(Z)$, and $C_M(Z)$ is a 3-group by 7.15.5. Therefore $C_M(U) \leq O_3(M) = F$. Hence $|M| \leq |F|N_n$, where N_n is the maximal order of a subgroup X of odd order in $GL_n(3)$ with $O_3(X) = 1$.

By 7.15.6, $n \leq 5$, so $|M|_{3'}$ divides $5 \cdot 11 \cdot 13$. Indeed if 11 divides $|M|$ then $n = 5$, so $U = J(S)$ for $S \in Syl_3(G)$ by 7.15.6, whereas by the last remark in 7.15.6, 11 does not divide the order of $N_G(J(S))$. So 11 does not divide the order of M. Further by 7.15.4, G has no subgroup of order $13 \cdot 5$, so by Hall's Theorem, (cf. 18.5 in [FGT]) $|M|_{3'} = 1$, 5, or 13. But $|G|_3 = 3^9$ and $3^9 \cdot 5 < 10^5 > 3^8 \cdot 13$, so we are left with the case $|M| = 3^9 \cdot 13$.

By 7.15.1, if Y is of order 13 in M then $C_F(Y) = 1$ and $|N_M(Y)| = 1$ or 3. Therefore $|F| = 3^{3k}$ for some k and hence $F \in Syl_3(G)$, contradicting 7.15.1. Q.E.D.

§8. Groups of type ${}^2E_6(2)$ are isomorphic to ${}^2E_6(2)$

In this section we assume the hypotheses and notation of section 6. In particular G is of type ${}^2E_6(2)$, z is a 2-central involution in G, $H = C_G(z)$, etc. Further let $G_0 = {}^2E_6(2)$ and z_0 a long root involution of G_0. By 7.1, G_0 is of type ${}^2E_6(2)$ with z_0 2-central in G_0. Let $H_0 = C_{G_0}(z_0)$, $Q_0 = O_2(H_0)$, etc.

(8.1) $\tilde{H} \cong H_0/\langle z_0 \rangle$.

Proof. First $Q_0 \cong Q$, so we may identify the two groups. Further by 6.2, the representation of H_0^* on $\tilde{Q}_0$ is quasiequivalent to that of H^* on $\tilde{Q}$, so $\tilde{H} \cong \tilde{H}_0$ by 3.1. Q.E.D.

By 8.1, $\tilde{H}_0 \cong \tilde{H}$, so by 7.8 there is $h \in H - C_H(\tilde{t})$ with $t^h \in E$. Let $k = gh$, $V_3 = \langle z, t, z^k \rangle$, $U_3 = Q \cap Q^g \cap Q^k$, $X_3 = \langle Q, Q^g, Q^k \rangle$, $R_3 = C_{X_3}(V_3)$,

$$S_3 = (Q \cap Q^g)(Q \cap Q^k)(Q^g \cap Q^k),$$

and $P_3 = N_G(V_3)$. By 8.16 in [SG],

$$R_3 = C_Q(V_3)C_{Q^g}(V_3)C_{Q^k}(V_3) = O_2(X_3),$$

$X_3/R_3 = GL(V_3) \cong L_3(2)$, $[X_3, U_3] \leq V_3$, $\Phi(U_3) = 1$, $P_3 = X_3C_H(V_3)$, and $P_3/R_3 = X_3/R_3 \times C_H(V_3)/R_3$.

By 7.8, $C_H(V_3)/R_3 \cong A_5$, so $P_3/R_3 \cong L_3(2) \times A_5$. Again by 7.8, $m(U_3) = 6$, so by 8.16 in [SG], S_3/U_3 is the sum of 4 copies of the dual V_3^* of V_3 as an X_3/R_3-module, and R_3/S_3 is the sum of 4 copies of V_3 as an X_3/R_3-module. By 7.8, $C_H(V_3)$ has chief series $0 < \tilde{V} < \tilde{V}_3 < \tilde{U}_3 < \tilde{E}$ on $\tilde{E}$ with E/U_3 the $\Omega_4^-(2)$-module and U_3/V_3 the $L_2(4)$-module for $C_H(V_3)$. Finally by 7.8, $C_H(V_3)$ has four $L_2(4)$-sections and three $\Omega_4^-(2)$-sections on R_3. We summarize all this as:

(8.2) (1) *$P_3/R_3 = X_3/R_3 \times C_H(V_3)/R_3$ with $X_3/R_3 \cong L_3(2)$ and $C_H(V_3)/R_3 \cong A_5$.*

(2) *R_3 has chief series*

$$0 < V_3 < U_3 < S_3 < R_3$$

with V_3 the natural module for X_3/R_3, $[X_3, U_3] \leq V_3$ and U_3/V_3 is the $L_2(4)$-module for $C_H(V_3)/R_3$, S_3/U_3 is the tensor product of the dual of V_3 as an X_3/R_3-module with the $\Omega_4^-(2)$-module for $C_H(V_3)/R_3$, and R_3/S_3 is the tensor product of V_3 as an X_3/R_3-module with the $L_2(4)$-module for $C_H(V_3)/R_3$.

(8.3) *There exists $s \in z^G$ with sz of order 3, $C_G(\langle s, z\rangle) \cong U_6(2)$, and $N_G(\langle sz\rangle) = \langle s, z\rangle \times C_G(\langle s, z\rangle)$.*

Proof. Let $X_2 = \langle Q, Q^g\rangle$. Then $X_2 \leq X_3$ so there is x of order 3 in X_2 fused to $y \in X_3 \cap H$. Notice y^* is inverted by a transvection in H^* as $\tilde{H}_0 \cong \tilde{H}$ and the remark holds in H_0^* since y is inverted by some conjugate $c \in Q^g$ of z in H_0 and c^* is a transvection in H_0^* by 7.2 and 7.3.2. Therefore $C_Q(y) \cong D_8^4$ and $C_H(y)/C_Q(y)\langle y\rangle \cong U_4(2)$. Let $T_y \in Syl_2(C_H(y))$; then $\langle z\rangle = Z(T_y)$ and T_y is of order 2^{15}. As $\langle z\rangle = Z(T_y)$, $T_y \in Syl_2(C_G(y))$.

Next let $T_x \in Syl_2(C_{P_2}(x))$. From the structure of P_2 described in 6.1,

$$C_{P_2}(x)/\langle x\rangle \cong L_3(4)/E_{2^9}$$

with $O_2(C_{P_2}(x))$ quasiequivalent to the Todd module for $C_{P_2}(x)/O_2(C_{P_2}(x))\langle x\rangle$. In particular T_x is of order 2^{15} and hence as x and y are conjugate, the previous paragraph says that $T_x \in Syl_2(C_G(x))$ and $Z(T_x)$ is generated by a conjugate of z. Now the hypotheses of Theorem 30.1 in [3T] are satisfied, so by that Theorem, $C_G(x)/\langle x\rangle \cong C_G(y)/\langle y\rangle \cong U_6(2)$.

Next x is inverted by an involution $u \in Q$ with $[C_{P_2}(x), u] = \langle x\rangle$, so u induces an automorphism of $C_G(x)/\langle x\rangle \cong U_6(2)$ centralizing the parabolic $C_{P_2}(x)/\langle x\rangle$, and hence centralizing $C_G(x)/\langle x\rangle$. Therefore $N_G(\langle x\rangle) = \langle x, u\rangle \times E(C_G(x))$ with $E(C_G(x)) \cong U_6(2)$.

Finally $u \in Q$ centralizes a $L_3(4)$-section of H, so as $\tilde{H} \cong \tilde{H}_0$, 7.5 says that $u \in t^H \subseteq z^G$. Hence there exists $s \in z^G$ with $\langle s, z\rangle$ conjugate to $\langle u, x\rangle$, completing the proof. Q.E.D.

(8.4) $H \cong H_0$.

Proof. By 8.3 there is $s \in z^G$ with $C_G(\langle s, z\rangle)$ a complement to Q in H. Hence 7.13.5 completes the proof. Q.E.D.

By 8.4 there is an isomorphism $\alpha : H \to H_0$. Let $t_0 = t\alpha$, $t_0 = t^{g_0}$, $h_0 = h\alpha$ where $k = gh$, $V_3^0 = V_3\alpha$, and $P_3^0 = N_{G_0}(V_3^0)$.

(8.5) *There exist an isomorphism* $\zeta : P_3 \to P_3^0$ *such that* $\alpha = \zeta$ *on* $H \cap P_3$.

Proof. We appeal to 21.12 in [3T]. The P_3-chief series required in that lemma is:

$$1 < V_3 < U_3 < S_3 < R_3$$

and by 8.2, the image of this series under α is the corresponding series in R_3^0. Namely by definition, $V_3^0 = V_3\alpha$. Also as $t_0 = t\alpha$, $V_0 = V\alpha$ and then as $E/V = C_{Q/V}(O_2(C_H(\tilde{V})))$,

$$(Q \cap Q^g)\alpha = E\alpha = E_0 = Q_0 \cap Q_0^{g_0}.$$

Therefore $U_3\alpha = (E \cap E^h)\alpha = E_0 \cap E_0^{h_0} = U_3^0$.

Next $(Q \cap H^g)/E$, $(Q^g \cap H)/E$, and $(Q^{gu} \cap H)/E$, $u \in Q - C_Q(t)$, are the three $C_H(\tilde{t})$-invariant subspaces of $O_2(C_H(\tilde{t}))/E$, with $Q^g \cap H$ distinguished by $\Phi(Q^g \cap H) = \langle t\rangle$, so $(Q^g \cap H)\alpha = Q_0^{g_0} \cap H_0$. Then

$$(Q^g \cap Q^{gh})\alpha = Q_0^{g_0} \cap H_0 \cap Q_0^{g_0h_0} \cap H_0 = Q_0^{g_0} \cap Q_0^{g_0h_0},$$

so

$$S_3\alpha = (Q \cap Q^g)((Q \cap Q^{gh})(Q^g \cap Q^{gh})\alpha = S_3^0.$$

Finally $R_3 = O_2(C_H(V_3))$, so $R_3\alpha = R_3^0$.

Next 8.2 says that hypotheses (2), (3), (5) and (6) of 21.12 in [3T] are satisfied. To check hypothesis (4) of that lemma, use Remark 21.9 and Lemma 21.13 of [3T]. Now 21.12 in [3T] supplies the extension $\zeta : P_3 \to P_3^0$ of $\alpha : P_3 \cap H \to P_3^0 \cap H_0$. Q.E.D.

(8.6) $G = \langle H, P_3 \rangle$.

Proof. Let $K = \langle H, P_3 \rangle$ and assume that $K \neq G$. Then by induction on the order of G, $K \cong {}^2E_6(2)$. By 7.7, K has 3 classes of involutions with representatives j_i, $1 \leq i \leq 3$, while by 7.5, each class is fused into Q under K. By 4.7.2,

$$z^G \cap Q = \{z\} \cup t^H = z^K \cap Q,$$

so $z^G \cap K = z^K$. Hence as also $C_G(z) = H \leq K$, 7.3 in [SG] says K is the unique point of G/K fixed by z. We show K is strongly embedded in G; then 7.6 in [SG] contradicts the fact that K has more than one class of involutions.

To show K is strongly embedded in G it remains to show $C_G(j) \leq K$ for each involution $j \in K$. So assume $Y = C_G(j) \not\leq K$ for some involution $j \in K$ and let $Y^* = Y/\langle j \rangle$. We have seen $j \neq j_1 = z$. If $j = j_2$, then from 7.5, we may take $j \in Z_4 = Z(P_4)$ with $R_4 \leq C_K(j) \leq P_4$ and $C_K(j)/R_4 \cong Sp_6(2)$. By 7.4 in [SG], $C_K(j)$ controls 2-fusion in $C_K(j)$, so Z_4^* is a strongly closed abelian subgroup of $C_K(j)^*$ in Y^*. From 7.5, Z_4 has the structure of an 8-dimensional orthogonal space over $\mathbf{F}_2$ with $z^G \cap Z_4$ the singular points and $j^G \cap Z_4$ the nonsingular points. The subspace U_4 of this orthogonal space orthogonal to j is $C_K(j)$ invariant.

Pick $u \in Y - K$ to be fused to an element of $z^G \cap Z_4 - U_4$ under Y. As $C_K(j)$ controls 2-fusion in $C_K(j)$, z^* and u^* are not conjugate in Y^*, so z^*u^* has even order. Let i^* be the involution in $\langle z^*u^* \rangle$. Then $i^* \in C_{Y^*}(z^*) \leq C_K(j)^*$ and z^*i^* is fused to z^* or u^*, and hence is in Z_4^*, so $i^* \in Z_4^*$. Then as $C_{Y^*}(i^*) \not\leq C_K(j)^*$, it follows that $\langle i, j \rangle = J$ contains no conjugate of z, so J is a definite line in Z_4. Then $R_4 \leq C_K(J) \leq P_4$ with $C_K(J)/R_4 \cong \Omega_6^+(2)$ and $X = C_G(J) \not\leq K$.

Let $X' = X/J$. Again $C_K(J)'$ controls 2-fusion in $C_K(J)'$, so Z_4' is a strongly closed abelian subgroup of $C_K(J)'$ in X'. This time there are two X'-classes of involutions z' and v' in Z_4' corresponding to the singular and nonsingular points of the orthogonal space Z_4'. As both zJ and vJ contain a member of z^G, both z' and v' fix a unique point of $X'/C_K(J)'$. But now the argument of the previous paragraph applied to $u \in X - K$ fused under Y to v supplies a contradiction.

So $C_G(j_2) \leq K$ and $j = j_3$. By 7.5 we may take $j \in E$ and $C_K(j) \leq P_2$. Then V^* and E^* are strongly closed abelian subgroups of $C_K(j)^*$ and we argue as above on $u \in Y - K$ fused under Y to a conjugate of z in $E - V$ to obtain a contradiction and complete the proof. Q.E.D.

Theorem 8.7. *Each group of type* ${}^2E_6(2)$ *is isomorphic to* ${}^2E_6(2)$.

Proof. We must show G is isomorphic to G_0. We use the machinery of Section 37 of [SG] to do so. In particular we construct uniqueness systems $\mathcal{U}$ and $\mathcal{U}_0$ for G and G_0.

Let Δ be the graph with vertex set z^G and $\Delta(z) = t^H$. Then G is an edge and vertex transitive group of automorphisms. Define Δ_0 for G_0 similarly. By 7.9, Δ_0 is simply connected.

Let θ be the complete graph with vertex set z^{P_3}. Then θ is a subgraph of Δ and P_3 is vertex and edge transitive on θ. Define θ_0 for G_0 similarly. As $C_H(t)$ is transitive on $t^H \cap E - V$, G has two orbits on triangles of Δ, so each triangle in Δ is fused under G_0 into θ.

Let $\mathcal{U} = (G, \Delta, P_3, \theta)$ and $\mathcal{U}_0 = (G_0, P_3^0, \Delta_0, \theta_0)$. As G_0 is simple, Δ_0 is simply connected, and each triangle in Δ_0 is fused into θ_0, so to show $G \cong G_0$ it suffices by Exercise 13.1 in [SG] to show that $\mathcal{U}$ and $\mathcal{U}_0$ are equivalent uniqueness systems.

It is trivial that $\mathcal{U}$ and $\mathcal{U}_0$ are uniqueness systems, given 8.6. The maps α, ζ define a similarity of $\mathcal{U}$ and $\mathcal{U}_0$ in the sense of section 37 of [SG]. To complete the proof we appeal to Exercise 13.3.3 in [SG]. For this we need geometries Γ and Γ_0 for G and G_0 respectively. Define $\Gamma = \Gamma(G, \mathcal{F})$ to be the coset geometry of $\mathcal{F} = (H, P_2, P_3)$ and define Γ_0 similarly. Hypothesis (Γ0) of section 38 of [SG] can be seen to be satisfied by Γ and Γ_0 by checking the conditions at the top of page 205 of [SG]. Observe Γ is isomorphic to the geometry with point set z^G, line set V^G, and plane set V_3^G, with incidence defined by inclusion. A similar remark holds for Γ_0. Thus Δ and Δ_0 are isomorphic to the collinearity graphs of Γ and Γ_0, respectively, via the map $z^x \mapsto Hx$. Using these isomorphisms, Hypotheses (Γi), $1 \leq i \leq 5$, of section 38 of [SG] are easy to check as are the remaining conditions of Exercise 13.3.3 of [SG].

Q.E.D.

§9. Groups of type $\mathbf{Z}_2/{}^2E_6(2)$

Define a group $\hat{G}$ to be of *type* $\mathbf{Z}_2/{}^2E_6(2)$ if $\hat{G}$ possesses an involution z such that $\hat{H} = C_{\hat{G}}(z)$ satisfies $Q = F^*(\hat{H}) \cong 2^{1+20}$ and $\hat{H}$ has a subgroup H of index 2 with $H/Q \cong U_6(2)$, and z is not weakly closed in Q with respect to $\hat{G}$.

Throughout this section assume $\hat{G}$ is of type $\mathbf{Z}_2/{}^2E_6(2)$ and let z be an involution in $\hat{G}$ such that $\hat{H} = C_{\hat{G}}(z)$ and $Q = F^*(\hat{H})$ satisfy our hypotheses. We will show that $\hat{G}$ has a subgroup G of index 2 such that $H = C_G(z)$. Hence G is of type ${}^2E_6(2)$ and hence by Theorem 8.7:

Theorem 9.1. *If $\hat{G}$ is of type $\mathbf{Z}_2/{}^2E_6(2)$ then $F^*(\hat{G})$ is of index*

2 in $\hat{G}$ and isomorphic to $^2E_6(2)$.

Much of the initial analysis is the same as that for groups of type $^2E_6(2)$, so rather than repeat all details we only indicate where more needs to be said. Adopt the notation of section 6. In particular let $t = z^g \in Q - \{z\}$ and $E = Q \cap Q^g$. We observe first that

(9.2) (1) *$\hat{H}/\hat{Q}$ is the extension of $H^* \cong U_6(2)$ by an involutory outer automorphism τ.*

(2) *Lemma* 6.1 *holds in $\hat{G}$ with $N_{\hat{H}}(R^*)$ the split extension of $R^* \cong E_{2^9}$ by $L_3(4)$ extended by a field automorphism. This time $\hat{P}_2 = N_{\hat{G}}(V) = XC_{\hat{H}}(V)$ with*

$$R = O_2(N_{\hat{G}}(V)) = C_X(V),$$

$\hat{P}_2/R = X/R \times C_{\hat{G}}(V)/R$, $X/R \cong S_3$, and $C_{\hat{G}}(V)/R$ the extension of $L_3(4)$ by a field automorphism.

Proof. As $F^*(\hat{H}) = Q$ and H is of index 2 in $\hat{H}$, $F^*(\hat{H}/Q) = H^* \cong U_6(2)$ and hence (1) holds. The proof of Lemma 6.1 then goes through virtually unchanged once we observe that if $R \leq \hat{T} \in Syl_2(\hat{H})$ and $T = \hat{T} \cap H$, then $J(\hat{T}/Q) = J(T^*) \cong E_{2^9}$. This follows from the fact that $N_{H^*}(J(T^*))$ is the parabolic described in 6.1.2 and $N_{\hat{H}/Q}(J(T^*))$ is the split extension of $J(T^*)$ by $L_3(4)$ extended by a field automorphism τ. Then as $m(J(T^*)/C_{J(T^*)}(\tau)) = 3$ while $C_{J(T^*)}(\tau)$ is not centralized by a complement $L_3(2)$ in $N_{H^*}(J(T^*)) \cap C_{H^*}(\tau)$, we conclude $J(T^*) = J(\hat{T})$ as claimed. Q.E.D.

Now with the analogue of 6.1 established, Lemma 6.2 also holds in $\hat{G}$ since its proof goes through verbatim. Similarly the analogue of Lemma 8.1 holds. Indeed if we let $\hat{G}_0$ be the extension of $G_0 = {}^2E_6(2)$ by the graph-field automorphism σ of Lemma 7.10, then $\hat{G}_0$ is of type $\mathbf{Z}_2/{}^2E_6(2)$ with $\hat{H}_0 = H_0\langle\sigma\rangle$. By 8.1, $\tilde{H}_0 \cong \tilde{H}$, and hence by 7.14, we have an isomorphism $\varphi : \hat{H}_0/\langle z_0\rangle \to \hat{H}/\langle z\rangle$. Let $\tilde{L}_0$ be then image in $\tilde{H}_0$ of a σ-invariant Levi factor of H_0 and $\tilde{L} = \varphi(\tilde{L}_0)$. Finally let $u \in \hat{H}$ with $\tilde{u} = \varphi(\sigma)$. Then by 7.10:

(9.3) (1) *$C_H(u)/C_Q(u) \cong Sp_6(2)$, $C_Q(u) = D_1D_2$ where $D_1 \cap D_2 = \langle z\rangle$, $\tilde{D}_1$ is the natural module for $C_H(u)/C_Q(u)$, and $C_Q(u)/D_1$ is the spin module.*

(9.4) *u is an involution.*

Proof. As $\tilde u$ is an involution, $u^2 = 1$ or z, so it remains to show $u^2 \neq z$. To see this we consider the local subgroup $\hat P_2$ of 9.2. Let $\bar P_2 = \hat P_2/V$. The isomorphism φ induces an isomorphism $\varphi : N_{\hat H_0}(V_0)/V_0 \to N_{\hat H}(V)/V$ which extends to an isomorphism $\psi : \bar P_{2,0} = P_{2,0}/V_0 \to \bar P_2$ by 21.12 in [3T] and 9.2. Hence by 7.10, $\bar u$ centralizes a subgroup $\bar I \cong S_3$ faithful on V. Then $I \cong S_4$ and $\langle u\rangle V \trianglelefteq I\langle u\rangle$, so it follows that $u^2 \neq z$, and hence indeed u is an involution. Q.E.D.

(9.5) (1) *All involutions in H are fused under $\hat G$ into Q.*

Proof. Let $j \in H$ be an involution. We wish to show $j^{\hat G} \cap Q \neq \varnothing$, so we may assume $j^* \neq 1$. Then by 7.7 and as $\varphi : \tilde H_0 \to \tilde H$ is an isomorphism, we may take $j^* \in R^*$ and j^* of type j_1, j_2 or j_3. Then by 7.4, $m([j, \tilde Q]) = 6, 8, 10$ in the respective case. Further by 7.4.2, if j^* is of type j_3 then Q is transitive on the involutions in jQ, so as $Q^g \cap H$ contains an involution in jQ, each involution j with j^* of type j_3 is fused into Q under $\hat G$.

In the remaining cases if $i \in jQ$ is an involution then $i = jx$ for some $\tilde x \in C_{\tilde Q}(j)$ and if $\tilde x \in [j, \tilde Q]$ then i is fused to j or jz under Q. From the proof of 7.4 and recalling that $\tilde H \cong \tilde H_0$, $\tilde L$ contains a subgroup $\tilde M = \tilde M_1 \times \tilde M_2$ with $\tilde M_1 \cong S_3$, $\tilde M_2 \cong U_4(2)$, and $\tilde Q = (\tilde Q_1 \oplus \tilde Q_2)\perp\tilde Q_3$ corresponding to the decomposition described in the proof of 7.4.

Suppose j^* is of type j_1. Then as we saw during the proof of 7.4, we may choose $\tilde j \in \tilde M_1$, so that $\tilde M_2 \leq C_{\tilde L}(j)$, $\tilde Q_1 = [\tilde Q, j]$, $C_{\tilde Q}(j) = \tilde Q_1 \oplus \tilde Q_3$, and $C_{\tilde Q}(j) = [C_{\tilde Q}(j), M_2]$. Then as $C_{\tilde L}(j) = O^2(C_{\tilde L}(j))$, also $C_{\tilde H}(j) = O^2(C_{\tilde H}(j))$, and hence $C_{\tilde H}(j) = C_H(j)/\langle z\rangle$. Thus if jx is an involution then x is an involution, so as $\tilde M_2$ is transitive on singular vectors of $\tilde Q_3$, each involution in jQ is conjugate under $C_H(j)$ to j, jz, jx, or jxz, for some fixed $\tilde x \in \tilde Q_3$ singular. Then as we may choose $x \in E$ and $j \in Q^g \cap H$, each involution $j \in H$ with j^* of type j_1 is fused into Q under $\hat G$.

Finally the case j^* of type j_2 is quite similar. Namely from the proof of 7.4, we may take $\tilde j \in \tilde M_2$ and $C_{\tilde Q}(j) = [\tilde Q, j] \oplus \tilde Q_4$ with $\tilde Q_4 \leq \tilde Q_1 \oplus \tilde Q_2$ a nondegenerate 4-dimensional space of sign $+1$ and a Sylow 3-subgroup of $C_L(j)$ is transitive on the singular vectors of $\tilde Q_4$ and one such is contained in E. So we can repeat the argument of the previous paragraph.

Q.E.D.

(9.6) $u^{\hat G} \cap H = \varnothing$.

Proof. Assume otherwise. Then by 9.5, $u^{\hat{G}} \cap Q \neq \varnothing$. Suppose first that $u = z^y$ for some $y \in \hat{G}$. Then as H^* has no $Sp_6(2)$-sections in parabolics, $z \in C_Q(u) = [C_Q(u), C_H(u)] \leq Q^y$, so $u \in Q$, a contradiction.

Therefore $u \notin z^{\hat{G}}$. Let $S \in Syl_2(C_{\hat{H}}(u))$ and $S \leq T_1 \in Syl_2(C_{\hat{G}}(u))$. By 4.3, $Z(T_1) = \langle z^y, u\rangle$ with $u \in Q^y$. Then $Z(T_1) \leq C_{T_1}(z) \leq S$, so $Z(T_1) \leq Z(S) = \langle z, a, u\rangle \cong E_8$ with $\langle z, a\rangle \leq Q$ by 7.10.4. In particular $1 \neq Z(T_1) \cap \langle z, a\rangle$.

Suppose $z^y \in Q$. Then $u \in Q^y \cap \hat{H} \leq H$, a contradiction. Therefore $uz^y \in Q$. Next $uz^y \in u^{Q^y}$ and $u^{\hat{G}} \neq z^{\hat{G}}$, so $uz^y \neq z$. Now $\tilde{a} \in [\tilde{Q}, u]$, so ua or $uaz \in u^Q$, and without loss $ua \in u^Q$. Thus $ua \neq z^y$, so $uz^y \neq a$. This leaves $uz^y = az$, so $z^y = uaz \in (uz)^Q$. Thus $uz \in z^{\hat{G}}$, so we have a contradiction by symmetry between u and uz. Q.E.D.

We are now in a position to complete the proof of Theorem 9.1. By 9.6 and a standard transfer argument such as 37.4 in [FGT], $\hat{G}$ has a subgroup G of index 2 with $u \notin G$. Then as H is the unique subgroup of $\hat{H}$ of index 2, $H = G \cap \hat{H}$. Therefore G is of type ${}^2E_6(2)$, so Theorem 8.7 completes the proof of Theorem 9.1.

References

[A] M. Aschbacher, On the maximal subgroups of the finite classical groups, Invent. Math., **76** (1984), 469–514.

[FGT] M. Aschbacher, “Finite Group Theory”, Cambridge University Press, Cambridge, 1986.

[SG] M. Aschbacher, “Sporadic Groups”, Cambridge University Press, Cambridge, 1994.

[3T] M. Aschbacher, “3-Transposition Groups”, Cambridge University Press, Cambridge, 1997.

[ASe] M. Aschbacher and G. Seitz, Involutions in Chevalley groups over fields of even order, Nagoya Math. J., **63** (1976), 1–91.

[CKS] C. Curtis, W. Kantor and G. Seitz, The 2-transitive permutation representations of the finite Chevalley groups, Trans. Amer. Math. Sci., **218** (1976), 1–59.

[S] M. Suzuki, Finite groups in which the centralizer of any element of order 2 is 2-closed, Ann. Math., **82** (1965), 191–212.

California Institute of Technology
Pasadena, CA 91125
U.S.A.

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 245–254

Some Results on Modular Forms — Subgroups of the Modular Group Whose Ring of Modular Forms is a Polynomial Ring

Eiichi Bannai, Masao Koike, Akihiro Munemasa and Jiro Sekiguchi

§1. Introduction

This paper is the first of the sequel of papers on the joint work of these authors on modular forms. We consider the problem of determining finite index subgroups of the modular group $\mathrm{SL}(2,\mathbb{Z})$ whose ring of modular forms is isomorphic to a polynomial ring. First, in this paper, we consider this question for modular forms of integral weights. In subsequent papers, we will consider the problem for modular forms of half-integral weights, and more generally, of $1/l$-integral weights. It turns out that the case of $l = 5$ is particularly interesting in connection with the classical work of F. Klein [9], as well as its analogy with the other two cases of $l = 1$ and $l = 2$, which are related to ternary and binary self-dual codes, respectively. In this first paper, we explain our overall motivation, and we prove the results only for the integral weight case. We remark that some preliminary announcements of some of the results given in the present paper have been made in two unofficial publications [2] and [17] written in Japanese.

§2. Statement of Results

Let $\Gamma$ be a finite index subgroup of $\mathrm{SL}(2,\mathbb{Z})$. We denote by $\mathfrak{M}(\Gamma)$ the ring of modular forms of integral weights on the group $\Gamma$. It is well known that

$$\mathfrak{M}(\mathrm{SL}(2,\mathbb{Z})) = \mathbb{C}[E_4, E_6], \tag{1}$$

Received October 26, 1999.
Revised September 4, 2000.

where E_4 and E_6 are the Eisenstein series of weights 4 and 6, respectively. Since E_4 and E_6 are algebraically independent, $\mathfrak{M}(\mathrm{SL}(2,\mathbb{Z}))$ is isomorphic to the polynomial ring in two variables. There are proper subgroups Γ of $\mathrm{SL}(2,\mathbb{Z})$ whose rings of modular forms of integral weights are isomorphic to polynomial rings. Note that, if a subgroup Γ has this property, then its ring of modular forms of integral weights is isomorphic to the polynomial ring in two variables. It is the purpose of the present paper to give a classification of such subgroups up to conjugacy in $\mathrm{SL}(2,\mathbb{Z})$.

Theorem 1. *Let $\mathfrak{M}(\Gamma)$ be the ring of modular forms on a finite index subgroup Γ of the modular group $\mathrm{SL}(2,\mathbb{Z})$. Suppose that $\mathfrak{M}(\Gamma) = \mathbb{C}[\phi_1,\phi_2]$ where ϕ_1 and ϕ_2 are algebraically independent modular forms of integral weights. Then Γ is conjugate in $\mathrm{SL}(2,\mathbb{Z})$ to one of the seventeen subgroups listed in Table 1.*

	wt	μ	ν_2	ν_3	$u+v$	index		Γ	No.
					$=\nu_\infty$	Γ	$C(\Gamma)$		
(a)	4,6	1	1	1	1	1	1	$\mathrm{SL}(2,\mathbb{Z})$	1
(b)	2,4	3	1	0	2	3	6	$\Gamma_0(2)$	2
(c)	2,2	6	0	0	3	6	6	$\Gamma(2)$	3
							24	$\Gamma_0(4)$	4
(d)	1,3	4	0	1	2+0	8	24	$\Gamma_1(3)$	5
(e)	1,2	6	0	0	2+1	12	48	$\sigma_0^{-1}\Gamma_1(4)\sigma_0$	6
							48	$\sigma_0^{-1}\sigma_1^{-1}\Gamma_1(4)\sigma_1\sigma_0$	7
							48	$\sigma_0^{-1}\sigma_2^{-1}\Gamma_1(4)\sigma_2\sigma_0$	8
							48	$\Gamma_1(4)$	9
							48	$\sigma_1^{-1}\Gamma_1(4)\sigma_1$	10
							192	$\sigma_2^{-1}\Gamma_1(4)\sigma_2$	11
(f)	1,1	12	0	0	4+0	24	24	$\Gamma(3)$	12
							48	$\Gamma_1(4)\cap\Gamma(2)$	13
							120	$\Gamma_1(5)$	14
							144	$\Gamma_1(6)$	15
							192	$\Gamma_0(8)\cap\Gamma_1(4)$	16
							648	$\Gamma_0(9)\cap\Gamma_1(3)$	17

Table 1. List of Subgroups

In Table 1, The column labeled as "wt" gives the weights of the modular forms ϕ_1,ϕ_2 in Theorem 1. The parameters $\mu,\nu_2,\nu_3,\nu_\infty,u,v$ will be defined in Section 3. The intersection of all conjugates of Γ in

$\mathrm{SL}(2,\mathbb{Z})$ is denoted by $C(\Gamma)$, so that the index in $\mathrm{SL}(2,\mathbb{Z})$ of $C(\Gamma)$ is the order of the permutation group induced by the action of $\mathrm{SL}(2,\mathbb{Z})$ on $\mathrm{SL}(2,\mathbb{Z})/\Gamma$. The columns labeled as "index" give the indices of Γ and $C(\Gamma)$ in $\mathrm{SL}(2,\mathbb{Z})$. The elements $\sigma_0, \sigma_1, \sigma_2$ appearing in case (e) will be defined in Section 4, where we give a proof of Theorem 1. In Section 5, we show that for each of the seventeen subgroups Γ, the ring of modular forms of integral weights on Γ is indeed the polynomial ring in two modular forms.

§3. Preliminaries

We assume that the reader is familiar with basic concepts of modular forms of integral weights on finite index subgroups of $\mathrm{SL}(2,\mathbb{Z})$, as they are available in [13] and [16]. For $\Gamma \subset \mathrm{SL}(2,\mathbb{Z})$, let us set $\overline{\Gamma} = \Gamma \cdot \{\pm 1\}/\{\pm 1\} \subset \mathrm{PSL}(2,\mathbb{Z})$. The following parameters of a finite index subgroup Γ of $\mathrm{SL}(2,\mathbb{Z})$ are commonly used:

$$\begin{aligned}
\mu &= |\,\mathrm{PSL}(2,\mathbb{Z}) : \overline{\Gamma}|,\\
\nu_2 &= \text{ the number of inequivalent elliptic points of order 2},\\
\nu_3 &= \text{ the number of inequivalent elliptic points of order 3},\\
\nu_\infty &= \text{ the number of inequivalent cusps},\\
g &= \text{ the genus of } \Gamma\\
&= 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}.
\end{aligned}$$

Furthermore, if $-1 \notin \Gamma$, then we distinguish two types of cusps, called regular and irregular. Namely, suppose that x is a cusp of Γ, $\sigma(x) = \infty$, $\sigma \in \mathrm{SL}(2,\mathbb{Z})$. Then we have $\sigma \Gamma_x \sigma^{-1} = \langle \psi^h \rangle$ or $\langle -\psi^h \rangle$ for some positive integer h, where

$$\psi = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

In the former case the cusp x is called regular, otherwise it is called irregular. Let us denote by u (resp. v) the number of inequivalent regular (resp. irregular) cusps. Then, obviously $\nu_\infty = u + v$ holds. Let $\mathfrak{M}_k(\Gamma)$ denote the space of modular form of weight k on Γ. Then $\dim \mathfrak{M}_k(\Gamma)$ $(k \geq 2)$ can be calculated by using just the above parameters. Namely, we have

$$\dim \mathfrak{M}_2(\Gamma) = \begin{cases} g + \nu_\infty - 1 & \text{if } \nu_\infty > 0, \\ g & \text{if } \nu_\infty = 0, \end{cases}$$

and

$$\dim \mathfrak{M}_k(\Gamma) = (k-1)(g-1) + \nu_2[\frac{k}{4}] + \nu_3[\frac{k}{3}] + \frac{k}{2}\nu_\infty,$$

if k is even and $k \geq 4$,

$$\dim \mathfrak{M}_k(\Gamma) = (k-1)(g-1) + \nu_2[\frac{k}{4}] + \nu_3[\frac{k}{3}] + \frac{k}{2}u + \frac{k-1}{2}v,$$

if k is odd, $k \geq 3$, and $-1 \notin \Gamma$. If $-1 \in \Gamma$, then $\mathfrak{M}_k(\Gamma) = 0$ for odd k. Note that the formula for $\dim \mathfrak{M}_1(\Gamma)$ is not known in general.

To conclude this section, we explain the notation used to describe the subgroups in Table 1. Recall the standard notation for certain subgroups of $\mathrm{SL}(2,\mathbb{Z})$:

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \;\middle|\; \begin{matrix} b \equiv c \equiv 0 \pmod{N} \\ a \equiv d \equiv 1 \pmod{N} \end{matrix} \right\},$$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{N} \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \;\middle|\; \begin{matrix} c \equiv 0 \pmod{N} \\ a \equiv d \equiv 1 \pmod{N} \end{matrix} \right\},$$

The groups No. 6–11 are pairwise conjugate in $\mathrm{GL}(2,\mathbb{Q})$. The elements $\sigma_0, \sigma_1, \sigma_2$ are defined by

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \; \sigma_1 = \sigma_0 \psi \phi \sigma_0^{-1}, \; \sigma_2 = \sigma_0 \psi \sigma_0^{-1}, \text{ where } \phi = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

The group No. 16 is conjugate in $\mathrm{GL}(2,\mathbb{Q})$ to the group No. 13:

$$\Gamma_0(8) \cap \Gamma_1(4) = \sigma_0 \left(\Gamma_1(4) \cap \Gamma(2)\right) \sigma_0^{-1}. \tag{2}$$

Also, the group No. 17 is conjugate in $\mathrm{GL}(2,\mathbb{Q})$ to the group No. 12:

$$\Gamma_0(9) \cap \Gamma_1(3) = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} \Gamma(3) \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}^{-1}. \tag{3}$$

§4. Proof of Theorem 1

Suppose that $\mathfrak{M}(\Gamma) = \mathbb{C}[\phi_1, \phi_2]$, where ϕ_1, ϕ_2 are algebraically independent modular forms of weight a_1, a_2, respectively, on Γ. Then we have, as formal power series,

$$\Phi(\Gamma) := \sum_{k=0}^{\infty} \dim \mathfrak{M}_k(\Gamma) \cdot t^k = \frac{1}{(1-t^{a_1})(1-t^{a_2})}. \tag{4}$$

Without loss of generality we may assume $a_1 \leq a_2$. Since $\mathfrak{M}(\Gamma) \supset \mathfrak{M}(\mathrm{SL}(2,\mathbb{Z}))$, (1) implies $a_1 \leq 4$ and $a_2 \leq 6$.

First consider the case where $-1 \notin \Gamma$. For fixed a_1, a_2, comparing the coefficients in (4), we obtain a system of linear equations with unknowns g, ν_2, ν_3, u, v. Taking the conditions $\mu > 0$, $\nu_2 \geq 0$, $\nu_3 \geq 0$ into account, the list of solutions consists of the cases (d)–(f) in Table 1 and the case

$$\text{(g)} \qquad (a_1, a_2, g, \mu, \nu_2, \nu_3, u, v) = (1, 4, 0, 3, 1, 0, 2, 0).$$

In order to classify subgroups Γ of $\mathrm{SL}(2, \mathbb{Z})$ of given parameters, we use a modification of the technique used in Millington [12]. If we put $\lambda = \phi^{-1}\psi$, then $\mathrm{SL}(2, \mathbb{Z})$ has a presentation $\langle \phi, \lambda \mid \phi^4 = \lambda^3 = 1,\ [\lambda, \phi^2] = 1\rangle$. Let Γ be a finite index subgroup of $\mathrm{SL}(2, \mathbb{Z})$, $X = \mathrm{SL}(2, \mathbb{Z})/\Gamma$, $\overline{X} = \mathrm{SL}(2, \mathbb{Z})/\langle \Gamma, -1\rangle$. Then $\mathrm{SL}(2, \mathbb{Z})$ acts on X, $\overline{X}$, and we have $|\overline{X}| = \mu$.

Lemma 2. *ϕ fixes ν_2 elements of $\overline{X}$, λ fixes ν_3 elements of $\overline{X}$, and ψ has ν_∞ cycles on $\overline{X}$. If $-1 \notin \Gamma$, then a cusp x is regular if and only if $\langle \psi \rangle$ has two orbits on $\langle \psi, -1\rangle \sigma\Gamma/\Gamma$, where $\sigma(x) = \infty$, $\sigma \in \mathrm{SL}(2, \mathbb{Z})$. In particular, ψ has $2u + v$ cycles on X.*

Proof. The statement on the action on $\overline{X}$ has been proved in [12]. As for the regularity of a cusp x, it suffices to prove that x is irregular if and only if $\langle \psi \rangle$ acts transitively on $\langle \psi, -1\rangle\sigma\Gamma/\Gamma$. The latter condition is equivalent to the existence of a positive integer h satisfying $\psi^h \sigma\Gamma = -\sigma\Gamma$. This implies $-\psi^h \in \sigma\Gamma_x\sigma^{-1}$, hence the cusp x is irregular. The proof of the converse is similar. Q.E.D.

We now describe how to obtain the list of subgroups in the cases (d)–(f), and how to prove the nonexistence of a subgroup in the case (g). First, we enumerate all subgroups $\overline{\Gamma}$ of index μ in $\mathrm{PSL}(2, \mathbb{Z})$. This can be done by GAP [6], using the command `LowIndexSubgroupsFpGroup`, if one defines $\mathrm{PSL}(2, \mathbb{Z})$ as $\langle \overline{\phi}, \overline{\lambda} \mid \overline{\phi}^2 = \overline{\lambda}^3 = 1\rangle$. Since $\overline{X}$ can be identified naturally with $\mathrm{PSL}(2, \mathbb{Z})/\overline{\Gamma}$, the parameters ν_2, ν_3 and ν_∞ make sense for $\overline{\Gamma}$. Thus we can extract only those subgroups $\overline{\Gamma}$ of index μ having the parameters ν_2, ν_3, ν_∞ as prescribed in the cases (d)–(g).

The next step is to find subgroups Γ of index 2μ in $\mathrm{SL}(2, \mathbb{Z})$ whose images are one of the $\overline{\Gamma}$ found in the previous step. We need to check whether Γ satisfies the condition on the parameters u, v described in Lemma 2. This step can also be done easily by GAP, and we obtain the subgroups No. 5–17. We remark that the six subgroups in the case (f) appeared in [3].

Next consider the case where $-1 \in \Gamma$. The method is similar to the previous case, and the computation is far simpler. Comparing the coefficients in (4), we see that the list of possible parameters is as described in the cases (a)–(c) in Table 1. Then we enumerate all subgroups $\overline{\Gamma}$ of index μ in $\mathrm{PSL}(2,\mathbb{Z})$ having the parameters as in (a)–(c). The subgroup Γ is the full inverse image of $\overline{\Gamma}$ in $\mathrm{SL}(2,\mathbb{Z})$.

§5. Generators of the rings of modular forms

In this section, we show that for each of the seventeen subgroups Γ in Table 1, its ring of modular forms is isomorphic to a polynomial ring. We have seen that this is the case for $\mathrm{SL}(2,\mathbb{Z})$. Indeed, for the cases (a)–(c) in Table 1, since the weights are even, it is sufficient to check (4) using the dimension formula; it follows from (4) that there exist algebraic independent modular forms of weight a_1, a_2. To be more precise, let $\theta_3(\tau), \theta_2(\tau)$ be Jacobi's theta functions. It is well known and easy to see that $\mathfrak{M}(\Gamma(2)) = \mathbb{C}[\theta_3(2\tau)^4, \theta_2(2\tau)^4]$ and that $\Gamma_0(4) = \sigma_0\Gamma(2)\sigma_0^{-1}$. So, we have the assertions for the groups No. 3 and No. 4. As for cases (b) and (d), more explicit information can be found in [11, p.52, Corollary] for $\Gamma_0(2)$, [11, p.53, Theorem 2] for $\Gamma_1(3)$. We note that the notation of subgroups in [11] is different from ours. The groups No. 6–11 are pairwise conjugate in $\mathrm{GL}(2,\mathbb{Q})$, so it suffices to give generators for No. 6 only. The result for the group No. 6 is given in [8, p.186] as $\mathfrak{M}(\sigma_0^{-1}\Gamma_1(4)\sigma_0) = \mathbb{C}[\theta_3(2\tau)^2, \theta_2(2\tau)^4]$.

Let Γ be one of the subgroups No. 12–17. Suppose that there exist modular forms ϕ_1, ϕ_2 of weight 1 on Γ such that the leading terms of their Fourier expansion with respect to $q = e^{2\pi i\tau}$ are 1, q, respectively. Considering the leading terms of $\phi_1^n, \phi_1^{n-1}\phi_2, \dots, \phi_2^n$, we can prove that $\phi_1^n, \phi_1^{n-1}\phi_2, \dots, \phi_2^n$ are linearly independent. Hence ϕ_1, ϕ_2 are algebraically independent. Since $\dim \mathfrak{M}_2(\Gamma) = 3$, we have $\dim \mathfrak{M}_1(\Gamma) \leq 2$. Therefore, to prove the claim, we have only to find modular forms ϕ_1, ϕ_2 of weight 1 on Γ such that the leading terms of their Fourier expansion are 1, q, respectively. This means that, we only need to find two linearly independent modular forms of weight 1 on Γ.

Let N be a positive integer, χ a primitive Dirichlet character mod N such that $\chi(-1) = -1$. Then the Eisenstein series

$$E_\chi(\tau) = \frac{1}{2}L(0,\chi) + \sum_{n=1}^{\infty}\Big(\sum_{d|n, d>0} \chi(d)\Big)q^n$$

is a modular form of type $(1,\chi)$ on $\Gamma_0(N)$ (see Hecke [7]).

The subgroup No. 12, 17. For the group $\Gamma(3)$, the result is well known (see [5, Theorem 5.4]). Namely, $\mathfrak{M}(\Gamma(3)) = \mathbb{C}[\varphi_1, \varphi_2]$ with

$$(5) \qquad \varphi_1 = \sum_{(x,y)\in\mathbb{Z}^2} q^{x^2-xy+y^2}, \qquad \varphi_2 = q^{\frac{1}{3}} \sum_{(x,y)\in\mathbb{Z}^2} q^{x^2-xy+y^2+x-y}.$$

Interestingly enough, this fact was known in connection with the weight enumerators of ternary self-dual codes. For a future use, we remark that $\mathrm{SL}(2,\mathbb{Z})$ acts on the 2-dimensional space spanned by φ_1, φ_2 as the unitary reflection group (No. 4 in [15])

$$\langle \frac{1}{i\sqrt{3}}\begin{pmatrix}1 & 2\\ 1 & -1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 0 & e^{\frac{2\pi i}{3}}\end{pmatrix}\rangle \cong \mathrm{SL}(2,\mathbb{Z}/3\mathbb{Z}) \cong \mathrm{SL}(2,\mathbb{Z})/\Gamma(3).$$

The ring of polynomial invariants of this group is the polynomial ring in f, g, where

$$f(x,y) = x^4 + 8xy^3, \qquad g(x,y) = x^6 - 20x^3y^3 - 8y^6.$$

Moreover, $f(\varphi_1,\varphi_2) = E_4$ and $g(\varphi_1,\varphi_2) = E_6$ hold. The ring of invariants $\mathbb{C}[f,g]$ contains the ring of weight enumerators of ternary self-dual codes (see [4]). In view of (3), the ring $\mathfrak{M}(\Gamma_0(9)\cap\Gamma_1(3))$ is generated by $\varphi_1(3\tau), \varphi_2(3\tau)$. However, we also give different generators of this ring as follows.

Let χ_1 be the non-trivial Dirichlet character mod 3. Then the Eisenstein series $E_{\chi_1}(\tau)$ is a modular form of type $(1,\chi_1)$ on $\Gamma_0(3)$. This implies that $E_{\chi_1}(\tau)$ and $E_{\chi_1}(3\tau)$ are linearly independent modular forms of type $(1,\chi_1)$ on $\Gamma_0(9)$. Hence they are modular forms of weight 1 on $\Gamma_0(9)\cap\Gamma_1(3)$.

Let $\eta(\tau)$ be the Dedekind eta-function. Then it is shown in [10] that $\eta(9\tau)^3/\eta(3\tau)$ and $\eta(\tau)^3/\eta(3\tau)$ also are modular forms of type $(1,\chi_1)$ on $\Gamma_0(9)$. The relations between these forms are:

$$\begin{aligned}\eta(9\tau)^3/\eta(3\tau) &= E_{\chi_1}(\tau) - E_{\chi_1}(3\tau),\\ \eta(\tau)^3/\eta(3\tau) &= -3(E_{\chi_1}(\tau) - 3E_{\chi_1}(3\tau)).\end{aligned}$$

Moreover, we have

$$\begin{aligned}\varphi_1(3\tau) &= 6E_{\chi_1}(\tau),\\ \varphi_2(3\tau) &= E_{\chi_1}(\tau) - E_{\chi_1}(3\tau).\end{aligned}$$

The subgroups No. 13, 16. Let χ_2 be the non-trivial Dirichlet character mod 4. Then the Eisenstein series $E_{\chi_2}(\tau)$ is a modular form of type $(1,\chi_2)$ on $\Gamma_0(4)$. This implies that $E_{\chi_2}(\tau)$ and $E_{\chi_2}(2\tau)$ are linearly independent modular forms of type $(1,\chi_2)$ on $\Gamma_0(8)$. Hence they are modular forms of weight 1 on the subgroup No. 16: $\Gamma_0(8)\cap\Gamma_1(4)$. Alternatively, it is shown in [10] that $\eta(8\tau)^4/\eta(4\tau)^2$ and $\eta(\tau)^4/\eta(2\tau)^2$ also are modular forms of type $(1,\chi_2)$ on $\Gamma_0(8)$. The relations between these forms are:

$$\begin{aligned}\eta(8\tau)^4/\eta(4\tau)^2 &= E_{\chi_2}(\tau) - E_{\chi_2}(2\tau),\\ \eta(\tau)^4/\eta(2\tau)^2 &= -4(E_{\chi_2}(\tau) - 2E_{\chi_2}(2\tau)).\end{aligned}$$

Note that $\mathfrak{M}(\Gamma_1(4) \cap \Gamma(2)) = \mathbb{C}[\theta_3(\tau)^2, \theta_4(\tau)^2]$ (see [8, p.186]) follows from (2). More explicitly, we have

$$\begin{aligned}\theta_3(2\tau)^2 &= 4E_{\chi_2}(\tau),\\ \theta_4(2\tau)^2 &= -4(E_{\chi_2}(\tau) - 2E_{\chi_2}(2\tau)).\end{aligned}$$

The subgroup No. 14. Let χ_3 be the Dirichlet character mod 5 such that $\chi_3(2) = \sqrt{-1}$. Then the Eisenstein series $E_{\chi_3}(\tau)$ and $E_{\overline{\chi_3}}(\tau)$ are modular forms of type $(1, \chi_3), (1, \overline{\chi_3})$, respectively on $\Gamma_0(5)$. Hence they are linearly independent modular forms of weight 1 on $\Gamma_1(5)$.

The subgroup No. 15. Recall that $E_{\chi_1}(\tau)$ is a modular form of type $(1, \chi_1)$ on $\Gamma_0(3)$, where χ_1 is the non-trivial Dirichlet character mod 3. This implies that $E_{\chi_1}(\tau)$ and $E_{\chi_1}(2\tau)$ are linearly independent modular forms of type $(1, \chi_1)$ on $\Gamma_0(6)$. Hence they are modular forms of weight 1 on $\Gamma_1(6)$. It is shown in [10] that $\eta(\tau)\eta(6\tau)^6/\eta(2\tau)^2\eta(3\tau)^3$ and $\eta(6\tau)\eta(\tau)^6/\eta(3\tau)^2\eta(2\tau)^3$ also are modular forms of type $(1, \chi_1)$ on $\Gamma_0(6)$. The relations between these forms are:

$$\begin{aligned}\eta(\tau)\eta(6\tau)^6/\eta(2\tau)^2\eta(3\tau)^3 &= E_{\chi_1}(\tau) - E_{\chi_1}(2\tau),\\ \eta(6\tau)\eta(\tau)^6/\eta(3\tau)^2\eta(2\tau)^3 &= -6(E_{\chi_1}(\tau) - 2E_{\chi_1}(2\tau)).\end{aligned}$$

§6. Concluding remarks

We note that the classification of the subgroups $\Gamma \subset \mathrm{SL}(2, \mathbb{Z})$ whose ring of modular forms is isomorphic to a polynomial ring is regarded as an analogue of the classification of the finite unitary reflection groups of dimension 2. We expect that higher dimensional analogue for this is the classification of the subgroups in the Siegel modular groups whose ring of Siegel modular forms is isomorphic to a polynomial ring. There are many possible generalizations of the ideas and the motivations presented in this paper. We will discuss some of the generalizations in subsequent papers, we briefly mention some of them below.

(1) Classify discrete subgroups of $\mathrm{SL}(2, \mathbb{R})$, not necessarily contained in $\mathrm{SL}(2, \mathbb{Z})$, whose ring of modular forms is isomorphic to a polynomial ring.

(2) Classify subgroups of $\mathrm{SL}(2, \mathbb{Z})$ whose ring of modular forms of half-integral weights is isomorphic to a polynomial ring.

Furthermore, we can consider a similar problem for $1/l$-integral weights (see Rankin [14] for the definition of modular forms of fractional weights). In general, if the ring of modular forms of $1/l$-integral weights on Γ is isomorphic to the polynomial ring generated by two modular forms of weight $1/l$, then we see that Γ must be a subgroup of index $24l$ in $\mathrm{SL}(2,\mathbb{Z})$. A recent work of A. Sebbar on the classification of genus zero congruence subgroups with no elliptic points implies that they are noncongruence subgroups except for finitely many exceptions. The complete classifications of such subgroups of index $24l$ seems very difficult in general. In the case $l = 2$, using the method described in Section 4, we can see that there are 191 possible such subgroups Γ of index 48 in $\mathrm{SL}(2,\mathbb{Z})$ up to the conjugacy. Some of them are congruence subgroups and others are noncongruence subgroups. We expect that many of them, hopefully all of them, satisfy the property mentioned in (2). Note that some results on modular forms on noncongruence subgroups are given in [1].

As we remarked in Section 1, the case $l = 5$ is interesting, and this will be treated in a subsequent paper. We also mention that, partly motivated by our present research, T. Ibukiyama is recently developing a theory of modular forms of fractional weights from a more general viewpoint, which will be published in due course.

References

[1] A. O. L. Atkin and H. P. F. Swinnerton-Dyer, Modular forms on noncongruence subgroups, Proc. Sympos. Pure Math., **19** (1971), 1–25.

[2] E. Bannai, Study of modular forms, a joint work with Masao Koike, Akihiro Munemasa and Jiro Sekiguchi, in Japanese, Surikaisekikenkyusho Kokyuroku 1109, Proceedings of Symposium at RIMS on Algebraic Combinatorics and Related Topics, Dec. 1998.

[3] A. Beauville, Les familles stables de courbes elliptiques sur $\mathbf{P}^1$ admettant quatre fibres singulières, C. R. Acad. Sci. Paris, **294** (1982), Série I, 657–660.

[4] M. Broué and M. Enguehard, Polynômes des poids de certains codes et fonctions thêta de certains réseaux, Ann. Sci. École Norm. Sup., **5** (1972) 157–181.

[5] W. Ebeling, Lattices and Codes, Vieweg, 1994.

[6] The GAP Group, Lehrstuhl D für Mathematik, RWTH Aachen, Germany and School of Mathematical and Computational Sciences, U. St. Andrews, Scotland, GAP — Groups, Algorithms, and Programming, Version 4, 1999. GAP is available from `http://www-gap.dcs.st-and.ac.uk/~gap/`.

[7] E. Hecke, Theorie der Eisensteinschen Reihen höherer Stufe und ihre Anwendung auf Funktionentheorie und Arithmetik, Abh. Math. Sem. Hamburg, **5** (1927), 199–224. (See also E. Hecke, Mathematische Werke, Vandenhoeck and Ruprecht, Gottingen, 1970.)

[8] T. Hiramatsu, Introduction to Higher Reciprocity Laws, in Japanese, Makino Shoten, 1998.

[9] F. Klein, Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade, 1884, reprinted 1993, Birkhauser.

[10] M. Koike, Moonshines of $\mathrm{PSL}_2(\mathbf{F}_p)$ and the automorphism group of Leech lattice, Japanese J. Math., **12** (1986), 283–323.

[11] D. P. Maher, Modular forms from codes, Canad. J. Math., **32** (1980), 40–57.

[12] M. H. Millington, Subgroups of the classical modular group, J. London Math. Soc., (2), **1** (1969), 351–357.

[13] T. Miyake, Modular Forms, Springer-Verlag, 1989.

[14] R. A. Rankin, Modular Forms and Functions, Cambridge University Press, 1977.

[15] G. C. Shephard and J. A. Todd, Finite unitary reflection groups, Canad. J. Math., **6** (1954), 274–304.

[16] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Iwanami Shoten and Princeton University Press, 1971.

[17] J. Sekiguchi, Klein's icosahedral equation and modular forms, in Japanese, Proceedings of the 16th Algebraic Combinatorics Symposium, Kyushu University, June, 1999.

Eiichi Bannai
Faculty of Mathematics
Kyushu University
Fukuoka 812-8581, Japan

Masao Koike
Faculty of Mathematics
Kyushu University
Fukuoka 812-8581, Japan

Akihiro Munemasa
Faculty of Mathematics
Kyushu University
Fukuoka 812-8581, Japan

Jiro Sekiguchi
Faculty of Science
Himeji Institute of Technology
Hyogo 678-1297, Japan

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 255–277

Steiner systems and Mathieu groups revisited

Helmut Bender

These notes about an old topic of Witt (Abh. Hbg. 1938) describe a further approach to the relevant existence and isomorphism theorems for Steiner systems. Some standard information about the automorphism groups is obtained along the way. Actually, I wish to proceed by group theoretic arguments as much as possible. Besides Sylow's Theorem, including

$$|G : N_G(P)| \equiv 1(p) \quad \text{for} \quad P \in Syl_p(G),$$

and the most obvious properties of the 2-dimensional linear groups over $GF(11)$ and $GF(9)$, they mainly require some formalities around transitive action of a group $G$ on a set $\Omega$, above all

$$|\Omega| = |G : G_\alpha| \quad \text{for} \quad \alpha \in \Omega.$$

I also mention the "Frattini argument", "Witt's Lemma", and the concept of a Frobenius group:

The first gives $G = HG_\alpha = G_\alpha H$ for any transitive subgroup $H$, the second states that the normalizer $N_G(X)$ of a subgroup (or subset) $X \subseteq G_\alpha$ is transitive on the set Ω_X of fixed points if (and only if) $X$ is "very weakly closed" in G_α, that is all $G$-conjugates $X^g \subseteq G_\alpha$ are already conjugate to $X$ in G_α. The standard $X$ besides $X = G_\alpha$ is a Sylow subgroup of G_α. Trivially, Witt's Lemma implies the analogous result for $n$-fold transitive groups.

Thirdly, to say that $G$ is a Frobenius group on $\Omega$, means that $1 \neq G_\alpha \neq G$ and $G_{\alpha\beta} = 1$ for all $\beta \neq \alpha$. We ignore Frobenius' famous theorem and assume also that G_α has a complement $K$ in $G$. Then $K$ is regular on $\Omega$, is the set of all elements of $G$ not conjugate to an element $\neq 1$ of G_α, and is called the Frobenius kernel of $G$. Accordingly, an abstract Frobenius group is a semi-direct product $G = KA$ (with $K$ normal) such that the above holds for a suitable "$G$-set" $\Omega$ and with $A = G_\alpha$, or equivalently no element of $K$ commutes with an element

Received September 22, 1999.

outside, or equivalently no element of A commutes with an element outside.

For other treatments of our topic see Lüneburgs paper (J. Alg. 1968) related to Witt's, Aschbacher's book "Sporadic Groups", and the bibliography in the "Atlas".

This paper is dedicated to the memory of Michio Suzuki. In 1964 I had to study one of his papers (characterizing linear groups) as a participant of Reinhold Baer's seminar at Frankfurt university, under the supervision of Baer's assistant Bernd Fischer. It was my third seminar already, but the first time that I found the mathematics confronting me attractive. Reading Suzuki's papers then became the main occupation for the rest of my student life.

Suzuki was a pioneer of modern group theory which culminated in the classification of the finite simple groups, and he contributed crucially to quite a few rather different main topics. To describe his role for the classification I like to compare the Sylow 2-subgroups of a finite group with fortresses in an area to be forced under one's complete control. In order to exert such a control, our fortresses must be strong and must have good lines of communications (good coherence in more group theoretic language). Thus, Suzuki laid much of the basis for a powerful 2-local structure theory.

Pioneers will be followed by others, more convenient ways will be constructed, and after a while their foot steps are not so apparent any more. This does however not apply to the bulk of Suzuki's work, on certain types of permutation groups and related topics, which in its depth and beauty will forever remain a jewel in the field of finite groups.

§1. Steiner systems

1.1. **Lemma.** *Let Ω be a finite set, $0 \le t \le k \le v = |\Omega|$, and $\mathcal{B}$ a set of k-subsets of Ω. Then, with*

$$\mathcal{B}(X) = \{B \in \mathcal{B} \mid X \subseteq B\} \text{ and } b(t,k,v) = \binom{v}{t} / \binom{k}{t},$$

the following conditions (a), (b), (c) *are equivalent*:

(a) $|\mathcal{B}(X)| = 1$ *for all t-subsets $X \subseteq \Omega$,*

(b) $|\mathcal{B}| = b(t,k,v)$ *and* $|\mathcal{B}(X)| \le 1$ *for all t-subsets $X \subseteq \Omega$,*

(c) $|\mathcal{B}| = b(t,k,v)$ *and* $|\mathcal{B}(X)| \ge 1$ *for all t-subsets $X \subseteq \Omega$.*

Proof. There are $\binom{v}{t}$ t-subsets X of Ω, and each $B \in \mathcal{B}$ contains $\binom{k}{t}$ such subsets X. Thus the number of pairs (X, B) with $X \subseteq B$ equals both $|\mathcal{B}| \cdot \binom{k}{t}$ and $\sum_X |\mathcal{B}(X)|$, and this sum has $\binom{v}{t}$ summands. Q.E.D.

1.2. **Definition.** In the situation of Lemma 1.1, with one (hence each) of (a), (b), (c) valid, $\mathcal{B}$ is a Steiner system of type (t, k, v), or just (t, k), on Ω.

We write $\mathcal{B} \in S(t, k, v, \Omega)$ and drop Ω or v whenever suitable.

The sets $B \in \mathcal{B}$ are called blocks, sometimes lines, and the elements $\alpha \in \Omega$ points. The block containing a t-set X is denoted by $\langle X \rangle$. A collinear subset of Ω is contained in some block.

An isomorphism from $\mathcal{B}$ onto another Steiner system $\hat{\mathcal{B}}$ with point set $\hat{\Omega}$ is a bijective mapping φ from Ω onto $\hat{\Omega}$ such that $\mathcal{B}\varphi = \hat{\mathcal{B}}$.

1.3. Thus the automorphism group of $\mathcal{B} \in S(t, k, v, \Omega)$ is the stabilizer of $\mathcal{B}$ in the symmetric group $Sym(\Omega)$. The number of conjugates of $\mathcal{B}$ under $Sym(\Omega)$ is $v!/|Aut(\mathcal{B})|$. All (t, k, v)-systems are isomorphic if and only if all $\mathcal{B}$ are conjugate under $Sym(\Omega)$.

1.4. For $\mathcal{B} \in S(t, k, v, \Omega)$ and $J \subseteq \Omega$, with $j = |J| \leq t$, the set

$$\mathcal{B}((J)) = \{B \setminus J \mid B \in \mathcal{B}(J)\}$$

is a $(t - j, k - j, v - j)$-system on $\Omega \setminus J$. In particular,

$$|\mathcal{B}(J)| = |\mathcal{B}((J))| = b(t - j, k - j, v - j).$$

From $b(t, k, v) = \frac{v}{k} \cdot b(t - 1, k - 1, v - 1)$ (for $t > 0$) we get the following table. There is no continuation to the right because neither $2 \cdot 66 \cdot \frac{13}{7}$ nor $23 \cdot 11 \cdot 3 \cdot \frac{25}{9}$ is an integer.

(t, k, v) :	$(1, 2, 8)$	$(2, 3, 9)$	$(3, 4, 10)$	$(4, 5, 11)$	$(5, 6, 12)$
$b(t, k, v)$:	4	12	30	66	$2 \cdot 66$

(t, k, v) :	$(1, 4, 20)$	$(2, 5, 21)$	$(3, 6, 22)$	$(4, 7, 23)$	$(5, 8, 24)$
$b(t, k, v)$:	5	21	77	$23 \cdot 11$	$23 \cdot 11 \cdot 3$

1.5. For $\alpha \in \Omega$ call $\mathcal{B}, \hat{\mathcal{B}} \in S(t, k, v, \Omega)$ α-equivalent if $\mathcal{B}(\alpha) = \hat{\mathcal{B}}(\alpha)$. We also say that $\mathcal{B}$ and $\hat{\mathcal{B}}$ agree on α. Clearly, the number of α-equivalence classes is at most $|S(t-1, k-1, \Omega \setminus \{\alpha\})|$ (assume $t \geq 1$).

So with $\ell(t, k, v)$ the maximal length of an α-equivalence class (where now α ranges over Ω, and $\ell(t, k, v) = 0$ if $S(t, k, v)$ is empty), we have

$$|S(t, k, \Omega)| \leq \ell(t, k, v) \cdot |S(t - 1, k - 1, \Omega \setminus \{\alpha\})|.$$

As an example, we consider the case $(t, k, v) = (5, 6, 12)$ and prove

$$\ell(5, 6, 12) \leq 1.$$

This means that any α-equivalent $\mathcal{B}, \hat{\mathcal{B}} \in S(t,k,v,\Omega)$ are actually equal. Assume $\mathcal{B} \neq \hat{\mathcal{B}}$, say some $B \in \hat{\mathcal{B}}$ does not belong to $\mathcal{B}$. Then $\alpha \notin B$, and each 5-set $X \subseteq B$ lies in a unique block $X \cup \{\beta\}$ of $\mathcal{B}$ (not in $\hat{\mathcal{B}}$). These (six) points $\beta = \beta(X)$ are pairwise distinct and distinct from α. Thus $\Omega \geq |B| + 6 + 1 = 13$, a contradiction. It is also true, though less obvious, that $\ell(5,8,24) \leq 1$.

1.6. **The Trivial Isomorphism Theorem.** *For $1 \leq t \leq k \leq v$ assume some $\mathcal{B} \in S(t,k,v)$ exists. Write g for $|Aut(\mathcal{B})|$. Then all $\mathcal{B}$ are isomorphic, with $g = g'v/n$, provided*

(i) *all $\mathcal{B}' \in S(t-1,k-1,v-1)$ are isomorphic, with $|Aut(\mathcal{B}')| = g'$, and*

(ii) *n is an integer such that $\ell(t,k,v) < 2n$ and gn divides $g'v$ for all $\mathcal{B}$.*

Proof. We apply 1.3 and 1.5. Fix $\mathcal{B}$ with point set Ω for a moment. Write $g'v = gnq$. Then the $Sym(\Omega)$-orbit containing $\mathcal{B}$ has length

$$\frac{v!}{g} = \frac{nqv!}{g'v} = \frac{nq(v-1)!}{g'}.$$

With q minimal and r the number of all orbits it follows that

$$r\frac{nq(v-1)!}{g'} \leq |S(t,k,\Omega)| < 2n\frac{(v-1)!}{g'}$$

and hence $rnq < 2n$, thus $r = q = 1$. Q.E.D.

1.7. **The Trivial Induction Lemma.** *Assume $2 \leq t \leq k \leq |\Omega|$.*

(a) *For each $\alpha \in \Omega$ let $\mathcal{B}_\alpha \in S(t-1,k-1,\Omega \setminus \{\alpha\})$, and assume $\mathcal{B}_\alpha((\beta)) = \mathcal{B}_\beta((\alpha))$ for all points $\beta \neq \alpha$. Then*

$$\mathcal{B} = \{B \subseteq \Omega \mid B \setminus \{\alpha\} \in \mathcal{B}_\alpha \text{ for some } \alpha \in B\}$$

is a Steiner system of type (t,k) on Ω.

(b) *Assume (a group) G acts on Ω, for each $\alpha \in \Omega$ there is a unique G_α-invariant $\mathcal{B}_\alpha \in S(t-1,k-1,\Omega\setminus\{\alpha\})$, and for any two distinct points $\alpha,\beta \in \Omega$ there is a unique $G_{\alpha\beta}$-invariant $\mathcal{B}_{\alpha\beta} \in S(t-2,k-2,\Omega\setminus\{\alpha,\beta\})$, or, more generally, $\mathcal{B}_\alpha((\beta)) = \mathcal{B}_\beta((\alpha))$.*

Then there is a unique G-invariant $\mathcal{B} \in S(t,k,\Omega)$.

Proof. The point about the condition $\mathcal{B}_\alpha((\beta)) = \mathcal{B}_\beta((\alpha))$ in (a) is that $B \setminus \{\alpha\} \in \mathcal{B}_\alpha$ holds not only for some, but for every element α of a given $B \in \mathcal{B}$: Assume it holds for α and let $\alpha \neq \beta \in B$. Then $D = (B\setminus\{\alpha\})\setminus\{\beta\}$ lies in $\mathcal{B}_\alpha((\beta)) = \mathcal{B}_\beta((\alpha))$, that is $B\setminus\{\beta\} = D \cup \{\alpha\}$ lies in $\mathcal{B}_\beta$.

To prove (a), hence (b), we have to show that a unique $B \in \mathcal{B}$ contains a given t-subset $X \subseteq \Omega$. Existence: Choose $\alpha \in X$, $U \in \mathcal{B}_\alpha(X \setminus \{\alpha\})$, and let $B = \{\alpha\} \cup U$. Uniqueness: If $X \subseteq A \in \mathcal{B}$, then, by the first paragraph, $A \setminus \{\alpha\}$ is also a block in $\mathcal{B}_\alpha$ which contains $X \setminus \{\alpha\}$, hence is equal to U. Q.E.D.

1.8. **Lemma.** *Assume G is a Frobenius group on a 9-set Ω, and the Frobenius kernel of G is elementary abelian (of order 9).*

(a) *There exists a unique G-invariant $\mathcal{B} \in S(2,3,\Omega)$.*

(b) *For each $\alpha \in \Omega$, $\mathcal{B}((\alpha))$ consists of the four orbits of length 2 under the subgroup of order 2 in G_α.*

Proof. First we consider any G-invariant $\mathcal{B} \in S(2,3,\Omega)$. A subgroup T of order 2 has one fixed point α and four orbits X of length 2 in Ω. For each X, the block $\langle X \rangle$ is T-invariant and hence equals $X \cup \{\alpha\}$. This proves (b), hence gives uniqueness in (a).

For existence we apply 1.7(a). For each $\alpha \in \Omega$ let $\mathcal{B}_\alpha$ be the set of all T-orbits of length 2, where T is the subgroup of order 2 in G_α. For $\alpha \neq \beta \in \Omega$ let $D \simeq S_3$ be the subgroup generated by T and the analogous subgroup of order 2 in G_β. Then βD is a D-invariant 3-subset of Ω, hence contains a fixed point of T, that is α. Now the third point γ in $\alpha D = \beta D$ satisfies $\mathcal{B}_\alpha((\beta)) = \{\gamma\} = \mathcal{B}_\beta((\alpha))$. Q.E.D.

1.9. **Corollary** (by 1.7(b)). *Let G be a transitive group of order $9 \cdot 4 \cdot 10$ or $9 \cdot 8 \cdot 10$ on a 10-set Ω. For $\alpha \in \Omega$, assume G_α to be a Frobenius group on $\Omega \setminus \{\alpha\}$.*

Then G leaves a unique $\mathcal{B} \in S(3,4,\Omega)$ invariant.

1.10. **Theorem.** *Let $t \geq 2$, $v = t+7$, $k = t+1$, and G a sharply t-transitive group on a v-set Ω.*

Then $t \leq 5$ and G leaves a unique $\mathcal{B} \in S(t,k,\Omega)$ invariant. All blocks are conjugate, and a k-subset B is a block if and only if $G_B \simeq S_k$.

Proof. The unique $\mathcal{B}$ comes from 1.8(a) for $t = 2$, from 1.9 for $t = 3$, then from 1.7(b) for $t = 4, 5, 6, \ldots$. By 1.4, $S(t,k,v)$ is empty for $t \geq 6$.

We have $|G| = v \cdot (v-1) \cdots (v-(t-1))$ and $|G_B| \leq k!$ because G_B is faithful on B. Thus

$$|B^G| = |G : G_B| \geq \frac{|G|}{k!} = b(t,k,v)$$

whence $G_B \simeq S_k$ means $|B^G| = b(t,k,v)$, hence $B^G \in S(t,k,\Omega)$ by Lemma 1.1 because each t-subset of Ω is conjugate to a subset of B. Q.E.D.

1.11. **Lemma.** *Some G as in 1.9 is isomorphic to A_6, and then any subgroup $H \simeq A_5$ is transitive.*

Conversely, If $H \simeq A_5$ acts transitively on a 10-set Ω, then there exists a unique H-invariant $\mathcal{B} \in S(3,4,\Omega)$ and for each $\alpha \in \Omega$, $\mathcal{B}((\alpha))$ is the only H_α-invariant (2,3)-system on $\Omega \setminus \{\alpha\}$.

Proof. Let Λ be any 6-set, $G = Alt(\Lambda)$, and Ω the set of all sets $\{X, Y\}$, where X and Y are disjoint 3-subsets of Λ. Then $|\Omega| = 10$, $|G| = 6!/2 = 9 \cdot 4 \cdot 10$, and no element order 5, 3, or 2 in G fixes 1, 2, or 3 points in Ω, respectively. Thus G and Ω are as in 1.9.

Then any subgroup H of order 60 is transitive because any stabilizer $|H_\alpha|$ $(\alpha \in \Omega)$, a subgroup of the Frobenius group G_α of order $9 \cdot 4$, has order at most 6.

All transitive H-sets of length 10 are isomorphic because all subgroups of order 6 in H are conjugate. As for uniqueness of $\mathcal{B}((\alpha))$, hence of $\mathcal{B}$, any such (2,3,9)-system consists of the 10 3-sets invariant under a subgroup of order 2 in $H_\alpha \simeq S_3$, and the two additional orbits under the subgroup of order 3. Q.E.D.

1.12. In analogy with $\ell(t,k,v) = \ell_1(t,k,v)$ defined in 1.5 we can define $\ell_p(t,k,v)$ for each integer $p \geq 1$ as the maximal length of a J-equivalence class in $S(t,k,v,\Omega)$, where J ranges over all p-subsets of Ω, and J-equivalence means α-equivalence for all $\alpha \in J$.

In other words, $\ell_p(t,k,v) \leq m$ means that not more than m (t,k,v)-systems $\mathcal{B}$ on Ω can "agree" on p points, in case $m = 1$ that any $\mathcal{B}$ is completely determined by any p 1-residues $\mathcal{B}((\alpha))$.

Obviously, the argument in 1.5 for $\ell(5,6,12) \leq 1$ also gives $\ell_2(4,5,11) \leq 1$ and $\ell_3(3,4,10) \leq 1$. In section 3 the latter will be improved to $\ell_2(3,4,10) \leq 1$ (actually to the stronger condition (*)(3,4,10) introduced below).

The condition $\ell_2(t,k,v) \leq 1$ is very convenient when we wish to get information on $\ell(t,k,v)$:

(a) To prove $\ell(t,k,v) \leq m$ it suffices to show that if $\mathcal{B}((\alpha))$ is given, there are at most m possibilities for any second 1-residue $\mathcal{B}((\beta))$.

More formally, with $\ell'(t,k,v)$ the maximal number of β-equivalence classes inside an α-equivalence class (in any case $\leq \ell(t,k,v)$),

$$\ell_2((t,k,v) \leq 1 \qquad \text{implies} \qquad \ell(t,k,v) = \ell'(t,k,v).$$

Below we also prove that for any $p \geq 1$,

(b) $\ell_2(t,k,v) \leq 1$ implies $\ell_p(t+1,k+1,v+1) \leq \ell_p(t,k,v)$.

This suffices for the small cases (3,4,10), (4,5,11), and (5,6,12). For the large cases (3,6,22), (4,7,23), and (5,8,24) a finer distinction appears to be appropriate. The following condition (*) lies between $\ell(t,k,v) \leq 1$ and $\ell_2(t,k,v) \leq 1$. For the small cases, when $k = t+1$, it means that two distinct (t,k,v)-systems on Ω which agree on a point α (are α-equivalent), have only those blocks in common which contain α, indeed a much stronger statement than $\ell_2(t,k,v) \leq 1$.

(*) Whenever distinct $\mathcal{B}_1, \mathcal{B}_2 \in S(t,k,v,\Omega)$ agree on a point $\alpha \in \Omega$, then $|B_1 \cap B_2| \leq t$ for all $B_1 \in \mathcal{B}_1$ and $B_2 \in \mathcal{B}_2$ not containing α.

We assume $2 < t < k < v$ and prove the following results.

(c) The above condition (*) is equivalent to the following condition

(**) Whenever $\mathcal{B}_1, \mathcal{B}_2 \in S(t,k,v,\Omega)$ agree on a point $\alpha \in \Omega$, and B_1, B_2 are blocks in $\mathcal{B}_1$, $\mathcal{B}_2$, respectively, which do not contain α and satisfy $|B_1 \cap B_2| > t$, then $\mathcal{B}_1(\beta) = \mathcal{B}_2(\beta)$ for all $\beta \in B_1 \cap B_2$.

(d) (*) implies the analogous condition $(*)(t+1,k+1,v+1)$.

Proof of (b): We rather assume $\ell_2(t-1,k-1,v-1) \leq 1$ and show that $m = \ell_p(t,k,v)$ is $\leq \ell_p(t-1,k-1,v-1)$.

Let $\mathcal{B}_1, \ldots, \mathcal{B}_m \in S(t,k,v,\Omega)$ be J-equivalent and pairwise distinct, with J a p-subset of Ω. For $\beta \in \Omega \setminus J$ the $(t-1,k-1,v-1)$-systems $\mathcal{B}_i((\beta))$ are J-equivalent. To show they are pairwise distinct (whence $m \leq \ell_p(t-1,k-1,v-1)$) assume $\mathcal{B}_1(\beta) = \mathcal{B}_2(\beta)$. For each further point $\gamma \in \Omega \setminus J$, the $(t-1,k-1,v-1)$-systems $\mathcal{B}_1((\gamma))$ and $\mathcal{B}_2((\gamma))$ agree on β and each of the $p \geq 1$ points $\alpha \in J$, hence are equal because $\ell_2(t-1,k-1,v-1) \leq 1$. It follows that $\mathcal{B}_1 = \mathcal{B}_2$, a contradiction.

Proof of (c): Trivially, (*) implies (**). So assume (**) and let B_1, B_2 contradict (*). Then $|B_1 \cap B_2| > t$ and (**) implies $\mathcal{B}_1(\beta) = \mathcal{B}_2(\beta)$ for all $\beta \in B_1 \cap B_2$. There exists $\gamma \in \Omega$ such that $\mathcal{B}_1(\gamma) \neq \mathcal{B}_2(\gamma)$, because $\mathcal{B}_1 \neq \mathcal{B}_2$. Fix β. There exists $B \in \mathcal{B}_1(\beta,\gamma) \setminus \mathcal{B}_1(\alpha,\beta,\gamma)$ because $t > 2$ and $v > k$. Then $B \in \mathcal{B}_2$, and we can apply (**) with B in place of B_1 and B_2 to get $\mathcal{B}_1(\gamma) = \mathcal{B}_2(\gamma)$, a contradiction.

Proof of (d): It suffices to derive (**) from $(*)(t-1,k-1,v-1)$. Assume the hypothesis of (**). For each $\beta \in B_1 \cap B_2$ apply $(*)(t-1,k-1,v-1)$ to $\mathcal{B}_i((\beta))$ to get $\mathcal{B}_1((\beta)) = \mathcal{B}_2((\beta))$.

Finally we combine most of the above to get

(e) $(**)(t,k,v)$ plus $\ell'(t,k,v) \leq m$ implies $(*)(t+i,k+i,v+i)$ and $\ell(t+i,k+i,v+i) \leq m$ for all $i \geq 0$.

§2. Affine planes of order 3 and 4

2.1. Let $L \in \mathcal{B} \in S(2,k,v,\Omega)$ and $\alpha \in \Omega \setminus L$. By 1.4 there are $b(1,k-1,v-1) = v-1/k-1$ blocks through α, and k of them meet B.

By definition, $\mathcal{B}$ is an affine plane (of order k) if (for all L and α) exactly one block through α does not meet L (is parallel to L). So this means $v - 1/k - 1 = k + 1$, hence also $v = k^2$. In case of an affine plane, blocks will henceforth also be called lines, and parallelism of lines is an equivalence relation on $\mathcal{B}$.

Also by definition, $\mathcal{B}$ is a projective plane (of order $k-1$) if any two blocks intersect non-trivially, that is $v - 1/k - 1 = k$. This also means that the set $\mathcal{B}^L$ of all the sets $B \setminus B \cap L$, where $L \neq B \in \mathcal{B}$, is an affine plane of order $k-1$ on $\Omega \setminus L$.

2.2. If $\mathcal{B}$ in 2.1 is an affine plane, any two non-parallel lines $H = \{a_{11}, \ldots, a_{1k}\}$ and $V = \{a_{11}, \ldots, a_{k1}\}$ yield a $k \times k$-matrix $A = (a_{ij})$ whose rows and columns are the parallels of H and V respectively. Just define a_{ij} to be the unique point on the parallel of H through a_{i1}, and the parallel of V through a_{1j} . Any further line contains exactly one point from each row and each column.

2.3. Assume $k = 3$ in 2.2, that is $\mathcal{B} \in S(2,3,9,\Omega)$, and write ij for a_{ij}. Quite obviously, the additional $b(2,3,9) - (3+3) = 6$ lines are the two diagonals 11 22 33, 13 22 31, and the four triangles

$$\begin{pmatrix} 11 & \cdot & \cdot \\ \cdot & \cdot & 23 \\ \cdot & 32 & \cdot \end{pmatrix} \begin{pmatrix} \cdot & \cdot & 13 \\ 21 & \cdot & \cdot \\ \cdot & 32 & \cdot \end{pmatrix} \begin{pmatrix} \cdot & 12 & \cdot \\ \cdot & \cdot & 23 \\ 31 & \cdot & \cdot \end{pmatrix} \begin{pmatrix} \cdot & 12 & \cdot \\ 21 & \cdot & \cdot \\ \cdot & \cdot & 33 \end{pmatrix}$$

So if another $\hat{\mathcal{B}} \in S(2,3,9)$ is analogously represented by a matrix $\hat{A} = (\hat{a}_{ij})$, then the mapping $a_{ij} \to \hat{a}_{ij}$ is an isomorphism from $\mathcal{B}$ onto $\hat{\mathcal{B}}$.

It follows that all $\mathcal{B}$'s are isomorphic, with $Aut(\mathcal{B})$ sharply transitive on the set of triples (a, b, x) of non-collinear points (each (a, b, x) equals $(11, 12, 21)$ for some unique A).

Thus $Aut(\mathcal{B})$ has order $9 \cdot 8 \cdot 6$, is doubly transitive on the points, and the stabilizer of two points a, b fixes the third point on the line through a and b, and is sharply transitive on the remaining 6 points.

2.4. If $k = 4$ in 2.2, that is $\mathcal{B} \in S(2,4,16)$, the lines are not determined by the matrix $A = (a_{ij}) = (ij)$. The line through 11 and 22 might be the diagonal 11 22 33 44 or the set 11 22 34 43. Interchanging the last two points in the sequence V however, results in interchanging the last two rows of the matrix. The diagonal of the new matrix is a line if and only if the diagonal of A is not.

So for a quadruple (a, b, c, x) of pairwise distinct non-collinear points, with a, b, c collinear, there is a unique matrix A with $(a, b, c, x) = (11, 12, 13, 21)$ and the diagonal 11 22 33 44 a line.

We show that such a "regular" quadruple determines $\mathcal{B}$ via its matrix. The only point sets containing exactly one point from each row, each column, and the diagonal, are

11 23 34 42 13 22 34 41 12 24 33 41 12 23 31 44
11 24 32 43 14 22 31 43 14 21 33 42 13 21 32 44

and all these sets must be lines because each point (on the diagonal) lies on exactly $v - 1/k - 1 = 5$ lines. Now there are only $b(2,5,21) - (4 + 4 + 1 + 8) = 3$ lines left, and the only candidates are 12 21 34 43, 13 24 31 42, and 14 23 32 41.

So in analogy with 2.3 all $\mathcal{B}$'s are isomorphic, with $Aut(\mathcal{B})$ sharply transitive on regular quadruples, hence of order $16 \cdot 15 \cdot 2 \cdot 12$.

§3. Steiner systems of type (3,4,10), (4,5,11) and (5,6,12)

3.1. Let $\mathcal{B} \in S(3,4,10,\Omega)$. Choose a block $\{a', a, b, c\}$ and a further point x. Apply 2.3 to the (2,3,9)-systems $\mathcal{B}((a'))$ and $\mathcal{B}((a))$ with the non-collinear triples (a, b, x) and (a', b, x). We get matrices

$$A = \begin{pmatrix} a & b & c \\ x & y & z \\ u & v & w \end{pmatrix} \qquad A' = \begin{pmatrix} a' & b & c \\ x & y' & z' \\ u & v' & w' \end{pmatrix}$$

such that the blocks through a', without a', are the rows, columns, diagonals, and the four triangles of the matrix A, likewise for a and A'. Given A, that is $\mathcal{B}(a')$, A' is one of

$$\begin{pmatrix} a' & b & c \\ x & w & v \\ u & z & y \end{pmatrix} \quad \begin{pmatrix} a' & b & c \\ x & v & y \\ u & w & z \end{pmatrix} \quad \begin{pmatrix} a' & b & c \\ x & z & w \\ u & y & v \end{pmatrix}$$

because $\{y, w\}$ and $\{y', w'\}$ are equal or disjoint ($a'ayw$ and $aa'y'w'$ are blocks),
$w' \neq w$ ($a'bxw$ and $abxw'$ are blocks),
$v' \neq v$ ($a'xvc$ and $axv'c$ are blocks), and
$\{y', v'\} \neq \{y, v\}$ ($a'byv$ and $aby'v'$ are blocks).

Accordingly, the fourth point in $B = \langle a, b, x \rangle$ is $w' = y, z$, or v. So if B is also a block in another $\hat{\mathcal{B}} \in S(3,4,\Omega)$ with $\hat{\mathcal{B}}(a') = \mathcal{B}(a')$, then the matrix $A'(\hat{\mathcal{B}})$ analogous to $A' = A'(\mathcal{B})$ (again with respect to (a', a, b, c, x)) is equal to A' (because one of the three above), and this means $\hat{\mathcal{B}}(a) = \mathcal{B}(a)$.

3.2. **Lemma.** (a) *Condition* 1.12(**)(3, 4, 10) *holds.*
(b) *We have* $\ell'(3,4,10) \leq 3$.
(c) *We have* $\ell(3,4,10) \leq 3$.
(d) *We have* $\ell(4,5,11) \leq 3$.
(e) *We have* $\ell(5,6,12) \leq 1$.

Proof. (a) Write $\mathcal{B}$ and $\hat{\mathcal{B}}$ for $\mathcal{B}_1$ and $\mathcal{B}_2$, respectively, and B for B_1 and $B_2 = B_1$. For $\beta \in B$ we have to verify $\mathcal{B}(\beta) = \hat{\mathcal{B}}(\beta)$. Apply 3.1 with $a' = \alpha$, $a = \beta$, and $b, x \in B$.

(b) In 3.1 we have seen that for arbitrary points $a' \neq a$, once $\mathcal{B}(a')$ is given, there are at most three possibilities for $\mathcal{B}(a)$

Now (c) and (d) follow from 1.12(e), and (e) has been proved in 1.5. Q.E.D.

3.3. **Lemma.** *For $\mathcal{B}$ as in* 3.1, *the stabilizer of three points in $G = Aut(\mathcal{B})$ has at most order* 2. *In particular, $|G|$ divides* $10 \cdot 9 \cdot 8 \cdot 2$.

Proof. Otherwise 2.3 shows that $\Omega_X \in \mathcal{B}$ for some subgroup X of order 3. For each of the four $\alpha \in \Omega_X$ there are two more X-invariant $B \in \mathcal{B}(\alpha)$ because $|\mathcal{B}(\alpha)| = b(2,3,9) = 12$. However, there are only two X-orbits of length 3 in Ω. Q.E.D.

3.4. **Theorem.** *All $\mathcal{B} \in S(3,4,10)$ are isomorphic, with $Aut(\mathcal{B})$ of order* $10 \cdot 9 \cdot 8 \cdot 2$, *triply transitive on the points, and isomorphic to* $P\Gamma L_2(9)$.

Proof. By 2.3 all $\mathcal{B}' \in S(2,3,9)$ are isomorphic, with $g' = Aut(\mathcal{B}') = 9 \cdot 8 \cdot 6$. Thus 3.2(c) and 3.3 allow to apply 1.6 with $n = 3$.

The group $P\Gamma L_2(9)$ acts faithfully on a 10-set, and we can apply 1.9 to the (sharply 3-transitive) normal subgroup $PGL_2(9)$ of index 2 (also to the normal subgroup $L_2(9) = PSL_2(9)$ of index 4). Q.E.D.

3.5. **Corollary** (by 1.11). *The alternating group A_6 is isomorphic to* $L_2(9)$.

3.6. **Theorem.** *All $\mathcal{B} \in S(4,5,11)$ are isomorphic, with $Aut(\mathcal{B})$ of order* $11 \cdot 10 \cdot 9 \cdot 8$ *and sharply* 4*-transitive on the points.*

Proof. Let $\mathcal{B} \in S(4,5,11,\Omega)$. First we show that the stabilizer X of four points is trivial, so that in particular $g = |Aut(\mathcal{B})|$ divides $11 \cdot 10 \cdot 9 \cdot 8$. Otherwise $|X| = 2$ by 3.3, and $|\Omega_X| = 5$ by 2.3. Let J be an X-orbit of length 2. Again by 2.3, X fixes only 3 points of $\mathcal{B}((J))$, a contradiction.

Now 3.2(d) and 3.4 allow to apply 1.6 with $g' = 10 \cdot 9 \cdot 8 \cdot 2$ and $n = 2$. Q.E.D.

3.7. **Theorem.** *All $\mathcal{B} \in S(5,6,12)$ are isomorphic, with $Aut(\mathcal{B})$ of order* $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$ *and sharply* 5*-transitive on the points.*

Proof. 3.2(e) and 3.6 allow to apply 1.6 with $n = 1$. Q.E.D.

Existence of a (5,6,12)-system (hence of a (4,5,11)-system) will be proved in 3.9 below. Then M_{12} (and M_{11}) will denote the automorphism group of such a Steiner system.

3.8. **Lemma.** *Let L be a group "of type $L_2(11)$", in the sense that L has order $11 \cdot 5 \cdot 12$ and a non-normal subgroup E of order 11.*

(a) *$N_L(E)$ has order $11 \cdot 5$.*

(b) *L acts transitively on some 12-set Ω such that $N_L(E) = L_\alpha$ for some $\alpha \in \Omega$.*

(c) *A subgroup $D \subseteq L_\alpha$ of order 5 fixes only one additional point $\beta \in \Omega$.*

(d) *$N_L(D) = D\langle t\rangle$ with $t \notin C_L(D)$ an involution.*

(e) *Any $11'$-subgroup containing D lies in $N_L(D)$ or is isomorphic to A_5.*

Proof. By Sylow's Theorem, $|L : N_L(E)| \equiv 1$ modulo 11. This yields (a), hence (b). D is not normal in L because otherwise L/D were a Frobenius group of order $11 \cdot 12$. Thus ED is a Frobenius group on $\Omega \setminus \{\alpha\}$. This implies (c) and $|N_L(D)| = 10$. If an involution t would centralize D, $C_L(t)/\langle t\rangle$ were a Frobenius group of order $5 \cdot 6$. Finally, a subgroup of order 60 is simple by (d). Q.E.D.

3.9. **Theorem.** *In the situation of 3.8, L leaves some $\mathcal{B} \in S(5,6,\Omega)$ invariant. In particular, M_{12} has a (point—) transitive subgroup isomorphic to L.*

Proof. No element of order 2 or 3 fixes a point. So t interchanges the two fixed points of D, as well as the two orbits X_1, X_2 of length 5. Furthermore, each 5-set $X \subseteq \Omega$ with $L_X \neq 1$ is conjugate to X_1 (and X_2) and satisfies $|L_X| = 5$. Hence there are $|L|/5 = 11 \cdot 12$ such 5-sets X and each other 5-set $X' \subseteq \Omega$ has $|L| = 11 \cdot 12 \cdot 5$ conjugates. Since the latter number equals $\binom{12}{5} - 11 \cdot 12$, all X' are conjugate.

The (global) stabilizer of any of the two 6-sets $B_i = X_i \cup \{\alpha\}$ is D because L has no subgroup of order $5 \cdot 6$. It follows that the L-invariant sets $\mathcal{B}_i = B_i{}^G$ are disjoint and have $11 \cdot 12 = b(5,6,12)$ elements.

We verify that $\mathcal{B}_1$ or $\mathcal{B}_2$ is as required. Define $f_i = \mathcal{B}_i(X)$ and $f_i' = \mathcal{B}_i(X')$ with X and X' as above. Then the number of pairs (Z, B) with $B \in \mathcal{B}_i$ and Z a 5-subset of B, equals both $11 \cdot 12 \cdot f_i + 11 \cdot 12 \cdot 5f_i'$ and $11 \cdot 12 \cdot 6$. It follows that $f_i + 5f_i' = 6$. However, $f_1 + f_2 \leq 7$ because a 5-subset of Ω lies in only seven 6-subsets. Thus $f_i' \neq 0$ for some i, and then $f_i = f_i' = 1$.

By the way, if $L = L_2(11)$ and Ω is a $PGL_2(11)$-set, then both $\mathcal{B}_i$ are conjugate under $PGL_2(11)$, hence are (5,6,12)-systems on Ω. Q.E.D.

3.10. Assume the notation of 3.8 and 3.9 with $L \subseteq G = Aut(\mathcal{B}) \simeq M_{12}$. Let $H = G_\alpha \simeq M_{11}$. Then

(a) $N_G(E) = N_H(E) = ED$,
(b) $N_G(D)$ has order $5 \cdot 8$,
(c) $N_H(D)$ is a Frobenius group of order $5 \cdot 4$ fixing two blocks in $\mathcal{B}$,
(d) the groups L, H, and G are simple,
(e) L has a subgroup isomorphic to A_5,
(f) L acts transitively on some 11-set Λ, and then leaves a unique (4,5)-system on Λ invariant,
(g) $M_{11} \simeq H$ has a subgroup isomorphic to L,
(h) H acts transitively on some 12-set Δ, and then leaves a unique (5,6)-system on Δ invariant.

Proof. (a) follows from $|G| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$, $|G : N_G(E)| \equiv 1(11)$, and $C_G(E) = E$ (whence $|N_G(E) : E|$ divides 10). The same argument proves (b) and (c) because no $5'$-element $\neq 1$ of $C_G(D)$ fixes the two D-orbits of length 5, and D fixes exactly one of the $b(4, 5, 11) = 66$ blocks in $\mathcal{B}(\alpha)$.

For (d) note that a proper normal subgroup K of the group X in question satisfies $N_K(E) = K \cap ED = 1$ if $E \not\subseteq K$, and $X = N_X(E)K = DK$ (by the Frattini argument) if $E \subseteq K$. The second case contradicts $N_X(D) \neq C_X(D)$. In the first case, $|K| - 1$ is divisible by 11, but $|K|$ is not equal to 12. Define $(X_0, X_1, X_2, X_3) = (ED, L, H, G)$ and let $X = X_{i+1}$ with $i = 0$ or X_i simple. Then $K \cap X_i = 1$, hence $|K| \leq |X : X_i| = 12$, that is $|K| = 1$.

(e) Since $|G : L| = 12 \cdot 12 = 144$, G acts transitively on some 144-set Λ such that $G_\lambda = L$ for some $\lambda \in \Lambda$. Since $N_G(E) \subseteq L$, λ is the only fixed point of E, by Witt's Lemma. So if (e) is false, 3.8(e) implies that the length of any other L-orbit is divisible by $11 \cdot 5$ or $11 \cdot 6$, contrary to $2 \cdot 66 < 143$ and $3 \cdot 55 > 143$.

(f) Existence comes from (e) because $|L| = 60 \cdot 11$. Conversely, for any Λ, a one-point-stabilizer $A = L_\lambda$ is isomorphic to A_5 by 3.8(e). A Sylow 2- or 5-subgroup S of A satisfies $N_L(S) \subseteq A$, hence fixes no second point in Λ, by Witt's Lemma. Thus A is transitive on $\Lambda \setminus \{\lambda\}$, and the second part of 1.11 allows to apply 1.7(b).

(g) follows from (f) and implies existence in (h). Conversely, for any Δ, a one-point-stabilizer H_δ is of type $L_2(11)$ and (trivially) transitive on the 11-set $\Delta \setminus \{\delta\}$. Thus

(f) and the fact (from 1.11) that A in the proof of (f) leaves a unique (3,4)-system on $\Lambda \setminus \{\lambda\}$ invariant, allow to apply 1.7(b) again. Q.E.D.

Remarks. (i) By 3.10(b)(c), $N_G(D)/D$ is the direct product of the cyclic groups $N_H(D)/D$ and $C_G(D)/D$ of order 4 and 2. Thus $N_G(D)$ has only two Frobenius subgroups of order $5 \cdot 4$. Since $H = \langle E, N_H(D)\rangle$, it follows that all transitive subgroups $\simeq M_{11}$ are conjugate in G, that is those not conjugate to H. Similarly, because $N_G(D)$ has only two non-abelian subgroups of order 10, G has exactly two classes of subgroups of type $L_2(11)$, and H has only one. In particular, all groups of type $L_2(11)$ are isomorphic. Conjugacy of transitive subgroups $\simeq M_{11}$ will also follow from 4.5 and 4.7.

(ii) Our existence proof for $S(5,6,12)$ is a slight variation (avoiding explicit calculations) of what Carmichael suggests in section 115 of his book "Groups of Finite Order" (1937). He suggests an analogous procedure for $S(5,8,24)$, based on the transitive action of $L_2(23)$ on 24 points. We will follow a different line in 4.11. It gives the inclusion of $Aut(M_{12})$ in M_{24} as a by-result, and has the inclusion of $L_2(23)$ as a consequence.

(iii) From 1.10 and the isomorphism theorems of this section one easily obtains all sharply t-transitive finite permutation groups for $t \geq 4$. Proceeding by induction on t, one only has to show that in case $t = 4$ the degree v equals 4, 6, or 11.

(iv) As indicated in 1.12, 1.12(a)(b) suffices for this section. Indeed, it suffices to have $\ell_2(3,4,10) \leq 1$ in place of 3.2(a). Here is a direct proof for $\ell_2(3,4,10) \leq 1$: It suffices to show (in 3.1) that $\mathcal{B}(a')$ and $\mathcal{B}(a)$ determine $\mathcal{B}(\gamma)$ for any third point γ, say $\gamma = b$. Let

$$A'' = \begin{pmatrix} a' & a & c \\ x & y'' & z'' \\ u'' & v'' & w'' \end{pmatrix}$$

be the matrix describing $\mathcal{B}((b))$ relative to the non-collinear triple (a', a, x). Then

u'' = fourth point on the block through a', x, b $(= w)$,
w'' = fourth point on the block through a, x, b $(= w')$,
z'' = fourth point on the block through a, u'', b,
y'' = fourth point on the block through a', w'', b, and
v'' = fourth point on the block through a, y'', b.

(v) In accordance with the three possibilities for the matrix A' in 3.1, there are three types of non-collinear quadruples. Each type occurs, and (hence) $Aut(\mathcal{B})$ permutes the quadruples of each type sharply transitively.

§4. The automorphism group of M_{12}

$G^* = Aut(M_{12})$ has a normal subgroup $G = Inn(M_{12}) \simeq M_{12}$ and acts transitively on a set Ω^* such that $M_{11} \simeq G^*_\alpha \subseteq G$ for some $\alpha \in \Omega^*$, and there exists a G-invariant (5,6,12)-system $\mathcal{B}$ on the G-orbit $\Omega = \alpha^G$ of length 12.

The set of subgroups $H \simeq M_{11}$ in G is denoted by $\mathcal{H}$. By 3.10(h) some H is transitive on Ω, that is not conjugate to $G_1 = G_\alpha$.

4.1. For $j = 1, 2, 3, 4$ the stabilizer G_j of j points $\alpha, \beta, \dots$ is sharply $(5-j)$-transitive on the set Ω_j of the remaining points.

The global stabilizer N_j of $\Omega^j = \{\alpha, \beta, \dots\}$ is equal to $N_G(G_j)$, and N_j/G_j is sharply j-transitive on Ω^j, hence isomorphic to S_j.

Acting faithfully on $\mathcal{B}_j = \mathcal{B}((\Omega^j)) \in S(5-j, 6-j, 12-j, \Omega_j)$, and having the right order, N_j induces the full automorphism group on $\mathcal{B}_j$ for $j \leq 3$.

In particular, N_2 is isomorphic to $P\Gamma L_2(9)$ (by 3.4).

4.2. **Corollary.** (a) *G_3 is a Frobenius group of order $9 \cdot 8$.*

(b) *$Q = G_4$ has order 8 and contains only one involution.*

(c) *$N_G(Q)/Q \simeq S_4$ and $N_{G_1}(Q)/Q \simeq S_3$.*

(d) *G_2 has a normal subgroup $G_2' \simeq L_2(9) \simeq A_6$ of index 2.*

4.3. **Lemma.** (a) *G_2 is not isomorphic to S_6.*

(b) *If G_1 acts transitively on some 11-set, then G_2 fixes a point and (hence) G_1 is sharply 4-transitive.*

Proof. (a) Q contains only one involution and has index 2 in some Sylow 2-subgroup of G_2, whereas S_6 has an elementary subgroup of order 8.

(b) Otherwise G_2' has an orbit X of length 6 and five orbits of length 1 ($L_2(9)$ cannot act transitively on $11, 9, 8, 7, 5, 4, 3,$ *or* 2 *points*). This contradicts (a) because X is G_2-invariant. Q.E.D.

4.4. **Corollary** (of 4.3(b) and 1.10). *If G acts transitively on a 12-set Ω', with $G_{\alpha'} \in \mathcal{H}$ for $\alpha' \in \Omega'$, then G is sharply 5-transitive and leaves a unique $\mathcal{B}' \in S(5, 6, \Omega')$ invariant.*

G is block-transitive, and a set B of six points is a block if and only if $G_B \simeq S_6$.

4.5. **Theorem.** *$Aut(G)$ is transitive on $\mathcal{H}$.*

Proof. For each $H \in \mathcal{H}$ there exist Ω' and α' as in 4.4 such that $H = G_{\alpha'}$. Since $\mathcal{B}'$ is isomorphic to $\mathcal{B}$, there exists a monomorphism from G into $M = Aut(\mathcal{B})$ which maps $G_{\alpha'}$ into M_α. Apply this also to $\mathcal{B}$ and α in place of $\mathcal{B}'$ and α', and recall that $M \simeq M_{12} \simeq G$. Q.E.D.

4.6. **Lemma.** *For $E \subseteq G$ of order 11, $C_{G^*}(E) = E$.*

Proof. By 3.10, $C_G(E) = E$ and $N_G(E) = ED$ with D of order 5. Assume $E \subset V = C_{G^*}(E)$. Choose $d \neq 1$ in D. Then the $|V : C_V(d)|$-set $[V, d]$ of commutators $[v, d] = v^{-1}d^{-1}vd$ with $v \in V$ lies in $C_G(E) = E$. It follows that $U = C_V(d) = C_V(D)$ is not trivial. By 3.10, $C_G(D)$ is cyclic of order 10, hence lies in $K = C_G(U)$.

By Sylow's Theorem, $|X : Y| \equiv 1$ modulo 11 for all subgroups $X \supseteq Y \supseteq ED$ of G. So $|K : ED|$ equals 12 or $12 \cdot 12$ because $|G : ED| = 12 \cdot 12 \cdot 12$. In the first case K is of type $L_2(11)$, contrary to 3.8(d).

Hence $|K : ED| = 12 \cdot 12$ and $|[G, u]| = |G : C_G(u)| = |G : K| = 12$ for each $u \neq 1$ in U. Since $[G, u]$ is invariant under $C_G(u)$, hence under ED, the 11 non-identity elements in $[G, u]$ are conjugate under E, and one of them is centralized by D. Thus all the commutators $[g, u]$ with $g \in G$ and $u \in U$ lie in K. However, the subgroup $[G, U]$ generated by them is normal in G, contrary to simplicity of $G \simeq M_{12}$. Q.E.D.

4.7. **Theorem.** *We have $|G^* : G| = 2$, $N_{G^*}(G_1) \subseteq G$, and G^* is transitive on $\mathcal{H}$.*

Proof. Since $|N_G(E) : E| = 5$ and $G^* = N_{G^*}(E)G$ by the Frattini argument, this follows from 4.5 and 4.6 because G is not transitive on $\mathcal{H}$. Q.E.D.

4.8. **Corollary.** (a) *There is exactly one G-orbit $\Omega' \neq \Omega$ in Ω^*.*

(b) *For (each) $f \in G^* \setminus G$ and $\mathcal{B}'$ as in 4.4 we have $\Omega' = \Omega^f$ and $\mathcal{B}' = \mathcal{B}^f$.*

(c) *Furthermore, G_1^f is transitive on Ω, and (hence) $G_1^f \cap G_1$ is of type $L_2(11)$.*

4.9. **Lemma.** *Each 4-subset of Ω is fixed elementwise by exactly one involution in G. The set J of these involutions has (therefore) $\binom{12}{4}$ elements and is invariant under G^* (whence $|\Omega'_t| = 4$ for each $t \in J$).*

Proof. $Q = G_4$ has only one involution by 4.2(b). Let $Q \simeq P \subseteq G$. Then the involution t in P is trivial on each P-orbit of length $< |P| = 8$. Thus one P-orbit has length 8, and the remaining four points in Ω are fixed by t. Q.E.D.

4.10. **Lemma.** *For each block $B \in \mathcal{B}$,*

(a) *$C = \Omega \setminus B \in \mathcal{B}$ and $L = G_B = G_C \simeq S_6$,*

(b) *L has a unique orbit $F = F(B)$ of length 2 in $\Omega^*(itliesin\Omega')$,*

(c) $F = F(A)$ *with* $A \in \mathcal{B}$ *implies* $A \in \{B, C\}$,
(d) $t \in G_F$ *with* Ω_t *not empty implies* $t \in L$,
(e) $|(A \cup F(A)) \cap (B \cup F)| \geq 5$ *implies* $A = B$,
(f) $|\Omega_t^* \cap (B \cup F)| \leq 4$ *for* $t \in J$, J *as in* 4.9, *and*
(g) $|\Omega_s \cap \Omega_t| \leq 2$ *for distinct* $s, t \in J$ *fixing* F *elementwise.*

Proof. The last assertion of 4.4 yields (a). The subgroup $M = G_2' \simeq L_2(9) \simeq A_6$ of $G_2 \subseteq G_1$ does not fix two points in Ω' because otherwise M^f $(f \in G^* \setminus G)$ were conjugate to M in G, contrary to 4.8(c). Hence Ω' has two M-orbits of length 6, say U and $V = \Omega' \setminus U$. Since M has order $6!/2$ and index 4 in $N = N_2 = N_G(M)$, it follows that U and V are interchanged by N and fixed by some subgroup $S \simeq S_6$ of index 2 (G_U is faithful on U). Then U is a block in the unique G-invariant $\mathcal{B}' \in S(5, 6, \Omega')$, hence conjugate to B by some $f \in G^* \setminus G$, and this completes the proof of (b) because $S = G_U$ leaves $\{\alpha, \beta\}$ invariant and is distinct from G_2 by 4.3(a).

The subgroup $L_0 \simeq A_6$ of L is the unique subgroup of index 4 in $G_F \simeq N_2$, and the only L_0-orbits in Ω are B and C. This yields (c), and for (d) note that t cannot interchange B and C.

Let $Y = A \cap B$ in (e). The case $|Y| \geq 5$ is trivial, also the case $|Y| = 3$ because then $F = F(A)$. Assume $|Y| = 4$. There still exists $x \in F \cap F(A)$. By 4.9, a unique involution $t \in G$ fixes Y elementwise. Since L induces $Sym(B)$ on B, t lies in L, but (as a transposition on B) not in L_0. Hence $\{x, x^t\}$ equals F and by symmetry also $F(A)$.

Let $Y = \Omega_t \cap B$ in (f). If $|Y| = 4$, then as above t does not fix a point in F. If $|Y| = 3$ and t fixes F elementwise, then $t \in L_0$ by (d), a contradiction because $Y \subseteq B_t$ implies t is a transposition on B.

Let $Y = \Omega_s \cap \Omega_t$ in (g) and assume $|Y| = 3$. Again s and t lie in L_0, and $\langle s, t\rangle$ is dihedral of order 6 by 4.2(a). Action on B and C shows that $|B \cap Y| \neq 2, 3$ and $|C \cap Y| \neq 2, 3$, a contradiction. Q.E.D.

4.11. **Theorem.** $G^* = Aut(M_{12})$ *leaves a Steiner system* $\mathcal{B}^*$ *of type* $(5, 8, 24)$ *on* Ω^* *invariant, namely* $\mathcal{B}^* = \mathcal{B}_1 \cup \mathcal{B}_2$ *where* $\mathcal{B}_1$ *is the set of all* 8*-sets* $B \cup F(B)$, *with* $B \in \mathcal{B} \cup \mathcal{B}'$ *and* $F(B)$ *defined by* 4.10(b) *and* $\mathcal{B}_2$ *is the set of all* 8*-sets* Ω_t^*, *with* $t \in J$, J *as in* 4.9.

Proof. From $|\mathcal{B}_1| = |\mathcal{B}| + |\mathcal{B}'| = 2 \cdot b(5, 6, 12) = 4 \cdot 66$ and $|\mathcal{B}_2| = |J| = \binom{12}{4} = 11 \cdot 5 \cdot 9$ we get $|\mathcal{B}^*| = |\mathcal{B}_1| + |\mathcal{B}_2| = 11 \cdot 3 \cdot (8+15) = b(5, 8, 24)$. So by 1.1 it suffices to verify $|\mathcal{B}^*(X)| \leq 1$ for each 5-set $X \subseteq \Omega$. Without loss, $|X \cap \Omega| \geq 3$. Thus 4.10(e)(f)(g) does the job. Note that the condition about F in (g) means no loss of generality because G is doubly transitive on Ω'. Q.E.D.

4.12. **Corollary.** *Assume (what will be shown in* 8.2) *that* $M = Aut(\mathcal{B}^*)$ *has order* $24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$. *Then* M *has a subgroup isomorphic to* $L_2(23)$, *and all these subgroups are conjugate.*

Proof. Regard G^* as a subgroup of M. A subgroup $L \simeq L_2(23)$ of $S = Sym(\Omega^*)$ is generated by a subgroup P of order 23, a subgroup $E \subseteq N_S(P)$ of order 11, and an involution $t \in N_L(E)$. Let $P \subseteq M$. Then $|N_M(P)| = 23{\cdot}11$ and (hence) $E \subseteq M$ because $|M : N_M(P)| \equiv 1(23)$ and $|N_S(P) : PE| = 2$. Let $E \subseteq G$. Then 4.6 yields an involution $f \in G^* \setminus G$ which inverts E (recall that $|N_G(E)| = 11 \cdot 5$). Interchanging Ω and Ω', f is fixed-point-free on $\Omega^* = \Omega \cup \Omega'$. However, because $|\Omega^*_E| = 2$, the elements of Et are the only fixed-point-free involutions of S which invert E (the product of any two such involutions x, y centralizes E, is inverted by x and y, and leaves the two fixed points of E and the two orbits of length 11 invariant). Q.E.D.

§5. Steiner systems of type (2,5,21)

5.1. Assume $\mathcal{B} \in S(2, 5, 21, \Omega)$ and $L \in \mathcal{B}$. By 2.1, $\mathcal{B}$ is a projective plane of order 4. For each line X of the affine plane $\mathcal{B}^L$ of order 4 defined in 2.1 there is a unique point $p = p(X)$ in L such that $X \cup \{p\} \in \mathcal{B}$, and a line Y is parallel to X if and only if $p(X) = p(Y)$.

Thus each isomorphism from $\mathcal{B}^L$ on a similar affine plane $\hat{\mathcal{B}}^{\hat{L}}$ extends uniquely to an isomorphism from $\mathcal{B}$ on $\hat{\mathcal{B}}$. Since $\mathcal{B}$ has 21 blocks, and by 2.4 there are $16 \cdot 15 \cdot 24$ isomorphisms between any two affine planes of order 4, it follows that all projective planes of order 4 are isomorphic and $Aut(\mathcal{B})$ has order $21 \cdot 16 \cdot 15 \cdot 24$.

5.2. More precisely, $G = Aut(\mathcal{B})$ is block-transitive and the block stabilizer G_L is sharply transitive on the set of regular quadruples (a, b, c, x) of $\mathcal{B}^L$ in the sense of 2.4.

So if a subgroup $T \neq 1$ of G_L fixes a block $B \neq L$ elementwise, then $\Omega_T \subseteq L \cup B$ and hence B is unique.

5.3. Assume a subgroup $T \subseteq G$ of order 2 fixes a block B elementwise. Then T fixes no additional point α.

Proof. Otherwise a second point $\beta \in \Omega \setminus B$ is fixed by T because $|\Omega \setminus B| = 16$ is even. By 5.2, β lies in each of the five blocks $L = \langle \alpha, \lambda \rangle$ $(\lambda \in B)$, a contradiction. Q.E.D.

5.4. Using the description of $\mathcal{B}^L$ by a 4×4-matrix $A = (ij)$ in 2.4, based on a regular quadruple $(a, b, c, x) = (11, 12, 13, 21)$, we get the following list of blocks:

H_1 : 11 12 13 14 h	V_1 : 11 21 31 41 v	L : $h\ v\ u\ t\ s$
H_2 : 21 22 23 24 h	V_2 : 12 22 32 42 v	
H_3 : 31 32 33 34 h	V_3 : 13 23 33 43 v	
H_4 : 41 42 43 44 h	V_4 : 14 24 34 44 v	
U_1 : 11 22 33 44 u	T_1 : 11 23 34 42 t	S_1 : 11 24 32 43 s
U_2 : 12 21 34 43 u	T_2 : 12 24 33 41 t	S_2 : 12 23 31 44 s
U_3 : 13 24 31 42 u	T_3 : 13 21 32 44 t	S_3 : 13 22 34 41 s
U_4 : 14 23 32 41 u	T_4 : 14 22 31 43 t	S_4 : 14 21 33 42 s

§6. Steiner systems of type (3,6,22)

Although a little less straightforward, this section is totally analogous to the first part of section 3.

6.1. Let $\mathcal{B} \in S(3,6,22,\Omega)$. We begin with a sequence (call it regular)

$$q = (a', L, a, b, c, x)$$

such that $a' \in L \in \mathcal{B}$ and a, b, c, x are non-collinear points outside L, with a', a, b, c however collinear.

Existence of q is quite obvious. Actually, for any four non-collinear points a', a, b, x there exists a block $L \in \mathcal{B}(a')$ containing none of them, because

$$|\mathcal{B}(a')| = 21 > 5 + 5 + 5 = |\mathcal{B}(a'a)| + |\mathcal{B}(a', b)| + |\mathcal{B}(a', x)|;$$

then choose the fifth point c in $\langle a', a, b\rangle$ outside L.

We apply 5.4 to $\mathcal{B}((a')) \in S(2,5,21)$ and get a matrix

$$A = \begin{pmatrix} 11 & 12 & 13 & 14 \\ 21 & 22 & 23 & 24 \\ 31 & 32 & 33 & 34 \\ 41 & 42 & 43 & 44 \end{pmatrix} = \begin{pmatrix} a & b & c & 14 \\ x & 22 & 23 & 24 \\ 31 & 32 & 33 & 34 \\ 41 & 42 & 43 & 44 \end{pmatrix}$$

and points $h, v, u, t, s \in L$ such that the blocks in $\mathcal{B}(a')$ are given by the list in 5.4 (add a' everywhere). The blocks H_1, V_1, U_1, T_1, S_1 constitute $\mathcal{B}(a, a')$ and are also denoted by H, V, U, T, S. Note that

$$H = h\ a'\ a\ b\ c\ 14 \quad \text{and} \quad V = v\ a'\ a\ x\ 31\ 41.$$

It follows that the sequence $q' = (a, L', a', b, c, x)$ with $L' = \langle a, h, v\rangle$ is regular too. It yields an analogous description of $\mathcal{B}(a)$ involving a matrix

$$A' = \begin{pmatrix} 11' & 12' & 13' & 14' \\ 21' & 22' & 23' & 24' \\ 31' & 32' & 33' & 34' \\ 41' & 42' & 43' & 44' \end{pmatrix} = \begin{pmatrix} a' & 12 & 13 & 14 \\ 21 & 22' & 23' & 24' \\ 31' & 32' & 33' & 34' \\ 41' & 42' & 43' & 44' \end{pmatrix}$$

and points $h', v', u', t', s' \in L'$. We have $h' = h$, $v' = v$, and $31\ 41 = 31'\ 41'$.

The fact that q'' equals q constitutes a useful symmetry in our situation.

6.2. Since $\mathcal{B}(a, a')$ also consists of $H' = H$, $V' = V$, U', T' and S', it follows that

$$\{U, T, S\} = \{U', T', S'\}$$

and that $X'_i \neq Y_j$ for any two letters X, Y among H, V, U, T, S and any two numbers i, j among 1, 2, 3, 4 not both 1.

6.3. Since $L' \cap L = h\ v = h'\ v'$, each of u', t', s' equals some ij ($i, j \in \{2, 3, 4\}$). No two of them lie in the same row or column of the matrix A.

Otherwise the block H_i or V_j corresponding to that row or column would have three points in common with L', namely those two plus h or v.

6.4. **Lemma.** *We have* $31' = 31$ *and* $41' = 41$.

Proof. Assume this key result is false, that is $31' = 41$ and $41' = 31$. Then $U'_4 \cap T_4 = 14\ 31$, $U'_3 \cap S_3 = 13\ 41$, and $S'_2 \cap T_2 = 12\ 41$. This implies

$$u' \neq 22, 43, 34 \qquad \text{and} \qquad s' \neq 24, 33$$

as well as $t \neq 23', 32', 44'$ and $s \neq 42'$, hence, by symmetry,

$$t' \neq 23, 32, 44 \qquad \text{and} \qquad s' \neq 42.$$

The remaining possibilities for u', t', and s' are listed in the three tables below. They contain also the corresponding values for U', T', and S' which follow from 6.2. The addition $[t']$ for example to the value $u' = 32$ means that in this case a look at t' immediately yields a contradiction: Indeed, the values 24 and 43 for t' violate $U' \neq T'$, and the remaining values 22, 33, 34, 42 violate 6.3.

u' :	$33[s']$	$44[t']$	$23[t']$	$42[s']$	$24[s']$	$32[t']$
U' :	U	U	T	T	S	S
t' :	22	33	34	42	24	43
T' :	U	U	T	T	S	S
s' :	22	44	23	34	32	43
S' :	U	U	T	T	S	S

Q.E.D.

6.5. **Lemma.** *We have $U' = U$, $T' = T$, and $S' = S$, that is*

$$u'\ 22'\ 33'\ 44' = u\ 22\ 33\ 44, \qquad t'\ 23'\ 34'\ 24' = t\ 23\ 34\ 24,$$

and $$s'\ 24'\ 32'\ 43' = s\ 24\ 32\ 43.$$

Proof. This is now very easy. From $U_2' \cap U_2 = 12\ 21$, $U_3' \cap U_3 = 13\ 31$, and $U_4' \cap U_4 = 14\ 41$ it follows that u' is distinct from 34, 43, 24, 42, 23, and 32, hence equal to 22, 33, or 44. This implies $U' = U$ by 6.2, and the same argument, now exploiting the intersections $T_i' \cap T_i$ $(i = 2, 3, 4)$, yields $T' = T$. Q.E.D.

6.6. Obviously, only three possibilities for (u', t', s') are compatible with 6.3 and 6.5, and analogously for (u, t, s):

u'	t'	s'	u	t	s
22	34	43	$22'$	$34'$	$43'$
33	42	24	$33'$	$42'$	$24'$
44	23	32	$44'$	$23'$	$32'$

Moreover, $u' = nn$ implies $u = nn'$:

To prove this addition, assume first the case $u' = 22$. Then $U_4' \cap T_4 = 14\ 22$ and hence $t \neq 23'$. Also, $U_3' \cap S_3 = 13\ 22$ and hence $s \neq 24'$. Thus the second table leaves only the case $(u, t, s) = (22', 34', 43')$.

By symmetry, $u = 22'$ implies $u' = 22$. So to complete the proof it suffices to verify $s \neq 32'$ in case $u' = 33$, and this follows from $U_4' \cap S_4 = 14\ 33$.

6.7. **Theorem.** *The matrix $A' = (ij')$ is one of the following:*

$$\begin{pmatrix} 11 & 12 & 13 & 14 \\ 21 & u & 42 & 32 \\ 31 & 24 & 44 & t \\ 41 & 23 & s & 33 \end{pmatrix} \begin{pmatrix} 11 & 12 & 13 & 14 \\ 21 & 44 & 34 & s \\ 31 & 43 & u & 23 \\ 41 & t & 32 & 22 \end{pmatrix} \begin{pmatrix} 11 & 12 & 13 & 14 \\ 21 & 33 & t & 43 \\ 31 & s & 22 & 42 \\ 41 & 34 & 24 & u \end{pmatrix}$$

Proof. Apply 6.4, 6.5, 6.6, and the fact that $ij' \neq ij$ for all $i, j \in \{2,3,4\}$ (otherwise $H_i = \langle h, i1, ij\rangle = H_i'$). Q.E.D.

6.8. **Corollary.** *In accordance with the three cases of* 6.7,

$$\langle a,b,x\rangle \setminus \{a,b,x\} = U_2' \setminus \{11,12,21\} = \{34', 43', u'\}$$

equals one of the pairwise disjoint sets t s 22, 23 32 33, *and* 42 24 44.

6.9. **Corollary.** *If* $\mathcal{B}_2 \in S(3,6,\Omega)$ *satisfies* $\mathcal{B}_2(a') = \mathcal{B}(a')$ *and* $B_1 \cap B_2 \supset \{a,b,x\}$ *for some* $B_2 \in \mathcal{B}_2$ *and* $B_1 \in \mathcal{B}$, *then* $\mathcal{B}_2(a) = \mathcal{B}(a)$.

Proof. Apply all the above to $\mathcal{B}_2$ in place of $\mathcal{B}$, relative to the same regular sequence (a', L, a, b, c, x), hence the same matrix A. Again, the matrix A_2' analogous to A' is one of the three in 6.7, and the non-disjoint sets $B_1 \setminus \{a,b,x\}$ and $B_2 \setminus \{a,b,x\}$ are among the three sets listed in 6.8, hence are equal. This means $A_2' = A'$, that is $\mathcal{B}_2(a) = \mathcal{B}(a)$. Q.E.D.

6.10. **Lemma.** (a) *Condition* 1.12(**)(3, 6, 22) *holds.*
(b) *We have* $\ell'(3,6,22) \leq 3$.

Proof. (a) Write $\mathcal{B}$ for $\mathcal{B}_1$, a' for α, and a for $\beta \in B_1 \cap B_2$. Choose further points b and x in $B_1 \cap B_2$. Then a', a, b, x are not collinear because $a' \notin B_i$. Thus q as in 3.1 exists, and we can apply 6.9.

(b) Recall that any two points can play the role of a' and a in 3.1. Thus (b) means that in 3.1, once $\mathcal{B}(a')$ is given, that is A is given, there are at most three possibilities for $\mathcal{B}(a)$, that is for A'. Now apply 6.7. Q.E.D.

6.11. **Lemma.** *Let W be the pointwise stabilizer in $G = Aut(\mathcal{B})$ of a block B. Then $W_\alpha = 1$ for all $\alpha \in \Omega \setminus B$. In particular, $|W|$ divides 16, the order of any three-point-stabilizer divides* $16 \cdot 6$, *and (hence)* $|G|$ *divides* $22 \cdot 21 \cdot 20 \cdot 16 \cdot 6$.

Proof. Assume $T \subseteq W_\alpha$ has prime order p. The 15 2-sets X of the 6-set B yield 15 T-invariant blocks $\langle X, \alpha\rangle$. Only two of them may lie in Ω_T, by 5.2 applied to $\mathcal{B}((\alpha))$. Thus Ω has 13 T-orbits of length p, a contradiction. Q.E.D.

6.12. **Theorem.** *All Steiner systems of type* $(3,6,22)$ *are isomorphic, and their automorphism group has order* $22 \cdot 21 \cdot 20 \cdot 16 \cdot 6$.

Proof. Recall from 5.1 that Steiner systems of type (2,5,21) are isomorphic and have $g' = 21 \cdot 20 \cdot 16 \cdot 6 \cdot 3$ automorphisms. By 6.10 and 1.12(e) we have $\ell(3,6,22) \leq 3$. This together with 6.11 allows to apply 1.6 with $n = 3$. Q.E.D.

6.13. **Corollary.** (a) *$G = Aut(\mathcal{B})$ is 3-transitive on Ω, and the stabilizer of three points has order* $16 \cdot 6$.

(b) *G is block-transitive, and the stabilizer $H = G_B$ of a block B is 3-transitive $(actually 6-transitive by(c))$ on B, and has order* $6{\cdot}5{\cdot}4{\cdot}16{\cdot}6 = 6! \cdot 16$.

(c) *W as in* 6.11 *has order* 16, *and H/W is isomorphic to S_6.*

(d) *A subgroup $D \subseteq H$ of order* 5 *fixes exactly two points and two (disjoint) blocks.*

(e) *D satisfies $C_H(D) = 1$, $|N_H(D)| = 5 \cdot 4$, $|N_G(D)| = 5 \cdot 8$, the involution s in $C_G(D)$ interchanges the two D-invariant points and blocks, and s has (therefore) no fixed-point.*

(f) *W is elementary abelian, sharply transitive on $\Omega \setminus B$, and equal to $C_G(W)$.*

(g) *If $E \subseteq G$ has order* 11, *then $N_G(E)$ is a Frobenius group of order* $11 \cdot 10$ *transitive on Ω.*

For (g) note that $|C_G(E) : E| \leq 2$, $|G : N_G(E)| \equiv 1(11)$, and in case $s \in C_G(E)$ also $|C_G(s) : N_G(E)| \equiv 1 \equiv |G : C_G(s)|$ modulo $11 \cdot 5$.

6.14. **Corollary.** *$G = Aut(\mathcal{B})$ has a subgroup isomorphic to $PGL_2(11)$, and all these subgroups are conjugate.*

Proof. Analogous to 4.12. A subgroup $L \simeq PGL_2(11)$ of $S = Sym(\Omega)$ is generated by a transitive Frobenius subgroup F of order $11 \cdot 10$, and an involution t which inverts a subgroup $D^* \subseteq F$ of order 10 and fixes the two D^*-orbits of length 10 as well as the two remaining points.

By 6.13(g), F is conjugate in S to a subgroup of G. Let $F \subseteq G$. By 6.13(e), G contains an involution like t. Obviously, the product of any two such involutions in S lies in D^*. Q.E.D.

§7. The Isomorphism Theorem for S(4,7,23)

7.1. Let $B \in \mathcal{B} \in S(4, 7, 23, \Omega)$ and $G = Aut(\mathcal{B})$. First we show that the order of the stabilizer of any four points (without loss in B) divides $16 \cdot 3$, and (hence) $|G|$ divides $23 \cdot 22 \cdot 21 \cdot 20 \cdot 16 \cdot 3$.

By 6.11, that order k divides $16 \cdot 6$. So if the assertion is false, then some subgroup $T \subseteq G_B$ of order 2 fixes a 5-set $X \subseteq B$ elementwise, and also some α in the 16-set $\Omega \setminus B$. This contradicts 5.3, applied to $\mathcal{B}((B \setminus X))$.

7.2. **Theorem.** *All Steiner systems of type $(4, 7, 23)$ are isomorphic and their automorphism group has order* $23 \cdot 22 \cdot 21 \cdot 20 \cdot 16 \cdot 3$.

Proof. We have $\ell(4,7,23) \leq 3$ by 6.10 and 1.12(e). This together with 7.1 allows to apply 1.6 with $n = 2$. Q.E.D.

7.3. **Corollary** (by 6.13). (a) *G is 4-transitive on Ω, and the stabilizer of four points has order* $16 \cdot 3$.

(b) *G is block-transitive, and the stabilizer $H = G_B$ of a block B is 4-transitive* (*actually* 5*-transitive by* (c)) *on B of order* $7 \cdot 6 \cdot 5 \cdot 4 \cdot 16 \cdot 3 = 16 \cdot 7!/2$.

(c) *The pointwise stabilizer W of B is sharply transitive on $\Omega \setminus B$, and H/W is isomorphic to A_7.*

(d) *W equals $C_G(W)$ and is elementary abelian of order* 16.

§8. The Isomorphism Theorem for $S(5,8,24)$

8.1. **Lemma.** *We have $\ell(5,8,24) \leq 1$.*

Proof. Let Ω be a 24-set, $\alpha \in \Omega$, $\mathcal{B}' \in S(4,7,\Omega \setminus \{\alpha\})$, and

$$\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_m\} = \{\mathcal{B} \in S(5,8,\Omega) \mid \mathcal{B}((\alpha)) = \mathcal{B}'\}.$$

The claim is $m \leq 1$. By 6.10 and 1.12(e) we have $\ell(5,8,24) \leq 3$, that is $m \leq 3$. Thus each $\mathcal{B}_i$ is fixed by any subgroup $D \subseteq Sym(\Omega)$ of order 5 which fixes α and $\mathcal{B}'$. Such a D exists because $|Aut(\mathcal{B}')|$ is divisible by 5 (Theorem 7.2).

Since $|\mathcal{B}'| = b(4,7,23) = 23 \cdot 11 \equiv 3(5)$ and $|\Omega_D| = 4$, some D-orbit $X \subseteq \Omega$ of length 5 is not contained in a block of $\mathcal{B}'$. The block $B_i \in \mathcal{B}_i$ which contains X is D-invariant, and hence contains 3 fixed points of D. This implies $|B_i \cap B_j| > 5$ for all i, j, hence $\mathcal{B}_i = \mathcal{B}_j$ because $(t,k,v) = (5,8,24)$ satisfies 1.12(*), again by 6.10 and 1.12(e). Q.E.D.

8.2. **Theorem.** *All Steiner systems of type* $(5,8,24)$ *are isomorphic and their automorphism group has order* $24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 16 \cdot 3$.

Proof. By 8.1 and 7.2, 1.6 applies with $n = 1$. Q.E.D.

Remark. $S(5,8,24)$ is not empty by 4.11. From 8.2 and 7.3 the corollary analogous to 7.3, with $A_8 \simeq H/W$ in place of A_7, follows immediately. Faithful action on W shows that A_8 is isomorphic to $L_4(2)$.

Math. Seminar
Universität Kiel
24098 Kiel
Germany

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 279–288

Rationally Determined Group Modules

Everett C. Dade

Abstract.

Green's correspondence of group modules finds its simplest expression when a finite multiplicative group $G$ has a trivial intersection Sylow $p$-subgroup $P$, for some prime $p$. Then it is between all isomorphism classes of projective-free $\mathbf{R}G$-lattices $\mathbf{L}$ and all isomorphism classes of projective-free $\mathbf{R}N$-lattices $\mathbf{K}$, where $\mathbf{R}$ is a suitable valuation ring and $N$ is the normalizer of $P$ in $G$. In that case we show in Theorem 3.2 below that the $\mathbf{R}G$-lattice $\mathbf{L}$ is determined by its associated lattices over the residue field and field of fractions of $\mathbf{R}$ if and only if $\mathbf{K}$ has this same property. By Theorem 3.7 some important $\mathbf{R}G$-lattices $\mathbf{L}$ have this property of being "rationally determined." So it would be worthwhile to see if the $\mathbf{R}N$-lattices with this property (and perhaps with other properties preserved by this Green correspondence) could be classified.

§1. Projective-Free Lattices

Let $\mathbf{S}$ be any principal ideal domain. As usual, an $\mathbf{S}$-*order* $\mathbf{O}$ is just an associative $\mathbf{S}$-algebra with identity element $1 = 1_{\mathbf{O}}$ such that $\mathbf{O}$ is free of finite rank when considered as an $\mathbf{S}$-module. When we speak of an $\mathbf{O}$-*lattice* $\mathbf{L}$ we mean a unitary right $\mathbf{O}$-module such that $\mathbf{L}$ is also free of finite rank as an $\mathbf{S}$-module. Of course, a *homomorphism* $\phi\colon \mathbf{L} \to \mathbf{K}$ of $\mathbf{O}$-lattices is just a homomorphism between $\mathbf{O}$-modules $\mathbf{L}$ and $\mathbf{K}$ which are $\mathbf{O}$-lattices. We write any such $\phi$ on the left, so that it sends any $l \in \mathbf{L}$ to $\phi(l) \in \mathbf{K}$.

In the special case where the principal ideal domain $\mathbf{S}$ is a field, an $\mathbf{S}$-order is just a finite-dimensional associative $\mathbf{S}$-algebra $\mathbf{O}$ with identity element. Furthermore, an $\mathbf{O}$-lattice is just a unitary right $\mathbf{O}$-module $\mathbf{L}$ which is finite-dimensional as a vector space over $\mathbf{S}$.

This research was supported by grant number DMS 96-00106 and by grant number DMS 99-70030, both from the National Science Foundation.

Received May 29, 1999.

Revised May 18, 2000.

Throughout this note we fix a finite group G and a prime p. We also fix $\mathbf{R}$, $\mathbf{p}$, $\mathbf{F}$ and $\overline{\mathbf{F}}$ satisfying

(1.1) $\mathbf{R}$ *is a local principal ideal domain* (*i.e., a real discrete valuation ring*) *with unique maximal ideal* $\mathbf{p}$, *such that the field of fractions* $\mathbf{F}$ *of* $\mathbf{R}$ *is a splitting field of characteristic zero for every subgroup of* G, *and the residue class field* $\overline{\mathbf{F}} = \mathbf{R}/\mathbf{p}$ *of* $\mathbf{R}$ *has characteristic* p.

Notice that each of $\mathbf{R}$, $\mathbf{F}$ and $\overline{\mathbf{F}}$ is a principal ideal domain $\mathbf{S}$, to which all the above definitions apply. Furthermore, the group algebra $\mathbf{S}H$ over $\mathbf{S}$ of any subgroup H of G is an $\mathbf{S}$-order. The following result says that $\mathbf{S}H$-lattices have the Krull-Schmidt property.

Proposition 1.2. *Suppose that* $\mathbf{S}$ *is either* $\mathbf{F}$, $\overline{\mathbf{F}}$ *or* $\mathbf{R}$, *and that* H *is any subgroup of* G. *Then any* $\mathbf{S}H$*-lattice* $\mathbf{L}$ *is isomorphic to a finite direct sum* $\mathbf{L}_1 \oplus \cdots \oplus \mathbf{L}_l$ *of indecomposable* $\mathbf{S}H$*-lattices* $\mathbf{L}_i$. *Furthermore, this direct sum is uniquely determined to within order and isomorphisms by the* $\mathbf{S}H$*-lattice* $\mathbf{L}$, *i.e., if* $\mathbf{L}$ *is also isomorphic to a finite direct sum* $\mathbf{K}_1 \oplus \cdots \oplus \mathbf{K}_k$ *of indecomposable* $\mathbf{S}H$*-lattices* $\mathbf{K}_i$, *then* $k = l$ *and there is some permutation* π *of* $1, 2, \ldots, k$ *such that* $\mathbf{K}_i$ *is* $\mathbf{S}H$*-isomorphic to* $\mathbf{L}_{\pi(i)}$ *for* $i = 1, 2, \ldots, k$.

Proof. When $\mathbf{S}$ is a field $\mathbf{F}$ or $\overline{\mathbf{F}}$, this is the usual Krull-Schmidt Theorem for the finite-dimensional $\mathbf{S}$-algebra $\mathbf{S}H$. When $\mathbf{S}$ is $\mathbf{R}$, its field of fractions $\mathbf{F}$ is a splitting field of characteristic zero for the finite group H by (1.1). So $\mathbf{F}H$ is a split, semi-simple algebra of finite dimension over $\mathbf{F}$. Since $\mathbf{R}H$ is an $\mathbf{R}$-order spanning $\mathbf{F}H$ over $\mathbf{F}$, the basic hypotheses [1, 4.1] and [1, 4.2] of [1, §4] are satisfied by $\mathbf{D} = \mathbf{R}H$. The proposition for $\mathbf{S} = \mathbf{R}$ now holds by [1, 4.7]. Q.E.D.

In the situation of the preceding proposition we follow Green [2] in saying that an $\mathbf{S}H$-lattice $\mathbf{K}$ *divides* an $\mathbf{S}H$-lattice $\mathbf{L}$ if $\mathbf{L}$ is isomorphic to the direct sum $\mathbf{K} \oplus \mathbf{M}$ of $\mathbf{K}$ and some $\mathbf{S}H$-lattice $\mathbf{M}$. We say that $\mathbf{L}$ is *projective-free* if the only projective $\mathbf{S}H$-lattice $\mathbf{P}$ dividing $\mathbf{L}$ is $\mathbf{P} = 0$. The Krull-Schmidt property implies that any $\mathbf{S}H$-lattice $\mathbf{L}$ is isomorphic to a direct sum $\mathbf{L}_{\text{pf}} \oplus \mathbf{L}_{\text{pr}}$ of a projective-free $\mathbf{S}H$-lattice $\mathbf{L}_{\text{pf}}$ and a projective $\mathbf{S}H$-lattice $\mathbf{L}_{\text{pr}}$, either or both of which could be zero. Furthermore, these conditions determine both $\mathbf{L}_{\text{pf}}$ and $\mathbf{L}_{\text{pr}}$ to within $\mathbf{S}H$-isomorphisms. We call $\mathbf{L}_{\text{pf}}$ and $\mathbf{L}_{\text{pr}}$ the *projective-free part* and the *projective part*, respectively, of $\mathbf{L}$.

If $\mathbf{L}$ is an $\mathbf{R}H$-lattice, then we denote by $\overline{\mathbf{L}}$ its *residual* $\overline{\mathbf{F}}H$-lattice

$$\overline{\mathbf{L}} = \mathbf{L}/(\mathbf{pL}).$$

We write $\eta_{\mathbf{L}}$ for the natural epimorphism of $\mathbf{L}$ onto its factor $\mathbf{R}H$-module $\overline{\mathbf{L}}$. When $\mathbf{L}$ is the regular $\mathbf{R}H$-lattice $\mathbf{R}H$, its residual $\overline{\mathbf{F}}H$-lattice $\overline{\mathbf{L}}$ can be identified with $\overline{\mathbf{F}}H$. In that case $\eta_{\mathbf{L}}$ is the natural epimorphism $\eta_{\mathbf{R}H}$ of $\mathbf{R}H$ onto $\overline{\mathbf{F}}H$ as $\mathbf{R}$-algebras.

Our hypotheses (1.1) allow us to lift projective lattices.

Lemma 1.3. *If* $\mathbf{Q}$ *is a projective* $\overline{\mathbf{F}}H$*-lattice, for some subgroup* H *of* G*, then there is some projective* $\mathbf{R}H$*-lattice* $\mathbf{P}$ *whose residual* $\overline{\mathbf{F}}H$*-lattice* $\overline{\mathbf{P}}$ *is isomorphic to* $\mathbf{Q}$*.*

Proof. The completion $\mathbf{R}^*$ of $\mathbf{R}$ is a local principal ideal domain with unique maximal ideal $\mathbf{p}^* = \mathbf{p}\mathbf{R}^*$. Since $\mathbf{F}$ is a splitting field of characteristic zero for H (see (1.1)), Heller's Theorem [4, 2.5] tells us that the map sending any $\mathbf{R}H$-lattice $\mathbf{L}$ to its completion $\mathbf{L}^*$ induces a bijection of the isomorphism classes of $\mathbf{R}H$-lattices onto those of $\mathbf{R}^*H$-lattices. Clearly any free $\mathbf{R}^*H$-lattice is the completion of a free $\mathbf{R}H$-lattice. Because completion preserves direct sums, we conclude that any projective $\mathbf{R}^*H$-lattice (i.e., any direct summand of a free $\mathbf{R}^*H$-lattice) is the completion of some projective $\mathbf{R}H$-lattice.

We may identify $\overline{\mathbf{F}} = \mathbf{R}/\mathbf{p}$ with the residue class field $\mathbf{R}^*/\mathbf{p}^*$ of $\mathbf{R}^*$. Since $\mathbf{R}^*$ is complete, there is some projective $\mathbf{R}^*H$-lattice $\mathbf{P}^*$ such that $\mathbf{P}^*/\mathbf{p}^*\mathbf{P}^*$ is isomorphic to the projective $\overline{\mathbf{F}}H$-lattice $\mathbf{Q}$. As we saw above, $\mathbf{P}^*$ is isomorphic to the completion of some projective $\mathbf{R}H$-lattice $\mathbf{P}$. Then $\overline{\mathbf{P}} = \mathbf{P}/\mathbf{p}\mathbf{P}$ is isomorphic to both $\mathbf{P}^*/\mathbf{p}^*\mathbf{P}^*$ and $\mathbf{Q}$ as an $\overline{\mathbf{F}}H$-lattice. Q.E.D.

Once we can lift projective $\overline{\mathbf{F}}H$-lattices to projective $\mathbf{R}H$-lattices, all the standard results about $\mathbf{p}$-adic lattices become available. As an example we have the following lemma from [5].

Lemma 1.4. *Suppose that* H *is a subgroup of* G*, that* $\mathbf{L}$ *is an* $\mathbf{R}H$*-lattice, and that* $\mathbf{Q}$ *is a projective* $\overline{\mathbf{F}}H$*-lattice dividing* $\overline{\mathbf{L}}$*. Then there is some projective* $\mathbf{R}H$*-lattice* $\mathbf{P}$ *such that* $\overline{\mathbf{P}}$ *is* $\overline{\mathbf{F}}H$*-isomorphic to* $\mathbf{Q}$*. Furthermore, any such* $\mathbf{P}$ *divides* $\mathbf{L}$*.*

Proof. Lemma 1.3 gives us some projective $\mathbf{R}H$-lattice $\mathbf{P}$ whose residual $\overline{\mathbf{F}}H$-lattice $\overline{\mathbf{P}}$ is isomorphic to $\mathbf{Q}$. Once we know that such a $\mathbf{P}$ exists, the rest of the proof of [5, Lemma 1] can be followed almost word for word to prove the rest of the present lemma. Q.E.D.

The preceding lemma allows us to characterize both projective and projective-free $\mathbf{R}H$-lattices by their residuals.

Proposition 1.5. *Let* H *be any subgroup of* G*, and* $\mathbf{L}$ *be any* $\mathbf{R}H$*-lattice. Then* $\mathbf{L}$ *is projective or projective-free if and only if its residual* $\overline{\mathbf{F}}H$*-lattice* $\overline{\mathbf{L}}$ *is respectively projective or projective-free.*

Proof. If the finitely-generated $\mathbf{R}H$-module $\mathbf{L}$ is projective, then it divides the direct sum $(\mathbf{R}H)^n$ of n copies of the regular $\mathbf{R}H$-module $\mathbf{R}H$, for some integer $n > 0$. It follows that $\overline{\mathbf{L}}$ divides the direct sum $(\overline{\mathbf{F}}H)^n$ of n copies of $\overline{\mathbf{F}}H$. So $\overline{\mathbf{L}}$ is a projective $\overline{\mathbf{F}}H$-lattice.

Conversely, if $\overline{\mathbf{L}}$ is $\overline{\mathbf{F}}H$-projective, then Lemma 1.4 with $\mathbf{Q} = \overline{\mathbf{L}}$ gives us some projective $\mathbf{R}H$-lattice $\mathbf{P}$ dividing $\mathbf{L}$ such that $\overline{\mathbf{P}}$ is $\overline{\mathbf{F}}H$-isomorphic to $\overline{\mathbf{L}}$. This can only happen when $\mathbf{L} \simeq \mathbf{P}$ is projective. Thus $\mathbf{L}$ is projective if and only if $\overline{\mathbf{L}}$ is projective.

If some non-zero projective $\mathbf{R}H$-lattice $\mathbf{P}$ divides $\mathbf{L}$, then its residual $\overline{\mathbf{F}}H$-lattice $\overline{\mathbf{P}}$ is non-zero and divides $\overline{\mathbf{L}}$. We saw above that $\overline{\mathbf{P}}$ is projective. Hence $\overline{\mathbf{L}}$ is not projective-free whenever $\mathbf{L}$ is not projective-free.

Conversely, suppose that some non-zero projective $\overline{\mathbf{F}}H$-lattice $\mathbf{Q}$ divides $\overline{\mathbf{L}}$. Then Lemma 1.4 gives us some projective $\mathbf{R}H$-lattice $\mathbf{P}$ dividing $\mathbf{L}$ such that $\overline{\mathbf{P}} \simeq \mathbf{Q} \neq 0$. Evidently $\mathbf{P}$ is not zero. Thus $\mathbf{L}$ is not projective-free if and only if $\overline{\mathbf{L}}$ is not projective-free. Q.E.D.

Another consequence of Lemma 1.4 is the standard correspondence between projective $\mathbf{R}H$-lattices and projective $\overline{\mathbf{F}}H$-lattices.

Proposition 1.6. *If H is a subgroup of G, then there is a one to one correspondence between all isomorphism classes of indecomposable projective $\mathbf{R}H$-lattices $\mathbf{P}$ and all isomorphism classes of indecomposable projective $\overline{\mathbf{F}}H$-lattices $\mathbf{Q}$. Here the isomorphism class of $\mathbf{P}$ corresponds to that of $\mathbf{Q}$ if and only if $\overline{\mathbf{P}}$ is $\overline{\mathbf{F}}H$-isomorphic to $\mathbf{Q}$.*

Proof. Any projective $\mathbf{R}H$-lattice $\mathbf{P}$ has a projective residual $\overline{\mathbf{F}}H$-lattice $\overline{\mathbf{P}}$ by Proposition 1.5. Any projective $\overline{\mathbf{F}}H$-lattice $\mathbf{Q}$ is isomorphic to such a residual $\overline{\mathbf{P}}$ by Lemma 1.3. If $\mathbf{P}_0$ is also a projective $\mathbf{R}H$-lattice, then any isomorphism $\mathbf{P} \simeq \mathbf{P}_0$ of $\mathbf{R}H$-lattices induces an isomorphism $\overline{\mathbf{P}} \simeq \overline{\mathbf{P}_0}$ of residual $\overline{\mathbf{F}}H$-lattices. So we only need show that $\mathbf{P}$ is $\mathbf{R}H$-isomorphic to $\mathbf{P}_0$ whenever $\overline{\mathbf{P}}$ is $\overline{\mathbf{F}}H$-isomorphic to $\overline{\mathbf{P}_0}$. But in that case Lemma 1.4, with $\mathbf{P}_0$ and $\overline{\mathbf{P}_0}$ in place of $\mathbf{L}$ and $\mathbf{Q}$, respectively, implies that $\mathbf{P}$ divides $\mathbf{P}_0$. Since $\overline{\mathbf{P}}$ is isomorphic to $\overline{\mathbf{P}_0}$, this can only happen when $\mathbf{P}$ is isomorphic to $\mathbf{P}_0$. Q.E.D.

§2. Green Correspondents

Let $\mathbf{S}$ be either $\mathbf{R}$ or $\overline{\mathbf{F}}$. Then any integer n relatively prime to the characteristic p of $\overline{\mathbf{F}} = \mathbf{R}/\mathbf{p}$ has an image $n1_{\mathbf{S}}$ which is a unit of $\mathbf{S}$. This and the Krull-Schmidt property are enough to imply all of Green's theory in [2] and [3] for $\mathbf{S}H$-lattices.

We're going to apply his theory when G has subgroups P and N satisfying

(2.1) *P is a Sylow p-subgroup of G, and N is its normalizer $\mathrm{N}_G(P)$ in G. Furthermore, the intersection $P \cap P^\sigma$ of P with its conjugate $P^\sigma = \sigma^{-1}P\sigma$ by any $\sigma \in G - N$ is the trivial subgroup 1 of G.*

Of course this last condition just says that P is a *trivial intersection subgroup* of G. Green's correspondence in this case simplifies to

Proposition 2.2. *If* (2.1) *holds and $\mathbf{S}$ is either $\mathbf{R}$ or $\overline{\mathbf{F}}$, then there is a one to one correspondence between all isomorphism classes of projective-free $\mathbf{S}G$-lattices $\mathbf{L}$ and all isomorphism classes of projective-free $\mathbf{S}N$-lattices $\mathbf{K}$. Here the isomorphism class of $\mathbf{L}$ corresponds to that of $\mathbf{K}$ if and only if $\mathbf{L}$ is isomorphic to the projective-free part $(\mathbf{K}^G)_{\mathrm{pf}}$ of the $\mathbf{S}G$-lattice $\mathbf{K}^G$ induced by $\mathbf{K}$. This happens if and only if $\mathbf{K}$ is isomorphic to the projective-free part $(\mathbf{L}_N)_{\mathrm{pf}}$ of the $\mathbf{S}N$-lattice $\mathbf{L}_N$ restricted from $\mathbf{L}$.*

Proof. Because $\mathbf{S}H$-lattices have the Krull-Schmidt property, for any subgroup H of G, we may apply all the arguments in [3] to our present situation. Following the notation of that paper as closely as possible, we denote by $a(H)$ the Green ring for the $\mathbf{S}H$-lattices. So $a(H)$ is generated as an additive group by the Green symbols $(\mathbf{U})$, one for each $\mathbf{S}H$-lattice $\mathbf{U}$, subject only to the relations that $(\mathbf{U}) = (\mathbf{U}')$ whenever $\mathbf{U}$ and $\mathbf{U}'$ are isomorphic $\mathbf{S}H$-lattices, and that $(\mathbf{U}) + (\mathbf{U}') = (\mathbf{U} \oplus \mathbf{U}')$ for any $\mathbf{S}G$-lattices $\mathbf{U}$ and $\mathbf{U}'$. (Multiplication in $a(H)$ is irrelevant to our purposes.) The Krull-Schmidt property implies that $a(H)$ is a free additive group with one basis element $(\mathbf{U})$ for each isomorphism class of indecomposable $\mathbf{S}H$-lattices $\mathbf{U}$. Those $(\mathbf{U})$ in this basis for which $\mathbf{U}$ is projective-free form a basis for an additive subgroup $a_{\mathrm{pf}}(H)$ of $a(H)$. Those for which $\mathbf{U}$ is projective form a basis for another additive subgroup $a_{\mathrm{pr}}(H)$. Furthermore, $a(H)$ is the direct sum

$$a(H) = a_{\mathrm{pf}}(H) \oplus a_{\mathrm{pr}}(H) \tag{2.3}$$

of these two subgroups.

As the subgroups D and H of G used in [3] we take the present P and N, respectively. Then $H = N$ contains the normalizer $\mathrm{N}_G(D) = N$ of $D = P$, as required on page 75 of [3]. The index $[G : D]$ of the Sylow p-subgroup $D = P$ is relatively prime to p. Hence its image $[G : D]1_{\mathbf{S}}$ is a unit of $\mathbf{S}$. As in [2, Theorem 2], this implies that any $\mathbf{S}G$-lattice is D-projective. So the additive subgroup $a_D(G)$, generated by the $(\mathbf{L})$ for D-projective $\mathbf{S}G$-lattices $\mathbf{L}$, is all of $a(G)$. Similarly, $a(N)$ is equal to its subgroup $a_D(N)$.

Because $D = P$ is a trivial intersection subgroup of G, the family $\mathbf{X} = \mathbf{X}(D, H)$ of all intersections $D^\sigma \cap D$ with $\sigma \in G - H = G - N$

just consists of the trivial subgroup 1 of G. Hence the additive subgroup $a_{\mathbf{X}}(G) = \sum_{D' \in \mathbf{X}} a_{D'}(G)$ of $a(G)$ is just the additive subgroup $a_1(G)$ generated by the $(\mathbf{P})$, where $\mathbf{P}$ runs over the 1-projective $\mathbf{S}G$-lattices. Since the 1-projective $\mathbf{S}G$-lattices are just the projective ones, we conclude that $a_{\mathbf{X}}(G) = a_{\mathrm{pr}}(G)$. This and (2.3) imply that

$$a_D(G)/a_{\mathbf{X}}(G) = a(G)/a_{\mathrm{pr}}(G) \simeq a_{\mathrm{pf}}(G)$$

as additive groups. Similarly

$$a_D(N)/a_{\mathbf{X}}(N) = a(N)/a_{\mathrm{pr}}(N) \simeq a_{\mathrm{pf}}(N).$$

In view of these natural isomorphisms, [3, Theorem 1] implies the present proposition. Q.E.D.

When $\mathbf{S}$ is either $\mathbf{R}$ or $\overline{\mathbf{F}}$, we say that a projective-free $\mathbf{S}G$-lattice $\mathbf{L}$ is an $\mathbf{S}G$-*Green correspondent* of a projective-free $\mathbf{S}N$-lattice $\mathbf{K}$ (or that $\mathbf{K}$ is an $\mathbf{S}N$-*Green correspondent* of $\mathbf{L}$) if the isomorphism classes of $\mathbf{L}$ and $\mathbf{K}$ correspond in the above proposition.

Proposition 2.4. *Let a projective-free $\mathbf{R}N$-lattice $\mathbf{K}$ be an $\mathbf{R}N$-Green correspondent of a projective-free $\mathbf{R}G$-lattice $\mathbf{L}$. Then both the residual $\overline{\mathbf{F}}N$-lattice $\overline{\mathbf{K}}$ of $\mathbf{K}$ and the residual $\overline{\mathbf{F}}G$-lattice $\overline{\mathbf{L}}$ of $\mathbf{L}$ are projective-free. Furthermore, $\overline{\mathbf{K}}$ is an $\overline{\mathbf{F}}N$-Green correspondent of $\overline{\mathbf{L}}$.*

Proof. Proposition 1.5 implies that both $\overline{\mathbf{K}}$ and $\overline{\mathbf{L}}$ are projective-free. The isomorphism $\mathbf{L}_N \simeq (\mathbf{L}_N)_{\mathrm{pf}} \oplus (\mathbf{L}_N)_{\mathrm{pr}}$ of $\mathbf{R}N$-lattices induces an isomorphism

$$\overline{\mathbf{L}_N} \simeq \overline{(\mathbf{L}_N)_{\mathrm{pf}}} \oplus \overline{(\mathbf{L}_N)_{\mathrm{pr}}}$$

of the $\overline{\mathbf{F}}N$-residuals of those lattices. By Proposition 1.5 the $\overline{\mathbf{F}}N$-lattices $\overline{(\mathbf{L}_N)_{\mathrm{pf}}}$ and $\overline{(\mathbf{L}_N)_{\mathrm{pr}}}$ are respectively projective-free and projective. Hence they are respectively isomorphic to the projective free part $(\overline{\mathbf{L}_N})_{\mathrm{pf}}$ and projective part $(\overline{\mathbf{L}_N})_{\mathrm{pr}}$ of $\overline{\mathbf{L}_N}$.

Since $\mathbf{K}$ is an $\mathbf{R}N$-Green correspondent of $\mathbf{L}$, it is $\mathbf{R}N$-isomorphic to $(\mathbf{L}_N)_{\mathrm{pf}}$. So $\overline{\mathbf{K}}$ is $\overline{\mathbf{F}}N$-isomorphic to $\overline{(\mathbf{L}_N)_{\mathrm{pf}}} \simeq (\overline{\mathbf{L}_N})_{\mathrm{pf}}$. But $\overline{\mathbf{L}_N}$ is equal to the restriction $\overline{\mathbf{L}}_N$ of $\overline{\mathbf{L}}$ to an $\overline{\mathbf{F}}N$-lattice. Hence $\overline{\mathbf{K}} \simeq (\overline{\mathbf{L}}_N)_{\mathrm{pf}}$ is an $\overline{\mathbf{F}}N$-Green correspondent of $\overline{\mathbf{L}}$. Q.E.D.

§3. Rationally Determined Lattices

Any $\mathbf{R}H$-lattice $\mathbf{L}$, for any subgroup H of G, extends to an $\mathbf{F}H$-lattice $\mathbf{FL} \simeq \mathbf{F} \otimes_{\mathbf{R}} \mathbf{L}$, determined to within isomorphisms by the fact that any basis for the free module $\mathbf{L}$ over $\mathbf{R}$ is also a basis for the vector space $\mathbf{FL}$ over $\mathbf{F}$. Thus any $\mathbf{R}H$-lattice $\mathbf{L}$ determines both an $\overline{\mathbf{F}}H$-lattice $\overline{\mathbf{L}} = \mathbf{L}/(\mathbf{pL})$ and an $\mathbf{F}H$-lattice $\mathbf{FL}$. Since $\overline{\mathbf{F}}$ and $\mathbf{F}$ are the two "domains of rationality" associated with $\mathbf{R}$, it is reasonable to make the

Definition 3.1. An $\mathbf{R}H$-lattice $\mathbf{L}$ is *rationally determined* if it is determined to within isomorphisms by its associated $\overline{\mathbf{F}}H$-lattice $\overline{\mathbf{L}}$ and $\mathbf{F}H$-lattice $\mathbf{FL}$, i.e., if $\mathbf{L}$ is $\mathbf{R}H$-isomorphic to any $\mathbf{R}H$-lattice $\mathbf{K}$ such that $\overline{\mathbf{L}}$ is $\overline{\mathbf{F}}H$-isomorphic to $\overline{\mathbf{K}}$ and $\mathbf{FL}$ is $\mathbf{F}H$-isomorphic to $\mathbf{FK}$.

The main observation of this note is

Theorem 3.2. *Suppose that* (1.1) *and* (2.1) *hold, that* $\mathbf{K}$ *is a projective-free* $\mathbf{R}N$*-lattice, and that* $\mathbf{L}$ *is an* $\mathbf{R}G$*-Green correspondent of* $\mathbf{K}$*. Then the projective-free* $\mathbf{R}G$*-lattice* $\mathbf{L}$ *is rationally determined if and only if the* $\mathbf{R}N$*-lattice* $\mathbf{K}$ *is rationally determined.*

Proof. Assume that $\mathbf{L}$ is rationally determined. We must show that $\mathbf{K}$ is rationally determined. In view of Definition 3.1 it suffices to prove that $\mathbf{K}$ is $\mathbf{R}N$-isomorphic to $\mathbf{K}_0$ whenever $\mathbf{K}_0$ is an $\mathbf{R}N$-lattice whose residual $\overline{\mathbf{F}}N$-lattice $\overline{\mathbf{K}_0}$ is isomorphic to $\overline{\mathbf{K}}$, and whose associated $\mathbf{F}N$-lattice $\mathbf{FK}_0$ is isomorphic to $\mathbf{FK}$.

The projective-free $\mathbf{R}N$-lattice $\mathbf{K}$ has a projective-free residual $\overline{\mathbf{F}}N$-lattice $\overline{\mathbf{K}}$ by Proposition 1.5. The isomorphic $\overline{\mathbf{F}}N$-lattice $\overline{\mathbf{K}_0}$ is also projective-free. So Proposition 1.5 implies that $\mathbf{K}_0$ is a projective-free $\mathbf{R}N$-lattice. Hence some projective-free $\mathbf{R}G$-lattice $\mathbf{L}_0$ is a Green correspondent of $\mathbf{K}_0$. Since the Green correspondence is the bijection of isomorphism classes in Proposition 2.2, we can prove that $\mathbf{K}$ is $\mathbf{R}N$-isomorphic to $\mathbf{K}_0$ by showing that $\mathbf{L}$ is $\mathbf{R}G$-isomorphic to $\mathbf{L}_0$. Because $\mathbf{L}$ is rationally determined, it will suffice to show that $\overline{\mathbf{L}}$ is $\overline{\mathbf{F}}G$-isomorphic to $\overline{\mathbf{L}_0}$, and that $\mathbf{FL}$ is $\mathbf{F}G$-isomorphic to $\mathbf{FL}_0$.

The isomorphic $\overline{\mathbf{F}}N$-lattices $\overline{\mathbf{K}} \simeq \overline{\mathbf{K}_0}$ induce isomorphic $\overline{\mathbf{F}}G$-lattices $\overline{\mathbf{K}}^G \simeq \overline{\mathbf{K}_0}^G$. Hence we have $\overline{\mathbf{F}}G$-isomorphisms

$$(\overline{\mathbf{K}}^G)_{\mathrm{pf}} \simeq (\overline{\mathbf{K}_0}^G)_{\mathrm{pf}} \quad \text{and} \quad (\overline{\mathbf{K}}^G)_{\mathrm{pr}} \simeq (\overline{\mathbf{K}_0}^G)_{\mathrm{pr}}. \tag{3.3}$$

By definition $(\overline{\mathbf{K}}^G)_{\mathrm{pf}}$ and $(\overline{\mathbf{K}_0}^G)_{\mathrm{pf}}$ are $\overline{\mathbf{F}}G$-Green correspondents of $\overline{\mathbf{K}}$ and $\overline{\mathbf{K}_0}$, respectively. So Proposition 2.4 tells us that $(\overline{\mathbf{K}}^G)_{\mathrm{pf}}$ is $\overline{\mathbf{F}}G$-isomorphic to the residual $\overline{\mathbf{L}}$ of the Green correspondent $\mathbf{L}$ of $\mathbf{K}$. Similarly $(\overline{\mathbf{K}_0}^G)_{\mathrm{pf}}$ is $\overline{\mathbf{F}}G$-isomorphic to $\overline{\mathbf{L}_0}$. Therefore the first isomorphism in (3.3) implies that $\overline{\mathbf{L}}$ is $\overline{\mathbf{F}}G$-isomorphic to $\overline{\mathbf{L}_0}$.

Evidently $\overline{\mathbf{K}}^G$ is $\overline{\mathbf{F}}G$-isomorphic to the residual $\overline{\mathbf{K}^G}$ of the $\mathbf{R}G$-lattice $\mathbf{K}^G$ induced by $\mathbf{K}$. As in the proof of Proposition 2.4, this implies that $(\overline{\mathbf{K}}^G)_{\mathrm{pr}}$ is $\overline{\mathbf{F}}G$-isomorphic to the residual $\overline{(\mathbf{K}^G)_{\mathrm{pr}}}$ of $(\mathbf{K}^G)_{\mathrm{pr}}$.

Similarly $(\overline{\mathbf{K}_0}^G)_{\mathrm{pr}}$ is $\overline{\mathbf{F}}G$-isomorphic to the residual $\overline{(\mathbf{K}_0^G)_{\mathrm{pr}}}$ of $(\mathbf{K}_0^G)_{\mathrm{pr}}$. So the second isomorphism in (3.3) implies that the projective $\mathbf{R}G$-lattices $(\mathbf{K}^G)_{\mathrm{pr}}$ and $(\mathbf{K}_0^G)_{\mathrm{pr}}$ have isomorphic $\overline{\mathbf{F}}G$-residuals. By Proposition 1.6 this forces $(\mathbf{K}^G)_{\mathrm{pr}}$ to be $\mathbf{R}G$-isomorphic to $(\mathbf{K}_0^G)_{\mathrm{pr}}$. It follows that $\mathbf{F}(\mathbf{K}^G)_{\mathrm{pr}}$ is $\mathbf{F}G$-isomorphic to $\mathbf{F}(\mathbf{K}_0^G)_{\mathrm{pr}}$.

The isomorphism $\mathbf{FK} \simeq \mathbf{FK}_0$ of $\mathbf{F}N$-lattices induces isomorphisms $\mathbf{F}(\mathbf{K}^G) \simeq (\mathbf{FK})^G \simeq (\mathbf{FK}_0)^G \simeq \mathbf{F}(\mathbf{K}_0^G)$ of $\mathbf{F}G$-lattices. Since $\mathbf{K}^G$ and $\mathbf{K}_0^G$ are $\mathbf{R}G$-isomorphic to $(\mathbf{K}^G)_{\mathrm{pf}} \oplus (\mathbf{K}^G)_{\mathrm{pr}}$ and $(\mathbf{K}_0^G)_{\mathrm{pf}} \oplus (\mathbf{K}_0^G)_{\mathrm{pr}}$, respectively, this gives us $\mathbf{F}G$-isomorphisms

$$\mathbf{F}(\mathbf{K}^G)_{\mathrm{pf}} \oplus \mathbf{F}(\mathbf{K}^G)_{\mathrm{pr}} \simeq \mathbf{F}(\mathbf{K}^G) \simeq \mathbf{F}(\mathbf{K}_0^G) \simeq \mathbf{F}(\mathbf{K}_0^G)_{\mathrm{pf}} \oplus \mathbf{F}(\mathbf{K}_0^G)_{\mathrm{pr}}.$$

We saw above that $\mathbf{F}(\mathbf{K}^G)_{\mathrm{pr}} \simeq \mathbf{F}(\mathbf{K}_0^G)_{\mathrm{pr}}$ as $\mathbf{F}G$-lattices. So the Krull-Schmidt property for $\mathbf{F}G$-lattices implies that $\mathbf{FL} \simeq \mathbf{F}(\mathbf{K}^G)_{\mathrm{pf}}$ is $\mathbf{F}G$-isomorphic to $\mathbf{FL}_0 \simeq \mathbf{F}(\mathbf{K}_0^G)_{\mathrm{pf}}$.

We have now shown that $\overline{\mathbf{L}}$ is $\overline{\mathbf{F}}G$-isomorphic to $\overline{\mathbf{L}_0}$, and that $\mathbf{FL}$ is $\mathbf{F}G$-isomorphic to $\mathbf{FL}_0$. As we remarked above, this is enough to imply that $\mathbf{K}$ is rationally determined whenever $\mathbf{L}$ is. A similar argument, using restriction of lattices from G to N instead of induction from N to G, shows that the converse statement also holds. Q.E.D.

Surprisingly enough, for any subgroup H of G there are some important rationally determined $\mathbf{R}H$-lattices. After embedding an arbitrary $\mathbf{R}H$-lattice $\mathbf{L}$ in an $\mathbf{F}H$-lattice $\mathbf{FL}$, we can multiply it by any central idempotent e in $\mathbf{F}H$, obtaining an $\mathbf{R}H$-sublattice $\mathbf{L}e$ spanning the $\mathbf{F}H$-submodule $(\mathbf{FL})e = \mathbf{F}(\mathbf{L}e)$ of $\mathbf{FL}$.

Proposition 3.4. *Suppose that H is a subgroup of G, that $\mathbf{P}$ is a projective $\mathbf{R}H$-lattice, and that e is a central idempotent of $\mathbf{F}H$. Then the $\mathbf{R}H$-lattice $\mathbf{L} = \mathbf{P}e$ is rationally determined.*

Proof. Let $\mathbf{K}$ be any $\mathbf{R}H$-lattice such that $\overline{\mathbf{K}}$ is $\overline{\mathbf{F}}H$-isomorphic to $\overline{\mathbf{L}}$ and $\mathbf{FK}$ is $\mathbf{F}H$-isomorphic to $\mathbf{FL}$. We must prove that $\mathbf{K}$ is $\mathbf{R}H$-isomorphic to $\mathbf{L}$.

Right multiplication by e is an $\mathbf{R}H$-epimorphism ρ of $\mathbf{P}$ onto $\mathbf{L} = \mathbf{P}e$. If we follow ρ by the natural epimorphism $\eta_{\mathbf{L}}$ of $\mathbf{L}$ onto $\overline{\mathbf{L}} = \mathbf{L}/(\mathbf{pL})$, and by some $\overline{\mathbf{F}}H$-isomorphism $\overline{\iota}$ of $\overline{\mathbf{L}}$ onto $\overline{\mathbf{K}}$, we obtain a homomorphism $\overline{\iota} \circ \eta_{\mathbf{L}} \circ \rho \colon \mathbf{P} \to \overline{\mathbf{K}}$ of $\mathbf{R}H$-modules. We also have the natural epimorphism $\eta_{\mathbf{K}}$ of $\mathbf{K}$ onto $\overline{\mathbf{K}} = \mathbf{K}/(\mathbf{pK})$ as $\mathbf{R}H$-modules. Because $\mathbf{P}$ is a projective $\mathbf{R}H$-module, there is some homomorphism $\theta \colon \mathbf{P} \to \mathbf{K}$ of $\mathbf{R}H$-lattices such that

$$\eta_{\mathbf{K}} \circ \theta = \overline{\iota} \circ \eta_{\mathbf{L}} \circ \rho \colon \mathbf{P} \to \overline{\mathbf{K}}. \tag{3.5}$$

The $\mathbf{R}H$-homomorphism $\theta\colon \mathbf{P} \to \mathbf{K}$ extends by $\mathbf{F}$-linearity to an $\mathbf{F}H$-homomorphism $\theta^{\mathbf{F}}\colon \mathbf{FP} \to \mathbf{FK}$. This last homomorphism commutes with multiplication by the central idempotent e of $\mathbf{F}H$. So it restricts to an $\mathbf{R}H$-homomorphism $\iota = (\theta^{\mathbf{F}})_{\mathbf{L}}$ of $\mathbf{L} = \mathbf{P}e$ into $\mathbf{K}e$. But right multiplication by the idempotent e is the identity on both $\mathbf{L} = \mathbf{P}e$ and $\mathbf{FL} = \mathbf{FP}e$. Hence it is the identity on both the $\mathbf{F}H$-lattice $\mathbf{FK}$ isomorphic to $\mathbf{FL}$, and on the $\mathbf{R}H$-sublattice $\mathbf{K}$ of $\mathbf{FK}$. We conclude that ι is an $\mathbf{R}H$-homomorphism of $\mathbf{L}$ into $\mathbf{K} = \mathbf{K}e$. Since the epimorphism ρ in the equation (3.5) is just multiplication by e, that equation implies that

$$\bar{\iota} \circ \eta_{\mathbf{L}} = \eta_{\mathbf{K}} \circ \iota\colon \mathbf{L} \to \overline{\mathbf{K}}.$$

Thus $\iota\colon \mathbf{L} \to \mathbf{K}$ is a homomorphism of $\mathbf{R}H$-lattices inducing the isomorphism $\bar{\iota}\colon \overline{\mathbf{L}} \to \overline{\mathbf{K}}$ of $\overline{\mathbf{F}}H$-lattices. Hence ι is an $\mathbf{R}H$-isomorphism of $\mathbf{L}$ onto $\mathbf{K}$. Q.E.D.

The $\mathbf{R}H$-lattice $\mathbf{P}e$ in the preceding proposition is projective-free in the most important case.

Proposition 3.6. *Suppose that H is a subgroup of G, that $\mathbf{P}$ is an indecomposable projective $\mathbf{R}H$-lattice, and that e is a central idempotent of $\mathbf{F}H$. Then the $\mathbf{R}H$-lattice $\mathbf{P}e$ is either equal to $\mathbf{P}$ or projective-free.*

Proof. Assume that $\mathbf{P}e$ is not projective-free. We must show that it is equal to $\mathbf{P}$, i.e., that right multiplication by e is the identity on $\mathbf{P}$. Since right multiplication by the idempotent e is certainly the identity on $\mathbf{P}e$, it will suffice to show that $\mathbf{P}$ is $\mathbf{R}H$-isomorphic to $\mathbf{P}e$.

Because $\mathbf{P}e$ is not projective-free, it is divisible by some non-zero projective $\mathbf{R}H$-lattice $\mathbf{Q}$. So there is some $\mathbf{R}H$-epimorphism π of $\mathbf{P}e$ onto $\mathbf{Q}$. Right multiplication by e is an $\mathbf{R}H$-epimorphism ρ of $\mathbf{P}$ onto $\mathbf{P}e$. Hence the composite map $\pi \circ \rho\colon \mathbf{P} \to \mathbf{Q}$ is an epimorphism of $\mathbf{R}H$-lattices. Since $\mathbf{Q}$ is $\mathbf{R}H$-projective, there is some $\mathbf{R}H$-monomorphism $\mu\colon \mathbf{Q} \to \mathbf{P}$ such that $\pi \circ \rho \circ \mu$ is the identity map of $\mathbf{Q}$ onto itself. In particular, the non-zero $\mathbf{R}H$-lattice $\mathbf{Q}$ divides the indecomposable $\mathbf{R}H$-lattice $\mathbf{P}$. This can only happen when $\pi \circ \rho$ is an isomorphism of $\mathbf{P}$ onto $\mathbf{Q}$, with μ as its inverse. But then the epimorphism ρ must be an $\mathbf{R}H$-isomorphism of $\mathbf{P}$ onto $\mathbf{P}e$. As we remarked above, this is enough to prove the proposition. Q.E.D.

Putting the preceding results together, we obtain

Theorem 3.7. *Suppose that* (1.1) *and* (2.1) *hold, that $\mathbf{P}$ is an indecomposable projective $\mathbf{R}G$-lattice, and that e is a central idempotent of $\mathbf{F}G$ such that $\mathbf{P}e \neq \mathbf{P}$. Then the $\mathbf{R}G$-lattice $\mathbf{P}e$ is projective-free, and its $\mathbf{R}N$-Green correspondents are rationally determined.*

Proof. The $\mathbf{R}G$-lattice $\mathbf{P}e$ is projective-free by Proposition 3.6, and is rationally determined by Proposition 3.4. So its $\mathbf{R}N$-Green correspondents are rationally determined by Theorem 3.2. Q.E.D.

References

[1] E. C. Dade, Counting characters in blocks, I, Invent. Math., **109** (1992), 187–210.

[2] J. A. Green, On the indecomposable representations of a finite group, Math. Z., **70** (1959), 430–445.

[3] J. A. Green, A transfer theorem for modular representations, J. Algebra, **1** (1964), 73–84.

[4] A. Heller, On group representations over a valuation ring, Proc. Natl. Acad. Sci. USA, **47** (1961), 1194–1197.

[5] J. G. Thompson, Vertices and sources, J. Algebra, **6** (1967), 1–6.

Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, IL 61801
U.S.A.
e-mail: dade@math.uiuc.edu

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 289–290

On the Lattice of all Subgroups of a Finite Noncyclic Simple Group

Walter Feit and M.A. Shahabi

In some of his earliest work Suzuki studied the lattice $L(G)$ of all subgroups of a group $G$. Amongst other results he showed that if $G$ is a finite noncyclic simple group and $L(H) \approx L(G \times G)$ then $H \approx G \times G$ [2, Theorem 19, p.53]. (Here of course $\approx$ denotes either a lattice isomorphism or a group isomorphism as appropriate.) In particular this implies that if $G$ and $H$ are finite simple groups with $L(G \times G) \approx L(H \times H)$ then $G \approx H$. (The case that $G$ is cyclic of prime order is clear.) If $G$ is cyclic of prime order then $L(G)$ has just 2 elements so that $L(G) \approx L(H)$ implies only that $H$ is cyclic of some prime order and so need not be isomorphic to $G$. However this leaves open the natural question of whether a finite noncyclic simple group is characterized by its lattice of subgroups. The purpose of this note is to show that by using the classification of the finite simple groups and further results from [2] that this is the case. More precisely:

Theorem. *Let $G$ and $H$ be finite noncyclic simple groups. Then $G \approx H$ if and only if $L(G) \approx L(H)$.*

It is clear that if $G \approx H$ then $L(G) \approx L(H)$. The proof of the converse needs some deep results. If $G$ is a finite group and $p$ is a prime let $n_p(G)$ denote the number of elements of order $p$ in $G$. Then $G$ contains exactly $n_p(G)/(p-1)$ subgroups of order $p$. The following will be needed:

(I) [2, Theorem 15, p.51] *If $G$ is a finite noncyclic simple group and $H$ is a finite group with $L(G) \approx L(H)$ then $H$ is a finite noncyclic simple group of the same order as $G$.*

(II) [2, Theorem 8, p.45] *Let $G$ be a finite noncyclic simple group and let $p$ be a prime. If $\varphi$ is a lattice isomorphism of $L(G)$*

Received December 9, 1998.
Revised April 26, 2000.

onto $L(H)$ then $\varphi$ maps every subgroup of $G$ of order $p$ onto a subgroup of $H$ of order $p$. In particular $n_p(G) = n_p(H)$.

(III) [A consequence of the classification of the finite simple groups] *The only pairs of nonisomorphic simple groups of the same order are the following:*

(i) $A_8, PSL_3(4)$

(ii) $PSp_{2m}(q), SO_{2m+1}(q)$ *for $m > 2$ and $q$ an odd prime power.*

Proof of the Theorem. Suppose that $L(G) \approx L(H)$. By (I) $G$and $H$ have the same order and so must be one of the pairs in (III). In Case (i) the character tables in the ATLAS imply that $n_5(PSL_3(4)) = 3n_5(A_8) \neq 0$ and so by (II) these groups do not have isomorphic subgroup lattices. In Case (ii) $n_2(PSp_{2m}(q)) \neq n_2((SO_{2m+1}(q))$ by [1, Lemma 2.5] and once again these groups do not have isomorphic subgroup lattices.

Added in Proof. Roland Schmidt has informed us that while the result of this paper has not appeared in a Journal, it is in his book "Subgroup Lattices of Groups" p. 439.

References

[1] W. Kimmerle, R. Lyons, R. Sandling and D.N. Teague, Composition factors from the group ring and Artin's Theorem on orders of simple groups, P.L.M.S., **60** (1990), 89–122.

[2] M. Suzuki, Structure of a group and the structure of its lattice of subgroups, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. **10** (1956), Springer Verlag, Berlin, Göttingen, Heidelberg.

Walter Feit
Department of Mathematics
Yale University
P.O. Box 208283
New Haven, CT 06520
U.S.A.

M. A. Shahabi
Department of Pure Mathematics
University of Tabriz
Tabriz, Iran

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 291–300

Generation Theorems for Finite Groups

Paul Flavell

§1. Introduction

This article is a survey of the author's work on generation theorems for finite groups. The starting point is:

Theorem A (J. G. Thompson 1968). *A finite group is soluble if and only if every two elements generate a soluble subgroup.*

Thompson obtained this result as a corollary of his classification of the minimal simple groups [12]. A direct proof has been obtained by the author [3]. A natural question to ask is:

what happens if we keep one of the generators fixed?

For a finite group $G$ we define

$$\mathrm{sol}(G)$$

to be the largest normal soluble subgroup of $G$.

Conjecture B. *Let $x$ be an element of the finite group $G$. Then*

$$x \in \mathrm{sol}(G) \quad \textit{if and only if} \quad \langle x, y\rangle \quad \textit{is soluble for all} \quad y \in G.$$

The author has not yet been able to prove this conjecture. However, much progress has been made and will be described in what follows.

In order to illustrate one of obstacles to proving Conjecture B, we present a small but crucial part of the author's proof of Theorem A. Henceforth, the word *group* will mean *finite group.*

Lemma 1.1 (D. Goldschmidt [2]). *Let $z$ be a $p$-element of the soluble group H. Then*

$$O_{p'}(C_H(z)) \leq O_{p'}(H).$$

Received June 1, 1999.
Revised April 20, 2000.

Lemma 1.2 (M. B. Powell [1]). *Let d be a p'-element of the group G. If dg is a p'-element for all p'-elements $g \in G$ then $d \in O_{p'}(G)$.*

Lemma 1.3. *Let G be a group in which every two elements generate a soluble subgroup. Let z be a p-element of G. Then*

$$O_{p'}(C_G(z)) \leq O_{p'}(G).$$

Proof. Choose $d \in O_{p'}(C_G(z))$, let g be a p'-element of G and set $H = \langle dz, g\rangle$. Since d and z are commuting elements with coprime orders, we have $d, z \in H$. By hypothesis, H is soluble so using Goldschmidt's Lemma we obtain

$$d \in O_{p'}(C_G(z)) \cap H \leq O_{p'}(C_H(z)) \leq O_{p'}(H).$$

Then as g is a p'-element we see that dg is a p'-element. Powell's Lemma forces $d \in O_{p'}(G)$. Q.E.D.

Consequently, if G is a minimal counterexample to Theorem A then we have

$$O_{p'}(C_G(z)) = 1$$

for every p-element z. This argument cannot be applied to the situation in Conjecture B. Thus we have:

Problem 1. *Obtain a generalization of Lemma* 1.3 *that is applicable to Conjecture B.*

§2. A characterisation of p-soluble groups

As a first step towards proving Conjecture B, the author has established the following:

Theorem C ([4]). *Let P be a Sylow p-subgroup of the group G. Then G is p-soluble if and only if $\langle P, g\rangle$ is p-soluble for all $g \in G$.*

We present an outline of the proof. The following elementary result, which is a precursor of the Goldschmidt Lemma, is the starting point.

Lemma 2.1. *Let P be a Sylow p-subgroup of the p-soluble group G. If D is a p'-subgroup of G that is normalized by P then $D \leq O_{p'}(G)$. In particular, if $d \in G$ then*

$$d \in O_{p'}(G) \quad \textit{if and only if} \quad \left\langle d^P \right\rangle \quad \textit{is a } p'\textit{-subgroup.}$$

Suppose now that G is a minimal counterexample to Theorem C. For each $Q \in \mathrm{Syl}_p(G)$ define

$$\Lambda(Q) = \{d \in G \mid \left\langle d^Q \right\rangle \ \text{ is a } p'\text{-subgroup}\}.$$

Define a graph Γ whose vertices are the Sylow p-subgroups of G and join two distinct vertices Q and R by an edge if and only if

$$\begin{aligned} &Q \cap R \neq 1, N_Q(Q \cap R) \in \mathrm{Syl}_p(N_G(Q \cap R)) \\ &\text{and there exists } \ n \in N_G(Q \cap R) \ \text{ such that } \ Q^n = R. \end{aligned}$$

Firstly it is shown that if $\{Q, R\}$ is an edge of Γ then $\Lambda(Q) = \Lambda(R)$. A connectivity argument is applied to prove that $\Lambda(Q)$ is independent of Q. It is then shown that $\Lambda(Q)$ is a subgroup and hence a normal subgroup of G. Thus

$$\Lambda(P) = O_{p'}(G).$$

However, G is simple since it is a minimal counterexample to Theorem C, so $\Lambda(P) = O_{p'}(G) = 1$.

Now let $g \in G$ and set $H = \langle P, g \rangle$. Then $O_{p'}(H) \leq \Lambda(P) = 1$ so as H is p-soluble we have $Z(P) \leq C_H(O_p(H)) \leq Z(O_p(H))$. Then $Z(P)$ commutes with $Z(P)^g$ and it follows that

$$Z(P) \leq O_p(G),$$

contrary to the simplicity of G.

This argument, when the details are examined, appears to be a generalization of Lemma 1.3. Unfortunately there is one case where it is inapplicable. If P is cyclic of order p then the graph Γ has no edges, so connectivity arguments are useless. This case is more difficult. A transfer argument is used to obtain a contradiction.

§3. The normal closure of a Sylow subgroup

The next step is to replace *p-soluble* by *soluble.*

Conjecture D. *Let P be a Sylow p-subgroup of the group G. Then*

$$P \leq \mathrm{sol}(G) \ \textit{ if and only if } \ \langle P, g \rangle \ \textit{ is soluble for all } \ g \in G.$$

This is much more difficult. Of course, a soluble group is p-soluble so using Theorem C it follows that a minimal counterexample to conjecture D satisfies:

Hypothesis 3.1.

(1) *P is a Sylow p-subgroup of the group G.*
(2) *$\langle P, g\rangle$ is soluble for all $g \in G$.*
(3) *$G = KP$ where $K \trianglelefteq G$ is a p'-subgroup and $|P| = p$.*
(4) *K is a non abelian characteristically simple group and $K = [K, P]$.*
(5) *If H is a proper P-invariant subgroup of K then $[H, P]$ is soluble.*

Thus we have a problem involving coprime action and so the subgroup $C_K(P)$ plays a prominent role. We immediately hit upon a fundamental difficulty: since $[C_K(P), P] = 1$, the fact that G is a minimal counterexample to Conjecture D tells us nothing about $C_K(P)$. Since $K = [K, P]$, we are trying to show that Hypothesis 3.1 implies that K, and hence $C_K(P)$ is soluble. So:

Problem 2. *Why cannot $C_K(P)$ be simple?*

As a final comment we note that the case where a Sylow p-subgroup is cyclic is the difficult case in the proof of Theorem C. Moreover, in the final configuration of the author's proof of Theorem A one has a group G in which the Sylow p-subgroups are cyclic for all $p > 3$. Consequently it seems probable that in any proof of Conjecture B that the configuration described in Hypothesis 3.1, with $P = \langle x\rangle$, will be the most difficult case.

§4. Signalizer functors

Throughout this section we assume Hypothesis 3.1. Fix a prime divisor q of $|C_K(P)|$. A good starting point is to analyze the subgroups $C_K(z)$ for q-elements $1 \neq z \in C_K(P)$. These are proper P-invariant subgroups of K so we know that $[C_K(z), P]$ is soluble. By analogy with Lemma 3.1, we would like to limit the structure of $O_{q'}(C_K(z))$.

We begin with the following extension of Goldschmidt's Lemma to groups that admit a coprime operator group.

Lemma 4.1. *Let $G = PH$ be a group with $P \in \mathrm{Syl}_p(G)$ and $H = O_{p'}(G)$. Suppose that $[H, P]$ is soluble. Let q be a prime and let z be a q-element of $C_H(P)$. Then*

$$(O_{q'}(C_H(z)) \cap O_{q'}(C_H(P)))\,[O_{q'}(C_H(z)), P] \leq O_{q'}(H).$$

Note that it is easy to construct examples in which $O_{q'}(C_H(z)) \nleq O_{q'}(H)$.

Returning now to Hypothesis 3.1, for each q-element $1 \neq z \in C_K(P)$ define

$$\theta(z) = (O_{q'}(C_K(z)) \cap O_{q'}(C_K(P)))\,[O_{q'}(C_K(z)), P)].$$

Just as in the proof of Lemma 1.3, we would like to be able to argue that $\theta(z) \leq O_{q'}(K)$ and hence deduce that $\theta(z) = 1$. Unfortunately there does not appear to be an easy extension of Powell's Lemma that will suffice.

We turn to ideas from Signalizer Functor Theory. In broad terms the idea is as follows:

(a) Start with some collection $\mathcal{C}$ of subgroups of the group G that ought to be contained in a proper normal subgroup of G.
(b) Show that the members of $\mathcal{C}$ intersect the proper subgroups of G as they 'ought to'.
(c) Using (b), show that $\langle \mathcal{C} \rangle$ is a proper subgroup and use a connectivity argument to force $\mathcal{C} \trianglelefteq G$.

This idea was used in the proof of Theorem C. It is also a basic tool in the classification of simple groups, see [11].

In the situation at hand, $\mathcal{C}$ is the collection of subgroups $\theta(z)$ as z ranges over the q-elements of $C_K(P)$. Turning to (b), let $1 \neq z \in C_K(P)$ be a q-element and let M be a proper P-invariant subgroup of K that contains z. We want to show that

$$\theta(z) \cap M \leq O_{q'}(M).$$

This amounts to showing that $D \leq O_{q'}(M)$ where

$$D = [O_{q'}(C_H(z)), P] \cap M.$$

Now $D = [D,P]C_D(P)$ and by Lemma 4.1 we have $[D,P] \leq O_{q'}(M)$. However, we still have $C_D(P)$ to consider. This lead the author to make the following discovery:

Theorem E ([5]). *Let P be a group of prime order $p > 2$ that acts as a group of automorphisms on the soluble p'-group H. Then*

$$C_{[H,P]}(P) = \left\langle C_{[h,P]}(P) \mid h \in H \right\rangle.$$

The restriction that $p \neq 2$ is essential. Indeed if $p = 2$ then since any pair of involutions generate a dihedral group we have $C_{[h,P]}(P) = 1$ for all $h \in H$.

Using Theorem E and additional arguments, the author has established the following:

Theorem F ([6]). *Assume Hypothesis* 3.1 *and that* $p > 2$. *Let* z *be a q-element of* $C_K(P)$ *and let* M *be a proper* P*-invariant subgroup of* K. *Then*

$$\theta(z) \cap M \leq O_{q'}(M).$$

Note that we do not require z to be contained in M. An illustration of how Theorem E is used will be given later. At the time of writing, it has not been possible to show that $\theta(z) \leq O_{q'}(K)$. However we have at least a partial solution to Problem 1.

§5. A characterisation of $F_2(G)$

Although it has not been possible to complete the program outlined in the previous section, the author feels that Theorem E will play a fundamental role in any proof of Conjecture B or D. Indeed the proof of the following special case of Conjecture B uses Theorem E. Recall that $F_2(G)$ is the inverse image of $F(G/F(G))$ in G.

Theorem G ([7]). *Let* G *be a group and* $x \in G$. *Then*

$$x \in F_2(G) \text{ if and only if } x \in F_2(\langle x, y\rangle) \text{ for all } y \in G.$$

Later we shall see how Theorems E and G can be used to solve Problem 2.

§6. A conjecture on coprime action

Conjecture H. *Let* P *be a group of prime order* $p > 2$ *that acts as a group of automorphisms on the* p'*-group* H. *Then*

$$C_{[H,P]}(P) = \langle C_{[h,P]}(P) \mid h \in H\rangle .$$

Theorem E shows this conjecture to be true when H is soluble. If proved, Conjecture H would have implications for Conjecture B. To see why, suppose that G is a minimal counterexample to Conjecture B and set $P = \langle x\rangle \cong \mathbf{Z}_p$. Assume further that G satisfies Hypothesis 3.1 and that $p > 2$. As we have remarked earlier, this could be the most difficult case in any proof of Conjecture B.

Now let k ∈K and consider $[k, P]$. Using Sylow's Theorem we may suppose that $k \in [k, P]$. Let $c \in C_K(P)$. Then

$$k \in [k, P] \leq \langle P, P^k\rangle = \langle P, P^{ck}\rangle \leq \langle P, ck\rangle .$$

By hypothesis, $\langle P, ck\rangle$ is soluble. As $k \in \langle P, ck\rangle$ we deduce that $\langle [k, P], c\rangle$ is soluble. Consequently $\left\langle C_{[k,P]}(P), c\right\rangle$ is soluble for all $c \in C_K(P)$ and then the minimality of G forces $C_{[k,P]}(P) \leq \mathrm{sol}(C_K(P))$. Recall that $K = [K, P]$. Then the truth of Conjecture H would imply that $C_K(P)$ is soluble.

Next we give an interpretation of Conjecture H. We have

$$H = C_H(P)[H, P]$$

so there is a natural epimorphism

$$H \longrightarrow C_H(P)/\left(C_H(P) \cap [H, P]\right).$$

Set

$$D = \left\langle C_{[h,P]}(P) \mid h \in H\right\rangle \trianglelefteq C_H(P).$$

Define a map

$$\delta : H \longrightarrow C_H(P)/D$$

as follows: let $h \in H$. By Sylow's Theorem there exists $k \in [h, P]$ such that $P^h = P^k$. Thus we can write

$$h = ck$$

with $k \in [h, P]$ and $c \in C_H(P)$. Define

$$\delta(h) = Dc.$$

It is easily verified that δ is well defined.

If Conjecture H is true then δ is a homomorphism and it coincides with the natural epimorphism $H \longrightarrow C_H(P)/\left(C_H(P) \cap [H, P]\right)$. Conversely, if δ is a homomorphism then Conjecture H is true.

§7. Large 2-generated soluble subgroups

When attempting to prove Conjecture B, it seems inevitable that one has to consider modules for a soluble group in which some critical element has a large fixed point subspace. Such modules arose in the proofs of Theorems E and F, a contradiction being obtained by showing that such a module could not exist. There was other information available so it was not necessary to delve too deeply into the structure of modules for soluble groups.

After many false starts, the author has been able to extend these arguments and put them in a more general setting. The following theory emerged.

Theorem I ([8]). *Let G be a soluble group, let P be a subgroup of G with prime order $p > 3$ such that $G = \langle P^G \rangle$. Suppose that V is a faithful irreducible G-module over a field of non zero characteristic. Then*

$$\dim C_V(P) < \frac{1}{2} \dim V.$$

This result appears to be highly non trivial.

Next, let G be a group and P a subgroup of G with prime order $p > 3$. Define

$$\Sigma_G(P) = \{A \leq G \mid A \text{ is soluble and } A = \langle P, P^a \rangle \text{ for some } a \in A\}.$$

This set is partially ordered by inclusion and we let

$$\Sigma_G^*(P)$$

denote the set of maximal elements of $\Sigma_G(P)$.

Using Theorem I it is possible to establish the following fundamental property of members of $\Sigma_G^*(P)$.

Theorem J ([8]). *Let G be a group and P a subgroup of G with prime order $p > 3$. Let $A \in \Sigma_G^*(P)$. Then*

$$F(A)V$$

is nilpotent for every nilpotent subgroup V that is normalized by A.

Corollary K ([8]). *If G is soluble then $\pi(F(A)) \subseteq \pi(F(G))$.*

Thus the members of $\Sigma_G^*(P)$ exert global control over the structure of a soluble group. In fact, one can go much further:

Corollary L ([9]). *Let G be a soluble group, P a subgroup of G with prime order $p > 3$ and suppose that $G = \langle P^G \rangle$. Then there exists $g \in G$ such that $\langle P, P^g \rangle$ has the same Fitting height as G and $g \in \langle P, P^g \rangle$.*

For a group G and a subgroup P of prime order $p > 3$ we let

$$\Sigma_G^f(P)$$

be the set of members of $\Sigma_G(P)$ with maximal Fitting height. If G is soluble we define

$$\psi(G)$$

to be the smallest normal subgroup of G such that $G/\psi(G)$ has Fitting height less than that of G. If $G \neq 1$ then $1 \neq \psi(G) \leq F(G)$.

Corollary M ([9]). *Let G be a soluble group and P a subgroup of G with prime order $p > 3$. If $A \in \Sigma_G^f(P)$ then*

$$\psi(A) \leq F(G).$$

Thus, just by examining the members of $\Sigma_G(P)$, one can write down a subnormal nilpotent subgroup of G. This suggests an obvious strategy for proving Conjecture B, one which involves aiming directly at the Fitting subgroup. The following result provides evidence that this strategy could work and also shows that the theory developed so far is effective in proving generation theorems.

Theorem N. *Let $\mathcal{C}$ be a conjugacy class of the group G and suppose that the members of $\mathcal{C}$ have order prime to* 6. *Then $\langle \mathcal{C} \rangle$ is soluble if and only if every four members of $\mathcal{C}$ generate a soluble subgroup.*

Proof. Let $x \in \mathcal{C}$. We may suppose that x has prime order $p > 3$. Set $P = \langle x \rangle$ and choose $A \in \Sigma_G^f(P)$. Let $g \in G$ and set $H = \langle A, A^g \rangle$. By hypothesis, H is soluble. Now A and A^g are members of $\Sigma_H^f(P)$ so Corollary M implies that $\langle \psi(A), \psi(A)^g \rangle$ is nilpotent. The Baer-Suzuki Theorem implies that $\psi(A) \leq F(G)$. Now apply induction to $G/F(G)$. Q.E.D.

The results I-M are invalid without the hypothesis that $p > 3$. However it should be a routine matter to extend the theory so that the hypothesis *prime to* 6 in Theorem N can be removed, provided that *four* is replaced by some larger number.

This theory can also be used to solve Problem 2, at least if $p > 3$.

Theorem O. *Assume Hypothesis 3.1 and that $p > 3$. Then*

$$F_2(C_K(P)) \neq 1.$$

Proof. By Theorem G there exists $g \in G$ such that $P \not\leq F_2(\langle P, g \rangle)$. Set $H = \langle P, g \rangle$ and $H_0 = \langle P^H \rangle \trianglelefteq H$, so that H_0 has Fitting height at least 3. Now P is a Sylow subgroup of H_0 so we have $H_0 = \langle P^{H_0} \rangle$. Corollary L implies that the members of $\Sigma_{H_0}^f(P)$ and hence the members of $\Sigma_G^f(P)$ have Fitting height at least 3.

Choose $A \in \Sigma_G^f(P)$. Let $\psi_2(A)$ denote the inverse image of $\psi(A/\psi(A))$ in A. Then $\psi_2(A)$ has Fitting height 2. As $A = \langle P^A \rangle$ we have $P \cap \psi_2(A) = 1$ so then $\psi_2(A) \leq K$.

Let $c \in C_K(P)$, choose $a \in A$ such that $A = \langle P, P^a \rangle$, and set $L = \langle A, c \rangle$. Now $a \in A = \langle P, P^a \rangle = \langle P, P^{ca} \rangle \leq \langle P, ca \rangle$ whence $L = \langle P, ca \rangle$ and L is soluble. Let $L_0 = \langle P^L \rangle \trianglelefteq L$. Then $A \leq L_0 = \langle P^{L_0} \rangle$ and

Corollary L implies that A has the same Fitting height as L_0. It follows that $\psi_2(A) \leq \psi_2(L_0)$ whence $\psi_2(A) \leq F_2(L)$. We deduce that

$$C_{\psi_2(A)}(P) \leq F_2\left(\langle C_{\psi_2(A)}(P), c\rangle\right)$$

for all $c \in C_K(P)$. Theorem G implies that

$$C_{\psi_2(A)}(P) \leq F_2\left(C_K(P)\right).$$

Since $\psi_2(A)$ has Fitting height 2 we have $C_{\psi_2(A)}(P) \neq 1$. This completes the proof of Theorem O. Q.E.D.

References

[1] Blackburn, N. and Huppert, B., *Finite groups II,* Grundlehren der Mathematischen Wissenschaften, vol. 242, Berlin, Heidelberg, New York, Springer-Verlag, 1981.

[2] Blackburn, N. and Huppert, B., *Finite groups III,* Grundlehren der Mathematischen Wissenschaften, vol. 243, Berlin, Heidelberg, New York, Springer-Verlag, 1982.

[3] Flavell, P.J., *Finite groups in which every two elements generate a soluble subgroup,* Invent. Math., **121** (1995), 279–285.

[4] Flavell, P.J., *A characterisation of p-soluble groups*, Bull. London Math. Soc., **29** (1997), 177–183.

[5] Flavell, P.J., *The fixed points of coprime action,* Submitted, Arch. Math..

[6] Flavell, P.J., *Soluble radicals an signalizer functors,* Preprint.

[7] Flavell, P.J., *A characterisation of $F_2(G)$,* Preprint.

[8] Flavell, P.J., *Large two generated subgroups of finite groups,* Preprint.

[9] Flavell, P.J., *On the Fitting height of a soluble group that is generated by a conjugacy class,* Preprint.

[10] Gorenstein, D., *Finite groups, 2nd edn.,* Chelsea Publishing Company, New York, 1980.

[11] Gorenstein, D., *Finite simple groups, an introduction to their classification,* University series in mathematics, Plenum Press, 1982.

[12] Thompson, J.G., *Non-solvable groups all of whose local subgroups are solvable, I-VI,* Bull. Amer. Math. Soc., **74** (1968), 383–437; Pacific J. Math., **33** (1970), 451–536; **39** (1971), 483–534; **48** (1973), 511–592; **50** (1974), 215–297; **51** (1974), 573–630.

The School of Mathematics and Statistics
The University of Birmingham
Birmingham B15 2TT, U.K.

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 301–314

Non-Abelian Representations of Geometries

A. A. Ivanov

Abstract.

Let $\mathcal{G}$ be a geometry in which the elements of one type are called *points* and the elements of some other type are called *lines*. Suppose that every line is incident to exactly $p+1$ points where $p$ is a prime number. A (non-abelian) representation of $\mathcal{G}$ is a pair $(R, \psi)$, where $R$ is a group and $\psi$ is a mapping of the set of points of $\mathcal{G}$ into the set of subgroups of order $p$ in $R$ such that $R$ is generated by the image of $\psi$ and whenever $\{x_\infty, x_0, ..., x_{p-1}\}$ is the set of points incident to a line, the subgroups $\psi(x_\infty), \psi(x_0), ..., \psi(x_{p-1})$ are pairwise different and generate in $R$ a subgroup of order p^2. In this article we discuss representations of some classical and sporadic geometries and their applications to certain problems in algebraic combinatorics and group theory.

§1. Abelian representations

Our terminology concerning diagram geometries is mostly standard [Pas94], [Iv99a]. The types of elements on a diagram increase rightward from 1 to the rank of geometry. The elements of type 1, 2 and 3 are called *points*, *lines* and *planes*, respectively. Many important geometries are naturally defined as collections of subspaces in a finite dimensional vector space $V$ so that the type of a subspace equals to its dimension and two subspaces are incident if one of them contains the other one (in this case we say that the incidence is via inclusion). For the projective geometry of $V$ we take all the proper subspaces and for a polar space we take the subspaces which are totally singular with respect to a fixed non-degenerate symplectic, orthogonal or unitary form $f$ on $V$. These constructions can be generalized as follows (we consider vector spaces over prime fields since they are sufficient to cover our main examples).

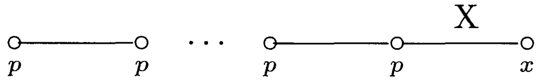
Construction A. Let $V$ be an $n$-dimensional $GF(p)$-space, where $p$ is a prime, let $G$ be a subgroup of $GL(V) \cong GL_n(p)$ and $U$ be a

Received February 4, 1999.
Revised April 19, 2000.

subspace of dimension m in V such that the stabilizer of U in G induces on U an action which contains $SL(U) \cong SL_m(p)$. Let $0 < U_1 < .... < U_{m-1} < U_m = U$ be a maximal flag in U. Define $\mathcal{G}_A(V, G)$ to be an incidence system whose elements of type i are the images of U_i under G, $1 \leq i \leq m$; the incidence is via inclusion.

Under some non-degeneracy assumptions $\mathcal{G}_A(V, G)$ is a geometry which belongs to the diagram

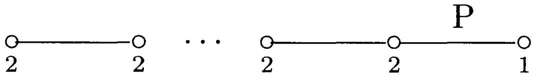
X_m :



where the rightmost edge indicates the rank 2 geometry formed by the images of U_{m-1} and $U_m = U$ under that stabilizer of U_{m-2} in G. Furthermore, G induces on $\mathcal{G}_A(V, G)$ a flag-transitive action. Notice that the structure of $\mathcal{G}_A(V, G)$ depends on U but not on the maximal flag in U.

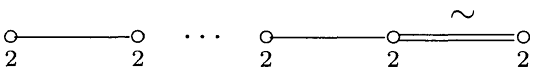
In these terms the projective geometry of V can be obtained as $\mathcal{G}_A(V, GL(V))$ for a hyperplane U in V while the polar space associated with a form f as $\mathcal{G}_A(V, G)$ where G is the subgroup in $GL(V)$ which preserves f up to scalar multiplication and U is a maximal totally isotropic subspace in V with respect to f. Some sporadic geometries can also be obtained by Construction A. Recall [Iv99a] that Petersen geometries of rank m have the following diagram (m nodes)

P_m :



where the rightmost edge indicates the geometry of edges and vertices of the Petersen graph with the natural incidence relation; and tilde geometries of rank m have the following diagram (m nodes)

T_m :



where the rightmost edge indicates the triple cover of the generalized quadrangle of order $(2, 2)$ associated with the non-split extension $3 \cdot Sp_4(2) \cong 3 \cdot Sym_6$.

If $\bar{\mathcal{C}}_{11}$ is the irreducible (11-dimensional) Todd module for the Mathieu group Mat_{24} then there is a 3-dimensional subspace U in $\bar{\mathcal{C}}_{11}$ such that $\mathcal{G}(Mat_{24}) := \mathcal{G}_A(\bar{\mathcal{C}}_{11}, Mat_{24})$ is a tilde geometry of rank 3. Consider the Mathieu group Mat_{22} as a subgroup in Mat_{24}. Then under a suitable choice of U the geometry $\mathcal{G}(Mat_{22}) := \mathcal{G}_A(\bar{\mathcal{C}}_{11}, Mat_{22})$ is a

Petersen geometry of rank 3 and by the construction it is a subgeometry in $\mathcal{G}(Mat_{24})$. Let V_{12} be the natural module for $SU_6(2)$ (considered as a 12-dimensional $GF(2)$-module). Then the non-split extension $3 \cdot Mat_{22}$ is embedded into $SU_6(2)$ and hence V_{12} is a module for this extension. There is a 3-dimensional subspace U in V_{12} such that $\mathcal{G}(3 \cdot Mat_{22}) := \mathcal{G}_A(V_{12}, 3 \cdot Mat_{22})$ is a Petersen geometry of rank 3 which is the universal (triple) cover of $\mathcal{G}(Mat_{22})$.

If $\bar{\Lambda}_{24}$ is the Leech lattice taken modulo 2 (a 24-dimensional $GF(2)$-space) then there is a 4-dimensional subspace U in $\bar{\Lambda}_{24}$ such that $\mathcal{G}(Co_1) := \mathcal{G}_A(\bar{\Lambda}_{24}, Co_1)$ is a tilde geometry of rank 4, containing $\mathcal{G}(Mat_{24})$ as a residue. The second Conway group Co_2 is the stabilizer in Co_1 of a vector $\bar{\lambda}$ in $\bar{\Lambda}_{24}$. Let $\bar{\Lambda}_{23}$ be the orthogonal complement of $\bar{\lambda}$ in $\bar{\Lambda}_{24}$ with respect to the unique non-zero orthogonal form preserved by Co_1. Then under a suitable choice of U and $\bar{\lambda}$ the geometry $\mathcal{G}(Co_2) := \mathcal{G}_A(\bar{\Lambda}_{23}, Co_2)$ is a Petersen geometry of rank 4 containing $\mathcal{G}(Mat_{22})$ as a residue. By the construction $\mathcal{G}(Co_2)$ is a subgeometry in $\mathcal{G}(Co_1)$.

It is natural to ask which geometries with diagrams X_m can be obtained by Construction A. This question leads the following.

Definition 1.1. Let $\mathcal{G}$ be a geometry in which the elements of one type are called *points* and the elements of some other type are called *lines.* Suppose that every line is incident to exactly $p+1$ points where p is a prime number. An *abelian representation* of $\mathcal{G}$ is a pair (V, ψ), where V is a vector space over $GF(p)$ and ψ is a mapping of the set of points of $\mathcal{G}$ into the set of 1-dimensional subspaces in V, such that V is generated by the image of ψ and whenever $\{x_\infty, x_0, ..., x_{p-1}\}$ is the set of points incident to a line l, the subspaces $\psi(x_\infty), \psi(x_0), ..., \psi(x_{p-1})$ are pairwise different and generate in V a 2-dimensional subspace denoted by $\psi(l)$.

An abelian representation (V, ψ) is said to be *faithful* if ψ is injective. If H is an automorphism group of $\mathcal{G}$ then the representation (V, ψ) as above is *H-admissible* if there is a subgroup G of $GL(V)$ and a homomorphism χ of G onto H such that $\psi(u)^g = \psi(u^{\chi(g)})$ for every point u and every $g \in G$. The following result is quite obvious.

Lemma 1.2. *Let $\mathcal{G}$ be a rank m geometry with diagram X_m and let H be a flag-transitive automorphism group of $\mathcal{G}$. Suppose that there is an isomorphism φ of $\mathcal{G}$ onto $\mathcal{G}_A(V, G)$ which commutes with the action of G and that the action of G induced on $\mathcal{G}$ via the isomorphism φ coincides with H. Let ψ be the restriction of φ to the point-set of $\mathcal{G}$. Then (V, ψ) is a faithful H-admissible abelian representation of $\mathcal{G}$ and for an element $u \in \mathcal{G}$ the subspace $\varphi(u)$ is generated by the 1-spaces $\varphi(x)$ taken for all the points x incident to u.*

Thus a possible way to decide whether or not a geometry $\mathcal{G}$ can be obtained by Construction A is to study the abelian representations of $\mathcal{G}$. Abelian representations of various geometries were intensively studied for a long time [Ti74], [RSm89], [Yos92] and [Sh93] (sometimes under different names like *embeddings*). Let us mention just one of the numerous applications of such representations.

Let $\mathcal{G}$ be a geometry with diagram X_m, $m \geq 3$. Then the points and lines incident to a plane z form a projective plane Π_z of order p. Let G be a flag-transitive automorphism group of $\mathcal{G}$ and suppose that the stabilizer of a plane z in G induces on the residual projective plane Π_z an action containing $L_3(p)$ and that the stabilizer of a line l in G induces on the set of points incident to l an action containing $L_2(p)$. Let x be a point and $\mathcal{G}_x$ be the residue of x in $\mathcal{G}$ whose points and lines are the lines and planes in $\mathcal{G}$ incident to x.

Lemma 1.3. *In the above terms let $G(x)$ be the stabilizer of x in G, L be the kernel of the action of $G(x)$ on the set of lines incident to x and K be the kernel of the action of L on the set of points collinear to x. Suppose that $O_p(L) \neq K$. Then $O_p(L)/K$ is an elementary abelian p-group and (V^*, ψ) is a abelian faithful $G(x)/L$-admissible representation of $\mathcal{G}_x$ where V^* is the module dual to $O_p(L)/K$ and if y is a line incident to x then $\psi(y)$ is the action induced by $O_p(L)$ on the set of points incident to y.*

Proof. Let l be a line incident to x. Then $G(l) \cap G(x)$ induces on the set of points incident to l a Frobenius group F of order $p(p-1)/\varepsilon$ where ε is 1 or 2. Then $O_p(F)$ is of order p and it is contained in every proper normal subgroup of F. Since $O_p(L) \neq K$ and $G(x)$ acts transitively on the set of points in $\mathcal{G}_x$, we conclude that $O_p(L)$ induces on the set of points incident to l the group $O_p(F)$ of order p. Hence $O_p(L)/K$ is an elementary abelian p-group and l corresponds to its pointwise stabilizer which is of index p in $O_p(L)/K$. Let z be a plane incident to x and M be the action induced on Π_z by $G(x) \cap G(z)$. Then $O_p(M)$ is of order p^2 and $M/O_p(M)$ acts on $O_p(M)$ irreducibly. By the above $O_p(L)$ is normal in $G(x) \cap G(z)$, this action coincides with $O_p(M)$ and the result follows. Q.E.D.

The above lemma can be used to decide whether or not a given geometry with diagram X_{m-1} can appear as a point residue in a flag-transitive geometry with diagram X_m.

§2. Non-abelian representations

Petersen and tilde geometries of "large" sporadic simple groups, J_4, BM and M do not possess abelian representations [ISh90], [ISh94a]. Using this fact and Lemma 1.3 it was shown that these geometries do not appear as residues in Petersen and tilde geometries of higher ranks. The latter result was of a crucial importance for completing the classification of the flag-transitive Petersen and tilde geometries [ISh94b]. By Lemma 1.2 the geometries $\mathcal{G}(J_4)$, $\mathcal{G}(BM)$ and $\mathcal{G}(M)$ can not be obtained by Construction A, but in fact they can be obtained by a similar construction [ISh89].

Construction B. Let R be a group, G be a subgroup in the automorphism group of R and U be an elementary abelian subgroup of order p^m in R where p is a prime number, such that the stabilizer of U in G induces on U an action which contains $SL_m(p)$. Let $0 < U_1 < ... < U_{m-1} < U_m = U$ be a maximal flag in U. Define $\mathcal{G}_B(R,G)$ to be an incidence system of rank m whose elements of type i are the images of U_i under G; the incidence is via inclusion.

Again under some non-degeneracy assumptions $\mathcal{G}_B(R,G)$ is a geometry with diagram X_m. For a suitable choice of subgroups U of order 2^4, 2^5 and 2^5, respectively, we have $\mathcal{G}(J_4) = \mathcal{G}_B(J_4, J_4)$, $\mathcal{G}(BM) = \mathcal{G}_B(2 \cdot BM, BM)$, $\mathcal{G}(M) = \mathcal{G}_B(M,M)$. Furthermore, $2 \cdot BM$ can be identified with a subgroup in the Monster M so that in the last two cases the subgroup U can be taken to be the same, which shows that $\mathcal{G}(BM)$ is a subgeometry in $\mathcal{G}(M)$. Construction B leads to the following

Definition 2.1. In terms of Definition 1.1 a pair (R,ψ) is a *representation* of $\mathcal{G}$ if R is a group and ψ is a mapping of the set of points of $\mathcal{G}$ into the set of subgroups of order p in R such that R is generated by the image of ψ and whenever $\{x_\infty, x_0, ..., x_{p-1}\}$ is the set of points incident to a line l, the subgroups $\psi(x_\infty), \psi(x_0), ..., \psi(x_{p-1})$ are pairwise different and generate in R a subgroup of order p^2 denoted by $\psi(l)$.

In order to distinguish the representations in the above definition from the abelian representations we sometimes call the former ones *non-abelian representations.* Since the group R might or might not be abelian the correct term would probably be *non-necessarily abelian representations.* The notions of faithful and H-admissible representations can be defined analogously to the abelian case. It is easy to see that a statement analogous to Lemma 1.2 holds where $\mathcal{G}_A(V,G)$ is changed to $\mathcal{G}_B(R,G)$ and (V,ψ) is changed to (R,ψ).

If (R,ψ) and (R',ψ') are representations of a geometry $\mathcal{G}$ and $\varphi : R' \to R$ is a homomorphism such that $\psi(x) = \varphi(\psi'(x))$ for every point

x, then φ is said to be a *morphism of representations.* For a representation (R, ψ) there is a *universal representation* (R_U, ψ_U) possessing a morphism φ_U onto (R, ψ) such that whenever a representation (R', ψ') possesses a morphism φ onto (R, ψ) there is a morphism φ' of (R_U, ψ_U) onto (R', ψ') such that φ_U is the composition of φ' and φ. The group R_U can be defined in terms of generators and relations as follows. For every point x choose a generator $r(x)$ of the subgroup $\psi(x)$. Then the generators of R_U are elements $u(x)$ of order p taken for all points x. If $\{x_\infty, x_0, ..., x_{p-1}\}$ are the points incident to a line l, then for $1 \leq i \leq p-1$ we have $r(x_i) = r(x_\infty)^{a(i)} r(x_0)^{b(i)}$ for some $1 \leq a(i), b(i) \leq p-1$. Then the relations of R_U associated with the line l are

$$[u(x_\infty), u(x_0)] = 1, \; u(x_i) = u(x_\infty)^{a(i)} u(x_0)^{b(i)}, \; 1 \leq i \leq p-1,$$

where the $a(i)$ and $b(i)$ are as above. The mapping ψ_U sends x onto the subgroup generated by $u(x)$ and $\varphi_U : u(x) \mapsto r(x)$ for every point x. In general the universal representation (R_U, ψ_U) depends on the particular choice of (R, ψ) although in some circumstances the universal representation is unique. This is the case, for instance, when $p = 2$ (in this case $a(1) = b(1) = 1$ and the relations are uniquely determined). Another uniqueness situation is described in the following.

Lemma 2.2. *Suppose that H is an automorphism group of $\mathcal{G}$ such that for every line l the stabilizer of l in H induces on the set of points incident to l an action containing $L_2(p)$. Then all H-admissible representations of $\mathcal{G}$ have isomorphic universal representations.*

Proof. Let (R, ψ) be an H-admissible representation and G be the corresponding automorphism group of R which possesses a homomorphism onto H. Let $\{x_\infty, x_0, ..., x_{p-1}\}$ be the set of points incident to a line l, $W = \psi(l)$ and F be the action induced on W by its stabilizer in G. Then W can be considered as a 2-dimensional $GF(p)$-space and by the hypothesis F contains $SL(W) \cong SL_2(p)$. Let W_0 be a 1-subspace in W, F_0 be its stabilizer in F and W_1 be the $GF(p)$-module of dimension $p+1$ for F induced from the module W_0 of F_0. Then the result follows from the following fact which is well known and easy to check: W_1 has a unique submodule of codimension 2. Q.E.D.

If (R, ψ) is an abelian representation then the corresponding *universal abelian representation* is a pair (V_U, ψ_U^a) where V_U is the quotient of R_U over the commutator subgroup of R_U and ψ_U^a is the composition of ψ_U and the natural homomorphism of R_U onto V_U.

By Lemma 1.2 and the analogous statement for the non-abelian case Constructions A and B produce geometries together with their representations. It was shown in [RSm89], [ISh89], [Sm92], [ISh94a], [IPS96] and

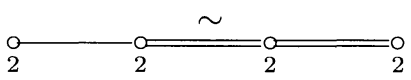
[ISh97] that the representations associated with the above constructions of $\mathcal{G}(Mat_{22})$, $\mathcal{G}(Mat_{24})$, $\mathcal{G}(Co_2)$, $\mathcal{G}(Co_1)$, $\mathcal{G}(J_4)$, $\mathcal{G}(BM)$ and $\mathcal{G}(M)$ are universal (among the non-abelian representations). If $\chi : \tilde{\mathcal{G}} \to \mathcal{G}$ is a covering of geometries and (R, ψ) is a representation of $\mathcal{G}$ then $(R, \psi\chi)$ is a representation of $\tilde{\mathcal{G}}$. In particular $\mathcal{G}(3 \cdot Mat_{22})$ possesses a (non-faithful) representation in $\bar{\mathcal{C}}_{11}$. It can be shown that $\mathcal{G}(3 \cdot Mat_{22})$ possesses a representation in the direct product of $\bar{\mathcal{C}}_{11}$ and the extraspecial group 2_+^{1+12} (a central extension of V_{12}). It is not known whether or not this representation is universal.

Some further examples of geometries and their representation can be obtained by the following

Construction C. Let $\mathcal{G}_A(W, H)$ be a geometry obtained by Construction A via a subgroup U of order p^m. Let R be a group, G be a subgroup in the automorphism group of R and V be a subgroup in R. Suppose that there are isomorphisms $\varphi_1 : W \to V$ and $\varphi_2 : H \to N_G(V)/C_G(V)$ such that $\varphi_1(w^h) = \varphi_1(w)^{\varphi_2(h)}$ for all $w \in W$ and $h \in H$. Suppose also that for $1 \le i \le m$ every subgroup contained in V and conjugate to $\varphi_1(U_i)$ in G is conjugate to $\varphi_1(U_i)$ in $N_G(V)$. Define $\mathcal{G}_C(R, V, H)$ to be an incidence system whose elements of type $m+1$ are the images of V under G and for $1 \le i \le m$ the elements of type i are the images of $\varphi_1(U_i)$ under G; the incidence is via inclusion.

Again under some non-degeneracy conditions $\mathcal{G}_C(R, V, H)$ is a geometry of rank $m+1$ in which the residue of V is isomorphic to $\mathcal{G}_A(W, H)$.

Let Fi_{24} be the largest Fischer 3-transposition group. The commutator subgroup Fi_{24}' of Fi_{24} contains a subgroup V which is isomorphic to $\bar{\mathcal{C}}_{11}$ as a module for $Mat_{24} \cong N_{Fi_{24}}(V)/C_{Fi_{24}}(V)$. Thus $\mathcal{G}(Mat_{24})$ can be realized in V by Construction A. The geometry $\mathcal{G}_C(Fi_{24}', 2^{11}, Mat_{24})$ (for $G = Fi_{24}$) is the minimal 2-local parabolic geometry $\mathcal{G}_2(Fi_{24}')$ of Fi_{24}' as in [RSt84] with the diagram

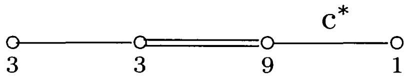


By the construction $\mathcal{G}_2(Fi_{24}')$ possesses a representation in Fi_{24}'. The following obvious result can be used to show that this representation is not universal.

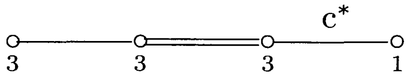
Lemma 2.3. *Let $\mathcal{G}$ be a geometry with $p+1$ points on a line and suppose that (R, ψ) is a representation of $\mathcal{G}$. Let $\tilde{R}$ be a perfect central extension of R whose kernel has order coprime to p. Then $(\tilde{R}, \tilde{\psi})$ is a representation of $\mathcal{G}$, where $\tilde{\psi}(x)$ is the unique Sylow p-subgroup in the preimage of $\psi(x)$ in $\tilde{R}$.*

By the above lemma $\mathcal{G}_2(Fi_{24}')$ possesses a representation in the extension $3 \cdot Fi_{24}'$ of Fi_{24}' by its Schur multiplier. Alternatively we could obtain $\mathcal{G}_2(Fi_{24}')$ by Construction C starting with $R = 3 \cdot Fi_{24}'$. This representation was shown in [Rch99] to be universal.

The Monster group M contains a subgroup V of order 3^8 which is the natural module for $N_M(V)/C_M(V) \cong \Omega_8^-(3).2$ so that the polar space of the latter group can be realized in V by Construction A. The geometry $\mathcal{G}(M, 3^8, \Omega_8^-(3).2)$ is the c-extended dual polar space $\mathcal{G}(M)$ [RSt84] with the diagram



Let μ be a subgroup of order 3 in V which is non-singular with respect to the $N_M(V)$-invariant quadratic form on V. Then $N_M(\mu) \cong 3 \cdot Fi_{24}$, $V = \mu \oplus W$ and W is the natural module for $N_M(W)/V \cong \Omega_7(3).2$. Then $\mathcal{G}_C(3 \cdot Fi_{24}', 3^7, \Omega_7(3).2)$ is a subgeometry in $\mathcal{G}(M)$ which is the c-extended dual polar space $\mathcal{G}_3(Fi_{24}')$ with the diagram



By the construction $\mathcal{G}(M)$ and $\mathcal{G}_3(Fi_{24}')$ possess representations in M and $3 \cdot Fi_{24}'$, respectively. It was realized in [BIP99] that these representations are not universal and the observation can be generalized as follows

Lemma 2.4. *Let $\mathcal{G}$ be a geometry with $p+1$ points on a line. Let (R, ψ) be a representation of $\mathcal{G}$ and for a point x let $r(x)$ be a generator of $\psi(x)$. Let $\tilde{\psi}$ be the mapping from the point set of $\mathcal{G}$ into the set of subgroups in the direct product $R^{p-1} = \{(r_1, r_2, ..., r_{p-1}) \mid r_i \in R\}$ of $p-1$ copies of R defined by*

$$\tilde{\psi}(x) = \langle (r(x), r(x)^2, ..., r(x)^{p-1}) \rangle$$

and $\tilde{R}$ be the subgroup in R^{p-1} generated by the image of $\tilde{\psi}$. Then $(\tilde{R}, \tilde{\psi})$ is a representation of $\mathcal{G}$.

Proof. If A is an abelian group, then for every positive integer n the mapping defined by $a \mapsto a^n$ for every $a \in A$ is an automorphism of A. This means that whenever X is a set of points such that $[r(x), r(y)] = 1$ for all $x, y \in X$, the subgroup in $\tilde{R}$ generated by $\{\tilde{\psi}(x) \mid x \in X\}$ is isomorphic to the subgroup in R generated by $\{\psi(x) \mid x \in X\}$. Now the result follows by taking X to be the set of points incident to a line. Q.E.D.

Let K be the smallest normal subgroup of R such that for every $2 \leq n \leq p-1$ the mapping $r(x) \mapsto r(x)^n$ for every point x induces an automorphism of R/K. Then one can show that $\tilde{R}$ is isomorphic to the direct product of $p-1$ copies of K extended by R/K. This shows that $\mathcal{G}(M)$ and $\mathcal{G}_3(Fi'_{24})$ possess representations in $M \times M$ and $3 \cdot Fi'_{24} \times 3 \cdot Fi'_{24}$, respectively. We conjecture that these representations are universal.

§3. Machinery

In this section we discuss some available technique for calculating universal representations of geometries.

Let $\mathcal{G}$ be a geometry of rank m with $p+1$ points per a line, (R, ψ) be a representation of $\mathcal{G}$ and $r(x)$ be a generator of $\psi(x)$. Let $\Gamma = \Gamma(\mathcal{G})$ be the collinearity graph of $\mathcal{G}$ which is a graph on the set of points of $\mathcal{G}$, where two points are adjacent if they are incident to a common line. For a point x let $\Gamma_i(x)$ be the set of points at distance i from x in Γ. Let $R_i(x)$ be the subgroup in R generated by the subgroups $\psi(y)$ taken for all points y which are at distance at most i from x in Γ. Let Δ_i be the graph on $\Gamma_i(x)$ in which two points are adjacent if they are incident to a common line, which is also incident to a point in $\Gamma_{i-1}(x)$.

Lemma 3.1. *Suppose that y and z are in the same connected component of Δ_i. Then $R_{i-1}(x)\psi(y) = R_{i-1}(x)\psi(z)$.*

The above lemma is useful for bounding the orders of the factors $R_i(x)/R_{i-1}(x)$ in the case of abelian representations. The first of these factors is of a particular importance (in both abelian and non-abelian cases).

Lemma 3.2. *Suppose that $m \geq 3$, $\mathcal{G}$ belongs to a string diagram and that the points and lines incident to a plane form a projective plane of order p. Let $\tilde{\psi} : l \to \psi(l)/\psi(x)$ where l is a line incident to x. Then $(R_1(x)/\psi(x), \tilde{\psi})$ is a representation of the residue of x in $\mathcal{G}$.*

Lemma 3.3. *Suppose that $p = 2$ and R is abelian. Let $(x_0, x_1, ..., x_k = x_0)$ be a cycle in Γ and for $0 \leq i \leq k-1$ let $\{x_i, x_{i+1}, y_i\}$ be the points incident to a line, then $\Pi_{j=0}^{k-1} r(y_j) = 1$.*

Recall that a *geometric hyperplane* in $\mathcal{G}$ is a proper subset S of points such that for every line l either all the points incident to l are contained in S or l is incident to exactly one point in S. Notice that whenever P is a subgroup of index p in R the set $S = \{x \mid \psi(x) \in P\}$ is a geometric hyperplane.

Lemma 3.4. *Suppose that $p = 2$ and that $\mathcal{G}$ contains a geometric hyperplane S such that the subgroups $\psi(x)$ taken for all $x \in S$ generate the whole R. Let T be a group of order 2 generated by an element t. Let $\hat{\psi}$ be a mapping of the set of points into the set of subgroups in the direct product of R and T which sends x to $\langle (r(x), t^{\alpha}) \rangle$ where $\alpha = 0$ if $x \in S$ and $\alpha = 1$ otherwise. Then $(R \times T, \hat{\psi})$ is a representation of $\mathcal{G}$.*

The following result is a slight generalization of Lemma 2.2 in [IPS96].

Lemma 3.5. *In the case $p = 2$ suppose that for every point x there are two subsets $A(x)$ and $B(x)$ of points such that*

(i) *if $y \in A(x)$ then $[r(x), r(y)] = 1$;*
(ii) *the graph on $B(x)$ in which two points are adjacent if there is a line incident to those points as well as to a point in $A(x)$, is connected;*
(iii) *if $z \in B(x)$ then $x \in B(z)$ and the graph on the set of points in which x is adjacent to the points in $B(x)$, is connected.*

Then the subgroup generated by the commutators $[r(x), r(z)]$ taken for every point x and every $z \in B(x)$ is of order at most 2 and contained in the centre of R. In particular, if $A(x) \cup B(x)$ is the whole set of points for every point x, then the commutator subgroup of R has order at most 2.

An important situation covered by Lemma 3.5 is when for every point x the set of points y such that $r(x)$ and $r(y)$ commute, form a geometric hyperplane $A(x)$ and the subgraph in the collinearity graph induced by the complement $B(x)$ of the hyperplane is connected. In a certain sense the next lemma deals with the opposite situation.

Lemma 3.6. *In the case $p = 2$ suppose that $\mathcal{G}$ contains a geometric hyperplane S such that the subgraph in Γ induced by the complement of S has at least two connected components T_1 and T_2. Then the universal representation group R_U of $\mathcal{G}$ is infinite.*

Proof. For a point x let $u(x)$ denote the corresponding generator of R_U. Let $D = \langle a_1, a_2 \mid a_1^2 = a_2^2 = 1 \rangle$ be the infinite dihedral group. Let χ be the mapping which sends $u(x)$ onto a_i if $x \in T_i$, $i = 1$ or 2 and onto the identity element of D otherwise. Then it is clear that χ induces a surjective homomorphism of R_U onto D and the result follows. Q.E.D.

It was checked by D.V. Pasechnik (private communication) that the tilde geometry $\mathcal{G}(3 \cdot Sp_4(2))$ of rank 2 contains a geometric hyperplane with disconnected complement and by the above lemma the universal representation group of $\mathcal{G}(3 \cdot Sp_4(2))$ is infinite.

For a group G containing a Klein four group let $\mathcal{I}(G)$ be a rank 2 geometry, whose points are the involutions in G, whose lines are the Klein four subgroups in G and the incidence is via inclusion. By the construction $\mathcal{I}(G)$ possesses a representation in G. The following result (Proposition 4.5 in [IPS96]), checked by D.V. Pasechnik on a computer, marked a breakthrough in our understanding of the non-abelian representations.

Lemma 3.7. *The universal representation group of $\mathcal{I}(Alt_7)$ is $3 \cdot Alt_7$.*

It follows immediately from Lemma 2.3 that $3 \cdot Alt_7$ is a representation group of $\mathcal{I}(Alt_7)$, but the universality fact is highly non-trivial. It would be interesting to learn more about representations of the geometries $\mathcal{I}(G)$ for other non-abelian simple groups G. The universal representation group of $\mathcal{I}(Mat_{22})$ is $3 \cdot Mat_{22}$ [IPS96] and of $\mathcal{I}(U_4(3))$ is $3^2 \cdot U_4(3)$ [Rch99].

The calculation of universal representations can be reduced to studying of covering of certain Cayley graphs. Suppose that (R, ψ) is faithful, let Q be the set of all non-identity elements contained in the subgroups $\psi(x)$ taken for all points x and let Ξ be the Cayley graph of R with respect to the set Q of generators. Let Ξ_U be the similar graph associated with the universal representation (R_U, ψ_U). Since (R_U, ψ_U) must also be faithful, the valency of both Ξ and Ξ_U is $p-1$ times the number of points in $\mathcal{G}$. This means that the homomorphism of R_U onto R induces a covering $\varphi : \Xi_U \to \Xi$. Furthermore, for the every line l the covering φ induces an isomorphism of the subgraph $\Xi_U(l)$ in Ξ_U induced by the elements in $\psi_U(l)$ onto the analogous subgraph $\Xi(l)$ in Ξ (both $\Xi_U(l)$ and $\Xi(l)$ are complete graphs on p^2 vertices.) This gives the following.

Lemma 3.8. *Suppose that (R, ψ) is faithful. Let C_0 be the set of triangles in Ξ which are contained in the subgraphs induced by the elements in $\psi(l)$ taken for all lines l and let C be the set of images of the triangles in C_0 under R. If the cycles in C generate the fundamental group of Ξ then the representation (R, ψ) is universal.*

For our last statement assume that every element of $\mathcal{G}$ can be identified with the set of points incident to this element so that the incidence is via inclusion. For an element e of $\mathcal{G}$ let $\psi(e)$ denote the subgroup in R generated by the subgroups $\psi(x)$ taken for all points x incident to e. We say that (R, ψ) is *separable* if $\psi(e) \neq \psi(f)$ whenever $e \neq f$. The separability particularly implies that (R, ψ) is faithful. Define $\mathcal{A}(\mathcal{G}, R)$ to be the incidence system of rank $m+1$ whose elements of type 1 are the elements of R (right cosets of the identity subgroup) and for $2 \leq i \leq m+1$

the elements of type i are all the right cosets of the subgroups $\psi(e)$ for all elements e of type $i-1$ in $\mathcal{G}$; the incidence is via inclusion. The following result is a generalization of Lemma 1.1 in [Iv98].

Lemma 3.9. *In the above terms suppose that (R,ψ) is separable. Then*

(i) *$\mathcal{A}(\mathcal{G},R)$ is a geometry in which the residue of an element of type 1 is isomorphic to $\mathcal{G}$ and the elements of type 1 and 2 incident to an element of type 3 form the affine plane of order p;*

(ii) *if G is a flag-transitive automorphism group of $\mathcal{G}$ then the semidirect product $R:G$ acts flag-transitively on $\mathcal{A}(\mathcal{G},R)$;*

(iii) *if (R',ψ') is another representation of $\mathcal{G}$ and $\chi : R' \to R$ is a morphism of representations, then χ induces a 2-covering of $\mathcal{A}(\mathcal{G},R')$ onto $\mathcal{A}(\mathcal{G},R)$.*

Notice that the Cayley graph Ξ introduced in the paragraph before Lemma 3.8 is the collinearity graph of $\mathcal{A}(\mathcal{G},R)$. The case $p=2$ is of a particular interest since the affine plane of order 2 is isomorphic to the c-geometry of 1- and 2-element subsets of a set of size 4. Thus the representations of Petersen and tilde geometries provide c-extensions of these geometries [SW01]. Similarly representations of the dual polar spaces with 3 points on a line (associated with $Sp_{2n}(2)$ and $U_{2n}(2)$) give their c-extensions. Notice that the universal representations of these dual polar spaces are known only for $n=2$ and 3. It was conjectured by A.E. Brouwer that the dimension of the universal abelian representation of the dual polar space associated with $Sp_{2n}(2)$ is

$$1+{\textstyle\left[{n \atop 1}\right]_2}+{\textstyle\left[{n \atop 2}\right]_2}=(2^n+1)(2^{n-1}+1)/3.$$

Recently this conjecture was proved in [Li00] using some earlier results and methods from [BI97], [McC00] and independently in [BB00] by a different method.

In some cases (compare Theorem 2 (iii) in [Iv98]) one can show that $\mathcal{A}(\mathcal{G},R_U)$ is the universal 2-cover of $\mathcal{A}(\mathcal{G},R)$ and this reduces calculation of the universal representation to the question about 2-simple connectedness. For example the universality of the representation of $\mathcal{G}(M)$ in M established in [IPS96] is equivalent to the 2-simple connectedness of the corresponding c-extension of $\mathcal{G}(M)$. The latter result has been used in [Iv99a] to obtain a new proof identifying Y_{555} with the Bimonster $M \wr 2$.

References

[BI97] M. Bardoe and A.A. Ivanov, Natural representations of dual polar space, Research report, Imperial College, 1997.

[BIP99] B. Baumeister, A.A. Ivanov and D.V. Pasechnik, The universal representation of the 3-local geometry related to $M(24)$, Preprint, 1999.

[BB00] A. Blokhuis and A.E. Brouwer, The universal embedding dimension of the binary symplectic polar spaces, Preprint 2000.

[Iv98] A.A. Ivanov, Affine extended dual polar spaces, In: *Trends in Mathematics*, A. Pasini ed., Birkhäuser Verlag, Basel, 1998, pp. 107–121.

[Iv99a] A.A. Ivanov, *Geometry of Sporadic Groups I, Petersen and Tilde Geometries*, Cambridge Univ. Press, Cambridge, 1999.

[Iv99b] A.A. Ivanov, Y-groups via transitive extension, *J. Algebra*, **218** (1999), 412–435.

[IPS96] A.A. Ivanov, D.V. Pasechnik and S.V. Shpectorov, Non-abelian representations of some sporadic geometries, *J. Algebra*, **181** (1996), 523–557.

[ISh89] A.A. Ivanov and S.V. Shpectorov, Geometries for sporadic groups related to the Petersen graph, II, *Europ. J. Combin,* **10** (1989), 347–362.

[ISh90] A.A. Ivanov and S.V. Shpectorov, P-geometries of J_4-type have no natural representations, *Bull. Soc. Math. Belgique*, (A) **42** (1990), 547–560.

[ISh94a] A.A. Ivanov and S.V. Shpectorov, Natural representations of the P-geometries of Co_2-type, *J. Algebra*, **164** (1994), 718–749.

[ISh94b] A.A. Ivanov and S.V. Shpectorov, Flag-transitive tilde and Petersen type geometries are all known, *Bull. Amer. Math. Soc.*, **31** (1994), 173–184.

[ISh97] A.A. Ivanov and S.V. Shpectorov, The universal non-abelian representation of the Petersen type geometry related to J_4, *J. Algebra*, **191** (1997), 541–567.

[Li00] P. Li, On the universal embedding of the $Sp_{2n}(2)$ dual polar space, *J. Comb. Theory* A (to appear).

[McC00] P. McClurg, On the universal embedding of dual polar space of type $Sp_{2n}(2)$, *J. Combin. Theory* A, **90** (2000), 104–122.

[Pas94] A. Pasini, *Diagram Geometries*, Clarendon Press, Oxford 1994.

[Rch99] P.J. Richardson, Sporadic geometries and their universal representation groups, Ph D Thesis, Imperial College, 1999.

[RSm89] M.A. Ronan and S.D. Smith, Computation of 2-modular sheaves and representations for $L_4(2)$, A_7, $3S_6$ and M_{24}, *Comm. Algebra*, **17** (1989), 1199–1237.

[RSt84] M.A. Ronan and G. Stroth, Minimal parabolic geometries for the sporadic groups, *Europ. J. Combin*, **5** (1984), 59–91.

[Sh93] S.V. Shpectorov, Natural representations of some tilde and Petersen type geometries, *Geom. Dedic.*, **54** (1995), 87–102.

[Sm92] S.D. Smith, Universality of the 24-dimensional embedding of the .1 2-local geometry, *Comm. Algebra*, **22(13)** (1994), 5159–5166.

[SW01] G. Stroth and C. Wiedorn, c-Extensions of P- and T-geometries, *J. Combin. Theory* A, **93** (2001), 261–280.

[Ti74] J. Tits, *Buildings of Spherical Type and Finite BN-pairs*, Lect. Notes Math., **386**, Springer-Verlag, Berlin 1974.

[Yos92] S. Yoshiara, Embeddings of flag-transitive classical locally polar geometries of rank 3, *Geom. Dedic.*, **43** (1992), 121–165.

Department of Mathematics
Imperial College
180 Queen's Gate,
London SW7 2BZ, U.K.
e-mail: a.ivanov@ic.ac.uk

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 315–324

3-transposition automorphism groups of VOA

Masaaki Kitazume and Masahiko Miyamoto

Abstract.

We will consider some vertex operator algebras (VOAs) whose automorphism groups are generated by 3-transpositions. Our main examples are some code VOAs. We will classify the structures of the automorphism groups of the code VOAs. We give explicit constructions of such code VOAs, and determine the full automorphism groups for some cases.

§1. Introduction

A vertex operator algebra $V$ is an infinite dimensional $\mathbb{Z}$-graded algebra, but it has sometimes a finite full automorphism group and a vertex operator subalgebra offers automorphisms of $V$, see [M1]. In this paper, we will treat the case where $\dim V_0 = 1$ and $V_1 = 0$. In this case, V_2 is a commutative (nonassociative) algebra with a symmetric invariant bilinear form $\langle *, * \rangle$ given by $\langle v, u \rangle \mathbf{1} = v_3 u$ for $u, v \in V_2$. This is called a Griess algebra in [M1]. Our purpose in this paper is to study several vertex operator algebras which have 3-transposition automorphism groups. A 3-transposition group is a group generated by a conjugacy class of involutions such that the product of two involutions in this class has the order less than or equal to 3. First examples are the code VOAs M_C which are constructed from even linear binary codes $C$ in [M2]. If $C$ has no codewords of weight 2, then $\dim(M_C)_0 = 1$ and $(M_C)_1 = 0$ and so $(M_C)_2$ is a Griess algebra. In this case, the full automorphism group of M_C is finite [M4] and the automorphism group of M_C has a normal subgroup which is a 3-transposition group. We will classify such 3-transposition groups $G$ and construct code VOAs with automorphism groups $G$. Other examples are the Weyl groups of the root lattices of simply laced finite dimensional Lie algebras, which are also 3-transposition groups. Actually, for every root lattice, we will construct a VOA whose automorphism group contains a semidirect product

Received May 31, 1999.
Revised June 22, 2000.

of the Weyl group and some 2-group. Our most interesting example is a VOA constructed from the E_8-lattice. This VOA also has a structure of a code VOA. We will show its full automorphism group is isomorphic to $O^+(10,2)$, which contains properly the semidirect product mentioned above. We note that this result is already shown by R. Griess [G].

The essential tool is a rational conformal vector with central charge $\frac{1}{2}$. Here a rational conformal vector e is an element in V_2 such that $\tilde{L}(n) = e_{n+1}$ satisfies Virasoro algebra relations:

$$[\tilde{L}(m), \tilde{L}(n)] = (m-n)\tilde{L}(m+n) + \delta_{m+n,0}\frac{m^3-m}{24}1_V$$

with central charge $\frac{1}{2}$ and $\{e_n\}$ generates a rational Virasoro VOA $L(\frac{1}{2},0)$ over the vacuum $\mathbf{1}$, where $Y(e,z) = \sum_{n\in\mathbb{Z}} e_n z^{-n-1}$ is a vertex operator of e.

§2. Griess Algebras

Let $V = \oplus_{n=0}^{\infty} V_n$ be a vertex operator algebra (VOA) with the vacuum $\mathbf{1} \in V_0$ and the Virasoro element $\mathbf{w} \in V_2$. In this paper, we assume that V is a VOA over the real field $\mathbb{R}$ and has a positive definite invariant bilinear form $\langle\cdot,\cdot\rangle$. For example, a lattice VOA or a code VOA satisfies these conditions.

We further assume the following conditions:

$$\dim(V_0) = 1 \ (\text{i.e.} V_0 = \langle \mathbf{1} \rangle), \quad \dim(V_1) = 0.$$

Then by [Li], the invariant bilinear form is uniquely determined up to scalar multiplication, and we may assume

$$\langle u,v\rangle\mathbf{1} = u_3 v$$

for every $u, v \in V_2$. Moreover we can define a binary symmetric product $u \times v$ on V_2 by

$$u \times v := u_1 v.$$

The triple $(V_2, \times, \langle\cdot,\cdot\rangle)$ is called a Griess algebra.

In [M1], the following theorems has been proved.

Theorem 2.1. *The following two conditions are equivalent to each other.*

(1) $\frac{1}{2}e \in V_2$ *is an idempotent (i.e.* $e \times e = 2e$*) with* $\langle e,e\rangle = \frac{1}{4}$

(2) e *is a rational conformal vector with central charge* $\frac{1}{2}$*, that is, the subVOA* $\mathrm{Vir}(e)$ *generated by* e *is isomorphic to* $L(\frac{1}{2},0)$.

Then V splits into the direct sum of irreducible $\mathrm{Vir}(e)$-submodules, which is isomorphic to $L(\frac{1}{2},0), L(\frac{1}{2},\frac{1}{2})$ or $L(\frac{1}{2},\frac{1}{16})$. If there exist no $\mathrm{Vir}(e)$-submodules isomorphic to $L(\frac{1}{2},\frac{1}{16})$, then we say that e is of type 2. An idempotent which is not of type 2 is called of type 1.

Theorem 2.2. (1) *For an idempotent e of type* 1, *define an endomorphism τ_e on V by*

$\tau_e = id$ *on submodules isomorphic to* $L(\frac{1}{2},0)$ *or* $L(\frac{1}{2},\frac{1}{2})$
$\tau_e = -id$ *on submodules isomorphic to* $L(\frac{1}{2},\frac{1}{16})$.

Then τ_e is a automorphism of the VOA V, and $\tau_e^2 = id_V$.

(2) *For an idempotent e of type 2, define an endomorphism σ_e on V by*

$\sigma_e = id$ *on submodules isomorphic to* $L(\frac{1}{2},0)$
$\sigma_e = -id$ *on submodules isomorphic to* $L(\frac{1}{2},\frac{1}{2})$.

Then σ_e is a automorphism of the VOA V, and $\sigma_e^2 = id_V$.

Theorem 2.3. *If $e, f (e \neq f)$ are conformal vectors of type* 2, *then one of the following holds.*

(1) $\langle e, f\rangle = 0$ *and* $(\sigma_e\sigma_f)^2 = 1$
(2) $\langle e, f\rangle = \frac{1}{32}$ *and* $(\sigma_e\sigma_f)^3 = 1$

§3. Code Vertex Operator Algebras

Let C be a binary even code of length n. We further assume that the minimal weight of C is four. Let M_C be the code VOA defined in [M2], that is,

$$M_C = \bigoplus_{c\in C} M_c$$

and $M_c(c = (c_1, c_2, ..., c_n) \in C)$ consists of all linear combinations of the form $u_1 \otimes u_2 \otimes ... \otimes u_n \otimes e^c$ $(u_i \in L(\frac{1}{2},\frac{c_i}{2}))$, where c_i are regarded as integers $0,1$, and e^c is a symbol with $e^c e^{c'} = (-1)^{\langle c,c'\rangle} e^{c'} e^c$. The degree of $u_1 \otimes u_2 \otimes ... \otimes u_n \otimes e^c$ is the sum of the degrees of u_i and $\frac{1}{2}\langle c, c\rangle$ and so the degrees of elements in M_C are integers since C is an even code. The element $\hat{\mathbf{1}} = \mathbf{1}\otimes\mathbf{1}\otimes ... \otimes \mathbf{1}\otimes e^0$ is the vacuum of M_C. Set $\hat{\mathbf{w}}^i = \mathbf{1}\otimes\mathbf{1}\otimes ... \otimes \mathbf{w} \otimes ... \otimes \mathbf{1}\otimes e^0$ ($\mathbf{w}$ is on the i-th component) and define $\hat{\mathbf{w}} = \hat{\mathbf{w}}^1 + ... + \hat{\mathbf{w}}^n$. Then $\hat{\mathbf{w}}$ is the Virasoro element of M_C. The following Lemmas and Theorem are proved in [M2]. In particular, $(M_C)_2$ becomes a Griess algebra by Lemma 3.1.

Lemma 3.1 ([M2]). (1) *M_C has an invariant bilinear form.*
(2) $\dim(M_C)_0 = 1$ *and* $(M_C)_1 = \{0\}$.

Lemma 3.2 ([M2]). (1) *$\hat{\mathbf{w}}^i$ is a conformal vector of type* 2.

(2) *Let H be a $[8,4,4]$-Hamming subcode of C with* $\mathrm{supp}(H) = \{i_1, i_2, i_3, i_4, i_5, i_6, i_7, i_8\}$. *Then for any $\alpha \in \mathbb{F}_2^n$,*

$$e = e_{\alpha,H} := \frac{1}{8}(\hat{\mathbf{w}}^{i_1} + \ldots + \hat{\mathbf{w}}^{i_8}) + \frac{1}{8} \sum_{\beta \in C,\ |\beta|=4} (-1)^{(\alpha,\beta)} u_\beta$$

is a conformal vector of $(M_C)_2$.

(3) *If* $\mathrm{supp}H \subset C^\perp$, *then $e_{\alpha,H}$ is of type* 2.

Remark 3.3. *If α equals to α' modulo $H^\perp$, we have $e_\alpha = e_{\alpha'}$. Hence there exist 2^4 elements $e_{\alpha,H}$ for each H.*

Theorem 3.4 ([M2]). *Let D_C be the set of involutions σ_e such that e is a conformal vector of type* 2. *and let K_C be the subgroup of* $\mathrm{Aut}(M_C)$ *generated by D_C. Then D_C is a set of* 3*-transpositions of K_C.*

Lemma 3.5. *Let $X = \{\sigma_1, \ldots, \sigma_n\}$, where $\sigma_i = \sigma_{\hat{\mathbf{w}}^i}$ for $i = 1, \ldots, n$. Let e be a conformal vector of type* 2 *and assume $\sigma_e \notin X$. Then* $|C_X(\sigma_e)| = n - 8$.

Proof. By the equations: $\frac{1}{4} = \langle e, e\rangle = \langle \mathbf{w}, e\rangle = \langle \hat{\mathbf{w}}^1 + \ldots + \hat{\mathbf{w}}^n, e\rangle$ and Theorem 2.3, there are exactly eight $\hat{\mathbf{w}}^i$, say $\hat{\mathbf{w}}^1, \ldots, \hat{\mathbf{w}}^8$, such that $\langle \hat{\mathbf{w}}^i, e\rangle = \frac{1}{32}$ for $i = 1, \ldots, 8$ and $\langle \hat{\mathbf{w}}^i, e\rangle = 0$ for $i = 9, \ldots, n$. Q.E.D.

Corollary 3.6. *The maximal number of mutually commuting elements of D_C is equal to the length n of the code C.*

Let G be a 3-transposition group generated by D. We will describe a 3-transposition group by the graph whose vertices are the elements of D and edges are defined by :

$$\{a, b\} \text{ is an edge} \iff a \neq b, (ab)^2 = 1.$$

We will denote this graph by $\Gamma(G)$ or $\Gamma(D)$. The graph $\Gamma(G)$ is connected if and only if D is a single conjugacy class of G.

If $O_2(G) \neq 1$, then $\bar{D} = DO_2(G)/O_2(G)$ is a set of 3-transpositions of $\bar{G} = G/O_2(G)$, and the number of the elements of $dO_2(G) \cap D$ is a power of 2 for any $d \in D$. If $\Gamma(G)$ is connected, then this number ($= 2^k$, say) does not depend on the choice of $d \in D$. Then we write $\Gamma(G) = O_2^{(2^k)} \cdot \Gamma(\bar{G})$. The set $dO_2(G) \cap D$ consists of mutually commuting elements, and $e \in dO_2(G) \cap D$ if and only if $C_D(d) = C_D(e)$.

If any two elements of D do not commute, then $G' = O_3(G)$ and $|D|$ is some power of 3. If $|D| = 3^t$ then we write $\Gamma(G) = \Gamma(H_t)$. Notice that $\Gamma(S_3) = \Gamma(H_1)$.

Now we will state the main result of this section. Here we denote by $O^+(2n, 2)$ the group generated by symplectic transvections preserving a given quadratic form with Witt index n. The group $O^+(2n,2)$ is a 3-transposition group and contains a simple subgroup $\Omega^+(2n,2)$ with its index 2.

Theorem 3.7. *Let K_C be the subgroup of $\mathrm{Aut}(M_C)$ generated by D_C, and E be a subset of D_C such that $\Gamma(E)$ is a connected component of $\Gamma(D_C)$. Then $\Gamma(E)$ is isomorphic to one of the following.*

	$\Gamma(E)$	$\lvert E\rvert$	ℓ
(i)	$\Gamma(O^+(10,2))$	496	16
(ii)	$\Gamma(Sp(8,2))$	255	15
(iii)	$O_2^{(2)}\cdot\Gamma(O^+(8,2))$	240	16
(iv)	$O_2^{(2)}\cdot\Gamma(Sp(6,2))$	126	14
(v)	$O_2^{(4)}\cdot\Gamma(S_{2m})\quad(m>1)$	$4m(2m-1)$	$4m$
(vi)	$O_2^{(8)}\cdot\Gamma(H_k)\quad(k>1)$	8×3^k	8

Here ℓ is the maximal number of mutually commuting elements of E.

Proof. Set $H=\langle E\rangle$ and let Y be a maximal set of mutually commuting element of E, that is, Y is the intersection of E and a Sylow 2-subgroup of H. By Lemma 3.5, $|Y\setminus C_Y(\tau)|=8$ for each $\tau\in E\setminus Y$, since each element of E commutes with $D_C\setminus E$,

Let $\bar H=H/O_2(H), \bar E=EO_2(H)/O_2(H), \bar Y=YO_2(H)/O_2(H)$. Then $\Gamma(H)=O_2^{(2^k)}\cdot\Gamma(\bar H)$ for some k and $\Gamma(\bar H)$ is also connected. Moreover $\bar H$ satisfies that $|\bar Y\setminus C_{\bar Y}(\tau)|=\frac{8}{2^k}$ for each $\tau\in\bar E\setminus\bar Y$. In particular, $k=0,1,2$ or 3.

Suppose $O_3(\bar H)\not\subset Z(\bar H)$. Let $\tau\in\bar Y$ and $\tau'\in\tau\in\bar E\setminus\{\tau\}$. Then $\bar Y\setminus C_{\bar Y}(\tau')=\{\tau\}$ and so $k=3$. Hence if $\bar Y=\{\tau_1,...,\tau_s\}$ for some s, then $\bar E=(\tau_1O_3(\bar H)\cap\bar E)\cup...\cup(\tau_sO_3(\bar H)\cap\bar E)$. Since $\Gamma(\bar H)$ is connected, we have $s=1$ Hence $\Gamma(\bar H)=\Gamma(H_t)$ for some t. By the same argument if $k=3$ then $\Gamma(\bar H)=\Gamma(H_t)$ for some t.

Now we may assume $O_3(\bar H)\subset Z(\bar H)\supset O_2(\bar H)$. Then we can use the list of Fischer's classification [Fi], and it is easily verified that $\Gamma(\bar H)$ is one of the following

$$\begin{array}{lll}
(k=0) & \Gamma(O^+(10,2)), & \Gamma(Sp(8,2)) \\
(k=1) & \Gamma(O^+(8,2)), & \Gamma(Sp(6,2)) \\
(k=2) & \Gamma(S_{2m})(m>2). &
\end{array}$$

The proof of Theorem is completed. Q.E.D.

Remark 3.8. (1) *The main parts of the groups of the cases* (*iii*), (*iv*) *are the Weyl groups $W(E_8)$, $W(E_7)$ respectively. Under such a viewpoint, the main parts of the groups of* (*v*) *are the Weyl groups $W(D_{2m})$* ($m=2for(vi)$). (*i.e.* $O_2^{(4)}\cdot\Gamma(S_{2m})\cong O_2^{(2)}\cdot\Gamma(W(D_{2m}))$)

(2) $O_2^{(4)} \cdot \Gamma(S_4)$ *is also written as* $O_2^{(8)} \cdot \Gamma(H_1)$.

(3) *We do not know any examples of (vi) of Theorem.*

In general, we can not determine the center $Z(K_C)$ from the graph $\Gamma(K_C)$. Under some assumption, we can prove $Z(K_C) = \{id\}$.

Lemma 3.9. *If C is spanned by the elements of weight* 4, *then M_C is generated by $(M_C)_2$ as a VOA.*

Proof. Since $L(\frac{1}{2}, 0)$ is generated by its Virasoro element as a VOA, $M_0 (0 \in C)$ is generated by the vectors $\hat{\mathbf{w}}^i$. Since $L(\frac{1}{2}, \frac{1}{2})$ is generated by its highest weight vector as an $L(\frac{1}{2}, 0)$-module, $M_c (c \in C, wt(c) = 4)$ is generated by the element of degree 2 as an M_0-module. The assertion of Lemma is easily deduced from the fact $M_c M_{c'} \subset M_{c+c'}$ and $M_c M_{c'} \neq \{0\}$ for $c, c' \in C$. Q.E.D.

Lemma 3.10. (1) *If M_C is generated by $(M_C)_2$ as a VOA, then we have $Z(K_C) = \{id\}$.*

(2) *Furthermore if $(M_C)_2$ is spanned by the conformal vectors $e_{\alpha,H}$, then* $\mathrm{Aut}(M_C)$ *is a subgroup of* $\mathrm{Aut}(K_C)$

Proof. (1) is trivial. Let $\phi \in C_{\mathrm{Aut}(M_C)}(K_C)$. Then ϕ commutes with all the element of D_C, and thus ϕ stabilize all the vectors $e_{\alpha,H}$. By the assumption of (2), ϕ acts trivially on M_C and we have ϕ is the identity. Since K_C is a normal subgroup of $\mathrm{Aut}(M_C)$, Lemma is proved. Q.E.D.

§4. Weyl groups

Let L be a root lattice of type X_n with root system Φ, where X be one of A, D, E, and $n = 6, 7, 8$ if $X = E$. Let $V_{\sqrt{2}L}$ be the VOA constructed from $\sqrt{2}L$ as in [FLM]. Since there are no roots in $\sqrt{2}L$, $(V_{\sqrt{2}L})_1 = \mathbb{C} \otimes L$. Let θ be an automorphism induced from -1 on L and $V(X_n) = (V_{\sqrt{2}L})^\theta$ the fixed point space of θ. We will show that $\mathrm{Aut}(V(X_n))$ contains a semidirect product of the Weyl group $W(X_n)$ and some 2-group.

By the construction, $V(X_n)_2$ is spanned by the vectors $v(-1)v(-1)\mathbf{1}$ and $e^{\sqrt{2}x} + e^{-\sqrt{2}x}$ for $v \in L$ and $x \in \Phi$. The former are identified with the vectors of the symmetric tensor $S^2(\mathbb{R} \otimes L)$. In particular,

Lemma 4.1. $\dim V(X_n)_2 = \dfrac{n(n+1)}{2} + \dfrac{1}{2}|\Phi|.$

For example, $\dim V(E_8)_2 = 36 + 120 = 156$, and $\dim V(D_n)_2 = \frac{n(n+1)}{2} + n(n-1) = \frac{1}{2}(3n^2 - n)$.

Let $x \in \Phi$, then $\sqrt{2}x$ has a squared length 4 and so

$$e(x)^i = \frac{1}{8}x(-1)x(-1)\mathbf{1} - (-1)^i\frac{1}{4}(e^{\sqrt{2}x} + e^{-\sqrt{2}x}) \qquad (\#)$$

are conformal vectors with central charge $\frac{1}{2}$ for $i = 1, 2$. Since $V_{\sqrt{2}L}$ has a positive definite invariant bilinear form, $e(x)^1$ and $e(x)^2$ are both rational conformal vectors. As we showed in [M3],

$$x(-1) \in L(\frac{1}{2}, \frac{1}{2}) \otimes L(\frac{1}{2}, \frac{1}{2})$$

and

$$e^y \in \left(L(\frac{1}{2}, 0) \oplus L(\frac{1}{2}, \frac{1}{2})\right) \otimes \left(L(\frac{1}{2}, 0) \oplus L(\frac{1}{2}, \frac{1}{2})\right)$$

as $\langle e(x)^1, e(x)^2\rangle$-modules for $y \in L$ with $\langle y, x\rangle \in 2\mathbb{Z}$. Therefore, we have proved the following result.

Lemma 4.2. *All conformal vectors $e(x)^i$ defined by roots in L as in (#) are of type* 2.

Let D be the set of all $\sigma_{e(x)^i}$ for $i = 1, 2$ and each root $x \in \Phi$. By Lemma 4.2 and Theorem 2.3, D is a set of 3-transpositions.

By direct calculations, we have:

Theorem 4.3. *Let x and y be distinct two roots. If $\langle x, y\rangle = 0$, then $\langle e(x)^i, e(y)^i\rangle = 0$ and $(\sigma_{e(x)^i}\sigma_{e(y)^i})^2 = 1$ for $i, j = 1, 2$. If $\langle x, y\rangle = \pm 1$, then $\langle e(x)^i, e(y)^i\rangle = \frac{1}{32}$ and $(\sigma_{e(x)^i}\sigma_{e(y)^i})^3 = 1$ for $i, j = 1, 2$.*

Notice that there exist two involutions $\sigma_{e(x)^1}, \sigma_{e(x)^2}$ for each root x. Hence the set $\{\sigma_{e(x)^1}, \sigma_{e(x)^2}\}$ is a nontrivial block of imprimitivity of the action of the group $\langle D\rangle$ on D by conjugation. ¿From a general theory of 3-transposition groups, all the products $\sigma_{e(x)^1}\sigma_{e(x)^2}$ generate the normal subgroup $O_2(\langle D\rangle)$. Hence the group $\langle D\rangle$ is a semidirect product of the Weyl group $W(X_n)$ and $O_2(\langle D\rangle)$, that is, $\Gamma(\langle D\rangle) \cong O_2^{(2)} \cdot \Gamma(W(X_n))$.

By [M5], we have the following Proposition.

Proposition 4.4. *The VOA $V(E_8)$ is isomorphic to the code VOA V_C, where C is the 2nd order Reed-Muller code $RM(4, 2)$ of length* 16.

Proof. We use the notation in Section 5 of [M5]. Let $\{x^1, ..., x^8\}$ be an orthonormal basis of an 8-dimensional Euclidean space. Set $L(1) = \langle x^i : i = 1, ..., 8\rangle$ and $E_8(4)$ be the lattice spanned by

$\frac{1}{2}(x^1 - x^3 - x^5 - x^7) + x^2$, $\quad \frac{1}{2}(x^1 - x^2 + x^5 - x^6) - x^3$,
$\frac{1}{2}(-x^1 + x^2 - x^3 - x^4) - x^7$, $\quad \frac{1}{2}(x^1 + x^3 - x^6 + x^8) + x^5$,
$2x^i \ (i = 1, ..., 8)$,

which is isomorphic to the root lattice of type E_8. Then the lattice VOA $V_{E_8(4)}$ contains the following 16 mutually orthogonal conformal vectors of type 1 :

$$e^{2i-j} = \frac{1}{4}x^i(-1)^2\mathbf{1} - (-1)^j\frac{1}{4}(e^{2x^i} + e^{-2x^i})\ (i = 1, ..., 8,\ j = 1, 0).$$

Let $P(4) = \langle \tau_{e^i} : i = 1, ..., 16\rangle$ and $L(4) = E_8(4) \cap L(1)$. Then $L(4)$ is isomorphic to $\sqrt{2}E_8$ and $(V_{E_8(4)})^{P(4)}$ coincides with $V_{L(4)}$.

Let V be a VOA constructed by the orbifold construction from $V_{E_8(4)}$. Then V is isomorphic to $V_{E_8(4)}$. Let $P = \langle \tau_{e^i} : i = 1, ..., 16\rangle$. (Here we use the same symbols τ_{e^i}. Notice that $P \subset \mathrm{Aut}(V)$, and $P(4) \subset \mathrm{Aut}(V_{E_8(4)})$.) Then V^P is also constructed by the orbifold construction from $(V_{E_8(4)})^{P(4)}$, and V^P is isomorphic to M_C by Proposition 5.1 of [M5]. Clearly V^P contains $((V_{E_8(4)})^{P(4)})^\theta = (V_{L(4)})^\theta$, which is isomorphic to $V(E_8)$. By Lemma 4.1 we have $\dim V(E_8)_2 = 156$, and we will show that $\dim(M_C)_2 = 156$ in Section 5. Hence we have $(((V_{E_8(4)})^{P(4)})^\theta)_2 = (V^P)_2$ and thus $V(E_8)$ is isomorphic to M_C by Lemma 3.9. Q.E.D.

Similarly the following isomorphism can be proved.

$$V(E_7) \cong M_{C''}, V(D_{2m}) \cong M_{C_m},$$

where m is a integer and C' and C_m will be defined in the next section.

§5. Examples

In this section, we will give some examples and consider the full automorphism groups. The notation of (1) will be used in (2)-(4).

(1) $M_C \cong V(E_8)$: Let Ω be the set of all the vectors of the 4-dimensional vector space V over the two element field F_2, that is, a point of Ω is a vector of V. We regard the power set $P(\Omega)$ of Ω (i.e. the set of all the subsets of Ω) as a vector space over F_2 by defining the sum $X + Y$ as their symmetric difference $(X \cup Y) \setminus (X \cap Y)$ for $X, Y \subset \Omega$.

We define the code $C \subset P(\Omega)$ as the subspace spanned by all the 2-dimensional affine subspaces of V. Then C is a $[16, 11, 4]$-code and is known as the extended Hamming code of length 16 or the 2nd order Reed-Muller code $RM(4, 2)$ of length 16.

A codeword of minimal weight of C corresponds with a 2-dimensional affine subspace of V. Hence C contains $140(= \frac{(16-1)(16-2)}{(4-1)(4-2)} \times 4)$ vectors of weight 4, and thus $\dim(M_C)_2 = 156$.

Let W be a 3-dimensional affine subspace of V, and H_W be a subcode of C spanned by all the 2-dimensional affine subspaces of W.

Then it is easy to see that H_W is a [8,4,4]-Hamming subcode of C, and $\mathrm{supp} H_W \subset C^{\perp}$. Since the number of the 3-dimensional affine subspaces of V is $30 (= \frac{(16-1)(16-2)(16-4)}{(8-1)(8-2)(8-4)} \times 2)$, we can obtain $480 (= 30 \times 2^4)$ involutions defined by a conformal vector e_{α, H_W} for some W. Hence the set D_C contains at least 496 elements. By Theorem 3.7, we have $|D_C| = 496$ and $\Gamma(K_C) \cong \Gamma(O^{+}(10,2))$. By Lemmas 3.9, 3.10 and the fact $|\mathrm{Out}(\Omega^{+}(10,2))| = 2$, we have $K_C = \mathrm{Aut}(M_C) \cong O^{+}(10,2)$.

We note that this result is already obtained by R. L. Griess ([G]).

(2) Let $\mathbf{0}$ be the zero vector of V, and set $\Omega' = \Omega \setminus \{\mathbf{0}\}$. We define the code $C' \subset P(\Omega')$ as the subspace spanned by all the 2-dimensional affine subspaces W of V satisfying $\mathbf{0} \notin W$. Then C' is a $[15,10,4]$-code.

By a similar calculations as in (1), we have that $\dim(M_{C'})_2 = 15 + \frac{(16-1)(16-2)}{(4-1)(4-2)} \times 3 = 120$, $|D_{C'}| = 15 + \frac{(16-1)(16-2)(16-4)}{(8-1)(8-2)(8-4)} \times 2^4 = 255$, and $\Gamma(K_{C'}) \cong \Gamma(Sp(8,2))$. By Lemma 3.10 and the fact $|\mathrm{Out}(Sp(8,2))| = 1$, we have $K_C = \mathrm{Aut}(M_C) \cong Sp(8,2)$.

(3) $M_{C''} \cong V(E_7)$: Let U be a one-dimensional subspace of V, and set $\Omega'' = \Omega \setminus U$. We define the code $C'' \subset P(\Omega'')$ as the subspace spanned by all the 2-dimensional affine subspaces W of V satisfying $U \cap W = \emptyset$. Then C'' is a $[14,7,4]$-code. There exist seven 2-(resp. 3-) dimensional linear subspaces containing U. Hence $\dim(M_{C''})_2 = 14 + 7 \times 3 + 28 \times 2 = 91$ and $|D_{C''}| = 14 + 7 \times 2^4 = 126$. Moreover we have $\Gamma(K_{C''}) \cong O_2^{(2)} \cdot \Gamma(Sp(6,2))$.

(4) $M_{C_m} \cong V(D_{2m})$: For an integer $m > 1$, we define a $[4m, 3m-2, 4]$-code C_m by the following generating matrix

$$\begin{pmatrix}
1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0 & \ldots & 0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0 & \ldots & 0\,0\,0\,0\,0\,0\,0\,0 \\
 & \ldots & \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & \ldots & 0\,0\,0\,0\,1\,1\,1\,1 \\
1\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,0 & \ldots & 0\,0\,0\,0\,0\,0\,0\,0 \\
 & \ldots & \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & \ldots & 1\,0\,1\,0\,1\,0\,1\,0
\end{pmatrix}.$$

Then $\dim(M_{C_m})_2 = 6m^2 - m$, $|D_{C_m}| = 8m^2 - 4m$, and $\Gamma(K_{C_m}) \cong O_2^{(4)} \cdot \Gamma(S_{2m})$.

(5) Let r be a integer greater than 1. Let $V_i, \Omega_i, C_i \subset P(\Omega_i)$ be a copy of V, Ω, C of (1) respectively for $i = 1, ..., r$. We fix a 1-dimensional subspace U_i of V_i for each i.

Set $\tilde{C} = C_1 \oplus C_2 \oplus ... \oplus C_r$, $\tilde{V_i} = \{\mathbf{0}\} \oplus ... \oplus \{\mathbf{0}\} \oplus V_i \oplus \{\mathbf{0}\} \oplus ... \oplus \{\mathbf{0}\}$, $\tilde{U_i} = \{\mathbf{0}\} \oplus ... \oplus \{\mathbf{0}\} \oplus U_i \oplus \{\mathbf{0}\} \oplus ... \oplus \{\mathbf{0}\}$, and $\tilde{U_{ij}} = \tilde{U_i} \cup \tilde{U_j}$ for $i \neq j$. Then the weight of $\tilde{U_{ij}}$ is 4. Let $C(r)$ be a code of length $16r$ spanned by $\tilde{C}$ and all $\tilde{U_{ij}}$ for $i \neq j$.

Let $\tilde{W}_i$ be a 3-dimensional affine subspace of $\tilde{V}_i$, and $H(\tilde{W}_i)$ be a subcode of $C(r)$ spanned by all the 2-dimensional affine subspaces of $\tilde{W}_i$. Then the condition supp$H(\tilde{W}_i) \subset C(r)^{\perp}$ holds if and only if $\tilde{W}_i$ contains $\tilde{U}_i + a$ for any $a \in \tilde{W}_i$. The number of $\tilde{W}_i$ satisfying this condition is $14(=\frac{(16-2)(16-4)}{(8-2)(8-4)} \times 2)$ for each i. It is easy to see that $|D_{C(r)}| = 240r$ and $\Gamma(K_{C(r)}) \cong \{O_2^{(2)} \cdot \Gamma(O^+(8,2))\}^r$. We note that this VOA does not satisfy the assumption of Lemma 3.10(2).

References

[Fi] B. Fischer, Finite groups generated by 3-transpositions, University of Warwick, Lecture notes, 1969.

[FLM] I. B. Frenkel, J. Lepowsky and A. Meurman, "Vertex Operator Algebras and the Monster", Pure and Applied Math., Vol. 134, Academic Press, 1988.

[G] R. L. Griess, A vertex operator algebra related to E_8 with automorphism group $O^+(10,2)$, *The Monster and Lie algebras* (*Columbus, OH, 1996*), 43–58, Ohio State Univ. Math. Res. Inst. Publ., **7**, de Gruyter Berlin, 1998.

[Li] H. Li, Symmetric invariant bilinear forms on vertex operator algebras, *J. Pure and Applied Algebra*, **96** (1994), 279–297.

[M1] M. Miyamoto, Griess algebras and conformal vectors in vertex operator algebras, *J. Algebra*, **179** (1996), 523–548.

[M2] M. Miyamoto, Binary codes and vertex operator (super)algebras, *J. Algebra*, **181** (1996), 207–222.

[M3] M. Miyamoto, Representation theory of code vertex operator algebra, *J. Algebra*, **201** (1998), 115–150.

[M4] M. Miyamoto, The moonshine VOA and a tensor product of Ising models, *The Monster and Lie algebras* (*Columbus, OH*, 1996), 99–110, Ohio State Univ. Math. Res. Inst. Publ., **7**, de Gruyter Berlin, 1998.

[M5] M. Miyamoto, A new construction of the moonshine vertex operator algebra over the real number field, preprint.

Masaaki Kitazume
Department of Mathematics and Informatics
Faculty of Science, Chiba University
Chiba 263-8522, Japan

Masahiko Miyamoto
Institute of Mathematics
University of Tsukuba
Tsukuba 305-8571, Japan

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 325–336

The calculation of the character of Moonshine VOA

Takeshi Kondo

§1. Introduction

In Miyamoto [M3], [M6] and Dong-Griess-Höhn [DGH], they described the structure of the Moonshine VOA $\mathbf{V}^\natural$ by using two binary codes $D^\natural, S^\natural$ and Ising models $L(\frac{1}{2},0)$, $L(\frac{1}{2},\frac{1}{2})$, $L(\frac{1}{2},\frac{1}{16})$.

The purpose of this note is to calculate the character of $\mathbf{V}^\natural$ and the Thompson series of two involutions of Monster $\mathrm{Aut}(\mathbf{V}^\natural)$ ($2A, 2B$-involutions of Monster) explicitly by following the descriptions of $\mathbf{V}^\natural$ in [M3],[M6] and [DGH]. As is well known (cf.[CN]), these are equal to

$$j(z)-744,\ \left(\frac{\eta(z)}{\eta(2z)}\right)^{24}+2^{12}\left(\frac{\eta(2z)}{\eta(z)}\right)^{24}+24,\ \left(\frac{\eta(z)}{\eta(2z)}\right)^{24}+24$$

respectively, where $j(z)$ is the well known elliptic modular function and $\eta(z)$ is Dedekind's $\eta$-function. Also see a remark at the end of §4 for the calculations of Thompson series for some other elements. Finally, in §5, we will mention a little bit about VOA of "Reed Müller type".

§2. Ising models

2.1. Virasoro Algebra

An infinite dimensional Lie algebra **Vir** having a basis $\{L(m)\ (m \in \mathbf{Z}),\ \mathbf{c}\}$ is called Virasoro algebra if they satisfies

$$[L(m),\mathbf{c}]=0,\ [L(m),L(n)]=(m-n)L(m+n)+\frac{m^3-m}{12}\delta_{m+n,0}\mathbf{c}.$$

Let $L(c,h)$ be an irreducible module of **Vir** with central charge c ($\in \mathbf{C}$) and highest weight h ($\in \mathbf{C}$). Namely, there exists a vector $v \in$

Received August 31, 1999.
Revised May 16, 2000.

$L(c,h)$ such that $L(n)v = 0$ $(n > 0)$, $L(0)v = hv$, $\mathbf{c}v = cv$ and $L(c,h)$ is spanned by $L(-n_1)L(-n_2)\cdots L(-n_r)v$ $(n_1 \geq n_2 \geq \cdots \geq n_r > 0$).

As is easily seen from the commutator relations between the $L(n)$, $L(-n_1)L(-n_2)\cdots L(-n_r)v$ is an eigen vector of $L(0)$ with an eigen value $h+n_1+n_2+\cdots+n_r$ and so $L(c,h)$ is a direct sum of eigenspaces $\mathbf{V}_{h+n}$ of $L(0)$ with eigen value $h+n$ $(0 \leq n \in \mathbf{Z})$ $:L(c,h) = \oplus_{n\geq 0}\mathbf{V}_{h+n}$. Now define a q-series

$$ch(L(c,h)) = \sum_{n\geq 0}(dim\ \mathbf{V}_{h+n})q^{h+n}.$$

This series is called the character of $L(c,h)$. More generally, for a graded space $\mathbf{U} = \oplus_{n\in\mathbf{Q}}U_n$, a q-series $ch(\mathbf{U}) = \sum_{n\in\mathbf{Q}}(dim\ U_n)q^n$ is called the character of a graded space $\mathbf{U}$.

An important thing is that, if $h = 0$, $L(c,0)$ has a structure of **VOA** . Such VOA is called Virasoro VOA and is the most fundamental example of VOA.

In the following, we will consider the case $c = \frac{1}{2}$.

2.2. Ising models

2.2.1. *Irreducible modules of* $L(\frac{1}{2},0)$. As for modules of **VOA** $L(\frac{1}{2},0)$, the following is known:

(2,1) *Any modules of* **VOA** $L(\frac{1}{2},0)$ *is completely reducible and* **VOA** $L(\frac{1}{2},0)$ *has just three irreducible modules* $L(\frac{1}{2},0)$, $L(\frac{1}{2},\frac{1}{2})$, $L(\frac{1}{2},\frac{1}{16})$. (cf. [DMZ])

Let $\mathbf{T}_n$ be the tensor product $L(\frac{1}{2},0)\otimes\cdots\otimes L(\frac{1}{2},0)$ of n copies of $L(\frac{1}{2},0)$. Then, by a general theory of **VOA**,

(2,2) $\mathbf{T}_n$ *has VOA-structure and any module of* $\mathbf{T}_n$ *is completely reducible. Also,* $\mathbf{T}_n$ *has just* 3^n *irreducible modules*

$$L(h_1,h_2,\cdots,h_n) = L(\frac{1}{2},h_1)\otimes L(\frac{1}{2},h_2)\otimes\cdots\otimes L(\frac{1}{2},h_n)\ (h_i = 0, \frac{1}{2}\ or\ \frac{1}{16})$$

2.2.2. *Characters of* $L(\frac{1}{2},h)$. As for the characters of $L(\frac{1}{2},h)$ $(h = 0, \frac{1}{2}$ *or* $\frac{1}{16})$, the followings are known: Let

$$q_+ = \prod_{n=0}^{\infty}(1+q^{n+\frac{1}{2}}),\ q_- = \prod_{n=0}^{\infty}(1-q^{n+\frac{1}{2}}),\ q_0 = \prod_{n=1}^{\infty}(1+q^n).$$

Then we have
$ch(L(\frac{1}{2},0)) = \frac{1}{2}(q_+ + q_-)$, $ch(L(\frac{1}{2},\frac{1}{2})) = \frac{1}{2}(q_+ - q_-)$, $ch(L(\frac{1}{2},\frac{1}{16})) = q^{\frac{1}{16}}q_0$.

The characters of $L(h_1, h_2, \cdots, h_n) = \otimes^n L(\frac{1}{2}, h_i)$ is

$$ch(L(h_1, h_2, \cdots, h_n)) = \prod_{i=1}^{n} ch(L(\frac{1}{2}, h_i)).$$

Let $\eta(z) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n)$ $(q = exp(2\pi i z))$ be Dedekind's η-function. Then it is clear that

$$q_0 = q^{-\frac{1}{24}} \frac{\eta(2z)}{\eta(z)}, \quad q_+q_- = q^{\frac{1}{24}} \frac{\eta(z)}{\eta(2z)}, \quad q_0q_+q_- = 1.$$

Also we have

$$16q^{\frac{1}{2}}q_0^8 = q_+^8 - q_-^8 \text{ (Jacobi)}.$$

Furthermore, for the calculations of the character of some VOA, it is convenient to note

$$j(z)^{\frac{1}{3}} = 2^8 \left(\frac{\eta(2z)}{\eta(z)}\right)^{16} + \left(\frac{\eta(z)}{\eta(2z)}\right)^8,$$

where $j(z)$ is the well known elliptic modular function.

2.2.3. *Fusion rules.* Let Λ_n be the set of all irreducible modules of $\mathbf{T}_n = \otimes^n L(\frac{1}{2}, 0) : \Lambda_n = \{L(h_1, h_2, \cdots, h_n) \mid h_i = 0, \frac{1}{2} \textit{ or } \frac{1}{16}\}$.
Let a binary word $\delta = (\delta_1, \delta_2, \cdots, \delta_n) \in \mathbf{F}_2^n$ of length n act on Λ_n as follows:For $\mathbf{F}_2^n \ni \delta = (\delta_1, \cdots, \delta_n)$

$$L(h_1, h_2, \cdots, h_n) \longrightarrow L(h_1 + \frac{\delta_1}{2}, h_2 + \frac{\delta_2}{2}, \cdots, h_n + \frac{\delta_n}{2}).$$

Here the sum " $h_i + \frac{\delta_i}{2}$" is defined as follows:

$$\frac{1}{2} + 0 = \frac{1}{2}, \ \frac{1}{2} + \frac{1}{2} = 0, \ \frac{1}{16} + 0 = \frac{1}{16}, \ \frac{1}{16} + \frac{1}{2} = \frac{1}{16}$$

These come from well known fusion rules of Ising models which are the most important in the theory of Framed VOA described in the next section. Note that every orbit of the action of $\mathbf{F}_2^n$ on Λ_n is the set of $L(h_1, h_2, \cdots, h_n)$ which have $h_i = \frac{1}{16}$ in the same position.

§3. Framed *VOA*

We will consider a simple **VOA** $\mathbf{V} = \oplus_{n=0}^{\infty} \mathbf{V}_n$ satisfying the following conditions:

(3.1) *$dim\mathbf{V}_0 = 1$, i.e. $\mathbf{V}_0 =< \mathbf{1} >$ where $\mathbf{1}$ is the vacuum of $\mathbf{V}$,*

(3.2) $\mathbf{V}$ *contains* $\mathbf{T}_n = \otimes^n L(\frac{1}{2},0)$ *as a subVOA which has Virasoro element in common.*
Recently VOA of this type is called Framed VOA. Viewing $\mathbf{V}$ as a $\mathbf{T}_n$-module, the complete reducibility (2,2) of $\mathbf{T}_n$ yields the decomposition

$$\mathbf{V} \simeq \oplus_{(h_1,h_2,\cdots,h_n)} a_{(h_1,h_2,\cdots,h_n)} L(h_1,h_2,\cdots,h_n) \text{ (as } \mathbf{T}_n\text{-module)}$$

where the $a_{(h_1,h_2,\cdots,h_n)}$ express multiplicity. This decomposition yields an isomorphism as graded space by the condition (3.2) and so we have

$$ch(\mathbf{V}) = \sum_{n=0}^{\infty}(dim\mathbf{V}_n)q^n = \sum_{(h_1,h_2,\cdots,h_n)} a_{(h_1,h_2,\cdots,h_n)} ch(L(h_1,h_2,\cdots,h_n)).$$

Thus , if we know the multiplicities $a_{(h_1,h_2,\cdots,h_n)}$, the character of $\mathbf{V}$ can be written down immediately by using the characters of Ising models. Note that $h_1+h_2+\cdots+h_n$ is a nonnegative integer, because the weights of VOA are integers.

Now Miyamoto [M3], [M6] and Dong-Griess-Höhn [DGH] showed that the above decomposition of $\mathbf{V}$ has a "2-structure " described in terms of two binary even codes S and D which will be explained in the following. However we will mention just the results and the proofs of the statements will be omitted. For the proofs, we refer the readers to [M1], [M4], [M6] (or [DGH]) together with [DM].

3.1. Code S

For $\mathbf{h} = (h_1,h_2,\cdots,h_n)$ ($h_i = 0, \frac{1}{2}$ or $\frac{1}{16}$), we assign a binary word $\tilde{\mathbf{h}} = (h'_1,h'_2,\cdots,h'_n) \in \mathbf{F}_2^n$ as follows:

$$h'_i = \begin{cases} 1 & \text{if } h_i = \frac{1}{16} \\ 0 & \text{if } h_i = 0 \text{ or } \frac{1}{2}. \end{cases}$$

Thus a word $\tilde{\mathbf{h}}$ shows positions in which the $h_i = \frac{1}{16}$ appear. Let

$$S = \{\tilde{\mathbf{h}} \mid a_{\mathbf{h}} = a_{(h_1,h_2,\cdots,h_n)} \neq 0\}.$$

Then we have

(3,1,1) *S is a linear code.*

(3,1,2) $S \ni \alpha \Longrightarrow 8|wt(\alpha)$, i.e.*the weight of every word of S is divisible by* 8.

(3,1,3) $\tilde{\mathbf{h}} = \tilde{\mathbf{h}'} \Longrightarrow a_{\mathbf{h}} = a_{\mathbf{h}'}$, i.e. *the multiplicities $a(h_1,h_2,\cdots,h_n)$ of two $L(h_1,h_2,\cdots,h_n)$ coincide if $\frac{1}{16}$ appear in the same positions.*
Therefore, gathering the $L(h_1,h_2,\cdots,h_n)$ with $\frac{1}{16}$ in the same positions, we get the decomposition.

(3,1,4) $\mathbf{V}^\alpha = a_\alpha(\oplus_{\tilde{\mathbf{h}}=\alpha} L(h_1,h_2,\cdots,h_n))$, $\mathbf{V} = \oplus_{\alpha\in S}\mathbf{V}^\alpha$.
We will call this decomposition $\mathbf{T}_n$*-decomposition of* $\mathbf{V}$.

3.2. Code D

In this subsection, we will consider the $L(h_1, h_2, \cdots, h_n)$ with $\tilde{\mathbf{h}} = 0$. Thus we have $h_i = 0$ *or* $\frac{1}{2}$. For $\mathbf{h} = (h_1, h_2, \cdots, h_n)$ with $\tilde{\mathbf{h}} = 0$, assign a binary word $(2h_1, 2h_2, \cdots, 2h_n) \in \mathbf{F}_2^n$ and set

$$D = \{(2h_1, 2h_2, \cdots, 2h_n) \mid \tilde{\mathbf{h}} = 0 \text{ and } a_{\mathbf{h}} \neq 0\}.$$

Then we have

(3,2,1) *D is an even linear code and $D^{\perp} \supset S$* ,

(3,2,2) $\tilde{\mathbf{h}} = 0 \Longrightarrow a_{\mathbf{h}} = 1$.

Let

$$V^0 = \oplus_{\tilde{\mathbf{h}}=0} L(h_1, h_2, \cdots, h_n) = \oplus_{\delta \in D} L(\frac{\delta_1}{2}, \frac{\delta_2}{2}. \cdots, \frac{\delta_n}{2})$$

where $\delta = (\delta_1.\delta_2, \cdots, \delta_n)$.

Then we have

(3,2,3) $\mathbf{V}^0$ is a subVOA of $\mathbf{V}$ and the $\mathbf{V}^{\alpha}$ $(\alpha \in S)$ are irreducible modules of $\mathbf{V}^0$.

3.3. The structure of $\mathbf{V}^{\alpha}$

$\mathbf{V}^0$ defined above is what is called Code VOA in a series of Miyamoto's papers [M2], [M4], [M5] and [M6]. In view of Miyamoto [M4], the multiplicities a_{α} $(\alpha \in S)$ are described as follows by using D, S, α:

For $\alpha \in S$, set $D_{\alpha} = \{\delta \in D \mid supp(\delta) \subset supp(\alpha)\}$.

(3,3,1) *Let H_{α} be a maximal selforthogonal subcode of D_{α}. Then* $a_{\alpha \cdot} = [D_{\alpha} : H_{\alpha}]$.

Now consider the decomposition $\mathbf{V}^{\alpha} = a_{\alpha}(\oplus_{\tilde{\mathbf{h}}=\alpha} L(h_1, h_2, \cdots, h_n))$.

Then *what is the set of the $L(h_1, h_2, \cdots, h_n)$ which appears in the righthandside?*

In order to examine this set, recall the action of $\mathbf{F}_2^n$ on Λ_n defined in §2.2.3. For $\alpha \in S$, we put

$$\Lambda_n(\alpha) = \{L(h_1, h_2, \cdots, h_n) \mid \tilde{\mathbf{h}} = \alpha\}$$

and consider the action of D on $\Lambda_n(\alpha)$. Then we have that

the set of $\{L(h_1, h_2, \cdots, h_n)\}$ which appear in the above decomposition of $\mathbf{V}^{\alpha}$ is equal to an orbit (with integral weight) of the action of D on $\Lambda_n(\alpha)$.

Note that D_{α} is one-point stabilizer of this action of D on $\Lambda_n(\alpha)$. Therefore,

the number of orbits of the action of D on $\Lambda_n(\alpha)$ $= \dfrac{2^{n-wt(\alpha)}}{[D : D_{\alpha}]}$.

Thus we see that the decomposition of a Framed VOA as $\mathbf{T}_n$-module

$$\mathbf{V} \simeq \oplus_{(h_1,h_2,\cdots,h_n)} a_{(h_1,h_2,\cdots,h_n)} L(h_1,h_2,\cdots,h_n) \text{ (as } \mathbf{T}_n\text{-module)}$$

can be completely described by two binary codes D, S and the choice of an orbit of the action of D on $\Lambda_n(\alpha)$ for each $\alpha \in S$.

Remark. Now we are naturally led to a problem:

When two binary codes D, S *satisfying* (3,1,2) *and* (3,2,1) *are given, can we construct a VOA by choosing suitably an orbit* (*with integral weight*) *of the action of* D *on* $\Lambda_n(\alpha)$ *for each* $\alpha \in S$?

In [M5], [M6], Miyamoto showed that, under suitable conditions for D, S, Framed VOA can be constructed (for some such examples, see §5 of this note) and, in particular, starting from two special binary codes $D^\natural, S^\natural$ which are described in the next section, Moonshine VOA can be reconstructed.

§4. Moonshine VOA

Dong-Mason-Zhu [DMZ] showed that Moonshine VOA $\mathbf{V}^\natural$ constructed by Frenkel-Lepowsky-Meurman [FLM] satisfies the conditions (3.1), (3.2) in the beginning of the previous section for $n = 48$, and then Miyamoto [M3] and Dong-Greiss-Höhn [DGH] determined two codes D, S. In this section, these codes $D^\natural, S^\natural$ for $\mathbf{V}^\natural$ will be described and the character of $\mathbf{V}^\natural$ will be calculated by using $D^\natural, S^\natural$. Also Thompson series for two involutions of $\mathrm{Aut}(\mathbf{V}^\natural)$ will be calculated.

4.1. Codes $D^\natural, S^\natural$

Firstly we define two binary codes $D^{\#}, S^{\#}$ of length 16. Let $S^{\#}$ be a binary code generated by the following five words of length 16: (1^{16}), $(1^8 0^8)$, $((1^4 0^4)^2)$, $((1^2 0^2)^4)$, $((1.0)^8)$

In coding theory, $S^{\#}$ is known to be the 1st order Reed-Müller code $RM(4,1)$ of length 16. Let $D^{\#} = (S^{\#})^{\perp}$ =(orthogonal complement of $S^{\#}$). $D^{\#}$ is known to be the 2nd order Reed-Müller code $RM(4,2)$.

The code $S^\natural$ is defined to be the set of words of length 48 which put three words of $S^{\#}$ in order as follows:

$$(\sigma,\sigma,\sigma), (\sigma,\sigma,\bar\sigma), (\sigma,\bar\sigma,\sigma), (\bar\sigma,\sigma,\sigma) \ \sigma \in S^{\#}, \ \bar\sigma = \sigma + (1^{16})$$

$S^\natural$ is a $(48,7,16)$-binary code and its weight enumerator is

$$x^{48} + 3x^{32}y^{16} + 120x^{24}y^{24} + 3x^{16}y^{32} + y^{48}.$$

Finally let $D^\natural = (S^\natural)^\perp$. Then $D^\natural$ is a $(48, 41, 4)$-binary code and when a word of $D^\natural$ is written in the shape like (ρ_1, ρ_2, ρ_3) $(\rho_i \in \mathbf{F}_2^{16})$, we have

$$(4.1.1) \quad \begin{aligned} &D^\natural \ni (\rho_1, \rho_2, \rho_3)(\rho_i \in \mathbf{F}_2^{16}) \\ &\iff \rho_i \textit{ is an even word and } \rho_1 + \rho_2 + \rho_3 \equiv 0 \textit{ mod } D^{\#}. \end{aligned}$$

These $D^\natural, S^\natural$ are codes for Moonshine VOA $\mathbf{V}^\natural$.

4.2. $\mathbf{T}_{48}$-decomposition of $\mathbf{V}^\natural$

The following table gives some datas which are necessary for the description of $\mathbf{T}_{48}$-decomposition (3.1.4) of $\mathbf{V}^\natural$:

	$wt(\alpha)$	# of α	$\lvert D^\natural_\alpha \rvert$	# of orbits	multi., a_α
I	0	1	1	2^7	1
II	16	3	$\lvert D^{\#}\rvert = \lvert H_8\rvert^2 \cdot 2^3$	4	2^3
III	24	120	$\lvert H_8\rvert^3 \cdot 2^6$	2	2^6
IV	32	3	$\lvert D^{\#}\rvert^2 \cdot 2^4 = \lvert H_8\rvert^4 \cdot 2^{10}$	2	2^{10}
V	48	1	$\lvert D^\natural\rvert = \lvert H_8\rvert^6 \cdot 2^{17}$	1	2^{17}

What the 1st and 2nd column of this table mean is clear. The most important column is the 3rd one which gives the order of $D^\natural_\alpha$ together with the structure of $D^\natural_\alpha$ for each $\alpha \in S^\natural$. For example, $|D^{\#}| = |H_8|^2 \cdot 2^3$ in the 2nd row means that $(D^\natural)_\alpha \simeq D^{\#}$ and $(D^\natural)_\alpha$ contains a direct sum of two copies of Hamming code H_8 as a maximal selforthogonal subcode which has the index 2^3 in $(D^\natural)_\alpha$. This can be easily from §4.1, (4.1.1). The 4th column gives the number of orbits of the action of $D^\natural$ on $\Lambda_{48}(\alpha)(= \frac{2^{n-wt(\alpha)}}{[D^\natural:(D^\natural)_\alpha]})$. The 5th column is the multiplicities$(= [(D^\natural)_\alpha : H_\alpha])$ appearing in irreducible module $(\mathbf{V}^\natural)^\alpha$ in $\mathbf{T}_{48}$-decomposition (3.1.4) of $\mathbf{V}^\natural$ (cf. (3.3.1)).

Now, for the description of $\mathbf{T}_{48}$-decomposition of $\mathbf{V}^\natural$, it remains to choose an orbit of the action of $D^\natural$ on $\Lambda_{48}(\alpha)$ for each $\alpha \in S^\natural$. Consider the 2nd row, for example. The number of orbits is 4. As is easily seen, the representatives of each orbit (say, for $\alpha = (1^{16}, 0^{16}, 0^{16})$) are $L((\frac{1}{16})^{16}, 0^{16}, 0^{16})$, $L((\frac{1}{16})^{16}, 0^{16}, \frac{1}{2}0^{15})$, $L((\frac{1}{16})^{16}, \frac{1}{2}0^{15}, 0^{16})$, and $L((\frac{1}{16})^{16}, \frac{1}{2}0^{15}, \frac{1}{2}0^{15})$.

The 2nd and the 3rd one is improper, because they have half-integral weight. The 1st one is also improper, because it has weight 1 but the Moonshine VOA $\mathbf{V}^\natural$ has no vector of weight 1. Thus we must choose the last one as a representative. This orbit is the set of all $L((\frac{1}{16})^{16}, *, *)$ such that $\frac{1}{2}$ appear odd times in each part of two $*$.

For other rows of the above table, the orbit is uniquely determined by "integral condition" of weight. Thus we have

	$wt(\alpha)$	a representative of orbit
I	0	$L(0^{48})$
II	16	$L((\frac{1}{16})^{16}(\frac{1}{2}0^{15})(\frac{1}{2}0^{15}))$
III	24	$L((\frac{1}{16})^{24}(\frac{1}{2}0^{23}))$
IV	32	$L((\frac{1}{16})^{32}0^{16})$
V	48	$L((\frac{1}{16})^{48})$

4.3. The calculation of the the character

Firstly let us remark about the character of Code VOA.
Let D be a binary even code and M_D be a code VOA for D:

$$M_D = \oplus_{\delta \in D} L(\frac{\delta_1}{2}, \frac{\delta_2}{2}, \cdots, \frac{\delta_n}{2}) \ (\delta = (\delta_1, \delta_2, \cdots, \delta_n)).$$

Let $W_D(x,y) = \sum_{\delta \in D} x^{n-wt(\delta)} y^{wt(\delta)}$ (the weight enumerator of D).

Then the character of M_D is expressed as follows:

$$ch(M_D) = W_D(ch(L(\frac{1}{2},0)), ch(L(\frac{1}{2},\frac{1}{2}))$$

Using formulas of $ch(L(\frac{1}{2},0))$, and $ch(L(\frac{1}{2},\frac{1}{2}))$ mentioned in §2.2.2 and MacWilliam's identity in coding theory, we have

$$ch(M_D) = \frac{1}{|D^{\perp}|} W_{D^{\perp}}(q_+, q_-).$$

Let us begin the calculation of the character of $\mathbf{V}^{\natural}$:

$$\mathbf{V}^{\natural} = \oplus_{\alpha \in S^{\natural}} (\mathbf{V}^{\natural})^{\alpha}.$$

For that purpose, let us calculate $ch((\mathbf{V}^{\natural})^{\alpha})$ since we know the $\mathbf{T}_{48}$-decomposition of $(\mathbf{V}^{\natural})^{\alpha}$ in §4.2.

Case I *where* $S^{\natural} \ni \alpha$ *is of Type* I , i.e. $\alpha = (0^{48})$:
In this case, $(\mathbf{V}^{\natural})^{\alpha} \simeq M_{D^{\natural}}$ (code VOA) and so

$$ch((\mathbf{V}^{\natural})^{\alpha}) = \frac{1}{2^7}(q_+^{48} + 3q_+^{32}q_-^{16} + 120q_+^{24}q_-^{24} + 3q_+^{16}q_-^{32} + q_-^{48}).$$

Using a formula $q_0 q_+ q_- = 1$ and Jacobi's formula $16q^{\frac{1}{2}}q_0^8 = q_+^8 - q_-^8$, we get

$$ch((\mathbf{V}^{\natural})^{\alpha}) = 2^{17}q^3q_0^{48} + 3 \cdot 2^{10}q^2q_0^{24} + (q_+q_-)^{24} + 24q = Q_I.$$

Here we put the righthandside as Q_I.

Case II *where* $S^\natural \ni \alpha$ *is of Type II* , i.e. $\alpha = (1^{16}0^{16}0^{16}), (0^{16}1^{16}0^{16})$ or $(0^{16}0^{16}1^{16})$.

For simplicity of notations, let

$$X = ch(L(\frac{1}{2},0)),\ Y = ch(L(\frac{1}{2},\frac{1}{2})),\ Z = ch(L(\frac{1}{2},\frac{1}{16})).$$

Then we have

$$\begin{aligned} ch((\mathbf{V}^\natural)^\alpha) &= 2^3 Z^{16}\left(\sum_{i=1}^{8}\begin{pmatrix} 16 \\ 2i-1 \end{pmatrix} X^{16-(2i-1)}Y^{2i-1}\right)^2 \\ &= 2^3\cdot\frac{1}{4}((X+Y)^{16}-(X-Y)^{16})^2 Z^{16}. \end{aligned}$$

Transforming this in the same way as Case I, we get

$$ch((\mathbf{V}^\natural)^\alpha) = 2^3(2^{14}q^3q_0^{48} + 2^8q^2q_0^{24}) = Q_{II}.$$

Calculating $ch((\mathbf{V}^\natural)^\alpha)$ for α of *Type III*, *IV*, *V* similarly, we get

$$\begin{aligned} ch((\mathbf{V}^\natural)^\alpha) &= 2^6(2^{11}q^3q_0^{48} + 3\cdot 2^3q^2q_0^{24}) &&= Q_{III} \text{ for } \alpha \text{ of } \textit{Type III}, \\ ch((\mathbf{V}^\natural)^\alpha) &= 2^{10}(2^7q^3q_0^{48} + q^2q_0^{24}) &&= Q_{IV} \text{ for } \alpha \text{ of } \textit{Type IV}, \\ ch((\mathbf{V}^\natural)^\alpha) &= 2^{17}q^3q_0^{48} &&= Q_V \text{ for } \alpha \text{ of } \textit{Type V}. \end{aligned}$$

Thus we have

$$\begin{aligned} ch(\mathbf{V}^\natural) &= \sum_{\alpha\in S^\natural} ch((\mathbf{V}^\natural)^\alpha) \\ &= Q_I + 3\cdot Q_{II} + 120\cdot Q_{III} + 3\cdot Q_{IV} + Q_V \\ &= 2^{24}q^3q_0^{48} + 3\cdot 2^{16}q^2q_0^{24} + (q_+q_-)^{24} + 24q \\ &= q\left(2^{24}\left(\frac{\eta(2z)}{\eta(z)}\right)^{48} + 3\cdot 2^{16}\left(\frac{\eta(2z)}{\eta(z)}\right)^{24} + \left(\frac{\eta(z)}{\eta(2z)}\right)^{24} + 24\right). \end{aligned}$$

Finally, using $j(z)^{\frac{1}{3}} = 2^8\left(\frac{\eta(2z)}{\eta(z)}\right)^{16} + \left(\frac{\eta(z)}{\eta(2z)}\right)^{8}$, we get

$$\frac{1}{q}ch(\mathbf{V}^\natural) = j(z) - 744.$$

4.4. Thompson series of some involutions of $Aut(\mathbf{V}^\natural)$

For $\tau \in Aut(\mathbf{V}^\natural)$ (Monster),

$$T_\tau(q) = \frac{1}{q}\sum_{n=0}^{\infty} Tr(\tau|(\mathbf{V}^\natural)_n)q^n$$

is called Thompson series of τ. We will calculate Thompson series of some involutions of $Aut(\mathbf{V}^\natural)$.

For each i ($1 \leq i \leq 48$), we define a linear transformation of $\mathbf{V}^\natural$ as follows:

$$\tau_i|(\mathbf{V}^\natural)^\alpha = \epsilon(i,\alpha)Id_{(\mathbf{V}^\natural)^\alpha}, \ \epsilon(i,\alpha) = \left\{ \begin{array}{rl} -1 & i \in supp(\alpha) \\ 1 & i \notin supp(\alpha) \end{array} \right.$$

Then τ_i is an automorphism (as VOA) of $\mathbf{V}^\natural$ (cf. [M1]). In the following, we will calculate Thompson series of $\tau_1 \in Aut(\mathbf{V}^\natural)$ ($2A$-involution) and $\tau_1\tau_2 \in Aut(\mathbf{V}^\natural)$ ($2B$-involution). For each $\alpha \in S^\natural$, let

$$\epsilon_\alpha = \left\{ \begin{array}{rl} -1 & 1 \in supp(\alpha) \\ 1 & 1 \notin supp(\alpha). \end{array} \right.$$

Then we have $qT_{\tau_1}(q) = \sum_{\alpha \in S^\natural} \epsilon_\alpha ch((\mathbf{V}^\natural)^\alpha)$ which is equal to

$$Q_I + (-1+1+1)Q_{II} + (1-1-1)Q_{IV} - Q_V + \left(\sum_{\alpha:Type\ III} \epsilon_\alpha \right) Q_{III}.$$

But since the number of α of *Type III* with $1 \in supp(\alpha)$ is equal to the number of α of *Type III* with $1 \notin supp(\alpha)$, the last term is canceled and so we get

$$qT_{\tau_1}(q) = Q_I + Q_{II} - Q_{IV} - Q_V = 2^{12}q^2q_0^{24} + (q_+q_-)^{24} + 24q$$

$$= q\left(2^{12}\left(\frac{\eta(2z)}{\eta(z)}\right)^{24} + \left(\frac{\eta(z)}{\eta(2z)}\right)^{24} + 24\right).$$

Thus Thompson series $T_{\tau_1}(q)$ is equal to a modular function corresponding to 2A-involution of Monster (cf. [CN]). Next, let

$$\epsilon'_\alpha = \left\{ \begin{array}{rl} 1 & 1,2 \in supp(\alpha) \text{ or } 1,2 \notin supp(\alpha) \\ -1 & \text{otherwise.} \end{array} \right.$$

Then the Thompson series $qT_{\tau_1\tau_2}(q) = \sum_{\alpha \in S^\natural} \epsilon'_\alpha ch((\mathbf{V}^\natural)^\alpha)$ is equal to

$$Q_I + (1+1+1)Q_{II} + (1+1+1)Q_{IV} + Q_V + \left(\sum_{\alpha:TypeIII} \epsilon'_\alpha \right) Q_{III}.$$

But since there exist 56 α of *Type III* with $\epsilon'_\alpha = 1$ and 64 α of *Type III* with $\epsilon'_\alpha = -1$, we get

$$\begin{aligned} qT_{\tau_1\tau_2}(q) &= Q_I + 3\cdot Q_{II} + 3\cdot Q_{IV} + Q_V - 8\cdot Q_{III} \\ &= (q_+q_-)^{24} + 24q = q\left(\left(\frac{\eta(z)}{\eta(2z)}\right)^{24} + 24\right). \end{aligned}$$

Thus Thompson series $T_{\tau_1\tau_2}(q)$ is equal to a modular function corresponding to 2B-involution of Monster (cf. [CN]).

Remark. For some $\tau \in Aut(\mathbf{V}^\natural)$ which come from $Aut(D^\natural)$, it is possible to calculate Thompson series $T_\tau(q)$ explicitly. In fact, Miyamoto [M6] has done it for such 3-element of $Aut(\mathbf{V}^\natural)$ (which corresponds to 3C-element of Monster and $T_\tau(q) = j(3z)^{\frac{1}{3}}$.) Also Sakuma [S], one of Miyamoto's graduate students, has written down $T_\tau(z)$ in terms of the characters of Ising models for such 5-element and 7-element which should be $(\frac{\eta(z)}{\eta(5z)})^6 + 6$ and $(\frac{\eta(z)}{\eta(7z)})^4 + 49\cdot(\frac{\eta(7z)}{\eta(z)})^4 + 4$ respectively, although it is a little bit unsatisfactory for these identifications.

§5. VOA of Reed Müller type

For $m \geq 4$, let

$S(m) = RM(m, 1)$ (1st order Reed Müller code of length 2^m)

$D(m) = S(m)^\perp = RM(m, m-2)$ (($m-2$)-th order Reed Müller code of length 2^m)

(Note that $S(4), D(4)$ is nothing but $S^\#, D^\#$ respectively in §4.1). It is easy to see that

(5,1) *$D(m), S(m)$ satisfy the conditions* (3.1.2), (3.2.1)

(5,2) *Orbit of the action of $D(m)$ on $\Lambda_{2^m}(\alpha)$ for each $\alpha \in S(m)$ is uniquely determined under integral condition of weight.*

Furthermore, in view of Miyamoto's theory [M5], [M6], there exists VOA for $D(m), S(m)$. We denote it by $\mathbf{V}(m)$.

Remark. $\mathbf{V}(m)$ can be constructed as VOA over the real number field with a positive definite invariant form and then, if $m \geq 6$, $Aut(\mathbf{V}(m))$ is a finite group (cf. [M6]). For $m = 4, 5$, we see $\mathbf{V}(4) = E_8$-Lattice VOA and $\mathbf{V}(5) = E_{16}$-Lattice VOA. As for the character of $\mathbf{V}(m)$, we can easily see that $q^{-\frac{2^m-1}{24}} ch(\mathbf{V}(m))$ is equal to $j(z)^{\frac{1}{3}}$, $j(z)^{\frac{2}{3}}$ and $j(z)^{\frac{1}{3}}(j(z) - 992)$ for $m = 3, 4$ and 5 respectively.

More generally, it seems very likely

$$q^{-\frac{2^m-1}{24}} ch(\mathbf{V}(m)) = j(z)^{\frac{\mu}{3}}(\text{a polynomial of } j(z))\ (\mu = 1 \textit{ or } 2).$$

But the author has not yet checked it.

References

[CN] J.H. Conway and S.P. Norton, Monstrous moonshine, Bull. London Math. Soc., **11**(1979), 308–339.

[DGH] C. Dong, R.L. Griess, Jr. and G. Höhn, Framed vertex operator algebras, codes, and the moonshine module, Comm. Math. Phys., **193**, No. 2(1998), 407–448.

[DM] C. Dong and G. Mason, On quantum Galois theory, Duke Math. J., **86**(1997), 305–321.

[DMZ] C. Dong, G. Mason and Y. Zhu, Discrete Series of the Virasoro algebra and the moonshine module, Proc. Symp. Pure. Math., American Math. Soc., **56** II (1994).

[FLM] I.B. Frenkel, J. Lepowsky and A. Meurman, Vertex Operator Algebra and the Monster, Pure and Applied Math., Vol. 134, Academic Press, 1988.

[M1] M. Miyamoto, Griess algebras and conformal vectors in vertex operator algebra, J. Algebra, **179** (1996), 523–548.

[M2] M. Miyamoto, Binary codes and vertex operator (super)algebra, J. Algebra, **181** (1996), 207–222.

[M3] M. Miyamoto, The moonshine VOA and a tensor product of Ising models, Proc. of the conference on the Monster and Lie Algebras at The Ohio State University, May 1996, ed. by J. Ferrar and K. Harada, Walter de Gruyter, Berlin-New York.

[M4] M. Miyamoto, Representation Theory of Code Vertex Operator Algebra, J. Algebra, **201** (1998), 115–150.

[M5] M. Miyamoto, A Hamming code vertex operator algebra and construction of Vertex operator algebras, J. Algebra, **215** (1999), 509–530.

[M6] M. Miyamoto, A new construction of the moonshine vertex operator algebra over the real number field, preprint.

[S] S. Sakuma, Master' thesis at Tsukuba University, (1999).

Department of Mathematics
Tokyo Woman's Christian University
Tokyo 167-8585, Japan

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 337–346

A Remark on the Loewy Structure for the Three Dimensional Projective Special Unitary Groups in Characteristic 3

Shigeo Koshitani[1] and Naoko Kunugi

§1. Introduction and Notation

The purpose of this note is to give an alternative and easier proof of a recent result by K. Hicks [6, Theorem 1.1], which was on the Loewy and socle structure of the projective indecomposable modules in the principal 3-block of the projective special unitary group $\mathrm{PSU}_3(q^2) = \mathrm{U}_3(q)$ for a power $q$ of a prime satisfying $q \equiv 2$ or $5 \pmod 9$ over an algebraically closed field of characteristic 3. In her paper K. Hicks used so-called Auslander-Reiten theory on representations of artin algebras (see [1]). Actually, in her paper [6], the key tool was a result, which was due to K. Erdmann [4] and S. Kawata [8] on Auslander-Reiten quivers of type A_∞ for group algebras of finite groups. On the other hand, our proof does not need the Auslander-Reiten theory (except a result due to P. Webb [15]) but just well-known results on modular representation theory of finite groups.

We use the following notation and terminology. Throughout this paper, $k$ is always an algebraically closed field of characterictic $p > 0$, and $G$ is always a finite group. For an element $g \in G$ we denote by $|g|$ the order of $g$. For a power $q$ of a prime, $\mathbb{F}_q$ is the field of $q$ elements, and we use the notation $\mathrm{GL}_n(q)$, $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$, $\mathrm{PGU}_n(q)$, $\mathrm{PSU}_n(q)$ for a positive integer $n$ in a standard fashion (see [7]). We denote by C_n the cyclic group of order $n$ for a positive integer $n$. Let $A$ be a finite-dimensional $k$-algebra. Then, $A^\times$ denotes the set of all units (invertible elements) in $A$, and $J(A)$ denotes the Jacobson radical of $A$. In this paper *modules* mean always finitely generated right modules, unless stated otherwise. Let $M$ be an $A$-module. We denote by $\mathrm{Soc}(M)$ and $P(M)$ the socle of $M$ and the projective cover of $M$, respectively.

[1] This work was partially supported by the JSPS (Japan Society for Promotion of Science).

Received March 3, 1999.

Let $J = J(kG)$. Then, we write $j(M)$ for the Loewy length of M, that is, $j(M)$ is the least positive integer j such that $M \cdot J^j = 0$. Then, for each $i = 1, \cdots, j(M)$, we can define the i-th Loewy layer $L_i(M)$ and i-th socle $\mathrm{Soc}_i(M)$ of M, namely, $L_i(M) = M \cdot J^{i-1}/M \cdot J^i$ and the i-th socle of M is defined inductively by $\mathrm{Soc}_0(M) = M$ and $\mathrm{Soc}_i(M)/\mathrm{Soc}_{i-1}(M) = \mathrm{Soc}(M/\mathrm{Soc}_{i-1}(M))$ for $i = 1, 2, \cdots, j(M)$. Let $M^* = \mathrm{Hom}_k(M, k)$ be the dual of M, which can be considered as a right kG-module as well via $(\phi \cdot g)(m) = \phi(mg^{-1})$ for any $m \in M$, $g \in G$ and $\phi \in \mathrm{Hom}_k(M, k)$. Then, M^* is called the (k-)*dual* of M. We say that M is *self-dual* if $M \cong M^*$ as right kG-modules.

From now on, let assume that A is a block ideal of the group algebra kG. Then, we write $\mathrm{Irr}(A)$ and $\mathrm{IBr}(A)$ respectively for the set of all irreducible ordinary characters of G in A and the set of all irreducible Brauer characters of G in A (note that sometimes we mean by $\mathrm{IBr}(A)$ the set of all non-isomorphic simple kG-modules in A). We write $k(A)$ and $\ell(A)$ respectively for the numbers of all elements in the sets $\mathrm{Irr}(A)$ and $\mathrm{IBr}(A)$. For simple kG-modules S and T, $c(S, T) = c_{S,T}$ denotes the Cartan invariant with respect to S and T. We denote by k_G the trivial kG-module. For other notation and terminology we follow the books of Landrock [12] and Nagao-Tsushima [13].

§1. $\mathbf{PSU}_3(q^2)$

In this section we give some remarks on $\mathrm{PSU}_3(q^2)$. First of all, we can define the 3-dimensional special unitary group $\mathrm{SU}_3(q^2)$ over the finite field $\mathbb{F}_{q^2}$ of q^2 elements for a power q of a prime such that

$$\mathrm{SU}_3(q^2) \;=\; \{X \in \mathrm{SL}_3(q^2) \mid X \cdot {}^t\overline{X} = I_3\}$$

where I_3 is the unit matrix of size 3×3, ${}^tY$ is the transposed matrix of a matrix Y and $\overline{Y}$ is the image of a matrix Y by the Frobenius map $\mathbb{F}_{q^2} \rightarrow \mathbb{F}_{q^2}$ with $\alpha \mapsto \alpha^q$, namely, $\overline{Y} = ({y_{ij}}^q)_{i,j}$ if $Y = (y_{ij})_{i,j}$ and $y_{ij} \in \mathbb{F}_{q^2}$, since there exists a normal orthogonal basis with respect to f, where f is a non-degenerate Hermite form over a 3-dimensional $\mathbb{F}_{q^2}$-vector space which defines $\mathrm{SU}_3(q^2)$ (see [7, II 10.4 Satz]). Throughout this paper, we assume that a power q of a prime satisfies a condition

$$\textbf{(2.1)} \qquad q \equiv\; 2 \;\text{ or } 5 \pmod 9.$$

Since the multiplicative group ${\mathbb{F}_{q^2}}^{\times}$ is a cyclic group of order $q^2 - 1$, let σ be a generator of it, namely, ${\mathbb{F}_{q^2}}^{\times} = \langle \sigma \rangle$ and we fix σ. Then, let

$\omega = \sigma^{(q^2-1)/3}$ and we fix ω (note that q^2-1 is divisible by 3 from (2.1)). Now, we can define

$$\textbf{(2.2)} \qquad G \;=\; \mathrm{PSU}_3(q^2) \;=\; \mathrm{SU}_3(q^2)/Z$$

where Z is the center of $\mathrm{SU}_3(q^2)$ and $Z \;=\; \{\omega^i \cdot I_3 \in \mathrm{SL}_3(q^2) \mid i = 0, 1, 2\}$ so that $Z \cong C_3$. Throughout this paper we write elements of G and $\mathrm{PGL}_3(q^2)$ just in forms of (3×3)-matrices. Let

$$\textbf{(2.3)} \qquad \beta \;=\; \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega \end{pmatrix} \;\in \mathrm{PGL}_3(q^2).$$

Then, $\beta \in \widetilde{G} - G$ and $|\beta| = 3$ where $\widetilde{G} = \mathrm{PGU}_3(q^2)$. As in [14], let

$$\textbf{(2.4)} \qquad st' = (q-1)(q^2-q+1)/3.$$

Notation. In the rest of this paper, we assume that k is an algebraically closed field of characteristic 3 and that q is a power of a prime satisfying (2.1), and we use the notation G, $\widetilde{G}$, β and st' as in (2.2)–(2.4).

§2. Decomposition matrix and Cartan matrix for G

In this section we list the decomposition matrix and the Cartan matrix for G for a prime 3. Here we use the notation k, G, $\widetilde{G}$, β and st' as in §2. We denote by A the principal block of kG.

(3.1) Lemma. (i) *The decomposition matrix and the Cartan ma-*

trix of the principal block A of G for a prime 3 *are*

	$S(0)$	$S(1)$	$S(2)$	$S(3)$	S
χ_1	1	.	.	.	.
$\chi_{st'}^{(1)}$	.	1	.	.	.
$\chi_{st'}^{(2)}$	.	.	1	.	.
$\chi_{st'}^{(3)}$	.	.	.	1	.
χ_{q^2-q}	.	.	.	.	1
χ_{q^3}	1	1	1	1	2

	$P(0)$	$P(1)$	$P(2)$	$P(3)$	$P(S)$
$S(0)$	2	1	1	1	2
$S(1)$	1	2	1	1	2
$S(2)$	1	1	2	1	2
$S(3)$	1	1	1	2	2
S	2	2	2	2	5

where $S(0) = k_G$, *the subindices of* χ*'s above mean the degrees,* $S(0)$, $S(1)$, $S(2)$, $S(3)$ *and* S *are all simple* kG*-modules in* A, *and* $P(i) = P(S(i))$ *for* $i = 0, 1, 2, 3$.

(ii) *All simple* kG*-modules in* A *are self-dual. and the element* $\beta \in \widetilde{G}$ *of order* 3 *acts on* $\mathrm{Irr}(A) = \{\chi_1, \chi_{st'}^{(1)}, \chi_{st'}^{(2)}, \chi_{st'}^{(3)}, \chi_{q^2-q}, \chi_{q^3}\}$ *such that*

$$\chi_1{}^{\beta} = \chi_1,$$

$$(\chi_{st'}^{(1)})^{\beta} = \chi_{st'}^{(2)}, \quad (\chi_{st'}^{(2)})^{\beta} = \chi_{st'}^{(3)}, \quad (\chi_{st'}^{(3)})^{\beta} = \chi_{st'}^{(1)},$$

$$(\chi_{q^2-q})^{\beta} = \chi_{q^2-q}, \quad (\chi_{q^3})^{\beta} = \chi_{q^3}.$$

Proof. (i) The assertion is obtained by the result of Geck [5, pp.571–573, Theorem 4.5], and a standard argument (see [3, Lemmas 66.1 and 64.3(1)]).

(ii) We get the self-dualities by (3.1), (i) and [5, Table 3.1, p.569]. It follows from [14, Table 2, p.492], [5, p.569, p.571] and [9, Tafel I, p.141] that $(\chi_{st'}^{(i)})^{\beta} = \chi_{st'}^{(i+1)}$ for $i = 0, 1, 2$, where the index i is considered modulo 3. The rest in (ii) is easy. Q.E.D.

Notation. In the rest of this paper, we use the notation χ_i, $\chi_i^{(j)}$, k_G, $S(i)$, S as in (3.1).

§3. Projectives in the principal 3-block of G

In this section we investigate the Loewy and socle series of projective indecomposable kG-modules in the principal block A of kG. We use the notation $S(0) = k_G$, $S(1)$, $S(2)$, $S(3)$ and S which means all non-isomorphic simple kG-modules in the principal block A of kG as in (3.1).

(4.1) Theorem. *The Loewy and socle series of the projective indecomposable kG-modules are*

$$P(S(i)) = \begin{array}{ccc} & S(i) & \\ & S & \\ S(j) & S(k') & S(\ell) \\ & S & \\ & S(i) & \end{array} \qquad P(S) = \begin{array}{cccc} & S & & \\ S(0) & S(1) & S(2) & S(3) \\ & S \quad S & \quad S & \\ S(0) & S(1) & S(2) & S(3) \\ & S & & \end{array}$$

where $\{i, j, k', \ell\} = \{0, 1, 2, 3\}$ *and* $S(0) = k_G$.

Proof. Let $J = J(kG)$ and $A = B_0(kG)$, the principal block of kG. Let $S(0) = k_G$, $S(4) = S$ and $P(i) = P(S(i))$ for each $i = 0, 1, 2, 3, 4$. We write $c(i, j)$ for $c(S(i), S(j))$ for each i, j. By (3.1)(i), we know that $k(A) - \ell(A) = 1$. Hence it follows from a result of Brandt [2, Theorem B] that

(0) $\quad \mathrm{Ext}^1_{kG}(S(i), S(i)) = 0 \qquad$ for all $i = 0, 1, 2, 3, 4$.

We get from (3.1)(ii) that $S(0)$ and $S(1)$ are both self-dual and that $c(0, 1) = 1$. Hence, if $\mathrm{Ext}^1_{kG}(S(0), S(1)) \neq 0$, then the self-duality implies that $S(1)$ is a direct summand of the heart $H(P(0)) = P(0){\cdot}J/\mathrm{Soc}(P(0))$ of $P(0)$, which means that $H(P(0))$ is decomposable by the Cartan matrix in (3.1)(i), contradicting a result of Webb [15, Theorem E].

Therefore, $\mathrm{Ext}^1_{kG}(S(0), S(1)) = 0$. Hence, by using the automorphism β of kG in (3.1)(ii), we have $\mathrm{Ext}^1_{kG}(S(0), S(i)) = 0$ for all $i = 1, 2, 3$.

Similarly, if we assume that $\dim_k[\mathrm{Ext}^1_{kG}(S(0), S(4))] = 2$, then it follows from the self-duality and the Cartan matrix for A in (3.1)(i) that the heart $H(P(0))$ is decomposable, contradicting [15, Theorem E].

Therefore, the self-duality says that $P(0)/P(0){\cdot}J^2$ and $\mathrm{Soc}_2(P(0))$ are both uniserial with

$$L_2(P(0)) \cong S(4) \cong \mathrm{Soc}_2(P(0))/\mathrm{Soc}_1(P(0)).$$

Hence, by the Cartan matrix in (3.1)(i), there left only $S(1)$, $S(2)$, $S(3)$ with multiplicity one in the composition factors of $P(0)$, respectively, whose positions in the Loewy series of $P(0)$ are not determined. So, the automorphism β in (3.1)(ii) implies that $S(1) \bigoplus S(2) \bigoplus S(3) \hookrightarrow L_3(P(0))$, completing the Loewy structure of $P(0)$. Hence, by the self-dualities, we get that the Loewy and socle series of $P(0)$ has the form

$$P(0) \;=\; \begin{array}{ccc} & S(0) & \\ & S(4) & \\ S(1) & S(2) & S(3). \\ & S(4) & \\ & S(0) & \end{array} \tag{1}$$

Now, it follows from a result of Landrock [11, Theorem E] and (1) that $S(0) \hookrightarrow L_3(P(i))$ for all $i = 1, 2, 3$, $S(0) \hookrightarrow L_2(P(4))$ and $S(0) \hookrightarrow L_4(P(4))$. Moreover, (1) implies that $S(4) \hookrightarrow L_2(P(i))$ for $i = 1, 2, 3$ and $S(4) \hookrightarrow L_3(P(4))$.

Next, we want to claim that there exists some $i \geqslant 4$ such that $S(4) \hookrightarrow L_i(P(1))$, $S(4) \hookrightarrow L_i(P(2))$ and $S(4) \hookrightarrow L_i(P(3))$. By (1), $P(1)$ has a uniserial submodule U with $L_1(U) \cong S(0)$, $L_2(U) \cong S(4)$ and $L_3(U) = UJ^2 \cong S(1)$. On the other hand, $c(1, 0) = 1$ from (3.1)(i). Moreover, we have already got $S(0) \hookrightarrow L_3(P(1))$. Therefore, by [10, (1.1)Lemma], $S(4) \hookrightarrow L_i(P(1))$ for some $i \geqslant 4$. Thus, this holds for $P(2)$ and $P(3)$ as well by using the automorphism β in (3.1)(ii).

Therefore, we know so far the Loewy series of $P(1), \cdots, P(4)$ have at least the following form.

$$P(j) \;=\; \begin{array}{c} S(j) \\ S(4)\cdots \\ S(0)\cdots \\ \vdots \\ S(4)\cdots \\ \vdots \\ S(j) \end{array} \qquad P(4) \;=\; \begin{array}{cccc} & S(4) & & \\ S(0) & S(1) & S(2) & S(3)\cdots \\ & S(4)\cdots & & \\ & S(0)\cdots & & \\ & \vdots & & \\ & \vdots & & \\ & S(4) & & \end{array} \tag{2}$$

for $j = 1, 2, 3$.

Assume that $\mathrm{Ext}^1_{kG}(S(1), S(2)) \neq 0$ and $\mathrm{Ext}^1_{kG}(S(1), S(3)) \neq 0$. Let $H = P(1){\cdot}J/\mathrm{Soc}(P(1))$ be the heart of $P(1)$. Since $c(1, 2) = c(1, 3) = 1$ by (3.2)(i), the assumption and the self-duality of $S(0), \cdots, S(4)$ in (3.1)(ii) imply that $S(2)$ and $S(3)$ are both direct summands of H. Hence, it follows from (2) and the Cartan matrix for A in (3.1)(i) that the Loewy and socle series of $P(1)$ have the form

$$P(1) \quad = \quad \begin{array}{ccc} & S(1) & \\ & S(4) & \\ S(0) & S(2) & S(3). \\ & S(4) & \\ & S(1) & \end{array}$$

Thus, again (1.3) shows that $S(1) \hookrightarrow L_4(P(4))$, so that $S(i) \hookrightarrow L_4(P(4))$ for all $i = 1, 2, 3$ by using β. Hence $P(4)$ has Loewy series

$$P(4) \quad = \quad \begin{array}{c} S(4) \\ S(0) \quad S(1) \quad S(2) \quad S(3)\cdots \\ S(4) \;\; \cdots \\ S(0) \quad S(1) \quad S(2) \quad S(3)\cdots \\ S(4) \end{array}$$

and there left only two $S(4)$'s form the Cartan matrix in (3.1)(i). Since $\mathrm{Ext}^1_{kG}(S(4), S(4)) = 0$ by (0), the only possibility for the Loewy series of $P(4)$ is that

$$P(4) \quad = \quad \begin{array}{c} S(4) \\ S(0) \quad S(1) \quad S(2) \quad S(3) \\ S(4) \quad S(4) \quad S(4) \\ S(0) \quad S(1) \quad S(2) \quad S(3) \\ S(4) \end{array} \quad .$$

Now, from the Loewy structure of $P(1)$ above, we know, by using the automorphism β again, that $P(4)$ has uniserial submodules U_1, U_2, U_3 of composition length 4 such that

$$U_1 = \begin{array}{c} S(1) \\ S(4) \\ S(0) \\ S(4) \end{array} \qquad U_2 = \begin{array}{c} S(2) \\ S(4) \\ S(0) \\ S(4) \end{array} \qquad U_3 = \begin{array}{c} S(3) \\ S(4) \\ S(0) \\ S(4). \end{array}$$

Hence, we can consider a submodule X of $P(4)$ defined by $X = U_1 + U_2 + U_3$. By (1), we have $\dim_k[\mathrm{Ext}^1_{kG}(S(0), S(4))] = 1$, which means that the multiplicity of $S(0)$ in $\mathrm{Soc}_2(X)/\mathrm{Soc}_1(X)$ is at most one. Hence, $\mathrm{Soc}_2(X)/\mathrm{Soc}_1(X) \cong S(0)$. Thus, since $\dim_k[\mathrm{Ext}^1_{kG}(S(4), S(0))] = 1$, we get that the multiplicity of $S(4)$ in $\mathrm{Soc}_3(X)/\mathrm{Soc}_2(X)$ is at most one Therefore, $\mathrm{Soc}_3(X)/\mathrm{Soc}_2(X) \cong S(4)$. Hence, X has Loewy and socle structure

$$X \;=\; \begin{array}{ccc} S(1) & S(2) & S(3) \\ & S(4) & \\ & S(0) & \\ & S(4) & \end{array} .$$

So that, by (1.1) again, we know that the $S(1)$ in $L_1(X)$ comes from that in $L_2(P(4))$. Similar thing holds for $S(2)$ and $S(3)$ as well. Namely, it follows that $P(4)/X$ has Loewy series

$$P(4)/X \;=\; \begin{array}{ccccc} & & S(4) & & \\ & & S(0) & & \\ & S(4) & & S(4) & \\ S(1) & & S(2) & & S(3) \end{array} .$$

This shows $\dim_k[\mathrm{Ext}^1_{kG}(S(0),S(4))] \geqslant 2$, contradicting (1).

Next, assume that $\mathrm{Ext}^1_{kG}(S(1),S(2)) \neq 0$ and $\mathrm{Ext}^1_{kG}(S(1),S(3)) = 0$. Then, by applying β^2 to $\mathrm{Ext}^1_{kG}(S(1),S(2))$, we get that $\mathrm{Ext}^1_{kG}(S(3),S(1)) \neq 0$, so that it follows $\mathrm{Ext}^1_{kG}(S(1),S(3)) \neq 0$ by the self-dualities, a contradiction. Similarly, we get a contradiction in the case that $\mathrm{Ext}^1_{kG}(S(1),S(2)) = 0$ and $\mathrm{Ext}^1_{kG}(S(1),S(\ 3)) \neq 0$ by using β^2 in (3.2)(ii).

Therefore, it holds that $\mathrm{Ext}^1_{kG}(S(1),S(2)) = \mathrm{Ext}^1_{kG}(S(1),S(3)) = 0$. Then, (2) and the Cartan matrix in (3.1)(i) imply that $L_2(P(1)) \cong S(4)$, so that $P(1)$ has Loewy series of the form

$$(3) \qquad P(1) \;=\; \begin{array}{c} S(1) \\ S(4) \\ S(0)\cdots \\ \vdots \\ S(4)\cdots \\ \vdots \\ S(1) \end{array} \qquad \text{and there left } S(2),\ S(3).$$

Next, we want to claim $L_3(P(1)) \ncong S(0)$. Assume $L_3(P(1\ )) \cong S(0)$. Since $\mathrm{Ext}^1_{kG}(S(0),S(2)) = \mathrm{Ext}^1_{kG}(S(0),S(3)) = 0$ by (1), it follows from (3) that $L_4(P(1)) \cong S(4)$, which implies from (3) that $\mathrm{Ext}^1_{kG}(S(2),S(1)) \neq 0$, so that $\mathrm{Ext}^1_{kG}(S(1),S(2)) \neq 0$ by the self-dualities. This is a contradiction. Thus, $L_3(P(1)) \ncong S(0)$.

Suppose that $L_3(P(1)) \cong S(0) \bigoplus S(2)$. Since $\mathrm{Ext}^1_{kG}(S(3),S(1)) = 0$

by the self-dualities, we get by (3) that $P(1)$ has Loewy series of the form

$$P(1) \;=\; \begin{array}{ccc} & S(1) & \\ & S(4) & \\ S(0) & & S(2) \\ & S(3) & \\ & S(4) & \\ & S(1) & \end{array} .$$

Let $V = [P(1) \cdot J^3]^*$. Then, by the self-dualities, V is a uniserial kG-module of composition length three with $L_1(V) \cong S(1)$, $L_2(V) \cong S(4)$, $L_3(V) = VJ^2 \cong S(3)$, which means that $S(3) \hookrightarrow L_3(P(1))$, contradicting the Loewy structure of $P(1)$ above. Hence, $L_3(P(1)) \not\cong S(0) \bigoplus S(2)$.

Similarly, we obtain that $L_3(P(1)) \not\cong S(0) \bigoplus S(3)$. Therefore, it follows that $L_3(P(1)) \cong S(0) \bigoplus S(2) \bigoplus S(3)$ by (3), so that we completely know the Loewy structure of $P(1)$. Thus, we get the Loewy and socle structure of $P(1)$, $P(2)$ and $P(3)$ as in the statement by making use of β. Hence, again by (1.3) and the Cartan matrix in (3.1)(i), $P(4)$ has Loewy series of the form

$$P(4) \;=\; \begin{array}{ccccc} & & S(4) & & \\ S(0) & S(1) & & S(2) & S(3)\cdots \\ & & S(4)\cdots & & \\ S(0) & S(1) & & S(2) & S(3)\cdots \\ & & S(4) & & \end{array} .$$

and there left only two $S(4)$'s. Since $\mathrm{Ext}^1_{kG}(S(4), S(4)) = 0$ by (0), we finally get the complete Loewy series of $P(4)$ as in the statement. This finishes the proof of the theorem. Q.E.D.

Acknowledgements.

The first author was in part supported by the Joint Research Project "Representation Theory of Finite and Algebraic Groups" 1997–99 under the Japanese-German Cooperative Science Promotion Program supported by JSPS and DFG.

References

[1] M. Auslander, I. Reiten and S.O. Smalø, Representation Theory of Artin Algebras, Cambridge Univ. Press, Cambridge.

[2] J. Brandt, A lower bound for the number of irreducible characters in a block, J. Algebra, **74** (1982), 509–515.

[3] L. Dornhoff, Group Representation Theory (part B), Marcel Dekker, New York.

[4] K. Erdmann, On Auslander-Reiten components for group algebras, J. Pure and Appl. Algebra, **109** (1995), 149–160.

[5] M. Geck, Irreducible Brauer characters of the 3-dimensional special unitary groups in non-defining characteristic, Commun. Algebra, **18** (1990), 563–584.

[6] K. Hicks, The Loewy structure and basic algebra structure for some linebreak-three dimensional projective special unitary groups in characteristic 3, J. Algebra, **202** (1998), 192–201.

[7] B. Huppert, Endliche Gruppen I, Springer-Verlag, Berlin.

[8] S. Kawata, On Auslander-Reiten components for certain group modules, Osaka J. Math., **30** (1993), 137–157.

[9] M. Klemm, Charakterisierung der Gruppen $PSL(2, p^f)$ and $PSU(3, p^{2f})$ durch ihre Charaktertafel, J. Algebra, **24** (1973), 127–153.

[10] S. Koshitani, On the Loewy series of the group algebra of a finite p-solvable group with p-length > 1, Commun. Algebra, **13** (1985), 2175–2198.

[11] P. Landrock, The Cartan matrix of a group algebra modulo any power of its radical, Proc. Amer. Math. Soc., **88** (1983), 205–206.

[12] P. Landrock, Finite Group Algebras and Their Modules, London Math. Soc. Lecture Note Series, Cambridge Univ. Press, Cambridge.

[13] H. Nagao and Y. Tsushima, Representations of Finite Groups, Academic Press, New York.

[14] W.A. Simpson and J.S. Frame, The character tables for $SL(3, q)$, $SU(3, q^2)$, $PSL(3, q)$, $PSU(3, q^2)$, Canad. J. Math., **25** (1973), 486–494.

[15] P. Webb, The Auslander-Reiten quiver of a finite group, Math. Z., **179** (1982), 97–121.

Shigeo Koshitani
Department of Mathematics and Informatics
Faculty of Science, Chiba University
Chiba 263-8522, Japan
e-mail: koshitan@math.s.chiba-u.ac.jp

Naoko Kunugi
Department of Mathematics, Graduate School of Science and Technology
Chiba University, Chiba 263-8522, Japan
e-mail: mkunugi@g.math.s.chiba-u.ac.jp

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 347–353

The Essentials of Monstrous Moonshine

John M^cKay

This is a fast introduction to Monstrous Moonshine.

All our functions expanded at $\tau = i\infty$ have the form:

$$(*) \qquad f(\tau) = \frac{1}{q} + \sum_{k\geq 0} a_k q^k, \quad q = e^{2i\pi\tau}, \quad \Im(\tau) > 0, \quad a_k \in \mathbb{C}.$$

We further assume that $a_0 = 0$ (standard form) for convenience, and that $a_k \in \mathbb{Q}$ (to ensure trivial Galois action). For replicable functions there is a reasonable conjecture that the a_k are algebraic integers - this, too, we assume. We find that the coefficients of classical modular functions known to Jacobi, Fricke, and Klein, are related to the characters of $\mathbb{M}$, the Monster simple sporadic group, in that, to each conjugacy class of cyclic subgroups $\langle g\rangle$, of $\mathbb{M}$, there is such a function, j_g with coefficient of $q^k = \text{Trace}\big(H_k(g)\big)$ for some representation, H_k, (the $k^{th}$ Head representation) of $\mathbb{M}$.

In November 1978 I wrote to John Thompson that $196884 = 1 + 196883$, relating the coefficient of $q$ in the elliptic modular function, $j(\tau)$, to the degree of the smallest faithful complex representation of $\mathbb{M}$. Little was then known to me of the degrees of irreducible characters of $\mathbb{M}$ but I did have access to those of $E_8(\mathbb{C})$ and related an initial sequence of them to the $q$-coefficients of the cube root of $j$. This was quickly disposed of by Vi̦ctor Kac [Kac], see also [Lep].

There are 194 conjugacy classes of $\mathbb{M}$, 172 classes of cyclic subgroups, and 171 distinct functions j_g. This, and more, is to be found in Conway-Norton [CN]. All these functions are genus zero in that this is the genus of the compactified Riemann surface $\widehat{G_f\backslash\mathcal{H}}$ where G_f is the discrete invariance group of $f$, acting on the upper half-plane, $\mathcal{H}$.

Research supported by the Natural Sciences and Engineering Research Council (Canada), and Fonds pour la Formation de Chercheurs et l'Aide à la Recherche (Québec)

Received August 25, 2000.

By axiomatizing the properties of these functions, we arrive at the notion of a replicable function, as one which behaves well under a generalized Hecke operator. These are now under scrutiny. My hope is that their properties will yield an intrinsic description of $\mathbb{M}$.

We study replicable functions, which generalize a degenerate family called by me the "modular fictions", namely $f(\tau) = 1/q + cq$. Cummins [CuN] has proved these are the unique replicable finite Laurent series, $(\forall k \geq k_0,\ a_k = 0)$. A further useful property to impose is that the replication power map (defined later): $f \to f^{(n)}$, is periodic, namely $\forall n \geq 1$, $f^{(\gcd(n,k))} = f^{(n)}$. When this is so, the modular fictions reduce to three cases, $1/q$, $1/q + q$, $1/q - q$, corresponding to exp, cos, and sin respectively. An amusing consequence of their replicability is that $\sin(2kt)$ is not a polynomial in $\sin(t)$, whereas $\cos(2kt)$ is a polynomial in $\cos(t)$. This follows from a study of the modular equation [Sil], [Mar] for f, with formal coefficients [McK]. The modular fictions play no further part in what follows.

Replicable functions are generalizations of the prototype, $j(\tau)$, the elliptic modular function which is characterized by its form and the property under the action of Hecke operators [Serre]:

$$\forall n \geq 1,\ nT_n\big(j(\tau)\big) = \sum_{\substack{ad=n \\ 0\leq b<d}} j(\frac{a\tau + b}{d}) = P_{n,j}\big(j(\tau)\big),$$

where T_n denotes the standard Hecke operator, and $P_{n,j} = P_n$ is the Faber [Fab], [Cur] polynomial of degree n. The notation is to remind one that the coefficients of the Faber polynomial come from its argument.

One characterization of these polynomials is that

$$P_{n,f}(f) - \frac{1}{q^n} \in q\,\mathbb{C}[[q]].$$

We find

$$\begin{aligned} P_{1,f}(f) &= f, \\ P_{2,f}(f) &= f^2 - 2a_1, \\ P_{3,f}(f) &= f^3 - 3a_1 f - 3a_2, \\ P_{4,f}(f) &= f^4 - 4a_1 f^2 - 4a_2 f + 2a_1^2 - 4a_3. \end{aligned}$$

More generally:

$$P_{n,f}(f) = \det(fI - A_n)$$

where

$$A_n = \begin{pmatrix} a_0 & 1 & & & & \\ 2a_1 & a_0 & 1 & & {\Large 0} & \\ \vdots & \vdots & \vdots & & & \\ (n-2)a_{n-3} & a_{n-4} & a_{n-5} & \cdots & 1 & \\ (n-1)a_{n-2} & a_{n-3} & a_{n-4} & \cdots & a_0 & 1 \\ na_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_1 & a_0 \end{pmatrix}.$$

This is related to expressing the power sums in terms of elementary symmetric functions. Truncating f and replacing q by $1/x$, we derive: $F(x) = x^m + a_0x^{m-1} + \cdots + a_{m-1}$, $m \geq n$, and we may identify the $\{e_k\}$ with the elementary symmetric functions of the roots of $F(x)$. Note that the power sum $s_n \in \mathbb{Z}[a_0, \ldots, a_{n-1}]$.

Expanding $P_{n,f}(f(\tau))$ in powers of q, the Grunsky [G] coefficients, $h_{m,n}$, are defined by

$$P_{n,f}(f(\tau)) = \frac{1}{q^n} + n\sum_{m\geq 1} h_{m,n}q^m.$$

We generalize j to a family of replicable functions (of standard form), $f^{(k)}$, $k \geq 1$, for which

$$\sum_{\substack{ad=n \\ 0\leq b<d}} f^{(a)}\left(\frac{a\tau+b}{d}\right) = P_{n,f}(f(\tau)).$$

This yields a new Hecke operator, $\hat{T}_n$ with $h_{m,n}$ as the coefficient of q^m in $\hat{T}_n(f)$. It is Grunsky's law of symmetry that $h_{m,n} = h_{n,m}$.

We now have an inductive definition of the important "replication power map" taking f to $f^{(n)}$, since $f^{(n)}(n\tau) = P_{n,f}(f) - \sum'$ where $\sum'$ omits the single term with $a = n$. This imposes the condition that the right side is a series in q^n. We take the principal branch to define $f^{(n)}(\tau)$. The replication power map f to $f^{(n)}$, f replicable, restricts on Monstrous Moonshine functions to the map induced on them by taking $g \in \mathbb{M}$ to g^n. Norton [N], in an important paper, defines the generating functions for the Faber polynomials and the $h_{m,n}$, unaware of the work of Faber [Fab] and Grunsky [G] preceding him. He gives a definition of replicability equivalent to the above, [ACMS], namely (paraphrased):

Definition. A function is replicable if $\gcd(m,n) = \gcd(r,s)$ and $\operatorname{lcm}(m,n) = \operatorname{lcm}(r,s)$ implies $h_{m,n} = h_{r,s}$.

[This suggests seeking an interpretation of the $\{h_{m,n}\}$ in terms of double coset representatives.]

Norton also proves his basis theorem:

Theorem. *The twelve coefficients* a_k,

$$k \in \{1, 2, 3, 4, 5, 7, 8, 9, 11, 17, 19, 23\},$$

determine a replicable function.

This remarkable result is useful for computing with replicable functions.

Newton's relations, which derive from the form of f, between the a_k and the Faber polynomials, together with Norton's defining properties of the $\{h_{m,n}\}$, show that replicable functions correspond to K-points on a variety. Norton has proved that K lies in a composite of quadratic extensions of $\mathbb{Q}$.

The Newton relations are equivalent to the generating function identity:

$$q\bigl(f(q) - f(p)\bigr) = \exp(-\sum_{n \geq 1} P_{n,f}\bigl(f(p)\bigr)q^n),$$

with $p = \exp(2\pi i \sigma)$ etc., where we abuse notation using $f(p)$ and $f(q)$ instead of $f(\sigma), f(\tau)$.

There is an outstanding conjecture of Norton [CuG], [CuN]:

Conjecture 1.2. *A function* $f = q^{-1} + \sum_{i \geq 1} a_i q^i$ *with rational integer coefficients is replicable if and only if either* f *is a modular fiction or it is the Hauptmodul for a group* $G \subset PGL_2(\mathbb{Q})^{>0}$ *satisfying*

1. G *has genus zero,*
2. G *contains a finite index* $\Gamma_0(N)$,
3. G *contains* $z \mapsto z + k$ *if and only if* $k \in \mathbb{Z}$.

Our model is Dedekind's (1877) [Ded] construction of $j(\tau)$ in terms of its Schwarz differential equation.

We define the Schwarz derivative $\{f, \tau\}$ to be $2(f''/f')' - (f''/f')^2$, where differentiation is with respect to τ. When f is a modular form, $\{f, \tau\}$ increases the weight by 4 and preserves the invariance properties, thus when f is a Hauptmodul, we have $\{f, \tau\} + R(f)f'^2 = 0$ with $R(f) = N(f)/[D(f)]^2$, the differential resolvent, and $f' = df/d\tau$ of weight 2. When expressed in partial fractions, we see $R(f)$ gives ramification data and also the critical points of f (namely those values of f for which $f'(\tau) = 0$).

From Dedekind (with normalization

$$1728\,j(\tau) = 1/q + 744 + 196884\,q + \cdots)$$

we find $R(j) = \frac{1-\frac{1}{2^2}}{(j-1)^2} + \frac{1-\frac{1}{3^2}}{j^2} - \frac{1-\frac{1}{2^2}-\frac{1}{3^2}}{j(j-1)}$, with ramification multiplicity 2 at $j\big(\exp(\pi i/2)\big) = 1$, and 3 at $j\big(\exp(\pi i/3)\big) = 0$.

To each f, there is a corresponding conformal invariance group, G_f acting on $\mathcal{H}$. From $R(f)$ we can find the critical points in $\mathcal{H}$, and the ramification gives the angles between bounding circular arcs intersecting at a critical point. A fundamental domain can be constructed and, once edges are identified, a presentation found for the group generated by hyperbolic reflections in the bounding circular arcs in $\mathcal{H}$. The Schwarz derivative takes us from f to G_f.

Over 600 Hauptmoduls, f, as above, are now known, some of which appear in [FMN]. For each, $R(f)$ has been computed. The Galois group of D is of "dihedral type", in that it has a unique cyclic subgroup of index 2. This provides an ordering of the critical points for Ohyama's construction of dynamical systems [Ohy1]. With a little more work, we should obtain a dynamical system of differential equations for each f, as shown by Ohyama [Ohy1] and exemplified by the Halphen system. This system was first studied in 1881 [Hal], and is a reduction of the self-dual Yang-Mills equations. For us, it is derived from the $\Gamma(4)$-Hauptmodul, namely $f = \big(\eta(\tau)/\eta(4\tau)\big)^8$. This has a triangular fundamental domain with angles $(0,0,0)$ at cusps $(0,1,\infty)$. It is remarkable that we have $\{f,\tau\} + E_4(2\tau) = 0$, where $E_4(\tau)$ is the Eisenstein series of weight 4:

$$E_4(\tau) = 1 + 240 \sum_{n\geq 1} \sigma_3(n) q^n.$$

In a further paper [Ohy2] the function $f = \big(\eta(\tau)/\eta(9\tau)\big)^3$ appears and we find it satisfies the Schwarz equation above with $E_4(2\tau)$ replaced by $E_4(3\tau)$.

Any function of the form $(*)$ satisfies

$$\frac{df}{dq} + \frac{1}{q^2}\,\exp(-v^t H v) = 0,$$

where $v^t = (q, q^2, q^3, \dots)$, and H is the semi-infinite matrix of Grunsky coefficients.

To each Hauptmodul there are two differential objects:

(1) A Schwarz equation, and
(2) a dynamical system.

There is also a pseudo-differential operator (roughly–treating the functions as Laplace transforms) which has not yet been studied.

A purpose of this approach is to learn more about analytic aspects associated with the Monster in the hope of better understanding the relation between the simple Lie groups and the sporadic simple groups.

Witten's ideas suggest there may be a finite-dimensional spin manifold with $\mathbb{M}$ acting on its loop space. A discussion of this is found in the book [Hir].

References

[ACMS] Alexander, D., Cummins, C., McKay, J., and Simons, C., Completely replicable functions, Lond. Math. Soc. Lecture Notes, **165**, edited by Liebeck and Saxl (1992), 87–98.

[CN] Conway, J.H., and Norton, S.P., Monstrous moonshine, Bull. Lond. Math. Soc., **11** (1979), 308–339.

[CuG] Cummins, C. J. and Gannon, T., Modular equations and the genus zero property of Moonshine functions, Inv. Math., **129** (1997), 413–443.

[CuN] Cummins, C. J. and Norton, S.P., Rational Hauptmoduls are replicable, Can. J. Math., **47** (1995), 1201–1218.

[Cur] Curtiss, J. and H., Faber polynomials and the Faber series, Amer. Math. Monthly **78** and **79** (1974), 577–596 and 363.

[Ded] Dedekind, R., Schreiben an Herrn Borchardt über die Theorie der elliptischen Modulfunktionen, Crelle, **83**, 265–292.

[Fab] Faber, G., Über polynomische Entwicklungen, Math. Annalen, **57** (1903), 389–408.

[FMN] Ford, D.J., McKay, J., and Norton, S.P., More on replicable functions, Comm. in Alg., **22** (1994), 5175–5193.

[G] Grunsky, H., Koeffizientenbedingungen für schlicht abbildende meromorphe Funktionen, Math. Z., **45** (1939), 29–61.

[Hir] Hirzebruch, F., Berger, T. and Jung R., "Manifolds and Modular Forms (Vieweg)", 1992.

[Kac,] Kac, V., An elucidation of: "Infinite-dimensional algebras, Dedekind's η-function, classical Möbius function and the very strange formula". $E_8^{(1)}$ and the cube root of the modular invariant j, Adv. in Math., **35** (1980), 264–273.

[Lep] Lepowsky, J., Euclidean Lie algebras and the modular function j, "Proc. Symp. Pure Math., **37**, Amer. Math. Soc.", 1980, pp. 567–570.

[Mar] Martin, Y., On modular invariance of completely replicable functions, Contemp. Math., **193** (1996), 263–286.

[McK] McKay, J., The formal modular equation, (unpublished).

[N] Norton, S.P., More on moonshine, "Computational group theory, edited by M.D. Atkinson, Academic", 1984, pp. 185–193.

[Ohy1] Ohyama, Y., Systems of nonlinear differential equations related to second order linear equations, Osaka J. Math., **33** (1996), 927–949.

[Ohy2] Ohyama, Y., Differential equations for modular forms with level three, To appear (),.

[Ser] Serre, J-P., "A course in arithmetic, Springer-Verlag", 1973.

[Sil] Silverman, J.H., "Advanced topics in the arithmetic of elliptic curves, Springer-Verlag", 1994, pp. 181.

Centre Interuniversitaire en
Calcul Mathématique Algébrique
Concordia University
Montreal
Canada
email: mckay@cs.concordia.ca

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 355–368

On the vertices of modules in the Auslander–Reiten quiver III

Tetsuro Okuyama and Katsuhiro Uno

§0. Introduction

Let $kG$ be the group algebra of a finite group $G$ over a field $k$ of characteristic $p$, where $p$ is a prime. We denote the stable Auslander–Reiten quiver (AR quiver for short) of $kG$ by $\Gamma_s(kG)$. For the definition of an AR quiver, see [B]. It is known that each connected component $\Gamma$ of $\Gamma_s(kG)$ has the uniquely determined tree class $\mathcal{T}$. The AR component $\Gamma$ is isomorphic as graphs to $\mathbf{Z}\mathcal{T}/\pi$, where $\mathbf{Z}\mathcal{T}$ is the graph obtained in a standard way from countably many copies of the tree $\mathcal{T}$ and $\pi$ is a certain subgroup of $Aut(\mathbf{Z}\mathcal{T})$. Since the important paper by Webb [W] was published, many results concerning the tree classes have been obtained. (See [Be], [E3], [E4], [ES] and [O1].) In the present paper, assuming that $k$ is a perfect field, we determine all the tree classes, not the possibilities of them, completely. The following should be the final result in this nature.

Theorem A. *Let $k$ be a perfect field. Then the tree class of a connected component of $\Gamma_s(kG)$ is one of the following: A_n, $\tilde{A}_{1,2}$, A_∞, $\tilde{B}_3$, B_∞, D_∞, or A_∞^∞. Moreover, each of the above in fact occurs. Furthermore, the following hold. Here $D$ is a defect group of the block to which the modules in $\Gamma$ belong.*

(i) *B_∞ occurs only when $D$ is dihedral.*

(ii) *D_∞ occurs only when $D$ is semidihedral.* ([E3], [E4])

(iii) *A_∞^∞ occurs only when $D$ is dihedral or semidihedral.* ([E3], [E4])

(iv) *$\tilde{A}_{1,2}$ or $\tilde{B}_3$ occurs only when $D$ is a four group.* ([Be], [ES])

For the notation of the tree classes, we follow 2.30 of [B]. In particular,

$$\tilde{A}_{1,2} : \cdot \xrightarrow{(2,2)} \cdot, \quad \tilde{B}_3 : \cdot \xrightarrow{(1,2)} \cdot \longrightarrow \cdot \xrightarrow{(2,1)} \cdot, \quad B_\infty : \cdot \xrightarrow{(1,2)} \cdot \longrightarrow \cdot \longrightarrow \cdots.$$

Received May 27, 1999.
Revised June 16, 2000.

Remark 1. Each of the possibilities in Theorem A occurs in the following case.

(i) A_n occurs if and only if D is cyclic. See [B].

(ii) $\tilde{A}_{1,2}$ occurs for a four group with $p=2$. See p. 180 of [B].

(iii) $\tilde{B}_3$ occurs for the alternating group on 4 letters with $p=2$ if k does not contain a cube root of unity. See p. 195 of [B].

(iv) An example of a B_∞-component is given in Section 4.

(v) A_∞^∞ occurs for dihedral groups of order greater than 4 with $p=2$.

(vi) D_∞ occurs for semidihedral groups with $p=2$.

Furthermore, the following are known.

(vii) If the tree class is A_∞^∞, then we have $\Gamma \cong \mathbf{Z}A_\infty^\infty$ unless D is a four group. (See [ES].)

(viii) If k is algebraically closed, then one of A_n, $\tilde{A}_{1,2}$, A_∞, D_∞, or A_∞^∞ must occur. (See p.160 of [B].)

(ix) If the modules in Γ are periodic, then its tree class is A_∞. (2.31.11 of [B])

Since B_∞ appears when we have a certain involutive automorphism of an A_∞^∞ component, the block is tame in this case, too. However, it seems that no example of a B_∞-component has been known so far, and this is the reason why we give an example here. From the results known so far, A_n is the only finite Dynkin tree class and $\tilde{A}_{1,2}$ and $\tilde{B}_3$ are only Euclidean tree classes. The rest are infinite Dynkin tree classes, and only A_∞, D_∞, A_∞^∞, B_∞ and C_∞ are possible. (See [B].) Hence, in order to prove Theorem A, it suffices to give an example of a B_∞-component and prove that C_∞ does not occur. In fact, we prove the following.

Theorem 1. *Let k be a perfect field. Then the following hold.*

(i) *As a tree class of a component of $\Gamma_s(kG)$, C_∞ does not occur.*

(ii) *If B_∞ occurs, then a defect group D of the block to which the modules in Γ belong is dihedral of order at least* 8.

On the vertices of modules, beginning with the result for p-groups in [E2], there are several developments [U2], [OU2] which were obtained by using the generalization of Green correspondence due to Kawata [K1] and the results on vertices of modules in the Auslander-Reiten sequences [U1], [OU1]. In this paper, we have the following, which would be also the final result for non-periodic components.

Theorem B. *Let k be a perfect field, and let Γ be a connected component of $\Gamma_s(kG)$. Suppose that it is not a tube. Then one of the following holds.*

(i) *All the modules in Γ have vertices in common.*

(ii) *We can take* $T : X_1 - X_2 - X_3 - \cdots - X_n - \ldots$ *in* Γ *with* $\Gamma \cong \mathbf{Z}T$ *and* $vx(X_1) < vx(X_2) = vx(X_3) = vx(X_4) = \cdots = vx(X_n) = \ldots$.

(iii) $p = 2$, $\Gamma = \mathbf{Z}A_\infty^\infty$, *and only two distinct vertices* P *and* Q *occur, with* $|P : Q| = 2$. *Moreover, one of the following holds.*

(iiia) Q *is a dihedral group of order greater than* 4, *and the modules with vertex* Q *lie in a subquiver* Γ_Q *such that both* Γ_Q *and* $\Gamma \setminus \Gamma_Q$ *are isomorphic to* $\mathbf{Z}A_\infty$ *as graphs.*

(iiib) Q *is a Kleinian four group and* P *is a dihedral group of order 8, and the modules with vertex* Q *lie in two or four adjacent* τ*-orbits.*

Moreover, each of the above possibilities in fact occurs.

Remark 2. The above (i) and (ii) occur in many cases, (iiia) occurs for a dihedral 2-group. See (3.3) of [E1]. (iiib) occurs for a dihedral group D_8 of order 8 and the symmetric group S_4 on 4 letters. The group algebra kD_8 has an AR component satisfying (iiib) above with two adjacent τ-orbits of modules having four group as vertex, and kS_4 has an AR component satisfying (iiib) above with four adjacent τ-orbits of modules having four group as vertex. See also [E1] and V.3 of [E2].

Most parts of Theorem B have been proved in [OU2]. More precisely, it has been shown there that there are only three possibilities (i), (ii) and (iii), of which (i) and (iii) are exactly the same as in Theorem B above. However, the part (ii) of the main theorem in [OU2] asserts that there are three possibilities, namely,

(iia) $vx(X_1) < vx(X_2) = vx(X_3) = vx(X_4) = \cdots = vx(X_n) = \ldots$,
(iib) $vx(X_1) < vx(X_2) = vx(X_3) < vx(X_4) = \cdots = vx(X_n) = \ldots$,
(iic) $vx(X_1) = vx(X_2) < vx(X_3) = vx(X_4) = \cdots = vx(X_n) = \ldots$.

Thus, in order to prove Theorem B, it suffices to show that (iib) and (iic) above do not occur. More precisely, it suffices to prove the following.

Theorem 2. *In the situation of Theorem B, suppose that* $\Gamma \cong \mathbf{Z}A_\infty$. *Then* (i) *or* (ii) *of Theorem B holds.*

The purpose of this paper is of course to prove Theorems 1 and 2. For the both theorems, semidihedral groups play an important role. Thus, after giving some preliminary results in Section 1, we consider modules over dihedral and semidihedral groups in Section 2. The theorems are proved in Section 3. Notation is standard. See [F] and [NT]. The Auslander-Reiten translate is denoted by τ. For symmetric algebras, τ is the composite Ω^2 of two Heller translates. For a non-projective indecomposable module M, the AR sequence terminating at M is denoted by $\mathcal{A}(M)$.

§1. Preliminaries

In this section, we first consider automorphisms of an AR component Γ of $\Gamma_s(kG)$. The following is well known.

Lemma 1.1. *Let σ be an automorphism of the graph Γ which commutes with τ. Suppose that σ has finite order.*

(i) *If $\Gamma \cong \mathbf{Z}A_\infty$, then σ is trivial.*

(ii) *If $\Gamma \cong \mathbf{Z}D_\infty$, then σ is trivial or interchanges the two modules in the end with the same predecessor.*

(iii) *If $\Gamma \cong \mathbf{Z}A_\infty^\infty$, then σ is trivial or a reflection with respect to a certain τ-orbit.*

Let k' be a finite Galois extension of k. Assume that every indecomposable direct summand of $M \otimes_k k'$ for $M \in \Gamma$ is absolutely indecomposable. The proof of the following can be found in 2.33.3 of [B].

Lemma 1.2. *In the situation above, direct summands of $M \otimes_k k'$ for $M \in \Gamma$ belong to a finite set of connected components $\Gamma_1, \cdots, \Gamma_m$ of $\Gamma_s(k'G)$ and $Gal(k'/k)$ acts transitively among the Γ_i's. In particular, Γ_i's are isomorphic to each other.*

Assume that Γ has tree class B_∞ or C_∞. In view of Remark 1 (viii), we have another tree class for components of $\Gamma_s(k'G)$. When tensoring Γ with k', we get the following tree classes.

Lemma 1.3. *In the situation of Lemma 1.2, the following hold.*

(i) *If $\Gamma \cong \mathbf{Z}B_\infty$, then $\Gamma_i \cong \mathbf{Z}A_\infty^\infty$ for each i, and some element in $Gal(k'/k)$ stabilizes Γ_i and gives a reflection with respect to a certain τ-orbit.*

(ii) *If $\Gamma \cong \mathbf{Z}C_\infty$, then $\Gamma_i \cong \mathbf{Z}D_\infty$ for each i, and some element in $Gal(k'/k)$ stabilizes Γ_i and interchanges its two ends.*

In [U2] the relationship between the tree classes of components of $\Gamma_s(kG)$ and $\Gamma_s(kN)$ for a normal subgroup N of G is investigated. There it is assumed that k is an algebraically closed field. However, those assertions hold in more general situation. One of the important and crucial points in the argument is to introduce two indices $a(M)$ and $b(M)$ for an indecomposable N-projective kG-module M. They are defined by $a(M) = \dim_k eE_G(V^G)/eJ(E_G(V^G))$ and $b(M) = \dim_k eE_G(V^G)/eL_G(V^G)$, where V is an indecomposable N-source of M, $E_G(V^G) = \mathrm{End}_{kG}(V^G)$, $L_G(V^G) = J(E_N(V))E_G(V^G)$, and e is the idempotent of $E_G(V^G)$ with $eV^G = M$. However, we use only the fact that the multiplicities of direct summands can be described in terms of them. Thus, if $E_N(V)/J(E_N(V)) \cong k$, then the same conclusions hold. On the other hand, if k is a perfect field, then a kG-module M is absolutely indecomposable if and only if $\mathrm{End}_{kG}(M)/J(\mathrm{End}_{kG}(M)) \cong k$ by VII.6.9 of [HB]. Thus modifying the results in sections 2, 3 and 4 of [U2] in such a way, we can summarize them as follows.

Lemma 1.4. *Let N be a normal subgroup of G and Λ a connected component of $\Gamma_s(kN)$. Suppose that k is a perfect field, all the modules in Λ are G-invariant absolutely indecomposable, and that all the arrows in Λ are multiplicity free. Let V be in Λ and M an indecomposable direct summand of V^G. Let Γ be the connected component of $\Gamma_s(kG)$ containing M. Then one of the following holds.*

(i) *All the modules in Γ are N-projective and $\Gamma \cong \Lambda$.*

(ii) *Γ is isomorphic to $\mathbf{Z}A_\infty$ or a tube, that is $\mathbf{Z}A_\infty/\langle\tau^n\rangle$.*

Proof. As remarked above, the arguments in sections 2, 3 and 4 in [U2] can be still applied. In particular, if the modules in $\mathcal{A}(M)$ are N-projective, then the conclusions of 3.5, 3.7, 3.8 and 3.9 of [U2] yield (i). If some direct summand of modules in $\mathcal{A}(M)$ is not N-projective, then the arguments in 4.1 and 4.2 of [U2] almost give (ii). Here we say "almost" because in the proof of 4.2 of [U2], only the D_∞ case is excluded in order to conclude that the tree class of Γ is A_∞. This works since we assume there that k is algebraically closed. However, in the present situation, we have to exclude also the case of B_∞, since this is the only remaining case where $\mathcal{A}(M)$ has an indecomposable (modulo projectives) middle term. Assume that M lies at the end of an AR component with tree class B_∞. Then we have AR sequences

$$\begin{aligned} \mathcal{A}(M) &: 0 \to \tau M \to X \oplus F \to M \to 0, \quad \text{and} \\ \mathcal{A}(X) &: 0 \to \tau X \to Y \oplus 2\tau M \oplus F' \to X \to 0, \end{aligned}$$

where X and Y are non-projective indecomposable kG-modules and F and F' are projective or zero. Note that we are considering the case where X is not N-projective. Hence $\mathcal{A}(X)_N$ splits and we have $Y_N \oplus 2b(M)\tau V \cong X_N \oplus \tau X_N$ modulo projectives. On the other hand, considering $\mathcal{A}(M)_N$, 2.6 of [U2] implies that $X_N \cong a(M)\mathcal{M}(V) \oplus (b(M) - a(M))(V \oplus \tau V)$ modulo projectives, where $\mathcal{M}(V)$ is the middle term of $\mathcal{A}(V)$. Since $\mathcal{M}(V)$ and $\mathcal{M}(\tau V)$ do not have τV as a direct summand and since modules in a B_∞-component are not periodic, we have $2b(M) \leq 2(b(M) - a(M))$. But this gives $a(M) \leq 0$, a contradiction.

Q.E.D.

§2. Modules over dihedral and semidihedral group algebras

We first consider a semidihedral group G of order 2^n. Here $n \geq 4$. For a filed k of characteristic 2, the group algebra kG is tame and $\Gamma_s(kG)$ has non-periodic components of type only of A_∞^∞ and D_∞. (See [E3].) Let A be a k-algebra generated by two elements a and b with the relations

$$a^3 = b^2 = a^2 - b(ab)^{2^{n-2}-1} = 0.$$

In [BD], Bondarenko and Drozd claim the following. Since we can not find a literature which describes an explicit isomorphism, we give it here.

Lemma 2.1. *Let k be a perfect field of characteristic* 2 *and G a semidihedral group of order 2^n, where $n \geq 4$. Then we have a k-algebra isomorphism $kG/\mathrm{soc}kG \cong A$.*

Proof. Write $G = \langle x, y | x^{2^{n-1}} = y^2 = 1, yxy = x^{-1+2^{n-2}} \rangle$, and define u in kG by

$$u = x^{2^{n-2}-2} + x^{2^{n-2}-3} + \cdots + x^2 + x + 1 = (x-1)^{2^{n-2}-1} + x^{2^{n-2}-1}.$$

Then, $u^{2^{n-2}} = x^{2^{n-2}}$, $(x-1)u = x^{2^{n-2}-1} - 1 = yxy - 1$, and

$$(1) \quad u - 1 = (x-1)^{2^{n-2}-1} + x^{2^{n-2}-1} + 1 = (x-1)^{2^{n-2}-1} + (x-1)u.$$

We also have

$$\begin{aligned}(2) \qquad (uy-1)(x-1) &= u(yxy-1)y - (x-1) \\ &= u(x-1)uy + (x-1) = (x-1)(u^2y-1).\end{aligned}$$

Let

$$\alpha = (uy-1) + (x-1)^{2^{n-1}-3}(y-1), \quad \beta = y-1, \quad \text{and} \quad \hat{G} = \sum_{g \in G} g.$$

Then, $\beta^2 = 0$. Moreover, $\alpha^2 = (x-1)^{2^{n-1}-2}(y-1)$, since we have

$$(3) \qquad (uy-1)^2 = (x-1)^{2^{n-1}-1},$$

$$(4) \qquad (uy-1)(x-1)^{2^{n-1}-3}(y-1) = \hat{G},$$

$$\begin{aligned}(5) \qquad &(x-1)^{2^{n-1}-3}(y-1)(uy-1) \\ &= \hat{G} + (x-1)^{2^{n-1}-1} + (x-1)^{2^{n-1}-2}(y-1),\end{aligned}$$

$$(6) \qquad ((x-1)^{2^{n-1}-3}(y-1))^2 = 0.$$

(6) is easy to show. For (3), note that $(uy)^2$ is equal to

$$\begin{aligned}u(yuy) &= u((yxy-1)^{2^{n-2}-1}+x) = u((x-1)^{2^{n-2}-1}u^{2^{n-2}-1}+x)\\ &= (x-1)^{2^{n-2}-1}u^{2^{n-2}}+ux\\ &= (x-1)^{2^{n-2}-1}x^{2^{n-2}}+(x-1)^{2^{n-2}-1}x+x^{2^{n-2}}\\ &= (x-1)^{2^{n-1}-1}+1.\end{aligned}$$

The left hand side of (4) is equal to $(x-1)^{2^{n-1}-4}(uy-1)(x-1)(y-1)$ as $(x-1)^{2^{n-1}-4}$ is central in $kG$. Then (4) can be seen by using (2). (5) is proved by using (1) and the following. (We use also (3) above.)

$$\begin{aligned}(y-1)(uy-1) &= (uy-1)(y-1)+(yuy-u)\\ &= (u-1)(y-1)+(1-u^2)u^{-1}+(x-1)^{2^{n-1}}.\end{aligned}$$

From $\alpha^2=(x-1)^{2^{n-1}-2}(y-1)$, we also obtain $\alpha^3=\hat{G}$.

Finally, we claim that $\beta(\alpha\beta)^{2^{n-2}-1}=\alpha^2+\hat{G}$. Note first that $\alpha\beta$ equals to $(uy-1)(y-1)=(u-1)(y-1)$. Thus,

$$\begin{aligned}\beta(\alpha\beta) &= (y-1)(u-1)(y-1) = (yuy-u)(y-1)\\ &= (u^{-1}-u)(y-1)+\hat{G} = (u^2-1)u^{-1}(y-1)+\hat{G},\end{aligned}$$

and by using induction, we obtain

$$\beta(\alpha\beta)^{2^{n-2}-1} = (u^2-1)^{2^{n-2}-1}u^{-2^{n-2}+1}(y-1).$$

Now by (1) we have

$$\begin{aligned}\beta(\alpha\beta)^{2^{n-2}-1} &= (x-1)^{2^{n-1}-2}u^{-2^{n-2}+1}(y-1) = (x-1)^{2^{n-1}-2}x(y-1)\\ &= (x-1)^{2^{n-1}-2}(y-1)+\hat{G} = \alpha^2+\hat{G}.\end{aligned}$$

Since $\alpha \equiv uy-1 \equiv (u-1)+(y-1) \equiv (x-1)+(y-1)$ modulo $(J(kG))^2$, the two elements $\alpha$ and $\beta$ generate $kG$. Note also that soc$kG$ is generated by $\hat{G}$ over $k$. Define a map $\varphi : A \to kG/\text{soc}kG$ by $\varphi(a) = \alpha + \text{soc}kG$ and $\varphi(b) = \beta + \text{soc}kG$. Then, the above computations show that $\varphi$ is a well defined $k$-algebra isomorphism. Q.E.D.

If $|k| \geq 3$, Crawley-Boevey gives a description of indecomposable A-modules in [CB]. Thus it gives a classification of indecomposable modules over semidihedral group algebras. We now give the following remark.

Lemma 2.2. *Let k be a perfect field of characteristic 2 and G a semidihedral group of order 2^n, where $n \geq 4$. Then all the non-periodic indecomposable kG-modules are absolutely indecomposable.*

Proof. Since k is perfect, by VII.6.9 of [HB], it suffices to prove that $M \otimes_k k'$ is indecomposable for any indecomposable kG-module M and any extension k' of k. In the classification of indecomposable kG-modules in [CB], it is required that k has at least 3 elements. However, if this is the case, then the classification is exactly the same in all the cases. Hence, if $|k| \geq 3$, the assertion holds. Now suppose that $k = GF(2)$. Let $k_1 = GF(2^2)$, $k_2 = GF(2^3)$ and $k_3 = GF(2^6)$. Let M be an indecomposable kG-module. Let

$$M \otimes_k k_1 = M_1 \oplus \cdots \oplus M_r \quad \text{and} \quad M \otimes_k k_2 = M'_1 \oplus \cdots \oplus M'_s$$

be decompositions of $M \otimes_k k_1$ and $M \otimes_k k_2$ into direct sums of indecomposable k_1G-modules and k_2G-modules, respectively. Then $M_1, \ldots, M_r$ are $Gal(k_1/k)$-conjugates and $M'_1, \ldots, M'_s$ are $Gal(k_2/k)$-conjugates. Here r is 1 or 2 and s is 1 or 3, since $Gal(k_1/k)$ and $Gal(k_2/k)$ are cyclic of order 2 and 3, respectively. However, we know that M_i's and M'_j's are absolutely indecomposable, and thus

$$(M_1 \otimes_{k_1} k_3) \oplus \cdots \oplus (M_r \otimes_{k_1} k_3) \quad \text{and} \quad (M'_1 \otimes_{k_2} k_3) \oplus \cdots \oplus (M'_s \otimes_{k_2} k_3)$$

are both indecomposable direct sum decompositions of $M \otimes_k k_3$. Hence, we have $r = s = 1$. Therefore, $M \otimes_k k_1$ is indecomposable, and it yields that M is absolutely indecomposable. Q.E.D.

Remark 2.3. The assertions in Lemma 2.2 can be proved also in the case where G is a dihedral 2-group, by using the classification of indecomposable kG-modules.

The following is a key result in this paper.

Proposition 2.4. *Let k be a perfect field, G a dihedral or semidihedral 2-group, and σ an automorphism of G sending each involution in G into its G-conjugate. Then every non-periodic indecomposable kG-module is σ-invariant. In particular, every non-periodic indecomposable module over a semidihedral group is invariant under any automorphism of the group.*

Proof. By Lemma 2.2 and Remark 2.3, we may assume that k is algebraically closed. Let M be a non-periodic indecomposable kG-module. If G is a four group, the result holds clearly. We assume that $|G| > 4$. Thus M lies in a component isomorphic to $\mathbf{Z}A_\infty^\infty$ or $\mathbf{Z}D_\infty$.

Consider first the case where M has at least two predecessors in the AR component. Take an indecomposable kG-module X and an irreducible map $f : X \to M$. Suppose that f is surjective. If this is not the case, we take its dual. Let U be the kernel of f. We use the argument in 3.2 of [E4]. There exists a shifted subgroup H of order 2 such that U_H is not projective. Let $V = k_H^G$, the module induced from the trivial module of H. It is concluded that $\dim V \leq |G|/2 \leq \dim U'$, where U' is U or ΩU. Moreover, it is shown that there is no monomorphism from U' to V or $U' \cong V$. Furthermore, in Case 1 (ℓ.-5 on p.155 of [E4]) a contradiction is derived when it is assumed that there is no monomorphism from U' to V. Consequently, $U \cong V$ holds and we have $|G|/2 = \dim V = \dim U$.

Notice that kH is a subalgebra of kN for some elementary abelian subgroup N of order 4 in G. Any such an N is generated by the central involution and a non-central involution of G. Thus from the assumption on σ, there exists $g \in G$ such that $H^\sigma = H^g$. Hence V is σ-invariant. Let $h_1 : V \to V^\sigma$ be an isomorphism. Consider the following commutative diagram. Here, by 1.1 of [E4], either h_1 or h_1^{-1} lifts to a map between X and X^σ, and we may assume that h_1 does.

$$\begin{tikzcd}
0 \arrow[r] & V \arrow[r, "g"] \arrow[d, "h_1"'] & X \arrow[r, "f"] \arrow[d, "h_2"'] & M \arrow[r] \arrow[d, "h_3"'] & 0 \\
0 \arrow[r] & V^\sigma \arrow[r, "g^\sigma"] & X^\sigma \arrow[r, "f^\sigma"] & M^\sigma \arrow[r] & 0
\end{tikzcd}$$

Since σ has finite order and since X and M are indecomposable, h_3 must be an isomorphism by Fitting's lemma.

Next consider the case where M lies at the end of a D_∞-component. There are indecomposable modules X, Y, Z and irreducible maps $f : X \to M$, $f' : X \to Y$ and $f'' : X \to Z$, where M and Y have only one predecessor. We already know that X and Z are σ-invariant by the above. Thus M^σ is either M or Y. We prove that $M^\sigma \cong M$ by showing that $\dim M \neq \dim Y$. By applying the argument in the first paragraph to the map $f'' : X \to Z$, we have $|G|/2 \equiv \dim X - \dim Z \mod |G|$. Moreover, considering $\mathcal{A}(M)$ and $\mathcal{A}(\tau^{-1}X)$, we have $\dim X \equiv 2\dim M \mod |G|$ and $2\dim X \equiv \dim M + \dim Y + \dim Z \mod |G|$. Hence $\dim M - \dim Y \equiv |G|/2 \mod |G|$. Therefore, we have $\dim M \neq \dim Y$ as desired. Q.E.D.

§3. Proof of Theorems

We prove Theorem 2 first.

Proof of Theorem 2. By the very final remark in [OU2], we may assume that $p = 2$, and G is a 2-group. Moreover, it suffices to consider the case where $vx(X_1) = vx(X_2) < vx(X_3) = vx(X_4) = \dots$ in the notation of the theorem. If this is the case, then by Theorem B of [E2], G has a normal subgroup H with $|G : H| = 2$ and $\Gamma_s(kH)$ has an AR component Θ isomorphic to $\mathbf{Z}D_\infty$. Furthermore, the two ends in Θ are G-conjugate. Now, by Theorem 4 of [E4], H must be semidihedral. However, this is impossible by Proposition 2.4. Q.E.D.

Proof of Theorem 1. Let $\bar{k}$ be the algebraic closure of k. Suppose that $\Gamma_s(kG)$ has an AR component Γ isomorphic to either $\mathbf{Z}B_\infty$ or $\mathbf{Z}C_\infty$. Let D be a defect group of the block of G to which the modules in Γ belong. By Theorem B, all the modules have the same vertex Q. Let M be in Γ. Let $\Gamma_1, \cdots, \Gamma_r$ be connected components of $\Gamma_s(\bar{k}G)$ containing indecomposable direct summands of $M \otimes_k \bar{k}$. All the modules in Γ_i have also vertex Q by III.4.14 of [F], and they belong to blocks whose defect group is D by III.9.10 of [F]. Now by Lemma 1.2, Γ_i's are $Gal(\bar{k}/k)$ conjugate, and by Lemma 1.3, $\Gamma_i \cong \mathbf{Z}A_\infty^\infty$ if $\Gamma \cong \mathbf{Z}B_\infty$, and $\Gamma_i \cong \mathbf{Z}D_\infty$ if $\Gamma \cong \mathbf{Z}C_\infty$. Hence D is either dihedral or semidihedral. ([E4]) We will show that $\Gamma \cong \mathbf{Z}B_\infty$ and D is dihedral. The proof consists of several lemmas.

Lemma 3.1. *We may assume that Q is normal in G. Moreover, Q is dihedral or semidihedral and we have $|D : Q| \leq 2$.*

Proof. By [K1] there is a quiver monomorphism from Γ to a component of $\Gamma_s(kN_G(Q))$ which preserves vertices. In particular, M is mapped to its Green correspondent. Since $\mathbf{Z}B_\infty$ and $\mathbf{Z}C_\infty$ can not be a proper subquiver of any AR component of the stable AR quiver, the image of the monomorphism must be a connected component. Moreover, the Green correspondent of M lies in a block of $N_G(Q)$ whose defect group is also dihedral or semidihedral. Hence, it follows from the same argument as in the second paragraph of 4.2 in [E4] (p.158) that the $kN_G(Q)$-modules in the image lie in a block whose defect group is D. Thus, we may assume that Q is normal in G. The last statement holds since Q is a non-cyclic normal subgroup of D. Q.E.D.

Let V be a Q-source of M and Θ the AR component of $\Gamma_s(kQ)$ containing V. Let N be the set of elements in G those which induce automorphisms of Q by conjugation sending each involution in Q into its Q-conjugate.

Lemma 3.2. *It follows that Q is a dihedral group of order at least*

8, $\Theta \cong \mathbf{Z}A_\infty^\infty$, $\Theta$ is $G$-invariant, and that any element in $G \setminus N$ induces a reflection on $\Theta$.

Proof. Recall that all the modules in $\Gamma$ are $Q$-projective. If $Q$ is a four group, then $kQ$ has two $\tau$-orbits of non-periodic indecomposable modules. Thus $\Gamma$ has only finitely many $\tau$-orbits, a contradiction. Thus $Q$ is not a four group. By Lemma 3.1, we have $|G : N| \leq 2$, and $G = N$ if $Q$ is semidihedral. Recall that every module in $\Theta$ is $N$-invariant by Proposition 2.4. Thus, if $G = N$, then it would follow from Lemma 1.4 that $\Gamma \cong \Theta$ or $\Gamma$ has tree class A_∞, a contradiction. Hence $G \neq N$, and in particular, $Q$ must be dihedral of order at least 8. This implies also that $\Theta \cong \mathbf{Z}A_\infty^\infty$. ([E3]) Moreover, if all the modules in $\Theta$ are $G$-invariant, or if $N = I_G(\Theta)$, the inertia group of $\Theta$ in $G$, then Lemma 1.4 and [K2] derive a contradiction similarly. Thus, $\Theta$ is $G$-invariant but some modules in $\Theta$ are not $G$-invariant. This means that every element in $G \setminus N$ induces a reflection on $\Theta$ by Lemma 1.1. Q.E.D.

Let $H = QC_G(Q)$. Then $H$ is a normal subgroup of $G$ contained in $N$. Let $X$ be an indecomposable $kH$-module such that $M$ is isomorphic to a direct summand of X^G and that the source of $X$ is $V$, and let $\Lambda$ be a connected component of $\Gamma_s(kH)$ containing $X$. Moreover, let $b$ be a block of $kH$ containing $X$.

Lemma 3.3. *It follows that $\Lambda \cong \Theta \cong \mathbf{Z}A_\infty^\infty$. Moreover, $b \cong kQ \otimes_k A$, where $A$ is the full matrix ring over some finite extension field of $k$. In particular, $Q$ is a defect group of $b$. Furthermore, we may assume that $b$ is $G$-invariant.*

Proof. Again by Lemma 1.4, $\Lambda \cong \Theta \cong \mathbf{Z}A_\infty^\infty$ and all the modules in $\Lambda$ are $Q$-projective. The results follow from the argument in the proof of 4.1 of [E4]. The last statement holds by [K2]. Q.E.D.

We fix an isomorphism $b \cong kQ \otimes_k A$ in Lemma 3.3 and identify these two algebras. Let $S$ be the unique (up to isomorphisms) simple $A$-module. Then, since $b$ is $G$-invariant, so is $S$. Moreover, by Lemma 3.3, there is an equivalence between mod$kQ$ and mod$b$, by which a $kQ$-module $U$ corresponds to $U \otimes_k S$. Let $A \otimes_k \overline{k} = \oplus_i A_i$ be the decomposition into a direct sum of simple algebras over $\overline{k}$. Accordingly, we have $S \otimes_k \overline{k} = \oplus_i S_i$ and $b \otimes_k \overline{k} \cong \overline{k}Q \otimes_{\overline{k}} (A \otimes_k \overline{k}) = \oplus_i (\overline{k}Q \otimes_{\overline{k}} A_i)$, where S_i is a simple A_i-module. For each $i$, let $b_i = \overline{k}Q \otimes_{\overline{k}} A_i$. Then b_i is a block of $\overline{k}H$ and its defect group is $Q$ by III. 9.10 of [F]. Moreover, there is also an equivalence between mod $\overline{k}Q$ and modb_i, by which a $\overline{k}Q$-module $W$ corresponds to $W \otimes_{\overline{k}} S_i$. Let $U$ be a $kQ$-module and suppose that the b-module $U \otimes_k S$ lies in Λ. Since U is not periodic, $U \otimes_k \overline{k}$ is indecomposable by Remark 2.3. Hence tensoring the modules in Λ with $\overline{k}$, the AR component Λ decomposes into a disjoint union $\cup_i \Lambda_i$. Here Λ_i is an AR component of $\Gamma_s(\overline{k}H)$ and isomorphic to $\mathbf{Z}A_\infty^\infty$ by Lemma 3.3. Write $X \otimes_k \overline{k} = \oplus_i X_i$, where X_i is the direct summand belonging to b_i. Then X_i lies in Λ_i. There is an indecomposable direct summand M_1 of $M \otimes_k \overline{k}$ such that $M_1 \cong X_1^G$. Without loss of generality, we may assume that M_1 lies in Γ_1.

Lemma 3.4. *It follows that $D = Q$, and the conclusions in Theorem* 1 *hold.*

Proof. Suppose that $D \neq Q$. Considering all the possibilities for Q and D, it follows that $G = DN$ and $D \cap N = Q$. Since G/H is a 2-group, by V.5.15 and V.5.16 of [NT], we may assume that DH is the inertia group $I_G(b_1)$ of b_1 in G. In particular, $DH = I_G(\Lambda_1)$. Without loss of generality, we may assume that V is D-invariant, that is, an element of $DH \setminus H$ induces a reflection on Θ with respect to the τ-orbit of V. Then, X_1 is D-invariant from the above argument. In fact, we have $I_G(X_1) = DH$. Now by 2.5 of [U2], the middle term of $\mathcal{A}(M_1)$ has a direct summand whose vertex is D, a contradiction. Therefore, $Q = D$. Finally, we recall that, if a defect group is dihedral, then D_∞ does not occur. Thus $\Gamma_i \cong \mathbf{Z}A_\infty^\infty$ and we can conclude that $\Gamma \cong \mathbf{Z}B_\infty$ by Lemma 1.3. Q.E.D.

§4. Examples

The following gives an example of a group G such that $\Gamma_s(kG)$ has a component isomorphic to $\mathbf{Z}B_\infty$. It is due to the first author ([O2]).

Let k be a perfect field of characteristic 2 which does not contain a cube root of unity. Let n be an integer with $n \geq 3$ and G a group generated by x, y , z and t with relations $x^2 = y^2 = z^3 = t^2 = 1$ and

$$(xy)^{2^{n-1}} = 1, xz = zx, yz = zy, tx = yt, ty = xt, tz = z^2t.$$

Then $|G| = 2^{n+1}3$ and G has normal subgroups $D = \langle x, y\rangle$ and $C = \langle z\rangle$ with $D \cap C = \{1\}$. Note that D is a dihedral group of order 2^n and C is a cyclic group of order 3. Let $H = D \times C$. Then G is a semidirect product of H and $\langle t\rangle$. Let σ be a Galois automorphism such that σ interchanges the two cube roots of unity. Since k does not contain a cube root of unity, kC has the unique (up to isomorphisms) simple module T of dimension 2. It is G-invariant, and since G/C is a 2-group, T can be extended to a simple kG-module S. Moreover, it follows that $T\otimes\overline{k}=T_1\oplus T_2$, where T_1 and T_2 are non-isomorphic simple $\overline{k}C$-modules with $T_1^\sigma=T_2$. However, $S\otimes\overline{k}$ is a simple $\overline{k}G$-module, since $T_1^t=T_2$ and $(S\otimes\overline{k})_C\cong T_1\oplus T_2$.

Let $X=(x-1)\overline{k}D/s\overline{k}D$ and $Y=(y-1)\overline{k}D/s\overline{k}D$, where s is the sum of all the elements in D. Then X and Y are non-projective indecomposable $\overline{k}D$-modules and we have $X^t=Y$ and $Y^t=X$, but X and Y are invariant under the Galois actions. (See Remark 2.3.) It is known that X and Y lie in the same connected component of $\Gamma_s(\overline{k}D)$ which is isomorphic to $\mathbf{Z}A_\infty^\infty$. (See [W] or [E2].) Now $X\otimes_{\overline{k}}T_1$, $Y\otimes_{\overline{k}}T_1$, $X\otimes_{\overline{k}}T_2$ and $Y\otimes_{\overline{k}}T_2$ are non-isomorphic indecomposable $\overline{k}H$-modules, and we have $(X\otimes_{\overline{k}}T_1)^t=Y\otimes_{\overline{k}}T_2$, $(Y\otimes_{\overline{k}}T_1)^t=X\otimes_{\overline{k}}T_2$, $(X\otimes_{\overline{k}}T_1)^\sigma=X\otimes_{\overline{k}}T_2$ and $(Y\otimes_{\overline{k}}T_1)^\sigma=Y\otimes_{\overline{k}}T_2$. Of course, $X\otimes_{\overline{k}}T_1$ and $Y\otimes_{\overline{k}}T_1$ lie in the same AR component Θ_1, and $X\otimes_{\overline{k}}T_2$ and $Y\otimes_{\overline{k}}T_2$ lie in the same AR component Θ_2. Both Θ_1 and Θ_2 are isomorphic to $\mathbf{Z}A_\infty^\infty$. Let $Z_1=(X\otimes_{\overline{k}}T_1)^G=(Y\otimes_{\overline{k}}T_2)^G$ and $Z_2=(X\otimes_{\overline{k}}T_2)^G=(Y\otimes_{\overline{k}}T_1)^G$. Then Z_1 and Z_2 are non-isomorphic indecomposable $\overline{k}G$-modules, and we have $Z_1^\sigma=Z_2$. Moreover, we have $\Theta_1^t=\Theta_2$ and Z_1 and Z_2 lie in the same AR component Γ isomorphic to $\mathbf{Z}A_\infty^\infty$.

Finally, we recall that $\Omega(\overline{k})\otimes_{\overline{k}}T_i$ lies in Θ_i for $i=1,2$. Here $\Omega(\overline{k})$ is the Heller translate of the trivial $\overline{k}D$-module $\overline{k}$, i.e., the kernel of the projective cover of $\overline{k}$. We have $(\Omega(\overline{k})\otimes_{\overline{k}}T_1)^t=\Omega(\overline{k})\otimes_{\overline{k}}T_2$ and $(\Omega(\overline{k})\otimes_{\overline{k}}T_1)^\sigma=\Omega(\overline{k})\otimes_{\overline{k}}T_2$. Therefore $(\Omega(\overline{k})\otimes_{\overline{k}}T_1)^G$ lies in Γ and is σ-invariant. Since $Z_1^\sigma=Z_2$ and since Z_1 and Z_2 lie in Γ, from Lemmas 1.1, 1.2 and 1.3, it follows that the tree class of the AR component containing $\Omega(S)$ must be B_∞.

References

[B] D. Benson, "Modular representation theory, New trends and methods", Lect. Notes Math., vol. 1081, Springer, Berlin, Heidelberg, New York, 1984.

[Be] C. Bessenrodt, The Auslander-Reiten quiver of a modular group algebra revisited, Math. Z., **206** (1991), 25–34.

[BD] V.M. Bondarenko and J.A. Drozd, The representation type of finite groups, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov, **57** (1977), 24–41, English translation : J. Soviet Math., **20** (1982), 2515–2528.

[CB] W.W. Crawley-Boevey, Functional filtrations III, J. London Math. Soc., **40** (1989), 31–39.

[E1] K. Erdmann, On modules with cyclic vertices in the Auslander–Reiten quiver, J. Algebra, **104** (1986), 289–300.

[E2] K. Erdmann, On the vertices of modules in the Auslander–Reiten quiver of p-groups, Math. Z., **203** (1990), 321–334.

[E3] K. Erdmann, "Blocks of tame representation type and related algebras", Lect. Notes Math., vol. 1428, Springer, Berlin Heidelberg New York, 1990.

[E4] K. Erdmann, On Auslander-Reiten components for group algebras, J. Pure and Appl. Algebra, **104** (1995), 149–160.

[ES] K. Erdmann and A. Skowroński, On Auslander–Reiten components of blocks and self–injective biserial algebras, Trans. Amer. Math. Sci., **330** (1992), 165–189.

[F] W. Feit, "The representation theory of finite groups", North Holland, Amsterdam, New York, Oxford, 1982.

[HB] B. Huppert and N. Blackburn, "Finite Groups II", Springer, Berlin Heidelberg New York, 1982.

[K1] S. Kawata, Module correspondences in Auslander-Reiten quivers for finite groups, Osaka J. Math., **26** (1989), 671–678.

[K2] S. Kawata, The modules induced from a normal subgroup and the Auslander-Reiten quiver, Osaka J. Math., **27** (1990), 265–269.

[NT] H. Nagao and Y. Tsushima, "Representations of Finite Groups", Academic Press, New York, 1987.

[O1] T. Okuyama, On the Auslander-Reiten quiver of a finite group, J. Algebra, **110** (1987), 425–430.

[O2] T. Okuyama, The Auslander-Reiten sequences for group algebras and subgroups (in Japanese), Proceeding of the 3rd symposium on representations of algebras (M.Sato Ed.) (1988).

[OU1] T. Okuyama and K. Uno, On vertices of Auslander–Reiten sequences, Bull. London Math. Soc., **22** (1990), 153–158.

[OU2] T. Okuyama and K. Uno, On the vertices of modules in the Auslander-Reiten quiver II, Math. Z., **217** (1994), 121–141.

[U1] K. Uno, Relative projectivity and extendibility of Auslander-Reiten sequences, Osaka J. Math., **25** (1988), 499–518.

[U2] K. Uno, On the vertices of modules in the Auslander–Reiten quiver, Math. Z., **208** (1991), 411–436.

[W] P. Webb, The Auslander–Reiten quiver of a finite group, Math. Z., **179** (1982), 97–121.

Tetsuro Okuyama
Department of Mathematics
Hokkaido University of Education
Asahikawa 070-0825, Japan

Katsuhiro Uno
Department of Mathematics
Osaka University
Toyonaka, Osaka 560-0043, Japan

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 369–378

Representations of finite Chevalley groups

Toshiaki Shoji

§1. Introduction

This note is a brief exposition of the representation theory of finite Chevalley groups. The main problem we are concerned here is the classification of irreducible ordinary representations of such groups, and giving a general algorithm of computing character tables. Lusztig succeeded, in 1980's, in classifying all the irreducible representations of finite reductive groups $G(\mathbf{F}_q)$ and in determining their degrees ([L1]). So the remaining problem is the determination of character values. In order to approach this problem from a general point of view, Lusztig founded the theory of character sheaves ([L2]), and showed that certain class functions arising from character sheaves are computable, and form a basis of the space of class functions of $G(\mathbf{F}_q)$. Under these circumstances he proposed a conjecture connecting such class functions with irreducible characters. Lusztig's conjecture provides us a general algorithm of computing irreducible characters. In the case where the center of $G$ is connected, Lusztig's conjecture was solved by the author, by using the theory of Shintani descent developed by Shintani, Kawanaka and Asai, (see e.g., [K]).

In this note, we review the classification of irreducible characters. We formulate Lusztig's conjecture, and summarize related results in the case where the center is connected. In the case of disconnected center, Lusztig's conjecture is not yet established. We discuss this case, in connection with recent results on Shintani descent, the Mackey formula and generalized Gelfand-Graev representations.

§2. The classification of irreducible representations

Let $G$ be a connected reductive algebraic group defined over $\mathbf{F}_q$, a finite field of $q$ elements with $ch\mathbf{F}_q = p$. We denote by $F : G \to G$

Received May 27, 1999.
Revised May 10, 2000.

the corresponding Frobenius map on G. The finite group $G(\mathbf{F}_q)$ of $\mathbf{F}_q$-rational points in G coincides with the subgroup G^F of fixed points by F in G. Let $\bar{\mathbf{Q}}_l$ be the algebraic closure of the l-adic number field $\mathbf{Q}_l$, for $l \neq p$. Then $\bar{\mathbf{Q}}_l \simeq \mathbf{C}$, and we consider the representations of G^F over $\bar{\mathbf{Q}}_l$ so that the l-adic cohomology theory can be applied. We are interested in the following problem.

Problem. Classify all the irreducible representations of G^F, and give a general algorithm of computing irreducible characters.

The fundamental tool for the classification is the virtual G^F-module $R_T^G(\theta)$ introduced by Deligne and Lusztig in 1976. For a pair (T, θ), where T is an F-stable maximal torus of G and θ is a linear character of T^F, $R_T^G(\theta)$ is constructed as an alternating sum of certain l-adic cohomology groups on which G^F acts naturally. Let G_{uni}^F be the set of unipotent elements in G^F. We define a function $Q_T^G : G_{\text{uni}}^F \to \bar{\mathbf{Q}}_l$ by

$$Q_T^G(u) = \mathrm{Tr}\,(u, R_T^G(\theta)).$$

Q_T^G is called the **Green function** of G^F, which does not depend on the choice of θ. The computation of character values of $R_T^G(\theta)$ is reduced, by a simple character formula, to the determination of Green functions of various reductive subgroups of G. More generally, one can define a virtual G^F-module $R_{L\subset P}^G(\pi)$ for a representation π of L^F, where L is an F-stable Levi subgroup of (not necessarily F-stable) parabolic subgroup P of G. The assignment $\pi \mapsto R_{L\subset P}^G(\pi)$ is extended to the Lusztig induction $R_{L\subset P}^G$ from virtual L^F-modules to virtual G^F-modules.

In what follows, we denote by $\widehat{G}^F$ the set of irreducible characters of G^F. The first step for the classification is the partition of $\widehat{G}^F$ into certain subsets. Let G^* be the dual group of G, i.e., G^* is a connected reductive group over $\mathbf{F}_q$, with Frobenius map F, and its root system is dual to the original one. For each F-stable maximal torus T in G, there corresponds an F-stable maximal torus T^* in G^* which is dual to T, (unique up to G^{*F}-conjugate). Then the set of pairs (T, θ) (up to G^F-conjugate) is in bijection with the set of pairs (T^*, s) for $s \in T^{*F}$ (up to G^{*F}-conjugate). For each F-stable semisimple class $\{s\}$ in G^*, we define a subset of $\widehat{G}^F$ by

$$\mathcal{E}(G^F, \{s\}) = \bigcup_{(T_1, \theta_1)} \{\rho \in \widehat{G}^F \mid \langle \rho, R_{T_1}^G(\theta_1)\rangle_{G^F} \neq 0\},$$

where (T_1, θ_1) runs over all the pairs such that (T_1, θ_1) corresponds to (T_1^*, s_1) with $s_1 \in T_1^{*F} \cap \{s\}$ under the above correspondence. In the case where the center of G is connected, the set $\{s\}^F$ consists of a single G^{*F}-class, and we may choose $s_1 = s$. Moreover in this case, the centralizer $Z_{G^*}(s)$ of s is connected.

Lusztig has proved the following result.

Theorem 2.1 (Lusztig [L1]). *Assume that the center of G is connected. Then*

(i) *$\widehat{G}^F$ is partitioned as $\widehat{G}^F = \coprod_{\{s\}} \mathcal{E}(G^F, \{s\})$, where $\{s\}$ runs over all semisimple classes in G^{*F}.*

(ii) *There exists a natural bijection $\mathcal{E}(G^F, \{s\}) \simeq \mathcal{E}(Z_{G^*}(s)^*, \{1\})$.*

An irreducible character ρ is called a unipotent character if ρ belongs to the set $\mathcal{E}(G^F, \{1\})$, i.e., if $\langle \rho, R_T^G(1)\rangle_{G^F} \neq 0$ for some T. In view of (ii) in the theorem, the classification of $\widehat{G}^F$ is reduced to that of unipotent characters whenever the center of G is connected.

- **The classification of unipotent characters.**

In order to explain the parameterization of unipotent characters due to Lusztig, we prepare some notation. Let T_0 be an F-stable maximal torus contained in an F-stable Borel subgroup B of G. Such a pair (B, T_0) is unique up to G^F-conjugate. Let $W = N_G(T_0)/T_0$ be the Weyl group of G, on which F acts naturally. We assume, for simplicity, that F acts trivially on W, i.e., G^F is of split type (or G^F is a finite Chevalley group). Then the G^F-conjugacy classes of F-stable maximal tori in G are in one to one correspondence with the conjugacy classes in W. We denote by T_w an F-stable maximal torus corresponding to $w \in W$. The torus T_0 coincides with T_w with $w = 1$, and in this case we have $R_{T_0}^G(1) = \operatorname{Ind}_{B^F}^{G^F} 1$. It is known that

$$\operatorname{End}_{G^F}(\operatorname{Ind}_{B^F}^{G^F} 1) \simeq H_q(W) \simeq \bar{\mathbf{Q}}_l[W],$$

where $H_q(W)$ is the Iwahori-Hecke algebra of W with parameter q. Hence $\operatorname{Ind}_{B^F}^{G^F} 1$ is decomposed, as $H_q(W) \times G^F$-module,

$$\operatorname{Ind}_{B^F}^{G^F} 1 \simeq \bigoplus_{E \in W^\wedge} V_E \otimes \rho_E,$$

where V_E is an irreducible character of $H_q(W)$ and ρ_E the corresponding irreducible character of G^F. In particular, we obtain (a part of) unipotent characters $\{\rho_E \mid E \in W^\wedge\}$ parametrized by the set of irreducible characters of W. We now define, for $E \in W^\wedge$,

$$R_E = |W|^{-1} \sum_{w \in W} E(w) R_{T_w}^G(1) \in \mathcal{V}_G.$$

Here $\mathcal{V}_G$ denotes the $\bar{\mathbf{Q}}_l$-space of class functions of G^F endowed with the usual inner product. Now it follows from the orthogonality relations for $R^G_T(\theta)$ that $\{R_E \mid E \in W^\wedge\}$ gives rise to an orthonormal system in $\mathcal{V}_G$.

According to Lusztig, the set $\mathcal{E}(G^F, \{1\})$ is parametrized by a set $X(W)$, which is completely described in terms of the data coming from two sided cells of $H_q(W)$. In particular, the parameterization depends only on the Coxeter diagram of W, and independent of p. He also showed the existence of a certain non-degenerate pairing $\{\ ,\ \} : X(W) \times X(W) \to \bar{\mathbf{Q}}_l$. We express the unipotent character corresponding to $x \in X(W)$ by ρ_x. By the previous argument, there exists an injection $W^\wedge \hookrightarrow X(W)$ via $E \mapsto x_E$ with $\rho_{x_E} = \rho_E$. The following formula gives the decomposition of R_E into irreducible characters of G^F.

$$R_E = \sum_{y \in X(W)} \{y, x_E\}\rho_y.$$

Note that in certain $E \in W^\wedge$ for type E_7 or E_8 (exceptional characters of W), some modification is needed for the above formula. We also note that except the above case, unipotent characters are characterized by the multiplicities for various R_E. This is the leading principle of the parameterization by Lusztig.

Now the above decomposition of R_E suggests to define formally a class function R_x on G^F for any $x \in X(W)$ by

$$R_x = \sum_{y \in X(W)} \{y, x\}\rho_y.$$

Then the orthogonality property holds also for such R_x, and we see that $\{R_x \mid x \in X(W)\}$ gives rise to an orthonormal basis of the subspace of $\mathcal{V}_G$ generated by unipotent characters.

Remark 2.2. (i) More generally, the set $\mathcal{E}(G^F, \{s\})$ is described in a similar way (cf. (ii) of Theorem 2.1), and we get the total parameter set $X(G^F)$ for G^F. Then one can define functions R_x for $x \in X(G^F)$ similar to the previous case. The set $\{R_x \mid x \in X(G^F)\}$ gives rise to an orthonormal basis of $\mathcal{V}_G$, and R_x's are called **almost characters** of G^F.

(ii) In the case where the center of G is disconnected, the classification of $\widehat{G}^F$ is done by reducing it to the case of connected center. However, the construction of almost characters in this case is not so clear.

§3. Character sheaves and Lusztig's conjecture

Character sheaves are certain G-equivariant simple perverse sheaves on G. In general, for an F-stable perverse sheaf K on G, by fixing an isomorphism $\varphi_K : F^*K \xrightarrow{\sim} K$, one can associate to K a characteristic function χ_{K,φ_K}. If K is G-equivariant (with respect to the adjoint action of G), χ_{K,φ_K} turns out to be a class function on G^F. In this way, a lot of useful class functions of G^F are produced from the geometric setting, though they are not virtual characters in general.

Before stating Lusztig's results on character sheaves, we prepare some notation. A prime $p = ch\mathbf{F}_q$ is called almost good for G if p satisfies the following conditions;

$$\begin{cases} p \neq 2, 3 & \text{if } G \text{ has factors of type } E_7, F_4, G_2, \\ p \neq 3 & \text{if } G \text{ has a factor of type } E_6, \\ p \neq 2, 3, 5 & \text{if } G \text{ has a factor of type } E_8, \end{cases}$$

and no conditions for factors of classical type. We denote by $(\widehat{G})^F$ the set of F-stable character sheaves on G. (Do not confuse this with $\widehat{G^F}$.) For each $A \in (\widehat{G})^F$, we choose $\varphi_A : F^*A \xrightarrow{\sim} A$, and consider the characteristic function χ_{A,φ_A} on G^F. Note that since A is simple, φ_A is unique up to scalar multiple.

Theorem 3.1 (Lusztig [L2]). *Assume that p is almost good for G. Then*

(i) *Under a certain choice of φ_A, $\{\chi_{A,\varphi_A} \mid A \in (\widehat{G})^F\}$ gives rise to an orthonormal basis of $\mathcal{V}_G$.*
(ii) *There exists a general algorithm of computing χ_{A,φ_A}.*

Based on his results, Lusztig proposed the following conjecture.

Conjecture 3.2 (Lusztig). *There exists a natural parameterization $X(G^F) \simeq (\widehat{G})^F$, (which we denote by $x \leftrightarrow A_x$, and write as $\varphi_{A_x} = \varphi_x : F^*A_x \xrightarrow{\sim} A_x$), such that*

$$\chi_{A_x,\varphi_x} = c_x R_x \qquad (c_x \in \bar{\mathbf{Q}}_l^*).$$

Lusztig's conjecture asserts that characteristic functions χ_{A,φ_A} coincide with almost characters up to scalar. Since we know the decomposition of almost characters into irreducible characters (especially in the case of connected center), Lusztig's conjecture provides us an algorithm of computing irreducible characters once we know the scalar constants c_x.

The following result gives a partial answer to Lusztig's conjecture.

Theorem 3.3 ([S2]). *Assume that the center of G is connected, and assume that p is almost good. Then Lusztig's conjecture holds for G^F.*

Remark 3.4. Here we give a remark on the computation of χ_{A,φ_A}. In the theory of character sheaves, there is a notion of cuspidal character sheaves, and induction from them. For example, the constant sheaf $\bar{\mathbf{Q}}_l$ gives, up to shift, a cuspidal character sheaf A_0 on a maximal torus T_0, and the induction $K = \text{ind}_B^G A_0$ is a semisimple perverse sheaf on G, whose simple factors are character sheaves A_E parametrized by $E \in W^\wedge$. One can choose an isomorphism $\varphi_w : F^*K \tilde{\to} K$ for each $w \in W^\wedge$, and we have

$$\chi_{K,\varphi_w} = \sum_{E \in W^\wedge} E(w)\chi_{A_E,\varphi_{A_E}}.$$

Thus the computation of χ_{A_E} is reduced to that of χ_{K,φ_w} for various w. Lusztig defined a Green function $\tilde{Q}_{T_w}^G$ associated to the character sheaves, and showed that the computation of χ_{K,φ_w} is reduced to that of Green functions. More generally, arbitrary χ_{A,φ_A} are computed by making use of generalized Green functions. He showed that there is a simple algorithm of computing generalized Green functions.

In [L4], Lusztig proved that $\tilde{Q}_T^G$ coincides with Q_T^G when q is large enough (for any p). This result was extended in [S2] for arbitrary q.

Concerning the Lusztig's conjecture, Lusztig has proved the following result for arbitrary G, under some restrictions on p and q.

Theorem 3.5 (Lusztig [L6]). *Let G be an arbitrary reductive group. Assume that p and q are large enough. Then for each cuspidal character sheaf A_x, the formula in the conjecture holds.*

Note that if the decomposition of the Lusztig induction $R_{L \subset P}^G$ is known, the above result implies the conjecture (for $p \gg 0, q \gg 0$). However such a decomposition is known, at present, only for the case of connected center (see, e.g., [S1]).

Once Lusztig's conjecture is established (for example, in the case of connected center), the next step is the determination of scalars c_x appearing in the conjecture. In this direction, Lusztig has proved the following.

Theorem 3.6 (Lusztig [L3]). *Let $G = SO_{2n+1}$ and assume that p is odd. Then for almost characters R_x which do not vanish on G_{uni}^F, the scalars c_x are determined.*

He also announced that similar results hold for other groups under some restriction on q.

We can determine the scalar c_x in some special cases. In the following, R_x is called a unipotent almost character if it is a linear combination of unipotent characters.

Theorem 3.7 ([S3]). *Assume that G^F is a Chevalley group of classical type with connected center. Assume further that p is odd. Then the scalar c_x is determined for a unipotent almost character R_x.*

This can be generalized to the case of exceptional groups.

Theorem 3.8 (Lübeck, Shinoda). *Assume that G^F is an exceptional group of adjoint type. Assume further that p is good. Then the scalar c_x is determined for a unipotent almost character R_x.*

Remark 3.9. The above results provide an algorithm of computing unipotent characters. In fact, Lübeck "computed" all the character values of unipotent characters for F_4 and E_6 by making use of the computer algebra system **CHEVIE** ([GPH]). His program will work also for E_7 and E_8. However in applying Lusztig's algorithm in practice, still there remains an ambiguity in choosing rational unipotent classes in a given geometric unipotent class. In order to justify Lübeck's computation, we need to determine some parameters related to the choice of representatives.

§4. The case of disconnected center

In the case where the center of G is disconnected, the main problem is the proof of Lusztig's conjecture. For this we need to know the decomposition of the Lusztig induction $R^G_{L\subset P}$. In the case of connected center, this decomposition was achieved by making use of the theory of Shintani descent ([S1]), which is a theory connecting characters of G^F and F-stable characters of G^{F^m} for some power F^m. This theory was also used in verifying Lusztig's conjecture in [S2]. Hence it is expected that it plays an important role also for the case of disconnected center. The typical example for such a group is $G^F = SL_n(\mathbf{F}_q)$, and the Shintani descent for this group was described in [S4].

In the remainder of this section we assume that G is an arbitrary reductive group.

• The Mackey formula

Another approach for getting the information on the Lusztig induction is the following Mackey formula for Lusztig induction which is an analogue of the usual Mackey formula of finite groups. We define a linear map ${}^*R^G_{L\subset P} : \mathcal{V}_G \to \mathcal{V}_L$, called the Lusztig restriction, as the adjoint functor of the Lusztig induction $R^G_{L\subset P}$. Let M be an F-stable Levi subgroup of another parabolic subgroup Q of G. Put

$$\mathcal{E}(L,M)=\{x\in G\mid L\cap {}^xM \text{ contains a maximal torus of } G\}.$$

The Mackey formula is formulated as follows.

$$^*R^G_{L\subset P}\circ R^G_{M\subset Q}=\sum_{x\in L^F\backslash\mathcal{E}(L,M)^F/M^F}R^L_{L\cap^xM\subset L\cap^xQ}\circ {}^*R^{^xM}_{L\cap^xM\subset P\cap^xM}.$$

It is not yet known whether the Mackey formula holds in a full generality. It has been verified in the special case where (a) P and Q are F-stable parabolic subgroups, or (b) L or M is a maximal torus of G. We note here that the Mackey formula implies that the Lusztig induction $R^G_{L\subset P}$ depends only on L and not on P.

Recently C. Bonnafé proved the following result.

Theorem 4.1 (Bonnafé [B1]). *Assume that q is large enough (but no assumption on p). Then the Mackey formula holds for any F-stable Levi subgroups L and M.*

He also showed in [B2] that if G is of type A_n, then the Mackey formula holds without restriction on q.

- **Generalized Gelfand-Graev representations.**

The concept of generalized Gelfand-Graev representations (by abbreviation GGGR) was introduced by Kawanaka, by generalizing the usual Gelfand-Graev representations. In the case of disconnected center, contrast to the case of connected center, Deligne-Lusztig theory does not give enough information for describing irreducible characters, and it is expected that GGGR provide us additional informations. In fact, in the case of $SL_n(\mathbf{F}_q)$, GGGR allows us to parameterize irreducible characters in a more precise way than Lusztig's one. Now to each unipotent element $u\in G^F$, one can associate an F-stable parabolic subgroup P with unipotent radical U_P, together with a certain irreducible representation Λ_u of U^F_P. Then $\varGamma_u=\operatorname{Ind}^{G^F}_{U^F_P}\Lambda_u$ depends only on the G^F-conjugacy class of u, and is called the **generalized Gelfand-Graev representation** of G^F associated to the class of u. Note that if u is a regular unipotent element, then $\varGamma_u$ coincides with the usual Gelfand-Graev representations.

Kawanaka decomposed $\varGamma_u$ into irreducible characters in the case of GL_n for arbitrary p and q, and also treated the exceptional groups of adjoint type (see, e.g., [K]). On the other hand, under the assumption that p and q are large enough, Lusztig described the decomposition of $\varGamma_u$ in terms of various χ_{A,φ_A}. Using this, he showed the following result.

Theorem 4.2 (Lusztig [L5]). *Assume that p and q are large enough. Then for any $\rho \in \widehat{G}^F$, there exists a unique unipotent class C in G such that $\sum_{g \in C^F} \rho(g) \neq 0$, and having maximal dimension among the classes with this property.*

The class C attached to ρ is called the **unipotent support** of ρ. Recently, M. Geck succeeded in removing the assumption on q of Lusztig's result in the case where p is good, and then extended it with G. Malle to the case where p is bad.

Theorem 4.3 (Geck [G], Geck-Malle [GM]). *The statement of Theorem* 4.2 *holds without any restrictions on p and q.*

We close this note by stating the following result, which discusses the Lusztig restriction of Gelfand-Graev characters.

Theorem 4.4 (Digne-Lehrer-Michel [DLM]). *Assume that p is good and that q is large enough. Let Γ_u be the Gelfand-Graev character of G^F associated to a regular unipotent element $u \in G^F$. Let L be an F-stable Levi subgroup of a (not necessarily F-stable) parabolic subgroup P of G. Then there exists a regular unipotent element $v \in L^F$ such that*

$$^*R^G_{L \subset P}(\Gamma_u) = \varepsilon_G \varepsilon_L \Gamma_{L,v},$$

where $\Gamma_{L,v}$ is the Gelfand -Graev character of L^F associated to v, and ε_G (resp. ε_L) is the split rank of G (resp. L).

Note that in the case of disconnected center, the theorem implies that a rational regular unipotent class in G^F determines a rational regular unipotent class in each F-stable Levi subgroup L. However, the explicit correspondence is not yet known.

References

[B1] C. Bonnafé, Formule de Mackey, J. Algebra, **201** (1998), 207–232.

[B2] C. Bonnafé, Mackey formula in type A, preprint.

[DL] P. Deligne and G. Lusztig, Representations of reductive groups over finite fields, Ann. of Math., **103** (1976), 103–161.

[DLM] F. Digne, G. I. Lehrer and J. Michel, On Gelfand-Graev characters of reductive groups with disconnected center, J. reine. angew. Math., **491** (1997), 131–147.

[G] M. Geck, On the average values of the irreducible characters of finite groups of Lie type on geometric unipotent classes, preprint (1996).

[GM] M. Geck and G. Malle, On the existence of a unipotent support for the irreducible characters of a finite group of Lie type, preprint (1996).

[GPH] M. Geck, G. Pfeiffer, G. Hiss, F. Lübeck and G. Malle, CHEVIE—Generic character tables of finite groups of Lie type, Hecke algebras and Weyl groups, preprint Heidelberg, 1993.

[K] N. Kawanaka, Shintani lifting and Gelfand-Graev representations, in "The Arcata conference on Representations of finite groups," Proceedings of Symposia in Pure Math., Vol. **47–1**, pp. 147–163. Amer. Math. Soc. Providence, R.I., 1987.

[L1] G. Lusztig, "Characters of reductive groups over a finite field," Ann. of Math. Stud., Vol. **107**, Princeton Univ. Press, Princeton, 1984.

[L2] G. Lusztig, Character sheaves, I, Adv. in Math., **56** (1985), 193–237, II, Adv. in Math., **57** (1985), 226–265, III, Adv. in Math., **57** (1985), 266–315, IV, Adv. in Math., **59** (1986), 1–63, V, Adv. in Math., **61** (1986), 103–155.

[L3] G. Lusztig, On the character values of finite Chevalley groups at unipotent elements, J. Algebra, **104** (1986), 146–194.

[L4] G. Lusztig, Green functions and character sheaves, Ann. of Math., **131** (1990), 355–408.

[L5] G. Lusztig, Unipotent support for irreducible representations, Adv. in Math., **94** (1992), 139–179.

[L6] G. Lusztig, Remarks on computing irreducible characters, J. Amer. Math. Soc., **5** (1992), 971–986.

[S1] T. Shoji, Shintani descent for exceptional groups over a finite field, J. Fac. Sci. Univ. Tokyo Sect., IA **34** (1987), 599–653.

[S2] T. Shoji, Character sheaves and almost characters of reductive groups, Adv. in Math., **111** (1995), 244–313, II, Adv. in Math., **111** (1995), 314–354.

[S3] T. Shoji, Unipotent characters of finite classical groups, in " Finite reductive groups: related structures and representations." Proceedings of an international conference held in Luminy, Progress in Math., Vol. **141** (1997), 373–413.

[S4] T. Shoji, Shintani descent for special linear groups, J. Algebra, **199** (1998), 175–228.

Department of Mathematics
Science University of Tokyo
Noda, Chiba 278-8510
Japan

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 379–390

The Shape of the Classification of the Finite Simple Groups

Ronald Solomon

This is a general survey of the Classification of the Finite Simple Groups with particular emphasis on the current project of Gorenstein, Lyons and Solomon (GLS) directed towards the revision of a substantial segment of the Classification proof.

There are two principal strategies at present directed towards a Classification proof. The one employed in the first successful proof and also, with certain modifications, in the GLS proof, I shall refer to as the Semisimple Approach to the Classification. The other, which has been the object of considerable activity recently, I shall refer to as the Unipotent Approach to the Classification. Each has its advantages and its drawbacks and neither is, at present, completely independent of the other. In unison they provide a complete proof of the Classification Theorem. A question at present is the natural domain for each of these methods. Of course the future may bring entirely new and wonderful approaches to the subject.

The modern history of the Classification began around 1950 when several mathematicians – notably Brauer, Suzuki and Wall – began to investigate simple groups of even order satisfying certain local conditions. This work eventually congealed into the Brauer-Suzuki-Wall Theorem [BSW] characterizing the two-dimensional projective special linear groups over finite fields. Brauer in particular championed the strategy of characterizing finite simple groups of even order by the centralizer of an involution. Suzuki, on the other hand, established the nonexistence of finite simple $CA$-groups of odd order [S1]. (A group $G$ is a $CA$-group if the centralizer of every nonidentity element of $G$ is abelian.) This result was the inspiration for the Feit-Thompson Theorem proving the nonexistence of nonabelian finite simple groups of odd order.

Meanwhile Suzuki pursued the classification of transitive permutation groups of odd degree in which the stabilizer of a point has a regular

Received May 27, 1999.
Revised June 16, 2000.

normal subgroup and a cyclic complement of odd order [S2]. This formed the foundation for the later classification by Bender of finite groups G with a strongly 2-embedded subgroup M. (M is a strongly p-embedded subgroup of G if M is a proper subgroup of G of order divisible by p such that $M \cap M^g$ has order prime to p for all $g \in G - M$.)

We remark that the Odd Order Theorem [FT] of Feit and Thompson can be regarded as a strong embedding result as well. Indeed the Feit-Thompson Theorem together with the Suzuki-Bender Theorem [B2] establish the following result.

Theorem. *Let G be a finite simple group and let p be the smallest prime divisor of $|G|$. If G has a strongly p-embedded subgroup, then $p = 2$ and G is isomorphic to $SL(2, 2^n)$, $Sz(2^{2n-1})$ or $PSU(3, 2^n)$ for some $n \geq 2$.*

Clearly this is a corollary of the Feit-Thompson and Suzuki-Bender Theorems. As remarked in [So], the Feit-Thompson Theorem is an easy consequence of the above theorem, although this observation does not seem to afford a route to a new proof of the Feit-Thompson Theorem.

The Feit-Thompson and Suzuki-Bender Theorems form the two principal Background Results underlying the GLS proof of the Classification Theorem. (Also in the background is the theory of linear algebraic groups, the determination of the Schur multipliers of the finite simple groups, and the existence, uniqueness and local structure of the sporadic simple groups. And in the "foreground", i.e. essential to the complete proof but not included in the GLS series, is the forthcoming proof of the Quasithin Theorem by Aschbacher and Smith.)

Chapter I. Semisimple Approach

When Brauer did specific characterizations of finite simple groups by the centralizer of an involution, the groups were almost always classical groups defined over fields of odd characteristic. (Of course M_{11} also arose, having an isomorphic involution centralizer to $PSL(3, 3)$.) This focus continued in the work of Brauer's students, Fong, Wong and Harris, who (along with Phan) systematically pursued the characterization of the finite simple groups of Lie type over fields of odd characteristic via the centralizer of an involution during the 1960's.

Of course, when the characteristic is odd, an involution is a semisimple (indeed split semisimple) element of the Lie type group G. Thus it is reasonable to expect (and indeed is true) that the characterization theorems established in particular by Wong and Phan can be generalized to characterizations of finite simple groups of Lie type in any characteristic via the centralizer of a semisimple element of prime order, or more precisely via the centralizer of a suitable element x of prime order contained either in the split maximal torus of G or in a "half-split" maximal torus, i.e. a torus which splits in a quadratic extension of the field of definition of G. Such a characterization over fields of characteristic 2 was accomplished by Gilman and Griess in [GG].

In order to convert this fact into a strategy for the classification, it is useful first to give a definition of a semisimple element for an abstract group, not simply for a group with a preferred linear representation. As our attention will focus on centralizers of such elements, it is natural that the definition should reflect a fundamental property of their centralizers. In the context of a semisimple linear algebraic group G, it is well-known that the centralizer C of a semisimple element is a reductive group, i.e. the product of a semisimple group and a torus (which is central in C if G is simply connected). Extending the work of Fitting, Bender in 1970 [B1] defined the appropriate subgroups of a finite group needed to formulate the analogous structural hypotheses. We recall some definitions.

Definition. A finite group K is *quasisimple* if $K = [K, K]$ and $K/Z(K)$ is a nonabelian simple group. A finite group E is *semisimple* if E is the commuting product of certain quasisimple subgroups, called its *components.*

Definition. Let H be a finite group. The join of all normal nilpotent subgroups of H is called the *Fitting subgroup* of H, $F(H)$. It is the unique maximal normal nilpotent subgroup of H. Similarly the join of all normal semisimple subgroups of H is denoted $E(H)$. It is the unique maximal normal semisimple subgroup of H. Moreover $E(H)$ and $F(H)$ commute with each other. Their commuting product is called the *generalized Fitting subgroup* of H, $F^*(H)$.

We can now identify a characteristic property of the centralizers of many semisimple elements in linear groups and make this a definition in an arbitrary finite group.

Definition. Let G be a finite group. We call an element x of G *semisimple* if $E(C_G(x)) \neq 1$.

We remark that if G is a classical linear group, then for every unipotent element y of G, $E(C_G(y)) = 1$, as a corollary of the Borel-Tits Theorem. On the other hand typically many of the semisimple (in the linear group sense) elements of G will also be semisimple in the above sense. However not all will be because for certain linear semisimple elements x, $C_G(x)$ will be a torus. In an extreme case like $SL(2,q)$, no noncentral linear semisimple element will be semisimple in the sense of the above definition. This reflects a fundamental limitation on the semisimple approach: it does not work for "very small"simple groups. (A good replacement for the term "very small"is quasithin, as we shall see below.)

The first goal of the semisimple approach to the Classification is to search for a semisimple element x such that $E(C_G(x))$ has a component K of maximum possible order. This corresponds in the context of linear groups to the search for a semisimple element with an eigenspace of maximum possible dimension. When chosen judiciously this component K will be a slightly smaller version of the target group G. Moreover by making a similar choice of a semisimple element y inside $K - Z(K)$, one can find a second large component, L, of $E(C_G(y))$ such that K and L generate G. Indeed it is possible not only to find generators for G but also to infer sufficient relations to characterize G via theorems of Coxeter, Steinberg or Curtis and Tits. This strategy was implemented for semisimple involutions by Aschbacher in his Classical Involution Paper [A2] and for semisimple elements of odd prime order by Gilman and Griess [GG].

However there is an important reason to modify this strategy slightly. It is extremely important to control the embedding of such subgroups as $C_K(y)$ in $C_G(y)$. More specifically it is desirable to know that

$$E(C_K(y)) \leq E(C_G(y)).$$

It is not however possible to achieve an a priori proof of this fact because of the following type of example:

Let $H = SL(V)$ with V a 6-dimensional vector space over the finite field F of odd order q. Let $G = VH$ be the semidirect product with the natural action of H on V. Let x be an involution in H with a 4-dimensional -1-eigenspace. Then $E(C_G(x)) = K \cong SL(4,q)$. Next let y be an involution in K with a 2-dimensional 1-eigenspace on V, contained in the -1-eigenspace for x. Then $E(C_K(y)) = L_1 * L_2$ with $L_i \cong SL_2(q)$ acting on the $(-1)^i$-eigenspace for y on V. We can easily compute that $L_1 \leq E(C_G(y))$ but $L_2 \not\leq E(C_G(y))$.

Of course in the example G is far from being a finite simple group. However it is precisely the problem of detecting from *local* information that such a G is not simple which constitutes one of the major chapters of the Classification proof. (A *local subgroup* of a group G is the normalizer of a non-identity p-subgroup of G. Local information is information about the structure of the local subgroups of G.)

Gorenstein and Walter [GW] discovered an important "gravitational principle", called *L-Balance* concerning a subgroup closely related to $E(H)$.

Definition. Let p be a prime and H a p-local subgroup of G. The *p-layer* of H, $L_{p'}(H)$ is the smallest normal subgroup of H covering $E(H/O_{p'}(H))$, where $O_{p'}(H)$ denotes the largest normal subgroup of H of order relatively prime to p.

The L-Balance Theorem. *Let G be a finite group all of whose proper simple sections satisfy the (weak) Schreier Conjecture. Let p be a prime and let x and y be commuting elements of G of order p. Let L_x and L_y denote the p-layers of $C_G(x)$ and $C_G(y)$ respectively. Then*

$$L_{p'}(C_{L_x}(y)) \leq L_y.$$

In the vernacular, the L-Balance Theorem asserts that the p-layer of a p-local subgroup of G always sinks into the p-layer of G. Hence it is a kind of gravitational (or non-buoyancy) principle. The proof of the L-Balance Theorem depends on a weak version of the following old conjecture.

Schreier's Conjecture. *Let S be a finite simple group. Then $Aut(S)/S$ is a solvable group.*

Schreier's Conjecture is a fairly easy corollary of the Classification Theorem. No independent proof is known. I shall not bother to state the weak version of the Schreier Conjecture here but I note that it was proved when $p = 2$ by Glauberman as a corollary of his Z^*-Theorem [Gl]. Thus for $p = 2$ the hypothesis on proper simple sections of G may be omitted. In the context of an inductive proof of the Classification Theorem, proper simple sections always satisfy the Schreier Conjecture and so the L-Balance Theorem may be used for all primes p.

Notice that the L-Balance Theorem provides a correct analogue of the wished-for property of Bender's subgroup $E(H)$. Inspired by this, we reformulate our semisimple strategy in the following language:

Definition. Let G be a finite group and p a prime. A p-element x of G is said to be *weakly semisimple* if $L_{p'}(C_G(x)) \neq 1$.

Of course every semisimple element of prime power order is weakly semisimple. The converse statement is false in general as is easily seen, for instance, by modifying the example above slightly. Take $G^* = VH^*$ where $H^* = SL^{\pm}(V)$, the group of linear transformations of determinant

± 1. Then an involution t with a 1-dimensional -1-eigenspace is weakly semisimple but not semisimple. However the converse statement is true (and deep) for finite simple groups. For the prime $p = 2$ it was first formulated by Thompson, who called it the B-Conjecture. Its proof for $p = 2$ forms a major chapter in the proof of the Classification Theorem and weak analogues of it for all primes p also play a pivotal role in the work of Gorenstein and Lyons [GL] on the classification of simple groups of characteristic 2-type (roughly speaking, groups in which no involution is semisimple). As a corollary of the Classification Theorem, we obtain the full B-Theorem.

B-Theorem. *Let G be a finite simple group. For all primes p, every weakly semisimple p-element of G is semisimple.*

We can now formulate a somewhat over-simplified version of the Semisimple Strategy for the Classification of Finite Simple Groups based on the Feit-Thompson and Suzuki-Bender Theorems.

Step 1. *Find a prime p for which G has a weakly semisimple of prime order p. Choose $p = 2$, if possible.*

Step 2. *Establish the B_p-Theorem for G, i.e. that every weakly semisimple p-element of G is semisimple.*

Step 3. *Among all semisimple p-elements of G choose one, x, with some component K of $E(C_G(x))$ as large as possible.*

Now the Component Theorem comes into play. This theorem was established first by Aschbacher [A1], extending an earlier result of Powell and Thwaites [PT]. It was reproved shortly thereafter by Gilman [Gi]. For a minimal counterexample to the Classification Theorem, analogues were established for all primes p by GLS [GLS2].

Component Theorem. *Let G be a finite simple group and x a semisimple element of G of prime order p chosen with some component K of $E(C_G(x))$ as large as possible. Suppose that the p-rank of K is greater than 1. Then K does not commute with any G-conjugate of K. Moreover a Sylow p-subgroup of $C_G(K)$ is either cyclic or of maximal class (with $p = 2$ in the latter case).*

A typical example to imagine is $G = SL(V)$ and x a diagonal element with one eigenspace W of codimension 1 or 2. Then $SL(W)$ will be the unique large component of $E(C_G(x))$ and its centralizer will have cyclic Sylow p-subgroups for odd p and a cyclic or quaternion Sylow 2-subgroup. A slightly different example arises when $G = A_n$ and x is a product of two transpositions. Then the Sylow 2-subgroup of the centralizer of the large component (isomorphic to A_{n-4}) is a Klein 4-group.

The point is that the Component Theorem assures us that the centralizer of x is almost precisely determined, the possibilities for K being afforded by the induction hypothesis. This permits us to proceed to the final step.

Step 4. *Identify G, given the approximate structure of $C_G(x)$, via the methodology developed by Brauer, Fong, Wong, Phan and Harris.*

This constitutes the Semisimple Strategy for the Classification of Finite Simple Groups, modulo one serious problem and one difficult theorem which I have swept under the rug. The difficult theorem is the Strongly p-Embedded Theorem, the analogue for odd primes of the Suzuki-Bender Theorem.

Strongly p-Embedded Theorem. *Let G be a finite simple group and p a prime such that G has p-rank at least* 3. *If M is a strongly p-embedded subgroup of G, then G is a finite simple group of Lie type of Lie rank* 1 *and M is a Borel subgroup of G.*

For odd primes p, this theorem is proved only as a corollary of the Classification Theorem. However a weak version of this theorem is required for the Classification proof, in particular for the proof of the B-Theorem. A sufficient theorem was established by Aschbacher [A3] and a slightly more general variant has been established recently by Stroth. Both proofs are quite long and difficult, and even the statements of the theorems established are long and obscure.

Let's move on from the difficult theorem to the serious problem:

What if G does not contain any weakly semisimple elements of prime order?

The answer to this question is: G is quasithin.

Definition. Let G be a finite simple group. We say that G is *quasithin* if either G has 2-rank at most 2 or every 2-local subgroup of G has p-rank at most 2 for every odd prime p.

In the usual definition of quasithin, G is assumed to be of characteristic 2-type (or even type) and to have 2-rank at least 3. We use the extended definition here for expository purposes.

Klinger-Mason Theorem. *Let G be a finite simple group with no weakly semisimple elements. Then G is quasithin.*

The proof relies on an easier version of some of the signalizer functor analysis used in the proof the the B-Theorem. The principal new ingredient is a lovely and elementary argument of John Thompson in [T2], which was later elaborated slightly in [KM] and has henceforth been known as the Klinger-Mason Method. Thompson's argument establishes easily under the given hypotheses that either G is quasithin or G contains an involution x such that $F^*(C_G(x))$ is a 2-group of symplectic type (indeed extraspecial) and $C_G(x)$ has p-rank at most 2 for all primes greater than 3. Indeed with the extra help of the Thompson-Bender Signalizer Lemma, it is possible to rule out the extraspecial case as well. (See [GLS1; 23.3; §24].)

The occurrence of extraspecial 2-groups in the Klinger-Mason argument reflects the proximity of many of the larger sporadic simple groups such as the sporadic Suzuki group, the Conway groups, the Fischer groups, the Harada group, the Thompson group, the Baby Monster and the Monster, as well as certain small classical linear groups. Although these groups do not satisfy the hypotheses of the Klinger-Mason Theorem, they are quite close. Indeed with slightly weakened hypotheses, Gorenstein and Lyons proved an analogous result whose conclusion is roughly that either G is quasithin or G is one of the large sporadic groups mentioned above or a small classical linear group. The full classification of simple groups containing an involution x such that $F^*(C_G(x))$ is a 2-group of symplectic type was accomplished in the mid 1970's largely through the efforts of Timmesfeld [Ti] and was rightly recognized by many as bringing down the final curtain on the search for sporadic simple groups.

I find the resulting Trichotomy Theorem, implicit in the work of Gorenstein and Lyons, to be one of the more elegant justifications for the Semisimple Approach to the Classification.

Trichotomy Theorem. *Let G be a finite simple group. Then one of the following holds:*

(1) *There is a prime p such that G has p-rank at least* 3 *and G contains generic weakly semisimple elements of order p; or*

(2) *G is quasithin; or*

(3) *G is on a (short) finite list including* A_{12}*, eleven sporadic simple groups and several small classical groups defined over* $\mathbf{F}_2$ *or* $\mathbf{F}_3$.

In the statement above, the term generic reflects a restriction on the allowable components in the centralizers of the semisimple elements of order p. In particular the centralizer of a generic semisimple element of order p must have a component which is not a group of Lie type in characteristic p. For $p = 2$ or 3, most sporadic components are likewise not allowed.

Chapter II. Unipotent Approach

The Semisimple Approach to the Classification runs aground on the rocks of the Quasithin Problem. The Classification proof is rescued at this juncture by the Unipotent Approach, which evolved from the methods developed by Thompson in his classification of simple groups all of whose local subgroups are solvable [T1]. (Clearly such a group has no non-identity weakly semisimple element.) In brief the Unipotent Approach, instead of studying semisimple elements, seeks to identify the *characteristic* of the finite simple group G by finding a prime p for which G has a rich supply of p-local subgroups of "parabolic type".

Definition. Let G be a finite group and p a prime. We say that a p-local subgroup H of G is of *parabolic type* if H contains a Sylow p-subgroup of G and $F^*(H)$ is a p-group.

Definition. Let G be a finite group and p a prime. We say that G is of *characteristic p-type* if every p-local overgroup of a Sylow p-subgroup of G is of parabolic type. G is of connected characteristic p-type if G is of characteristic p-type and G is generated by the overgroups of a fixed Sylow p-subgroup P of G.

When G has no semisimple involutions one is close to knowing that G is of connected characteristic 2-type. The final ingredient is provided by "pushing-up theorems"established in the mid 1970's by Baumann, Glauberman, Niles, Aschbacher and others, which establish that either G is of connected characteristic 2-type or G has a strongly 2-embedded subgroup.

Once G is known to be of connected characteristic p-type, the Unipotent Strategy in brief is to study, in the spirit of Tits, the coset geometry determined by the p-local subgroups of parabolic type and to recognize this geometry as that of a split BN-pair of rank at least 2. (Of course there are exceptions arising from the sporadic simple groups of characteristic p-type.) As noted above, many of the ideas for this approach originate in Thompson's N-group paper, whose main theorem may be paraphrased as:

N-Group Theorem. *Let G be a non-abelian simple group all of whose local subgroups are solvable. Assume that G has 2-rank at least 3 and G does not have a strongly 2-embedded subgroup. Then $G \cong {}^2F_4(2)'$, i.e. G is the Tits group.*

The idea of identifying simple groups of characteristic 2-type as split BN-pairs was initiated in the late 1960's by Suzuki [S3] and his students. This approach was temporarily sidetracked by the Gorenstein Program for the Classification announced in the early 1970's, which featured the Semisimple Approach. It was however pursued in the context of quasithin groups and uniqueness groups by Aschbacher, Gomi [Gm] and others. Later Goldschmidt developed a variant Amalgam Method [Go] aimed at a new proof of the N-Group Theorem, which was eventually obtained by Stellmacher.

In the Semisimple Approach to the Classification, the Unipotent Method is required to treat the Quasithin Problem and the Strongly p-Embedded 2-Local Problem. The latter appears in published work of Aschbacher and the former is currently being completed by Aschbacher and Smith. There is however a program underway, spearheaded by Meierfrankenfeld, Stellmacher and Stroth, to apply the Unipotent Method to all groups of connected characteristic p-type (possibly using a slightly different definition than the one given above).

As a strategy aimed at a complete proof of the Classification Theorem, the Unipotent Strategy collides with obstacles at two ends. One obstacle is the Strongly p-Embedded Subgroup Problem. At present the Unipotent Strategy presupposes that G is generated by the p-local subgroups containing a fixed Sylow p-subgroup P. Except when $p = 2$, there is no known approach to the case when P is contained in a unique maximal subgroup M of G. In particular this problem includes (and can probably be reduced to) the case when M is a strongly p-embedded subgroup of G. This is of course similar to the Strongly p-Embedded 2-Local Problem confronted by the Semisimple Approach and solved in that context by Aschbacher and later by Stroth using unipotent methodology. Conceivably a Unipotent Proof of the Classification could be structured in such a way that a solution of a similar nature would be possible.

A hybrid strategy which assigns to the Unipotent Approach precisely the task of classifying finite simple groups of characteristic 2-type would rely only on the Strongly Embedded Theorem of Suzuki-Bender. From my perspective this hybrid strategy is attractive inasmuch as it bypasses the morass of complicated definitions and difficult theorems related to groups with a strongly (or almost strongly) p-embedded 2-local subgroup. Of course a revolutionary new classification of groups with a strongly p-embedded subgroup would change the landscape for both the Semisimple and Unipotent Strategies, ironically improving the cases for each of them.

It is impossible to conjecture a flowchart for a Unipotent Approach to the entire Classification Theorem without an answer to the following question:

What if the simple group G is not of characteristic p-type for any prime p?

In this case of course G would be full of semisimple elements and the Semisimple Approach would be effective. The problem is that we are missing an analogue of the Klinger-Mason Reduction which would tell us that the residual semisimple problem was "bounded"in some good sense. For example one would like a comparatively short proof of a theorem of the following type.

Theorem. *Let G be a finite simple group of 2-rank at least 3 which is not of characteristic p-type for any prime p. Then for some involution t of G, there is a component K of $E(C_G(t))$ such that $K/Z(K)$ is an alternating group.*

Indeed the only simple groups with no characteristic are alternating groups and J_1. If one could give a proof of this fact of comparable length and elegance to the Klinger-Mason argument which rounds off the Semisimple Analysis, then there would be a strong argument for preferring the Unipotent Approach to the Classification proof. Even without it, there is great value in pursuing the Unipotent Analysis to its logical conclusions. If successful, it will bring to satisfying completion Michio Suzuki's program for the classification of finite simple groups of characteristic 2-type via the unipotent methods he helped to pioneer.

References

[A1] M. Aschbacher, On finite groups of component type, Illinois J. Math., **19** (1975), 78–115.

[A2] M. Aschbacher, A characterization of Chevalley groups over fields of odd order, Ann. of Math., **106** (1977), 353–468.

[A3] M. Aschbacher, The uniqueness case for finite groups, Ann. of Math., **117** (1983), 383–551.

[B1] H. Bender, On groups with Abelian Sylow 2-subgroups, Math. Z., **117** (1970), 164–176.

[B2] H. Bender, Transitive Gruppen gerader Ordnung, in dene jede Involution genau einen Punkt festlasst, J. Algebra, **17** (1971), 527–554.

[BSW] R. Brauer, M. Suzuki and G.E. Wall, A characterization of the one-dimensional unimodular groups over finite fields, Illinois Jour. Math., **2** (1958), 718–745.

[FT] W. Feit and J.G. Thompson, Solvability of groups of odd order, Pacific J. Math., **13** (1963), 775–1029.

[Gi] R. Gilman, Components of finite groups, Comm. Alg., **4** (1976), 1133–1198.

[GG] R. Gilman and R.L. Griess, Finite groups with standard components of Lie type over fields of characteristic two, J. Algebra, **80** (1983), 383–516.

[Gl] G. Glauberman, Central elements in core-free groups, J. Algebra, **4** (1966), 403–420.

[Go] D. Goldschmidt, Automorphisms of trivalent graphs, Ann. of Math., **111** (1980), 377–406.

[Gm] K. Gomi, On the 2-local structure of groups of characteristic 2 type, J. Algebra, **108** (1987), 492–502.

[GL] D. Gorenstein and R. Lyons, The local structure of finite groups of characteristic 2 type, Memoirs Amer. Math. Soc., **276** (1983).

[GLS1] D. Gorenstein, R. Lyons and R. Solomon, The Classification of the Finite Simple Groups, Amer. Math. Soc. Surveys and Monographs, **40, # 2** (1996).

[GLS2] D. Gorenstein, R. Lyons and R. Solomon, The Classification of the Finite Simple Groups, Number 4, Amer. Math. Soc. Surveys and Monographs, **40, # 4** (1999).

[GW] D. Gorenstein and J.H. Walter, Balance and generation in finite groups, J. Algebra, **33** (1975), 224–287.

[KM] K. Klinger and G. Mason, Centralizers of p-subgroups in groups of characteristic 2, p type, J. Algebra, **37** (1975), 362–375.

[PT] M. Powell and G. Thwaites, On the nonexistence of certain types of subgroups in simple groups, Quart. J. Math. Oxford Series(2), **26** (1975), 243–256.

[So] R. Solomon, An odd order remark, J. Algebra, **131** (1990), 626–630.

[S1] M. Suzuki, The nonexistence of a certain type of simple group of odd order, Proc. Amer. Math. Soc., **8** (1957), 686–695.

[S2] M. Suzuki, On a class of doubly transitive groups II, Ann. of Math., **79** (1964), 514–589.

[S3] M. Suzuki, Characterization of linear groups, Bull. Amer. Math. Soc., **75** (1969), 1043–1091.

[T1] J.G. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable I, Bull. Amer. Math. Soc., **74** (1968), 383–437.

[T2] J.G. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable II, Pacific J. Math., **33** (1970), 451–536.

[Ti] F.G. Timmesfeld, Finite simple groups in which the generalized Fitting group of the centralizer of some involution is extra-special, Ann. of Math., **107** (1978), 297–369.

Department of Mathematics
The Ohio State University
Columbus, OH 43210
U.S.A.

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 391–400

2F-modules with quadratic offender for the finite simple groups

Gernot Stroth

Abstract.

There is a long running project due to U. Meierfrankenfeld and the author to investigate the so called small modules for the finite simple groups. These modules show up in the amalgam method which recently became important for the revision of parts of the classification of the finite simple groups. A small module either is a quadratic module or a module on which an elementary abelian group acts such that the codimension of the centralizer is small compared with its order. In this paper we determine all irreducible modules $V$ over $GF(2)$ for the finite simple groups $G$ such that $|V : C_V(A)| \leq |A|^2$ for some nontrivial elementary abelian subgroup $A$ of $G$ where in addition we have $[V, A, A] = 1$.

In this paper we are going to determine the irreducible faithful $2F$-modules for the finite quasisimple groups. Here we just concern about $2F$-modules over $GF(2)$. A module $V$ is called $2F$-module for $G$, if there is a nontrivial elementary abelian subgroup $A$ in $G$ such that $|V/C_V(A)| \leq |A|^2$. The group $A$ then will be called an offending subgroup or an offender. The offender is called quadratic if $[V, A, A] = 1$. More precisely we prove

Theorem *Let $G$ be a quasisimple group and $V$ be an irreducible faithful $2F$-module in characteristic two for $G$ with a quadratic offender. Then one of the following holds*

(i) *$G/Z(G) \cong A_n$ and one of the following is true*
  (a) *$V$ is the natural module*
  (b) *$n \leq 8$ and $|V| = 16$*
  (c) *$n = 6$, $|Z(G)| = 3$ and $|V| = 64$*
  (d) *$n = 9$ and $|V| = 2^8$ is the spin module.*

(ii) *$G \cong 3M_{22}$ or $3U_4(3)$ and $V$ is the 12-dimensional $SU_6(2)$-module.*

Received June 19, 1999.
Revised January 26, 2001.

(iii) *$G/Z(G) = G(q)$ is a group of Lie type , $q = 2^t$, and one of the following is true*

(a) *$G(q) \cong L_n(q)$, $Sp(2n,q)'$, $\Omega^{\pm}(2n,q)$ or $U_n(q)$ and V is the natural or dual module.*

(b) *$G(q) \cong L_n(q)$ and V is the exterior square of the natural or dual module*

(c) *$G(q) \cong L_6(q)$, or $U_6(q)$ and V is the exterior cube of the natural module.*

(d) *$G(q) \cong Sp(6,q)$, $Sp(8,q)$ or $Sp(10,q)$ and V is the spin module*

(e) *$G(q) \cong \Omega^{\pm}(8,q)$, $\Omega^{\pm}(10,q)$ or $\Omega^{+}(12,q)$ and V is the half spin module*

(f) *$G(q) \cong E_6(q)$ and $V = V(\lambda_1)$ or $V(\lambda_6)$.*

(g) *$G(q) \cong E_7(q)$ and $V = V(\lambda_7)$.*

(h) *$G(q) \cong F_4(q)$ and $V = V(\lambda_1)$ or $V(\lambda_4)$.*

(i) *$G(q) \cong G_2(q)'$ and V is the natural module.*

(j) *$G(q) \cong Sz(q)$ and V is the natural module.*

The proof of the theorem will depend on two main results. First of all we will use the classification of F–modules. This can be found in an unpublished paper [MeiStr3] due to U. Meierfrankenfeld and the author. A preprint can be found on the homepage (http://coxeter.mathematik.uni-halle.de:8080/~stroth/rep_html). But there is also a classification in the literature. The F-modules for the sporadic groups, alternating groups and groups of Lie type in odd characteristic have been classified by M. Aschbacher [Asch]. The F-modules for the groups of Lie type in characteristic two have been classified by B. Cooperstein [Coop] and in an unpublished paper by B. Cooperstein and G. Mason [CM].

We further will use the classification of quadratic modules in [MeiStr1], [MeiStr2] and [Str] to end up with a very short list of modules and so it is easy to detect the $2F$-modules.

In fact there are still some open question. The module $V(\lambda_1)$ for $E_6(q)$ is a $2F$–module. But we do not know whether it allows a quadratic offender. If not then the cases (iii)(f) - (h) will not show up. Further the paper just considers irreducible modules. So for general module one has to have an overview over the possible offenders, one has to study extensions of the modules above and/or of irreducible $2F$–modules by trivial modules. This all has not been done so far but would be very useful for applications.

The main reason for the classification of these modules comes from the application in the so called amalgam method. This method basically provides us with $2F$–modules with quadratic offender for the groups involved, provided the parameter b is not 1. So we will use the results in this paper in the revision of the classification of the finite simple groups of characteristic two type.

The notations will be standard. Concerning the representations of the groups of Lie type we follow [Stei] and will use these results freely. In what follows G will always be a quasisimple group. A Chevalley group or a group of Lie type will always mean a central factor of the corresponding universal Chevalley group.

By the restriction given by the editors that we do not have more than 10 pages for the paper we had to drop all proofs. The interested reader may download a version containing proofs from the authors homepage.

§1. Preliminaries

For convenience of the reader we first state the main result of [MeiStr3].

Theorem 1.1. *Let $E(G) = F^*(G)$ be a quasisimple group and V be an irreducible faithful F-module in characteristic two for G. Then one of the following holds*

(i) *$E(G)/Z(E(G)) \cong A_n$ and one of the following is true*
   (α) *V is the natural module*
   (β) *$n \leq 8$ and $|V| = 16$*
   (γ) *$n = 6$, $|Z(E(G))| = 3$ and $|V| = 64$*

(ii) *$E(G)/Z(E(G)) = G(q)$ is a group of Lie type , $q = 2^t$, and one of the following is true*
   (α) *$G(q) \cong L_n(q)$, $Sp(2n,q)$, $\Omega^{\pm}(2n,q)$ or $U_n(q)$ and V is the natural or dual module.*
   (β) *$G(q) \cong L_n(q)$ and V is the exterior square of the natural or dual module*
   (γ) *$G(q) \cong Sp(6,q)$ and V is the spin module*
   (δ) *$G(q) \cong \Omega^+(8,q)$ or $\Omega^+(10,q)$ and V is the half spin module*
   (ϵ) *$G(q) \cong G_2(q)$ and V is the natural module.*

Lemma 1.2. *Let $q = 2^n$, G be quasisimple with $G/Z(G) = L_2(q)$ and V be a faithful module in characteristic two. Then for any involution $a \in G$ we have $|V : C_V(a)| \geq q$. If $G/Z(G) = Sz(q)$ or $U_3(q)$, then for any involution a we get $|V : C_V(a)| \geq q^2$.*

Lemma 1.3. *Let $q = 2^n$, G be quasisimple with $G/Z(G) = Sz(q)$ or $U_3(q)$ and V be an irreducible faithful $2F$-module for G with quadratic offender A. Then V is the natural module.*

The next five lemmas are more or less well known results on the representations of groups of Lie type. We will use them freely in the sequel.

Proposition 1.4. *Let $G = G(q)$ be a group of Lie type and V be an irreducible module over $GF(q)$. Then*

$$V = V_1^{\sigma_1} \otimes \cdots \otimes V_l^{\sigma_l}$$

where the V_i are basic irreducible $GF(q)G$–modules and the σ_i are field-automorphisms. Further distinct l–tuples $(V_1, \dots V_l)$, $(V_1', \dots, V_l')$ give nonisomorphic $GF(q)G$–modules.

Proof. [Stei, Th 41 and 43] Q.E.D.

Lemma 1.5. *Let $G = G(q)$ be a Chevalley group then $GF(q)$ is a splitting field for any irreducible module.*

Proof. [Stei, (7.5)] Q.E.D.

Lemma 1.6. *Let $G/Z(G) = G(q)$ be a Chevalley group and V an absolutely irreducible KG–module for some $K \subseteq \widetilde{GF(q)}$, where $\widetilde{GF(q)}$ is the algebraic closure of $GF(q)$. Let $\{\sigma_1, \dots \sigma_r\} = Gal_{GF(p)}(K)$. Let $GF(p)(\chi)$ be the field of definition, or splitting field for V. Then $K = GF(p)(\chi)$ iff V^{σ_1}, ... , V^{σ_r} are pairwise nonisomorphic KG–modules.*

We like to consider representations of twisted Chevalley groups as well. Here we fix notation as follows. We have ${}^\sigma G(q) \leq G(q^\sigma)$, where $G(q^\sigma)$ is the corresponding untwisted group, $G \neq F_4(q)$ or $B_2(q)$. Now following [Stei, chapter 9] we see that any basic module for $G(q^\sigma)$ reduced to ${}^\sigma G(q)$ remains irreducible. Moreover by [Stei, 9.3] all irreducible modules are given by the tensor product theorem. Further by [Stei, 7.5] $GF(q^\sigma)$ is a splitting field.

It remains the cases $G = F_4(q)$ or $B_2(q)$. Then there is a duality between the long and short roots. Just take all weights which vanish on all long roots. We call these modules restricted to ${}^\sigma G(q)$ the basic modules. Then again the tensor product theorem holds. If the rank is ℓ we now get $q^{\ell/2}$ modules. By [Stei, 12.2] $GF(q)$ is the field of definition for all these modules.

Proposition 1.7. *Let $G = A_\ell(q)$, $D_\ell(q)$, $E_6(q)$ or $D_4(q)$ and V be a basic module with high weight λ for ${}^\sigma G$. Then the following holds for γ the diagram automorphism*

(1) *If $\lambda \neq \gamma(\lambda)$. Then $GF(q^\sigma)$ is the field of definition for V.*

(2) *If $\lambda = \gamma(\lambda)$ then $GF(q)$ is the field of definition for V.*

Lemma 1.8. *Let $G = G(q), q = p^f$, be a Chevalley group and V be an irreducible module in characteristic p over the splitting field. Let P be a parabolic and $V_P = C_V(O_p(P))$. Then V_P is an irreducible P – module.*

Proof. This is [Sm]. Q.E.D.

Definition 1.9. Let V be a faithful $GF(p)$-module for G. For $\epsilon \in I\!R$ define $\mathcal{P}_\epsilon(G, V)$ to be the set of all non-identity p-subgroups X of G such that $|X|^\epsilon |C_V(X)| \geq |Y|^\epsilon |C_V(Y)|$ for all $Y \leq X$ (including $Y = 1$).

If V is a $2F$–module with quadratic offender there is always some quadratic offender in $\mathcal{P}_2(G, V)$.

Lemma 1.10. *Let V be a $2F$-module or F–module for G with quadratic offender and V_1 be an invariant subspace. Then V_1 is a trivial subspace for all quadratic offenders or V_1 is a $2F$-module, F–module respectively, with quadratic offender too.*

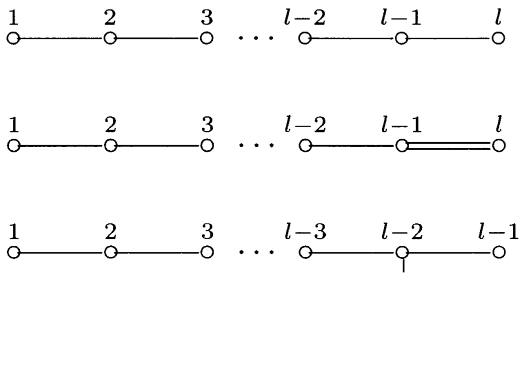
Lemma 1.11. *Let V be a $GF(p)$–module for G.*

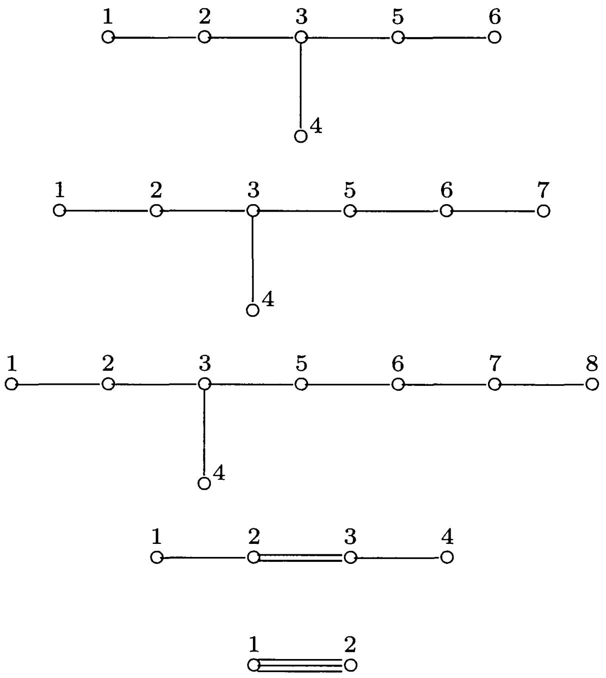
(a) *Let $A, B \in \mathcal{P}_\epsilon(G, V)$ be with $|C_V(A)||A|^\epsilon = |C_V(B)||B|^\epsilon$ be maximal. If $\langle A, B\rangle$ is a p–group then $AB \in \mathcal{P}_\epsilon(G, V)$ and $|C_V(AB)||AB|^\epsilon = |C_V(A)||A|^\epsilon$.*

(b) *Let $A \in \mathcal{P}_\epsilon(G, V)$, $A \leq O_p(G)$. If $|C_V(A)||A|^\epsilon$ is maximal among all such A, then $\langle A^G\rangle$ is a (maybe nonabelian) ϵ –offender on V, i.e. $|V : C_V(\langle A^G\rangle)| \leq |\langle A^G\rangle|^\epsilon$.*

Lemma 1.12. *Let V be a $GF(2)$–module for G with quadratically acting elementary abelian 2–subgroup A. Let $g \in G$ and $a \in A$ with $a^g = az$. Then also $\langle z, C_A(g)\rangle$ acts quadratically.*

Let W be a Weyl group with root system Φ and fundamental roots Π. We assume throughout this section that the Dynkin diagram on Π is connected. Let $l = |\Pi|$, $I = \{1, 2, \dots l\}$ and $\Pi = \{\alpha_1, \alpha_2, \dots \alpha_l\}$ where we choose the labeling as follows:





For the remainder of this paper we fix notation according to the labeling of the diagrams above. Let G be a group of Lie type. We fix a Sylow 2–subgroup S, $B = N_G(S)$, the Borel subgroup, and let $P_1, \dots P_\ell$ be the minimal parabolics containing B. Further for $i \in I$ we denote by $G_i = \langle P_j \mid j \in I \setminus \{i\}\rangle$. These are the maximal parabolics of G. Then G_i/B_{G_i} is a group of Lie type belonging to the diagram for $I \setminus \{i\}$, where B_{G_i} is the largest normal subgroup of G_i contained in B. We assume the reader to be familiar with the structure of the G_i at least those which belong to a connected diagram.

Let now G be as before. Set $K_i = O_2(P_i)$, $i \in I$. Let V be an irreducible module for G over $GF(q)$. Then V is uniquely determined by the action of P_i on $C_V(K_i)$. If $V = V(\lambda)$, $\lambda = \sum_{i=1}^{\ell} a_i\lambda_i$, this means that whenever P_i acts nontrivially on $C_V(K_i)$, we get $a_i \neq 0$ otherwise $a_i = 0$. If all $C_V(K_i)$ are trivial up to one, which is the natural module, then $V = V(\lambda)$ for some fundamental weight λ.

Most modules occurring in this paper, will be fundamental modules. We will get them via [Str], i.e. by showing that they are strong quadratic. Here a module V for $G = G(q)$ is called strong quadratic if there is a group A acting quadratically on V, intersects a root subgroup of G nontrivially but is not contained in that root subgroup.

Lemma 1.13. *Let $q = 2^n$, G be quasisimple with $G/Z(G) = L_n(q)$ or $U_n(q)$ and $V = V(\lambda_1 + \lambda_{n-1})$. Assume $A \leq G$ with $[V, A, A] = 1$. Then $|A| \leq q$.*

Lemma 1.14. *Let V, W be a faithful $GF(q)$–modules and A be quadratic on $X = V \otimes W$. Then $|A| \leq q$.*

Lemma 1.15. *Let $X = V \otimes W$, be a faithful $GF(q)$–modules. Suppose X to be irreducible. If X is a $2F$–module with quadratic offender, then $G \cong L_2(q)$ and $X = V \otimes V^\sigma$, V the natural module and σ some field automorphism of $GF(q)$.*

Lemma 1.16. *Let G be quasisimple with $G/Z(G) = G(q)$ be of Lie type of rank at least two.*

a) *Let $A \leq G$, $|A| \leq q$ and V be an irreducible module with $|V : C_V(A)| \leq |A|^2$ and A quadratic, then V is strong quadratic.*

b) *Let R be a root group in G with $|[V, R]| \leq q^2$ for some irreducible module V, then $G/Z(G) \cong L_n(q)$, $U_n(q)$, $\Omega^\pm(2n, q)$, $Sp(2n, q)$ and V is the natural module, or $G \cong G_2(q)$ and V is the 6–dimensional module.*

Lemma 1.17. *Let G be quasisimple with $G/Z(G) \cong L_n(q)$, $n \geq 5$, let $V = V(\lambda_2)$ and A be an offender as F-module. Then $|A| = q^{n-1} = |V : C_V(A)|$.*

§2. $2F$–modules for Lie type groups in even characteristic

Throughout this chapter we will assume that G is a quasisimple group with $G/Z(G)$ a group of Lie type over a field with $q = 2^n$ elements, including $G(2)'$ and A_6. We additionally assume that $G' \ncong 3 \cdot A_6$, as this will be handled in the last chapter together with the alternating groups. As G will act faithfully on a $GF(2)$–module, G will always be a factor of the universal group.

Further V is an $2F$-module and $A \in \mathcal{P}_2(G, V)$ is a quadratic offending subgroup. If G_i is a maximal parabolic in G we set $Q_i = O_2(G_i)$.

If V is an irreducible $GF(2)$–module for G. Then $V \otimes GF(q)$ is a direct sum of algebraic conjugates of some irreducible $GF(q)$–module M. If $V \otimes GF(q)$ is an algebraic conjugate of a fundamental module for a weight λ we also write $V = V(\lambda)$. In fact as we usually will have strong quadratic modules, which then by [Str] are defined over $GF(q)$, we usually just have to handle $GF(q)$–modules.

Lemma 2.1. *Let $G/Z(G) = G(q)$ be classical or $F_4(q)$ and $V = V(\lambda_2)$ be a $2F$-module with quadratic offender A. Then V is an F–module too.*

Lemma 2.2. *Let $G/Z(G) = G(q)$ and V be an irreducible faithful $2F$–module with quadratic offender. If $C_V(Q_i) = C_V(Z(S))$ for some i, then $V = V(\lambda_i)$ or $G/Z(G) \cong L_2(q)$ and $V = X \otimes X^\sigma$ for some field automorphism σ, X the natural module.*

Lemma 2.3. *Let $G/Z(G) = G(q) \not\cong L_n(q)$ be classical and V be an irreducible faithful $2F$-module with quadratic offender $A \leq Q_1$. Then the pair (G, V) is one of the theorem.*

Lemma 2.4. *Let $G/Z(G) = G(q)$ be of rank at most two and V be an irreducible faithful $2F$-module with quadratic offender A. Then $G/Z(G) \cong L_2(q)$, $L_3(q)$, $Sp(4,q)$, $U_4(q)$, $U_5(q)$, $\Omega^-(6,q)$ or $G_2(q)$ and V is the natural module, or $G \cong L_2(q)$ and V is a tensor product.*

Lemma 2.5. *Let $G/Z(G) = G(q) \not\cong L_n(q)$ be classical of rank at least three and $V = V(\lambda_n)$ be a $2F$-module with quadratic offender A. Then (G, V) is one of the theorem.*

Lemma 2.6. *Let $G \cong \Omega^-(2n, q)$, $n > 3$, and V be an irreducible faithful $2F$-module with quadratic offender A. Then $V \cong V(\lambda_1)$, or $n = 4, 5$ and $V \cong V(\lambda_n)$.*

Lemma 2.7. *Let $G \cong Sp(2n, q)$, $n \leq 6$, and $V \cong V(\lambda_1 + \lambda_n)$. Then V is not a $2F$-module with quadratic offender.*

Proposition 2.8. *Let $G/Z(G) = G(q)$ be classical and V be an irreducible faithful $2F$-module with quadratic offender A. Then one of the following holds*

(i) *$G(q) \cong L_n(q)$, $V \cong V(\lambda_1)$, $V(\lambda_2)$, $V(\lambda_{n-2})$, $V(\lambda_{n-1})$.*
(ii) *$G(q) \cong Sp(2n,q)$, $\Omega^{\pm}(2n,q)$, or $U_n(q)$ and $V \cong V(\lambda_1)$.*
(iii) *$G(q) \cong L_6(q)$, or $U_6(q)$ and $V \cong V(\lambda_3)$.*
(iv) *$G(q) \cong Sp(2n,q)$, $n = 3, 4, 5$, and V is the spin module.*
(v) *$G(q) \cong \Omega^{\pm}(2n,q)$, $n = 4, 5$, or $\Omega^+(12,q)$ and V is the half spin module.*
(vi) *$G(q) \cong L_2(q^2)$ and $V \cong V_1^\sigma \otimes V_1$, where V_1 is the natural module and σ the field automorphism of order two.*

Proposition 2.9. *Let $G/Z(G) = E_n(q)$, $n = 6, 7, 8$, and V be an irreducible faithful $2F$-module with quadratic offender A. Then $n = 6$ and $V \cong V(\lambda_1)$ or $V(\lambda_6)$, or $n = 7$ and $V \cong V(\lambda_7)$.*

Lemma 2.10. *If V is an irreducible faithful $2F$-module with quadratic offender A for the group $G \cong F_4(q)$, then $V \cong V(\lambda_1)$ or $V(\lambda_4)$.*

Lemma 2.11. *The group $G/Z(G) \cong {}^2E_6(q)$ does not possess a $2F$-module with quadratic offender.*

So we have shown

Proposition 2.12. *Let $G/Z(G) = G(q)$ be of Lie type, V be an irreducible faithful $2F$-module over $GF(2)$ with quadratic offending group. Then one of the following holds*

(i) $G(q) \cong L_n(q)$, $V \cong V(\lambda_1)$, $V(\lambda_2)$, $V(\lambda_{n-2})$, $V(\lambda_{n-1})$.
(ii) $G(q) \cong Sp(2n,q)$, $\Omega^{\pm}(2n,q)$ *or* $U_n(q)$ *and* $V \cong V(\lambda_1)$.
(iii) $G(q) \cong L_6(q)$ *or* $U_6(q)$ *and* $V \cong V(\lambda_3)$.
(iv) $G(q) \cong Sp(2n,q)$, $n = 3,4,5$, *and* V *is the spin module.*
(v) $G(q) \cong \Omega^{\pm}(2n,q)$, $n = 4,5$, *or* $\Omega^{+}(12,q)$ *and* V *is the half spin module.*
(vi) $G(q) \cong L_2(q^2)$ *and* $V \cong V_1^{\sigma} \otimes V_1$, *where* V_1 *is the natural module and* σ *the field automorphism of order two.*
(vii) $G(q) \cong E_6(q)$ *and* $V \cong V(\lambda_1)$ *or* $V(\lambda_6)$.
(viii) $G(q) \cong E_7(q)$ *and* $V \cong V(\lambda_7)$.
(ix) $G(q) \cong F_4(q)$ *and* $V \cong V(\lambda_1)$ *or* $V(\lambda_4)$.

§3. $2F$-modules for alternating, sporadic and Lie type groups in odd characteristic

Throughout this chapter we will assume that G is a perfect central extension of an alternating group, a sporadic group or a group of Lie type over a field of odd characteristic, which is not a group of Lie type over a field of characteristic 2 too. Further V is a $2F$-module over $GF(2)$ and $A \in \mathcal{P}_2(G,V)$ an offending subgroup which acts quadratically.

Lemma 3.1. *Let* $G = A_n$ *or* $G = 3A_m$, $m = 6,7$, *and* V *be an irreducible faithful* $2F$*–module over* $GF(2)$ *with quadratic offender* A, *then either* V *is the permutation module or*

(i) $G \cong A_8 \cong L_4(2)$ *and* V *is the natural* $L_4(2)$*-module.*
(ii) $G \cong A_7$ *and* V *is as in* (i).
(iii) $G \cong 3A_6$ *and* $|V| = 2^6$.
(iv) $G \cong A_5 \cong L_2(4)$ *and* V *is the natural* $L_2(4)$*-module.*
(v) $G \cong A_9$ *and* V *is the eight dimensional spin module.*

Lemma 3.2. *Let* $G/Z(G)$ *be sporadic and* V *be an irreducible faithful* $2F$*-module with quadratic offender* A. *Then* $G \cong 3M_{22}$ *and* V *is the* 12*-dimensional module coming from the embedding into* $SU_6(2)$.

Lemma 3.3. *Let* V *be an irreducible faithful* $2F$*-module with quadratic offender* A. *If* G *is some covering group of a group of Lie type in odd characteristic then it is a group of Lie type in even characteristic too, or* $G \cong 3 \cdot U_4(3)$ *and* V *is the* 12*-dimensional module, coming from the embedding into* $SU_6(2)$.

References

[Asch] M. Aschbacher, $GF(2)$-representations of finite groups, Amer. J. of Math., **104** (1982), 683–771.

[CM] B. Cooperstein and G. Mason, Some questions concerning the representations of Chevalley groups in characteristic two, preprint 1977.

[Coop] B. Cooperstein, An enemies list for factorization theorems, Comm. Alg., **6** (1978), 1239–1288.

[CurRei] C.W. Curtis and I. Reiner, Representation theory of finite groups and association algebras, Interscience, New York, 1962.

[Go] D. Gorenstein, Finite groups, Harper and Row, New York 1968.

[JLPW] C. Jansen, R. Lux, R. Parker and R. Wilson, An atlas of Brauer characters, Clarendon Press, Oxford 1995.

[MeiStr1] U. Meierfrankenfeld and G. Stroth, Quadratic $GF(2)$ - modules for sporadic simple groups and alternating groups, Comm. Algebra, **18** (1990), 2099–2139.

[MeiStr2] U. Meierfrankenfeld and G. Stroth, On quadratic $GF(2)$-modules for Chevalley groups over fields of odd order, Arch. Math., **55** (1990), 105–110.

[MeiStr3] U. Meierfrankenfeld and G. Stroth, F-modules for finite simple groups, preprint.

[Sm] S. Smith, Irreducible modules and parabolic subgroups, J. Algebra, **75** (1982), 286–289.

[Stei] R. Steinberg, Lectures on Chevalley groups, Notes by J. Faulkner and R. Wilson, Mimeographed notes, Yale University, Mathematics Department, 1968.

[Str] G. Stroth, Strong quadratic modules, Israel J. Math., **79** (1992), 257–279.

Fachbereich Mathematik und Informatik
Institut für Algebra und Geometrie
Martin-Luther-Universität Halle - Wittenberg
06099 Halle
Germany
e-mail: stroth@coxeter.mathematik.uni-halle.de

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 401–412

On the structure of special rank one groups

Franz Georg Timmesfeld

§1. Introduction

A group $X$ generated by two different nilpotent subgroups $A$ and $B$ satisfying:

$(*)$ For each $a \in A^{\#}$ there exists a $b \in B^{\#}$ satisfying $A^b = B^a$ and vice versa

is called a rank one group. The conjugates of $A$ (and $B$) are called the *unipotent subgroup* of the rank one group $X$ and the conjugates of $H = N_X(A) \cap N_X(B)$ will be called the *diagonal subgroups.* If $A$ is abelian $X$ is called a rank one group with *abelian unipotent* subgroups, abbreviated AUS. Moreover, if for each $a \in A^{\#}$ and $b \in B^{\#}$ which satisfy $(*)$ above, also

$$(**) \qquad a^b = b^{-a}(= (b^{-1})^a)$$

holds, $X$ is called a *special rank one group.*

Rank one groups with abelian unipotent subgroups played a fundamental role in the theory of "abstract root subgroups" [Ti1]. Indeed by (3.18)(3) and (4.15) of [Ti1] all rank one $\Sigma$-subgroups occurring in a group generated by a class $\Sigma$ of abstract root subgroups of "higher rank" are special. A theory of arbitrary rank one groups was developed in §2 of [Ti2]. In both papers one is not able to say very much about the structure of rank one groups, but one has to live with properties of such groups.

By Proposition (2.1) of [Ti2] the following are equivalent:

(i) $X = \langle A, B \rangle$ is a rank one group.

Received March 15, 1999.

(ii) The group Y is doubly transitive on a set Ω with $|\Omega| \geq 3$, such that for some $\alpha \in \Omega$, Y_α contains a nilpotent normal subgroup $A = A_\alpha$ which is regular on $\Omega \backslash \{\alpha\}$ and $X = \langle A^g \mid g \in Y \rangle$.

Namely if $X = \langle A, B \rangle$ is a rank one group one may set $\Omega = A^X$ and $Y = X$. Then it is easy to see that Y satisfies (ii). The reverse direction is also immediate. This shows that the notion of rank one groups and groups with a split BN-pair of rank one are equivalent. (Since $N_X(A) = AH$, $A \cap H = 1$, X has a split BN-pair of rank one!)

Moreover, if $X = \langle A, B \rangle$ is a rank one group, for given $a \in A^\#$ the element $b \in B^\#$ satisfying $A^b = B^a$ is by (2.2) of [Ti2] uniquely determined and so will be called $b(a)$. Further, if for given $b \in B^\#$ we call $a(b)$ the unique element of $A^\#$ satisfying $B^{a(b)} = A^b$, then the maps

$$a \longrightarrow b(a),\ b \longrightarrow a(b)$$

are bijections of $A^\#$ onto $B^\#$ resp. $B^\# \longrightarrow A^\#$. If we denote by χ both maps, then χ is a bijection of $A^\#$ onto $B^\#$, $B^\#$ onto $A^\#$ satisfying $\chi^2 = \mathrm{id}$ and

$$A^{\chi(a)} = B^a,\ A^b = b^{\chi(b)} \text{ for all } a \in A^\#, b \in B^\#.$$

With this notation we can formulate the main results of this note:

Theorem 1. *Let $X = \langle A, B \rangle$ be a special rank one group with AUS. Then the following hold:*

(a) *Either*

(i) *A is an elementary abelian p-group for some prime p.*

or (ii) *A is torsionfree and divisible.*

(b) *For all $a \in A^\#$ and $b \in B^\#$ we have*

$$a^{1/n} = \chi(\chi(a)^n),\ b^{1/n} = \chi(\chi(b)^n)$$

where in case (i) *$n \in \mathbb{N}$ with $(p, n) = 1$, while in* (ii) *$n \in \mathbb{N}$ is arbitrary.*

(Here $a^{1/n}$ denotes the unique $\overline{a} \in A$ with $\overline{a}^n = a$!)

Theorem 2. *Let $X = \langle A, B \rangle$ be a special rank with AUS. Then one of the following holds:*

(a) *If A is an elementary abelian p-group, then $\langle a,b(a) \rangle \simeq (P)SL_2(p)$ for each $a \in A^\#$ (and of course also $\langle b, a(b) \rangle \simeq (P)SL_2(p), b \in B^\#$!)*

(b) *If A is torsionfree and divisible, $a \in A^\#$ and $b = \chi(a) \in B^\#$ set*

$$\begin{aligned} A(a) &= \{a^{m/n} \mid m, n \in \mathbb{Z}, n \neq 0, a^0 = 1\} \\ B(b) &= \{b^{m/n} \mid m, n \in \mathbb{Z}, n \neq 0, b^0 = 1\} \end{aligned}$$

($a^{m/n}$ is well-defined by $a^{m/n} = (a^{1/n})^m$ and Theorem 1). Then $A(a) \simeq (\mathbb{Q}, +) \simeq B(b)$ and $X(a) = \langle A(a), B(b) \rangle$ is a factor group of the universal perfect central extension of $SL_2(\mathbb{Q})$.

Here $(P)SL_2$ denotes any center factor group of SL_2. It will be shown in §2 that the universal perfect central extension of $SL_2(k)$, k a field with $|k| > 4$ and $|k| \neq 9$, is a special rank one group with AUS. So in some sense, theorem 2 is the best possible. On the other hand, as the large list of examples in §2 shows, it seems unlikely that one can determine the exact structure (isomorphism type) of arbitrary special rank one groups with AUS, also there are some results in this direction under additional hypotheses. (i.e. A acts quadratically on some $\mathbb{Z}X$-module, see Theorem 1 of [Ti3]). Since arbitrary rank one groups occur in many situations in group theory, for example as classical groups of Witt-index 1, see [Ti2, (2.15)], or as a subgroup generated by two opposite root-subgroups on a Moufang building, see [Ti2, (2.12)], and since there is a connection between arbitrary rank one groups and special rank one groups with AUS (i.e. conditions under which $\langle Z(A), Z(B) \rangle$ is special [Ti2, (2.9)]), I believe that any result on the structure of special rank one groups is of interest.

§2. Examples and known properties of rank one groups

In this section we discuss certain examples of special rank one groups and state, for the convenience of the reader, basic properties which will be needed for the proof of theorem 1 and 2. These results are, with exception of (2.3), contained in §2 of [Ti1] and [Ti2].

(2.1) **Example** ([Ti1, (2.2)]). Let R be a ring with one element 1 and $L \subseteq R$ satisfying:

(1) $1 \in L$ and L is an additive subgroup of R.
(2) All elements of L^* are units of R and L^* is closed under inverses.
(3) If $t, c \in L$, then $tct \in L$.

Let $A = \{(\begin{smallmatrix} 1 & \\ c & 1 \end{smallmatrix}) \mid c \in L\}, B = \{(\begin{smallmatrix} 1 & c \\ & 1 \end{smallmatrix}) \mid c \in L\}$ and $X = \langle A, B\rangle$ (considered as subgroup of $GL_2(R)$!). Then X is a special rank one group with AUS. Further, if $|L| > 3$, then X is quasisimple. Abusing notation we call this group $SL_2(L)$.

A concrete example is given by: R a division ring, σ an antiautomorphism and $L = \{c \in R \mid c = \ c^\sigma \ \}$.

(2.2) **Example** ([Ti3]). Let K be a division ring or a Cayley division algebra, $V = K^2$ and $X = SL_2(K)$ be the subgroup of $\mathrm{Aut}(V)$ generated by the maps $a(t), b(t), t \in K$ that act on V as follows:

$$(c, d)^{a(t)} = (c + dt, d) \qquad ; \qquad (c, d)^{b(t)} = (c, ct + d).$$

Then X is a special rank one group with AUS with unipotent subgroups $A = \{a(t) \mid t \in K\}$ and $B = \{b(t) \mid t \in K\}$. Further, if $|K| > 3$, then X is quasisimple.
(If $L \subseteq K$ satisfying (1) - (3) of (2.1) one obtains similar examples as in (2.1). These will be contained in a forthcoming book of the author on "Abstract root subgroups".)

(2.3) **Example.** Let k be a field with $|k| > 4$ and $|k| \neq 9$ and let X be the universal perfect central extension of $SL_2(k)$ in the sense of [St]. Then, by theorem 10 of [St], X is the group generated by symbols

$$a(t), b(t); t \in k$$

subject to the relations:

(A) $a(t)a(\tau) = a(t + \tau), b(t)b(\tau) = b(t + \tau); t, \tau \in k.$
(B) $a(u)^{n(t)} = b(-t^{-2}u); u \in k$ and $t \in k^*$
where $n(t) = a(-t)b(t^{-1})a(-t)$.

($n(t)$ is defined slightly different as in §6 of [St]. This is necessary since we conjugate in the usual group-theoretic fashion, i.e. $x^y = y^{-1}xy$.)

Now it is easy to see that the relations (A) + (B) are equivalent to (A) +(B'), where

(B') $a(u)^{b(t^{-1})} = b(-t^{-2}u)^{a(t)}; u \in k, t \in k^*$.
If now $t \in k^*$ is fixed, then $k = \{-t^{-2}u \mid u \in k\}$, whence

$$A^{b(t^{-1})} = B^{a(t)} \text{ for } A = \{a(u)\},\ B = \{b(u)\}.$$

Further

$$a(t)^{b(t^{-1})} = b(-t^{-1})^{a(t)} = (b(t^{-1}))^{-a(t)}.$$

Hence, setting $b(a(t)) := b(t^{-1})$, it follows that X is a special rank one group with AUS.

Notice that if $|k| = \infty$ usually X is different from $SL_2(k)$, see §7 of [St].

For the rest of this section we assume that $X = \langle A, B\rangle$ is a special rank one group with AUS. We state some properties of such an X, which will be needed for the proof of theorem 1 and 2.

(2.4) Let $\Omega = A^X$. Then $X = \langle C, D\rangle = \langle C, d\rangle$ for all $C \neq D \in \Omega$ and $d \in D^{\#}$. Further $N_C(D) = 1$.

(2.5) For $a \in A^{\#}$ and $b \in B^{\#}$ one has

$$\chi(a^{-1}) = \chi(a)^{-1},\ \chi(b^{-1}) = \chi(b)^{-1}.$$

(2.6) Let $N \trianglelefteq X$. Then either $N \leq Z(X)$ or $X = NA$. Especially X is quasisimple if $X = X'$. Moreover, X is not nilpotent.

These results are contained in §2 of [Ti1]. Notice that, together with theorem 2, (2.6) implies that X is quasisimple, except when $p \leq 3$ in case (a)(i) of theorem 1. Now by (2.10) and (2.12) of [Ti1] we have

(2.7) One of the following holds:

(a) $X \simeq SL_2(2)$ or $X \simeq (P)SL_2(3)$.
(b) $X = X'A$, X' quasisimple and $|[A, H]| > 3$.

Actually I believe that either case (a) of (2.7) holds or X is quasisimple. A proof of this would simplify the known simplicity proofs for classical and Lie-type groups, which are not defined over $GF(2)$ or $GF(3)$. (See Theorem (3.17) of [Ti1]!)

§3. Proof of theorem 1

Assume in this section that $X = \langle A, B\rangle$ is a special rank one group with AUS with unipotent subgroups A and B. For each $n \in \mathbb{N}$ let $A_n = \{a \in A \mid a^n = 1\}$ and $A^n = \{a^n \mid a \in A\}$ and similarly B_n, B^n. If for some $a \in A^{\#}$ there exists a unique $\widetilde{a} \in A^{\#}$ with $\widetilde{a}^n = a$ we write $\widetilde{a} = a^{1/n}$ and similarly for $b \in B^{\#}$. We first show:

(3.1) Suppose there exists an $a \in A$ with $a^2 \neq 1$. Then the following hold:

(a) $A_2 = 1$ and $A = A^2$.

(b) For each $a \in A^{\#}$ and $b \in B^{\#}$ we have

$$a^{1/2} = \chi(\chi(a)^2),\ b^{1/2} = \chi(\chi(b)^2).$$

(χ as defined in the introduction. Notice that A and B are conjugate in X, so (a) also holds for B!)

Proof. It suffices to prove (b) only for $a \in A^{\#}$, since then it holds by symmetry also for $b \in B^{\#}$.

Pick $a \in A^{\#}$ with $a^2 \neq 1$ and set $b = \chi(a)$. Then, as $a^b = b^{-a}$ we have $o(b) = o(b^{-1}) = o(a) \neq 2$. Hence there exists a unique $\overline{a} \in A$ with $A^{b^2} = B^{\overline{a}}$. This implies $b^2 = \chi(\overline{a})$ and, since X is special,

$$\overline{a}^{b^2} = (b^2)^{-\overline{a}}.$$

Further by (2.5)

$$b^{-2} = (b^2)^{-1} = \chi(\overline{a})^{-1} = \chi(\overline{a}^{-1})$$

so that $B^{\overline{a}^{-1}} = A^{b^{-2}}$. Now

$$\begin{aligned} B^{\overline{a}} &= (A^b)^b = B^{ab} = B^{a^b} = B^{(b^{-1})^a} = B^{a^{-1}b^{-1}a} \\ &= A^{b^{-1}b^{-1}a} = A^{b^{-2}a} = B^{\overline{a}^{-1}a}, \end{aligned}$$

since by (2.5) $b^{-1} = \chi(a^{-1})$. We obtain $B^{\overline{a}^2a^{-1}} = B$. Hence $\overline{a}^2a^{-1} \in N_A(B)$ and thus $\overline{a}^2 = a$ by (2.4). Since $\overline{a} = \chi(b^2)$ (as $\chi^2 = \mathrm{id}$!) we obtain the equation:

$$(*) \qquad a = \chi(\chi(a)^2)^2 \text{ for each } a \in A^{\#} \text{ with } a^2 \neq 1.$$

Now $(*)$ shows that each element of A with $a^2 \neq 1$ is a square in A. This implies $A = A_2 \cup A^2$. Since no group is the union of two proper subgroups this implies $A = A^2$.

Suppose $\widetilde{a} \in A^{\#}$ has even order. If $o(\widetilde{a}) \neq 2$, then there exists by $(*)$ an $\overline{a} \in A$ with $\overline{a}^2 = \widetilde{a}$ and $\overline{a} = \chi(\chi(\widetilde{a}^2))$. Since the elements a and $\chi(a)^{-1}$ are conjugate in X by definition of χ, this implies

$$o(\overline{a}) = o(\chi(\widetilde{a}^2)) = o(\widetilde{a})^2,$$

which obviously contradicts $\overline{a}^2 = \widetilde{a}$.

This shows that each element of even order in $A^{\#}$ has order 2. But as $A^2 = A$, this implies that there exists no element of order 2 in A, whence $A_2 = 1$ which proves (a).

Now (a) and $(*)$ imply that $\widehat{a} = \chi(\chi(a)^2)$ is the unique element of A with $\widehat{a}^2 = a$. Hence by definition $\widehat{a} = a^{1/2} = \chi(\chi(a)^2)$, which proves (3.1). Q.E.D.

Next we show

(3.2) Suppose A is an elementary abelian q-group for some prime q. Then we have for all $m \in \mathbb{N}$ with $(m, q) = 1$ and for all $a \in A^{\#}, b \in B^{\#}$:

$$a^{1/m} = \chi(\chi(a)^m),\ b^{1/m} = \chi(\chi(b)^m).$$

Proof. We first show, that it suffices to prove (3.2) for $m \leq q - 1$. Namely let $m = n \cdot q + r, r \leq q - 1$. Then, since A and B are elementary abelian q-groups, we have $\chi(a)^m = \chi(a)^r$ and if $\chi(\chi(a)^r)^r = a$, then also $\chi(\chi(a)^m)^m = a$. Hence (3.2) holds for m if it holds for r.

We now prove (3.2) for $m \leq q - 1$ by induction on m, the induction assumption $m = 2$ being (3.1). So suppose that (3.2) holds for $n < m$. Pick $a \in A^{\#}$ and let $\overline{a} = \chi(\chi(a)^m)$. Then we have with $b = \chi(a)$:

$$B^{\overline{a}} = A^{b^m} = A^{b^{m-1}b} = B^{\chi(b^{m-1})b} = B^{a^{1/m-1}b} = B^{(a^{1/m-1})^b}$$

since (3.2) holds for $m - 1$.

Now, as $a^{ba^{-1}} = b^{-1}$, we have $(a^{1/m-1})^{ba^{-1}} = (b^{-1})^{1/m-1}$, whence $(a^{1/m-1})^b = ((b^{-1})^{1/m-1})^a$. This implies

$$\begin{aligned} B^{\overline{a}} &= B^{(a^{1/m-1})^b} = B^{((b^{-1})^{1/m-1})^a} = B^{a^{-1}(b^{-1})^{1/m-1}a} \\ &= A^{b^{-1}(b^{-1})^{1/m-1}a} = A^{(b^{-m})^{1/m-1}a} \end{aligned}$$

by (2.5) and since

$$b^{-1}(b^{-1})^{1/m-1} = (b^{-1})^{1+1/m-1} = (b^{-1})^{m/m-1} = (b^{-m})^{1/m-1}.$$

Now, since $\overline{a} = \chi(b^m)$, (2.5) implies

$$\overline{a}^{-1} = \chi(b^m)^{-1} = \chi(b^{-m})$$

and thus applying χ to this equation $b^{-m} = \chi(\overline{a}^{-1})$. We obtain:

$$(b^{-m})^{1/m-1} = \chi(\overline{a}^{-1})^{1/m-1} = \chi((\overline{a}^{-1})^{m-1})$$

by induction assumption and since $\chi^2 = \mathrm{id}$. Substituting this in the above equation, we obtain

$$B^{\overline{a}a^{-1}} = A^{(b^{-m})^{1/m-1}} = A^{\chi((\overline{a}^{-1})^{m-1})} = B^{(\overline{a}^{-1})^{m-1}}$$

and thus $B^{\overline{a}^m a^{-1}} = B$. Hence $\overline{a}^m a^{-1} \in N_A(B) = \{1\}$ by (2.4) and $\overline{a}^m = a$. This implies $\overline{a} = a^{1/m}$, which proves (3.2) by definition of $\overline{a}$. Q.E.D.

(3.2) shows that Theorem 1 holds if A is an elementary abelian q-group for some prime q. So we assume from now on that this is not the case. We show next:

(3.3) Let p be a prime and $a \in A$ with $a^p \neq 1$. Then the following holds:

(i) $A_p = 1$ and $A = A^p, B_p = 1$ and $B = B^p$.

(ii) For each $a \in A^\#$ and $b \in B^\#$ we have:

$$a^{1/p} = \chi(\chi(a)^p),\ b^{1/p} = \chi(\chi(b)^p).$$

Proof. If $p = 2$ (3.3) is (3.1). Proceeding by induction assume that p is the smallest prime for which (3.3) is false. Then it holds for all primes $q < p$. In particular, we obtain:

(1) If $q < p$ is a prime, then $q \not| o(a)$ for all $a \in A$.

Indeed if $q \mid o(a)$ for some $a \in A$ then some power of a has order q. But then $A = A_q$, since we assume (3.3) holds for q. This contradicts the assumption we made for the rest of section 3.

From (1) we obtain

(2) If $n \leq p - 1$ then the following hold:

(i) $A_n = 1$ and $A = A^n$.

(ii) $a^{1/n} = \chi(\chi(a)^n), b^{1/n} = \chi(\chi(b)^n)$ for all $a \in A^\#$ and $b \in B^\#$.

Indeed (2) holds for each prime $q \mid n$. Hence immediately $A = A^n$ and $A_n = 1$. To prove (ii) let $n = q \cdot r, (q, r) = 1$ and $q > 1, r > 1$ and, proceeding by induction, we may assume that (ii) holds for q and r. Pick $a \in A^\#$ and let $a_1 = a^{1/r}, a_2 = a_1^{1/q}$. Then

$$a_2^n = a_2^{qr} = a_1^r = a.$$

Further, by induction assumption:

$$a_1 = \chi(\chi(a)^r) \text{ and } a_2 = a_1^{1/q} = \chi(\chi(a_1)^q).$$

This implies

$$\begin{aligned} a^{1/n} &= a_1^{1/q} = \chi(\chi(a_1)^q) = \chi(\chi(a^{1/r})^q) \\ &= \chi((\chi(a)^r)^q) = \chi(\chi(a)^{rq}) = \chi(\chi(a)^n) \end{aligned}$$

since $\chi^2 = \mathrm{id}$.

We now lead the existence of p to a contradiction. Let $a \in A$ with $a^p \neq 1$. Then by (2)(ii) $a^{p-1} \neq 1$ and $a^{1/p-1} = \chi(\chi(a)^{p-1})$. Now we argue as in the proof of (3.2). Let $\overline{a} = \chi(\chi(a)^p)$. (Since a and $\chi(a)^{-1}$ are conjugate, also $\chi(a)^p \neq 1$!) Then we have for $b = \chi(a)$:

$$\begin{aligned} B^{\overline{a}} &= A^{b^p} = A^{b^{p-1}b} = B^{a^{1/p-1}b} = B^{(a^{1/p-1})^b} \\ &= B^{(b^{-1/p-1})^a} = B^{a^{-1}b^{-1/p-1}a} = A^{b^{-1}b^{-1/p-1}a} \\ &= A^{(b^{-1})^{p/p-1}a} = A^{(b^{-p})^{1/p-1}a} \end{aligned}$$

Hence $B^{\overline{a}a^{-1}} = A^{(b^{-p})^{1/p-1}}$. Now arguing as in (3.2) $\overline{a} = \chi(b^p)$ implies by (2.4)

$$\overline{a}^{-1} = \chi(b^p)^{-1} = \chi(b^{-p})$$

and so, since $\chi^2 = \mathrm{id}$

$$\chi(\overline{a}^{-1}) = b^{-p}.$$

Now by (2) (ii) applied to $\chi(\overline{a}^{-1})$ we obtain:

$$(b^{-p})^{1/p-1} = \chi(\overline{a}^{-1})^{1/p-1} = \chi((\overline{a}^{-1})^{p-1}).$$

Substituting this in the above equation we get

$$B^{\overline{a}a^{-1}} = A^{\chi((\overline{a}^{-1})^{p-1})} = B^{(\overline{a}^{-1})^{p-1}}.$$

Hence $B^{\overline{a}^p a^{-1}} = B$ and $\overline{a}^p = a$ by (2.4). This shows that we have:

$$(*) \qquad \chi(\chi(a)^p)^p = a \text{ for all } a \in A^{\#} \text{ with } a^p \neq 1.$$

Next we show, as in the proof of (3.1), that if $p \mid o(a)$ for some $a \in A^{\#}$, then $o(a) = p$. Namely if $o(a) \neq p$ then $(*)$ holds for a. But since a and $\chi(a)^{-1}$ are conjugate we have $o(a) = o(\chi(a))$ and thus by the same argument

$$o(\chi(\chi(a)^p) = o(\chi(a)^p) = \frac{o(a)}{p},$$

which obviously contradicts $(*)$. This shows that each $a \in A^{\#}$ with $o(a) \neq p$ satisfies $(o(a), p) = 1$ and thus is a p-power. Hence $A = A_p \cup A^p$ and so as in (3.1) $A = A^p$. If now $\widetilde{a} \in A$ has order p, then because of $A = A^p$ we know that $\widetilde{a}$ is a p-th power. But this is impossible since each element whose order is divisible by p has order p. Thus $A_p = 1$ and (3.3)(i) holds. But then $a^{1/p}$ exists for each $a \in A^{\#}$ and $(*)$ implies $a^{1/p} = \chi(\chi(a)^p)$ which proves (3.3). Q.E.D.

Now (3.3) implies that $A_p = 1$ and $A = A^p$ for each prime p. Namely if $A_p \neq 1$, then $A = A_p$ by (3.3) contradicting our assumption. This shows that A is torsionfree and divisible by each prime p, whence it is divisible. Now it follows from (3.3)(ii) with the same argument as in the proof of (2)(ii) that

$$a^{1/n} = \chi(\chi(a)^n) \text{ for each } a \in A^{\#} \text{ and } n \in \mathbb{N}.$$

Hence Theorem 1 holds. Q.E.D.

§4. Proof of theorem 2.

Pick $a \in A^{\#}$ and set $b = \chi(a)$. If A is an elementary abelian p-group, set

$$A_0 = \{a^m \mid m \leq p\} \text{ and } B_0 = \{b^m \mid m \leq p\}$$

while in case A is torsionfree and divisible set $A_0 = \{a^{m/n} \mid m, n \in \mathbb{Z}, n \neq 0\}$ with the convention $a^0 = 1$ and similarly B_0. We treat both cases (a) and (b) of theorem 2 together, with the convention that, if A is an elementary abelian p-group, all exponents m, n, ℓ, k occurring in the proof are elements of $\mathbb{Z}_p$. Then by definition of $(\overline{a})^{1/n}, \overline{a} \in A^{\#}$ we have

$$(a^m)^{1/n} = a^{m/n} = (a^{1/n})^m, \; n \neq 0.$$

Hence

$$(a^{\ell/m} \cdot a^{k/n})^{mn} = a^{\ell n} \cdot a^{km} = a^{\ell n + kn}$$

for $m \neq 0 \neq n$ and thus:

$$a^{\ell/m} \cdot a^{k/n} = (a^{\ell n + kn})^{1/mn} = a^{\frac{\ell n + kn}{mn}} = a^{\ell/m + k/n}.$$

This implies that the map $\sigma : \ell/m \to a^{\ell/m}$ is an isomorphism of $(\mathbb{Q}, +)$ (resp. $(\mathbb{Z}_p, +)$) onto A_0. We next show that:

$$(*) \qquad \chi(a^{m/n}) = b^{n/m} \text{ for all } n \neq 0 \neq m.$$

Now to prove $(*)$ it suffices to show that:

$$(+)\qquad \begin{array}{l}\chi(\overline{a}^m) = \chi(\overline{a})^{1/m}\\ \chi(\overline{a}^{1/m}) = \chi(\overline{a})^m\end{array} \qquad \text{for all } \overline{a} \in A^{\#} \text{ and } m \neq 0.$$

Indeed if these equations hold, then

$$\begin{aligned}\chi(a^{m/n}) &= \chi((a^{1/n})^m) = \chi(a^{1/n})^{1/m} = (\chi(a)^n)^{1/m}\\ &= \chi(a)^{n/m} = b^{n/m}.\end{aligned}$$

Now, as $\chi^2 = \mathrm{id}$, the second equation in $(+)$ is a consequence of part (b) of theorem 1. Let $\overline{b} = \chi(\overline{a})$. Then also by theorem 1

$$\chi(\overline{a})^{1/m} = \overline{b}^{1/m} = \chi(\chi(\overline{b})^m) = \chi(\overline{a}^m).$$

Hence $(*)$ holds, which shows that χ induces a bijection of $A_0^{\#}$ onto $B_0^{\#}$ (and also $B_0^{\#}$ onto $A_0^{\#}$). Now for $\lambda = m/n, n \neq 0$ set $a(\lambda) = a^{m/n}$ and $b(\lambda) = b^{m/n}$. Then the group $X_0 = \langle A_0, B_0\rangle$ is generated by elements $a(\lambda), b(\lambda)$ where $\lambda \in \mathbb{Q}$ (resp. $\lambda \in \mathbb{Z}_p$). Further, since σ is an isomorphism, the relations (A) of (2.3) are satisfied. Hence to prove theorem 2, it suffices to show that also the relations (B') are satisfied. (We may assume $p > 3$, since otherwise $A_0^{\#} = \{a, a^{-1}\}$, $B_0^{\#} = \{b, b^{-1}\}$, whence $\{A_0\} \cup B_0^{A_0}$ is X_0-invariant.)

Now $(*)$ can be expressed as:

$$(**)\qquad \chi(a(\lambda)) = b(\lambda^{-1}),\ \lambda \in \mathbb{Q}^* \text{ resp. } \mathbb{Z}_p^*.$$

Hence we have

$$a(\lambda)^{b(\lambda^{-1})} = a(\lambda)^{\chi(a(\lambda))} = b(\lambda^{-1})^{-a(\lambda)} \text{ for all } \lambda \neq 0.$$

Now let $\lambda = n/m$ and $\mu = r/s$ with $n \neq 0 \neq m$ and $r \neq 0 \neq s$. Then $a(\lambda) = a(\mu)^{sn/rm}$. Hence we obtain:

$$\begin{aligned}a(\lambda)^{b(\mu^{-1})} &= (a(\mu)^{sn/rm})^{b(\mu^{-1})} = (b(\mu^{-1})^{-a(\mu)})^{sn/rm}\\ &= (b(-\mu^{-1})^{sn/rm})^{a(\mu)} = ((b^{-1})^{s^2n/r^2m})^{a(\mu)}\\ &= b(-\frac{\lambda}{\mu^2})^{a(\mu)},\end{aligned}$$

Since as shown in the proof of (3.2) we have for all $\overline{a} \in A^{\#}$:

$$(\overline{a}^{m/n})^{b(\overline{a})} = (\overline{a}^{b(\overline{a})})^{m/n},\ m \neq 0 \neq n.$$

This shows that the relations (B') are also satisfied which proves theorem 2. Q.E.D.

References

[St] R. Steinberg: Lectures on Chevalley Groups.

[Ti1] F. G. Timmesfeld: Abstract Root Subgroups and Quadratic Action. Advances in Math., **142** (1999), 1–150.

[Ti2] F. G. Timmesfeld: Structure and Presentations of Lie-type Groups. Proc. London Math. Soc., (3) (2000), 428–484.

[Ti3] F. G. Timmesfeld: Moufang planes and the groups E_6^K and $SL_2(K)$, K a Cayley division algebra. Forum Math., **6** (1994), 209–231.

Mathematisches Institut
Arndtstrasse 2
35392 Giessen
Germany

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 413–421

Principal blocks with extra-special defect groups of order 27

Yoko Usami

§1. Introduction

Let $G$ be a finite group and $p$ be a prime number. Let $b$ be a $p$-block of $G$, $P$ be a defect group of $b$ and $k(b)$ (respectively, $l(b)$) be the number of irreducible ordinary characters (respectively, irreducible Brauer characters) in $b$. Suppose that

(1) *two blocks $b$ and b' of finite groups $G$ and G' respectively, have the common defect group $P$ and their Brauer categories $Br_{b,p}(G)$ and $Br_{b',p}(G')$ are equivalent.*

(See [FH] for Brauer categories.) When we consider only principal $p$-blocks, their defect groups are Sylow $p$-subgroups and having the same Brauer category is equivalent to having the same $p$-local structure. See the definition in section 4 in [R] : Finite groups $G$ and $H$ have the same $p$-local structure if they have a common Sylow $p$-subgroup $P$ such that whenever Q_1 and Q_2 are subgroups of $P$ and $f : Q_1 \to Q_2$ is an isomorphism, then there is an element $g \in G$ such that $f(x) = x^g$ for all $x \in Q_1$ if and only if there is an element $h \in H$ such that $f(x) = x^h$ for all $x \in Q_1$.

Under condition (1) there is a question whether we have

$$k(b) = k(b') \text{ and } l(b) = l(b') \tag{2}$$

or not. We have a following conjecture.

Conjecture 1. *When $b$ and b' are principal blocks satisfying condition* (1), *the equalities in* (2) *hold.*

When $P$ is an abelian group, it is known that a block $b$ of $G$ and its Brauer correspondent $Br_P(b)$ in $N_G(P)$ have the same Brauer category

Received May 31, 1999.
Revised June 15, 2000.

(Proposition 4.21 in [AB]), and Broué conjectured that they are derived equivalent (respectively, isotypic). See Conjecture 6.1 and Question 6.2 in [Br2]. Note that each of these conjectures implies that we have

$$(3) \qquad k(b)=k(Br_P(b)) \text{ and } l(b)=l(Br_P(b))$$

for any block b with abelian defect group P. As is stated in [Br2] Broué's conjectures above do not necessarily hold when P is not an abelian group. The principal 2-block b of any one of Suzuki groups $Sz(q)$ and its Brauer correspondent have the same Brauer category (actually, fusion of P is controlled by its normalizer, since Sylow 2-subgroups are T.I. sets), but they are not derived equivalent nor isotypic ; nevertheless (3) holds for them (cf. Consequences 5 and 7 in [A]). Here we have to add one more remark. M. Kiyota pointed out that a semidirect product of an elementary abelian 3-group $Z_3 \times Z_3$ of order 9 by a quaternion group of order 8 whose unique involution acts on $Z_3 \times Z_3$ trivially, has only two 3-blocks (i.e. the principal block b_0 and the other block b_1) and their Brauer categories are equivalent to each other but we have $l(b_0) \neq l(b_1)$.

In this paper we fix P as an extra-special group of order 27 and of exponent 3, and consider principal 3-blocks b having P as a defect group and check Conjecture 1. Note that in this case having the same Brauer category implies having the same inertial quotient $E(= N_G(P)/PC_G(P)$ here) and the same fusion of P. At any rate, using the classification of finite simple groups, we determine $k(b), l(b)$ and $k_0(b)$ completely and proves that Conjecture 1 is true for such blocks, and consequently we prove that Dade's conjecture of ordinary form holds for b. (Here $k_0(b)$ is the number of irreducible ordinary characters in b of height zero.)

When the author visited l'Université Paris 7, Lluis Puig suggested an idea of using his construction of characters as functions on local pointed elements which can be found in Corollary 4.4, Theorem 5.2 and Theorem 5.6 in [P]. The author uses his idea to prove Theorem 1 below.

In the following we denote a cyclic group of order m by Z_m, a quaternion group of order 8 by Q_8, a dihedral group of order 8 by D_8 and a semidihedral group of order 16 by SD_{16} respectively.

Theorem 1. *Let b be the principal 3-block of a finite group G with an extra-special defect group P of order 27 and of exponent 3. Let E be the inertial quotient of b (i.e. $E = N_G(P)/PC_G(P)$) and let u be a non-trivial element in $Z(P)$. Then we have the following.*

(1) *When $N_G(P) \subseteq C_G(Z(P))$, fusion of P in G is controlled by $N_G(P)$ and one of the following holds :*

(i) *If $E=1$, then b is 3-nilpotent, $k(b)=11, k_0(b)=9$ and $l(b)=1$.*

(ii) *If $E \cong Z_2$, then $k(b)=10, k_0(b)=6$ and $l(b)=2$. (In this case E acts on $P/Z(P)$ fixed-point-freely.)*

(iii) *If $E \cong Z_4$, then $k(b)=14, k_0(b)=6$ and $l(b)=4$.*

(iv) *If $E \cong Q_8$, then $k(b)=16, k_0(b)=6$ and $l(b)=5$.*

(2) *When $N_G(P) \not\subseteq C_G(Z(P))$, E is isomorphic with either $Z_2, Z_2 \times Z_2, Z_8, D_8$ or SD_{16} and we have an estimate of $k(b)$ as below according to E and the number of conjugacy classes of elements of order* 3*. When $E \cong Z_2$, E does not act on $P/Z(P)$ fixed-point-freely. In each case $k(b)-l(b)$ takes a constant value. When $E \cong Z_8$, each case is further divided into two subcases according to fusion of a basic set of $C_G(u)$ in the extended centralizer $C_G^*(u)$ $(=\{g \in G \mid u^g = u \text{ or } u^{-1}\})$. The subcase where each element of a basic set of $C_G(u)$ is fixed by $C_G^*(u)$ corresponds to subcase* 1*. Otherwise it is subcase* 2*.*

(i) *Suppose that $E \cong Z_2$.*

(i)–(1) *If fusion of P is controlled by $N_G(P)$, then $P-\{1\}$ consists of* 6 *classes and $k(b)-l(b)=8$ and $k(b)=10$.*

(i)–(2) *Otherwise, $P-\{1\}$ consists of* 5 *classes and $k(b)-l(b)=7$ and $9 \leq k(b) \leq 11$.*

(ii) *Suppose that $E \cong Z_2 \times Z_2$. Then one of the following holds.*

(ii)–(1) *If fusion of P is controlled by $N_G(P)$, then $P-\{1\}$ consists of* 4 *classes and $k(b)$–$l(b)=7$ and $k(b)=11$.*

(ii)–(2) *$P-\{1\}$ consists of* 3 *classes, $k(b)-l(b)=5$ and $8 \leq k(b) \leq 11$.*

(ii)–(3) *$P-\{1\}$ consists of* 3 *classes, $k(b)-l(b)=6$ and $10 \leq k(b) \leq 12$.*

(ii)–(4) *$P-\{1\}$ consists of* 2 *classes, $k(b)-l(b)=4$ and $7 \leq k(b) \leq 12$.*

(ii)–(5) *$P-\{1\}$ consists of* 2 *classes, $k(b)-l(b)=3$ and $6 \leq k(b) \leq 11$.*

(ii)–(6) *$P-\{1\}$ consists of* 1 *class, $k(b)-l(b)=2$ and $5 \leq k(b) \leq 18$.*

(iii) *Suppose that $E \cong Z_8$.*

(iii)–(1) *If fusion of P is controlled by $N_G(P)$, then $P-\{1\}$ consists of* 2 *classes and $k(b)-l(b)=5$. In subcase* $1, 8 \leq k(b) \leq 14$*. In subcase* $2, 8 \leq k(b) \leq 12$*.*

(iii)–(2) *Otherwise, $P-\{1\}$ consists of* 1 *class and $k(b)-l(b)=4$. In subcase* $1, 8 \leq k(b) \leq 18$*. In subcase* $2, 7 \leq k(b) \leq 15$*.*

(iv) *Suppose that* $E \cong D_8$. *Then one of the following holds.*

(iv)-(1) *If fusion of* P *is controlled by* $N_G(P)$, *then* $P-\{1\}$ *consists of* 3 *classes,* $k(b)-l(b)=8$ *and* $k(b)=13$.

(iv)-(2) $P-\{1\}$ *consists of* 2 *classes,* $k(b)-l(b)=6$ *and* $9 \leq k(b) \leq 13$.

(iv)-(3) $P-\{1\}$ *consists of* 1 *class,* $k(b)-l(b)=4$ *and* $7 \leq k(b) \leq 15$.

(v) *Suppose that* $E \cong SD_{16}$.

(v)-(1) *If fusion of* P *is controlled by* $N_G(P)$, *then* $P-\{1\}$ *consists of* 2 *classes,* $k(b)-l(b)=7$ *and* $10 \leq k(b) \leq 15$.

(v)-(2) *Otherwise,* $P-\{1\}$ *consists of* 1 *class,* $k(b)-l(b)=5$ *and* $7 \leq k(b) \leq 14$.

Using the classification of finite simple groups we obtain the following theorem. As is well known, we can assume that $O_{p'}(G)=1$ when we treat the principal p-block of G.

Theorem 2. (*Using the classification of finite simple groups.*) *Let* G *be a finite group with* $O_{3'}(G)=1$ *having an extra-special Sylow* 3-*subgroup* P *of order* 27 *and of exponent* 3. *Let* M *be a minimal normal subgroup of* G. *Then one of the following holds* :

(i) $M \cong Z_3$ *and* $Z(P)$ *is a normal subgroup of* G *and fusion of* P *in* G *is controlled by* $N_G(P)$. *As for the principal* 3-*block* $b, k(b)$ *and* $l(b)$ *are uniquely determined according to its inertial quotient.*

(ii) $M \cong Z_3 \times Z_3$ *and* G/M *is embedded in* $GL(2,3)$. *In particular,* G *is* 3-*solvable.*

(iii) $M \cong PSL(3,q)$ *where* $q \equiv 4,7 \pmod 9$. *Furthermore we have*

$$PGL(3,q) \subseteq G \subseteq Aut(PSL(3,q))$$

(iv) $M \cong PSU(3,q^2)$ *where* $q \equiv 2,5 \pmod 9$. *Furthermore we have*

$$PGU(3,q^2) \subseteq G \subseteq Aut(PSU(3,q^2)).$$

(v) $M \cong M_{24}$, Ru or J_4. *Furthermore* $G=M$.

(vi) $M \cong PSL(3,3)$, $PSU(3,3^2)$, ${}^2F_4(2)'$, M_{12}, J_2 or He. *Furthermore* $G=M$ *or* $Aut(M)$.

(vii) $M \cong G_2(q)$ *where* $q \equiv 2,4,5,7 \pmod 9$. *Furthermore* $M \subseteq G \subseteq Aut(M)$.

(viii) $M \cong {}^2F_4(q)$ *where* $2^{2m+1}=q \equiv 2,5 \pmod 9$. *Furthermore* $M \subseteq G \subseteq Aut(M)$.

The number $k(b)$ *in case of* $N_G(P) \subseteq C_G(Z(P))$ (*see* Theorem 1 (2)) *is uniquely determined by* E *as follows: If* $E \cong Z_2$ (*respectively* $Z_2 \times Z_2$, Z_8, D_8 *and* SD_{16}), *then* $k(b) = 10$ (*respectively,* 11, 13, 13 *and* 14). *When* $N_G(P) \not\subseteq C_G(Z(P))$, *we have always* $k_0(b) = 9$. *Furthermore, Dade's conjecture of ordinary form holds for* b *in any case. The above groups in* (ii) *through* (viii) *fall into the cases described in* Theorem 1 (2) *as follows. The numbers in the statements below correspond to those in* Theorem 1 (2). *The semidirect product of* $Z_3 \times Z_3$ *by* $SL(2,3)$, *some groups in* (iii) *above and* $PGU(3,q^2) \cdot$ (*odd order*) *with* $q \equiv 2, 5 \pmod 9$ *satisfy* (i)-(2). *The semidirect product of* $Z_3 \times Z_3$ *by* $GL(2,3)$, *all the remaining groups in* (iii) *above and* $PGU(3,q^2) \cdot$ (*even order*) *with* $q \equiv 2, 5 \pmod 9$ *satisfy* (ii)-(2). $PSL(3,3)$ *and* M_{12} *satisfy* (ii)-(5). $PSU(3,3^2)$ *and* J_2 *satisfy* (iii)-(1). M_{24}, $Aut(M_{12})$, $Aut(PSL(3,3))$, He *and* $Aut(He)$ *satisfy* (iv)-(2). ${}^2F_4'(2)$ *satisfies* (iv)-(3). $Aut(PSU(3,3^2))$, $Aut(J_2)$ *and all the groups in* (vii) *above satisfy* (v)-(1). Ru, J_4 *and all the groups in* (viii) *above satisfy* (v)-(2).

§2. Remarks on Theorem 1

(1) After the author obtained Theorem 1, Masao Kiyota told the author that several years ago he already determined $k(b)$, $k_0(b)$ and $l(b)$ for principal blocks b when $N_G(P) \subseteq C_G(Z(P))$ by Brauer and Olsson's method using the orthogonality relation between columns of generalized decomposition matrix.

(2) Outline of the proof is as follows. First, list up all possible Broué's (or Alperin's) conjugation families for b-subpairs (with an aid of 3-strongly embedded subgroups) in order to determine fusion of b-subpairs in G ([Br1, CP]). This work means that we list up all possible Brauer categories as in [CP]. Note that when b is a principal p-block, b-subpairs are equivalent to p-subgroups. Second, collect information about blocks b_Q such that

$$(1, b) \not\subseteq (Q, b_Q) \subseteq (P, e),$$

where (P, e) is a fixed maximal b-subpair. Third, construct a Z-basis of generalized characters in b which vanish on 3-regular elements. Here we apply L.Puig's Theorem 5.6 in [P], where he gave some equivalent conditions of a function on local pointed elements to be a generalized character. Fourthly, determine the decomposition of each character in the above Z-basis into irreducible characters in order to know $k(b)$. It is known that any irreducible character in b appears in some generalized character in this Z-basis. In order to determine these decompositions the author used a computer and also checked the elementary divisors of Cartan matrices by a computer. Unfortunately, when $N_G(P) \not\subseteq C_G(Z(P))$, we can not determine $k(b)$ uniquely. There are huge number of possible decompositions. But, as for $k(b)$, it seems that we can get almost the same estimate of $k(b)$ as this by hand.

(3) When E is of order 2, either G has a normal subgroup of index 3, or G is a 3-solvable group of 3-length 1 by S.D. Smith and A.P. Tyrer's theorem in [ST].

§3. Remarks on Theorem 2

(1) Using the strong assumption that $Z(P) \lhd G$, $k(b)$ in (i) is determined. Here we already use the classification of finite simple groups to determine the number of irreducible ordinary characters in the principal 3-block with an elementary abelian defect group of order 9 and with the cyclic inertial quotient of order 8.

(2) If G is a 3-solvable group with $O_{3'}(G) = 1$ and has an extraspecial Sylow 3-subgroup of order 27 and of exponent 3, then G is completely determined, that is, *either* the semidirect product of P and a group E isomorphic with 1, Z_2, $Z_2 \times Z_2$, Z_4, Q_8, D_8, or SD_{16} or the semidirect product of $Z_3 \times Z_3$ by $SL(2,3)$ or $GL(2,3)$ (with faithful actions). (cf. Proposition 53.4 in [Ka] or [Ko]).

(3) It is not easy to choose the irreducible characters in b among all irreducible characters in G when G belongs to one of infinite series in (iii), (iv), (vii) and (viii). Fortunately, any nonprincipal 3-block of a simple group in these infinite series has some proper subgroup of P as a defect group. So using the estimate of $k(b)$ in Theorem 1 and the known facts on the number of irreducible ordinary characters in other 3-blocks and some more information about b itself, we determine $k(b)$ effectively in these cases. The author thanks Ken-ichi Shinoda and Meinolf Geck for information about ${}^2F_4(q)$.

(4) In order to prove Dade's conjecture in this case, we consider the set of G-conjugacy classes of radical 3-chains as the disjoint union of two subsets, one of which consists of classes of chains whose final subgroups are defect groups of the principal blocks of the normalizers of the chains and the other consists of the rest. There is a bijection from the former subset to the latter given by the Brauer correspondence between the corresponding principal blocks, sending a class of chains of length m into that of length $m-1$. Then by cancellation we get the conclusion (cf. 2.3 in [U1]).

§4. Perfect isometries and Morita equivalences

Having the same p-local structure does not always guarantee a derived category equivalence between the principal p-blocks (see counter examples in §1). But the author thinks that we can still expect something. Recall Broué's theorem :

Theorem 3 (Broué, Theorem3.1 [**Br2**]). *If two blocks are derived category equivalent, then there is a perfect isometry between these blocks.*

In view of this theorem, we can expect a derived equivalence between blocks if there exists a perfect isometry between them, although it is not proved that they are equivalent. In any case, it is meaningful to check whether a perfect isometry exists, as the first step towards checking the existence of a derived equivalence. The author and her student M.Nakabayashi did it in the following cases. (cf. Theorem 2 and [N]).

Proposition 4. *The groups in* (i) (*respectively* (ii), (iii), (iv), (v), (vi) *and* (vii)) *below have the same* 3*-local structure and there is a perfect isometry between the principal* 3*-blocks of any two of them.*

(i) $PSU(3,3^2)$, J_2.
(ii) $PSL(3,3)$, M_{12}.
(iii) M_{24}, He, $Aut(He)$.
(iv) $Aut(M_{12})$, $Aut(PSL(3,3))$.
(v) Ru, J_4.
(vi) *the semidirect product of* $Z_3 \times Z_3$ *by* $SL(2,3)$, $PGU(3,q^2)$ *with* $q \equiv 2,5 \pmod 9$, $PGL(3,q)$ *with* $q \equiv 4,7 \pmod 9$.
(vii) $G_2(q)$ *with* q *a power of* 2 *and* $q \equiv 2,4,5,7 \pmod 9$.

Proposition 5. *The groups in* (i)′ (*respectively* (ii)′, (iii)′, (iv)′, (v)′ *and* (vi)′) *have the same* 3*-local structure, but there is no perfect isometry between their principal* 3*-blocks which sends the trivial character to the trivial character. Here* P *is the extra-special group of order* 27 *and of exponent* 3.

(i)′ *the semidirect product of* P *by* Z_8, $PSU(3,3^2)$,
(ii)′ M_{24}, $Aut(M_{12})$
(iii)′ Ru, ${}^2F_4(2)$
(iv)′ $G_2(2)$, $Aut(J_2)$
(v)′ $Aut(J_2)$, *the semidirect product of* P *by* SD_{16} *with the faithful action*
(vi)′ $G_2(4)$, *the semidirect product of* P *by* SD_{16} *with the faithful action.*

On the other hand, there are Koshitani and Kunugi's results on the principal 3-blocks of $PSU(3,q^2)$ and $PSL(3,q)$ with elementary abelian defect groups of order 9 ([KK], [Ku]). Based on them we have got the following theorem.

Theorem 6 (N. Kunugi and Y. Usami [KU], [U2]). *The principal 3-blocks of all the groups in* (i) (*respectively* (ii), (iii) *and* (iv)) *below are Morita equivalent.*

(i) $PGU(3, q^2)$ *defined over the finite field* $GF(q^2)$ *satisfying* $q \equiv 2, 5 \pmod 9$.
(ii) $PGL(3, q)$ *satisfying* $q \equiv 4, 7 \pmod 9$.
(iii) $SU(3, q^2)$ *defined over the finite field* $GF(q^2)$ *satisfying* $q \equiv 2, 5 \pmod 9$.
(iv) $SL(3, q)$ *satisfying* $q \equiv 4, 7 \pmod 9$.

Moreover, let q be a power of 2 and satisfying $q \equiv 2$ or $5 \pmod 9$. Then the author and M.Nakabayashi have almost finished proving that the principal 3-blocks of $G_2(q)$ and $G_2(2)$ are Morita equivalent to each other.

For the characters of groups in Theorem 2, see the following:

1. J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, Atlas of Finite Groups, Clarendon Press, (1985) Oxford.
2. B. Chang, The conjugate classes of Chevalley groups of type (G_2), J. Algebra, 9 (1968), 190–211.
3. B. Chang and R. Ree, The characters of $G_2(q)$, Symposia Mathematica XIII, Instituto Nazionale de Alta Mathematica, (1974), 395–413.
4. V. Ennola, On the characters of the finite unitary groups, Ann. Acad. Sci. Fenn., 323 (1963), 1–34.
5. H. Enomoto, The conjugacy classes of Chevalley groups of type (G_2) over finite fields of characteristic 2 or 3, J. Fac. Sci. Univ. Tokyo Sect. I Math., 16 (1970), 497–512.
6. H. Enomoto and H. Yamada, The characters of $G_2(2^n)$, Japan. J. Math., 12 (1986), 325–377.
7. K. Shinoda, The conjugacy classes of the finite Ree groups of type (F_4), J. Fac. Sci. Univ. Tokyo Sect. IA Math., 22 (1975), 1–15.
8. G. Malle, Die unipotenten Charaktere von ${}^2F_4(q^2)$, Comm. in Algebra, 18(7) (1990), 2361–2381.
9. R. Steinberg, The representation of $GL(3, q), GL(4, q), PGL(3, q)$ and $PGL(4, q)$, Canadian J. Math., 3 (1951), 225–235.

References

[A] J. Alperin, Weights for finite groups, Proc. Sympos. Pure Math., **47** (1987), 369–379.

[AB] J. Alperin and M. Broué, Local methods in block theory, Ann. of Math., **110** (1979), 143–157.

[Br1] M. Broué, Theorie locale des blocs d'un groupe fini, Proceedings of the International Congress of Mathematicians, Berkeley, 1986, 360–368.

[Br2] M. Broué, Isometries parfaites, types de blocs, catégories, dérivées, Astérisque, **181-182** (1990), 61–92.

[CP] M. Cabanes and C. Picaronny, Types of blocks with dihedral or quaternion defect groups, J. Fac. Sci. Univ. Tokyo Sect. IA, Math., **39** (1992), 141–161.

[FH] P. Fong and M. Harris, On perfect isometries and isotypies in finite groups, Invent. Math., **114** (1993), 139–191.

[Ka] G. Karpilovsky, "Structure of Blocks of Group Algebras", Longman Scientific and Technical, 1987

[KK] S. Koshitani and N. Kunugi, The principal 3-blocks of the 3-dimensional projective special unitary groups in non-defining characteristic, preprint.

[Ko] S. Koshitani, On group algebras of finite groups, Proc. 4th Internat. Conf. on Representations of Algebras, Springer Lecture Note Series, **1178**, 109–128.

[KU] N. Kunugi and Y. Usami, The principal 3-blocks of the 3-dimensional projective general linear and projective general unitary groups and Morita equivalences, preprint.

[Ku] N. Kunugi, Morita equivalent 3-blocks of the 3-dimensional projective special linear groups, to appear in J. London Math. Soc..

[N] M. Nakabayashi, Principal 3-blocks with extra-special 3-defect groups of order 27 and exponent 3, preprint.

[P] L. Puig, Pointed groups and construction of characters, Math. Z., **176** (1981), 265–292.

[R] J. Rickard, Derived equivalences as derived functors, J. London. Math. Soc., **43** (1991), 37–48.

[ST] S.D. Smith and A.P. Tyrer, On finite groups with a certain Sylow normalizer. I., J. Algebra, **26** (1973), 343–365.

[U1] Y. Usami, Perfect isometries for principal blocks with abelian defect groups and elementary abelian 2-inertial quotients, J. Algebra, **196** (1997), 646–681.

[U2] Y. Usami, Principal blocks with extra-special defect groups of order 27, preprint.

Department of Mathematics
Ochanomizu University
Tokyo 112-8610, Japan

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 423–436

Bases of Chambers of Linear Coxeter Groups

John H. Walter

§1. Introduction

Let $V$ be a vector space over the real numbers $\mathbb{R}$. The subgroups of $\mathrm{GL}(V)$ that are generated by reflections are called *reflection groups.* We study in this paper those reflection groups from which a polyhedral cone may be constructed and which lead to a chamber system in $V$. Using a result of J. Tits [5], it follows that these groups are obtained from representations of Coxeter groups. So they are called *linear Coxeter groups.* From this point of view, these groups were also extensively studied by E.B. Vinberg [6] in the case where they have a finite number of canonical generators. We extend this theory in order to investigate the reflection subgroups of a linear Coxeter group. We make no restriction on the number of generators or on the dimension of $V$. Our object is to present this subject using the concrete geometric methods that are associated with the chamber systems in a real vector space.

We apply these results to give a proof that a reflection subgroup of a linear Coxeter group is again a linear Coxeter group. This generalizes the result that asserts that a reflection subgroup of a Coxeter group is a Coxeter group which was independently proved by M. Dyer [3] and V.V. Deodhar [2]. Our results also characterize a base for the reflection subgroup, which will be useful in a sequel to this paper.

§2. Linear Coxeter Groups

2.1. Polyhedral Cones

Let $V$ be a vector space over $\mathbb{R}$, and denote its dual by $V^\vee$. Let $T$ be a subset of $V$. We are interested in reflection groups that act on $T$. Commonly the choice for $T$ will be $V$ itself, but in dealing with reflection subgroups, it is useful to choose $T$ to be the convex set that

Received June 21, 1999.
Revised February 8, 2001.

is left invariant by the associated linear Coxeter group, namely, its Tits cone.

Let $\Lambda^\vee$ be a subset of $V^\vee$ and set

$$C(\Lambda^\vee) = \{v \in T \mid \lambda^\vee(v) \geq 0 \text{ for all } \lambda^\vee \in \Lambda^\vee\}, \tag{1}$$

$$C(\Lambda^\vee)^o = \{v \in T \mid \lambda^\vee(v) > 0 \text{ for all } \lambda^\vee \in \Lambda^\vee\}. \tag{2}$$

For $\lambda^\vee \in V^\vee$, respectively set $D_{\lambda^\vee}$ and $D^o_{\lambda^\vee}$ to be the half-spaces $C(\{\lambda^\vee\})$ and $C(\{\lambda^\vee\})^o$. Then

$$C(\Lambda^\vee) = \bigcap_{\lambda^\vee \in \Lambda^\vee} D_{\lambda^\vee} \text{ and } C(\Lambda^\vee)^o = \bigcap_{\lambda^\vee \in \Lambda^\vee} D^o_{\lambda^\vee}. \tag{3}$$

Likewise set $H_{\lambda^\vee} = \lambda^{\vee -1}(0)$ for $\lambda^\vee \in V^\vee$. Then $H_{\lambda^\vee}$ is the hyperplane in V which is the envelope for $D_{\lambda^\vee}$. A convex subset $C(\Lambda^\vee)$ of V given in (3) is said to be a *polyhedral cone* in T if $C(\Lambda^\vee)^o \neq \emptyset$. If $|\Lambda^\vee| = 2$, it is sometimes called a *dihedral cone.*

Definition 2.1. Let $\Pi^\vee \subseteq V^\vee$. For $\alpha^\vee \in \Pi^\vee$, set $F_{\alpha^\vee}(\Pi^\vee) = H_{\alpha^\vee} \cap C(\Pi^\vee) = H_{\alpha^\vee} \cap C(\Pi^\vee \setminus \{\alpha^\vee\})$ and $F^o_{\alpha^\vee}(\Pi^\vee) = H_{\alpha^\vee} \cap C(\Pi^\vee \setminus \{\alpha^\vee\})^o$. Given $\Lambda^\vee \subseteq V^\vee$, a subset $\Pi^\vee$ is said to be a *base* for $C(\Lambda^\vee)$ if $C(\Pi^\vee) = C(\Lambda^\vee)$, and $F^o_{\alpha^\vee}(\Pi^\vee) \neq \emptyset$ for all $\alpha^\vee \in \Pi^\vee$. In this case, $F_{\alpha^\vee}(\Pi^\vee)$ is said to be a *face* of $C(\Pi^\vee)$. We say that $\Pi^\vee$ is a *base* if it is a base for $C(\Pi^\vee)$.

Clearly if $\Pi^\vee$ is a base, it is a base for $C(\Lambda^\vee)$ for any $\Lambda^\vee \supseteq \Pi^\vee$ such that $C(\Lambda^\vee) \supseteq C(\Pi^\vee)$. If $\Pi^\vee$ is a base for $C(\Lambda^\vee)$, then the hyperplanes $H_{\alpha^\vee}$ with $\alpha^\vee \in \Pi^\vee$ are called the *walls* of $C(\Lambda^\vee)$. Note that having $F^o_{\alpha^\vee}(\Pi^\vee) \neq \emptyset$ is equivalent to having $C(\Pi^\vee) \supset C(\Pi^\vee \setminus \{\alpha^\vee\})$. Thus if $\Pi^\vee$ is a minimal subset of $\Lambda^\vee$ such that $C(\Pi^\vee) = C(\Lambda^\vee)$, it is a base for $C(\Lambda^\vee)$.

2.2. Reflection Groups

Denote the pairing $V^\vee \times V \to \mathbb{R}$ given by $(\lambda^\vee, x) \longmapsto \langle \lambda^\vee, x\rangle = \lambda^\vee(x)$. A reflection $r \in \mathrm{GL}(V)$ is determined by two elements $\alpha_r \in V$ and $\alpha_r^\vee \in V^\vee$ with

$$\langle \alpha_r^\vee, \alpha_r\rangle = 2 \tag{4}$$

so that

$$r : x \to x - \langle \alpha_r^\vee, x\rangle \alpha_r. \tag{5}$$

The vectors $\alpha_r^\vee$ and α_r respectively are said to be a *coroot* and *root* of r. Hence $H_r = \alpha_r^{\vee -1}(0)$ is the fixed hyperplane of r and $R\alpha_r$ is its complementary eigenspace. When $\alpha_r^\vee$ and α_r satisfy (4), they are said to be paired to r. Thus $(c\alpha_r^\vee, c^{-1}\alpha_r)$, $c \neq 0$, are the coroots and roots that are paired to r.

Given a set S of reflections, $W(S)$ will designate the reflection group given by $W(S) = \langle s \mid s \in S\rangle$. Designate by $w^\vee$ the transformation of V which is contragredient to $w \in \mathrm{GL}(V)$. Associated with $W(S)$ is the contragredient group $W(S)^\vee = \{w^\vee \mid w \in W(S)\}$, which acts on $V^\vee$. If r is given by (5), then $r^\vee : x^\vee \to x^\vee - \langle x^\vee, \alpha_r\rangle\alpha_r^\vee$. Because $\langle\alpha_r^\vee, x\rangle = 0$ implies $\langle w^\vee\alpha_r^\vee, wx\rangle = 0$, it follows that $wH_{\alpha_r^\vee} = H_{w^\vee\alpha_r^\vee}$.

Set $\mathcal{H}\,(W(S)) = \{H_r \mid r \text{ is a reflection in } W(S)\}$.

Definition 2.2. Let T be a subset of V, and $\Pi^\vee = \{\alpha_i^\vee \in V^\vee \mid i \in I\}$. Take $C(\Pi^\vee)$ to be a polyhedral cone in T. Let $S = S(\Pi^\vee)$ be a set of reflections s_i, $i \in I$, where for each $i \in I$, $\alpha_i^\vee$ is a coroot of s_i. Assume that T is $W(S(\Pi^\vee))$-invariant. Then $C(\Pi^\vee)$ is said to be a *chamber* of $W(S(\Pi^\vee))$ for the action of $W(S(\Pi^\vee))$ on T if

$$wH_{\alpha_i^\vee} \cap C(\Pi^\vee)^\circ = \emptyset \tag{6}$$

for all $w \in W(S(\Pi^\vee))$ and $\alpha_i^\vee \in \Pi^\vee$.

Set $\mathcal{H}(W(S); \Pi^\vee) = \{H_{\beta^\vee} \mid \beta^\vee \in W(S)^\vee\Pi^\vee\}$. As $wH_{\alpha_i^\vee} = H_{w^\vee\alpha_i^\vee}$, (6) is equivalent to having $H_{\beta^\vee} \cap C(\Pi)^\circ = \emptyset$ for all $H_{\beta^\vee} \in \mathcal{H}\,(W(S), \Pi^\vee)$.

Definition 2.3. If $C(\Pi^\vee)$ is a chamber such that $wC(\Pi^\vee) = C(\Pi^\vee)$ implies $w = 1$, then $C(\Pi^\vee)$ is said to be a *regular chamber* for the action of $W(S(\Pi^\vee))$ on T and $W(S(\Pi^\vee))$ is said to be a *linear Coxeter group*[1].

The translates $wC(\Pi^\vee)$ of $C(\Pi^\vee)$, $w \in W(S)$, will also be called *chambers* of $W(S(\Pi))$, and we set $\mathcal{C}\,(W(S))$ to be the set of chambers of $W(S)$. When considering a given reflection group $W(S(\Pi^\vee))$ acting on a set T, it will be understood that the chambers in $\mathcal{C}\,(W\,(S))$ are chambers for the action on T. The set $\mathcal{C}(W(S))$ is sometimes called the *chamber system* for $W(S)$. When $C(\Pi^\vee)$ is a regular chamber, then

$$wC(\Pi^\vee)^\circ \cap C(\Pi^\vee)^\circ = \emptyset \tag{7}$$

for every $w \in W(S(\Pi^\vee)) \setminus \{1\}$, in which case $C(\Pi^\vee)^\circ$ is a fundamental domain for the action of $W(S(\Pi^\vee))$ on the subset $T(W(S(\Pi^\vee))) = \bigcup_{w\in W(S)} wC(\Pi^\vee)$.

Proposition 2.1. *Let* $\Pi^\vee = \{\alpha_i^\vee \mid i \in I\} \subseteq V^\vee$. *Take* $S(\Pi^\vee)$ *to be a set of reflections* s_i *with coroots* $\alpha_i^\vee$, $i \in I$, *and let* T *be a* $W(S(\Pi^\vee))$*-invariant subset of* V. *A polyhedral cone* $C(\Pi^\vee)$ *is a chamber for the*

[1] Linear Coxeter groups were defined as such by E.B.Vinberg [6].

action of $W(S(\Pi^\vee))$ on T if and only if for all $w \in W(S(\Pi^\vee))$, either $wC(\Pi^\vee)^\circ \cap C(\Pi^\vee)^\circ = \emptyset$ or $wC(\Pi^\vee)^\circ = C(\Pi^\vee)^\circ$. If it is a regular chamber, then $H_r \cap wC(\Pi)^\circ = \emptyset$ for all $H_r \in \mathcal{H}(W(S))$ and $w \in W(S(\Pi^\vee))$.

Proof. Assume that $C(\Pi^\vee)$ is a chamber so that $wH_{\alpha_i^\vee} \cap C(\Pi^\vee)^\circ = \emptyset$ for all $i \in I$ and $w \in W(S(\Pi^\vee))$. So either $w^\vee\alpha_i^\vee(C(\Pi^\vee)^\circ) > 0$ or $w^\vee\alpha_i^\vee(C(\Pi^\vee)^\circ) < 0$ for $i \in I$. If $w^\vee\alpha_i^\vee(C(\Pi^\vee)^\circ) > 0$ for all $i \in I$, then $wC(\Pi^\vee)^\circ = C(w^\vee\Pi^\vee)^\circ \supseteq C(\Pi^\vee)^\circ$. But also $w^\vee\alpha_i^\vee(x) = \alpha_i^\vee(wx)$ for $x \in V$; then $\alpha_i^\vee(wC(\Pi^\vee)^\circ) > 0$ for all $i \in I$. Hence $C(\Pi^\vee)^\circ \supseteq C(w^\vee\Pi^\vee)^\circ = wC(\Pi^\vee)^\circ$. Thus $C(\Pi^\vee)^\circ = wC(\Pi^\vee)^\circ$. On the other hand, if $w^\vee\alpha_i^\vee(C(\Pi^\vee)^\circ) < 0$ for some $i \in I$, then $wC(\Pi^\vee)^\circ \cap C(\Pi^\vee)^\circ \subseteq -D^\circ_{\alpha_i^\vee} \cap D^\circ_{\alpha_i^\vee} = \emptyset$.

Conversely, assume that $wC(\Pi^\vee)^\circ \cap C(\Pi^\vee)^\circ = \emptyset$ or $wC(\Pi^\vee)^\circ = C(\Pi^\vee)^\circ$. Then in first instance, $wH_{\alpha_i^\vee} \cap C(\Pi^\vee)^\circ = \emptyset$ for $i \in I$. In the second instance, $wH_{\alpha_i^\vee}$ intersects only the envelope $C(\Pi^\vee) \setminus C(\Pi^\vee)^\circ$ of $C(\Pi^\vee)$, and again $wH_{\alpha_i^\vee} \cap C(\Pi^\vee)^\circ = \emptyset$ for $i \in I$.

Finally consider that $C(\Pi^\vee)$ is a regular chamber. Suppose that $H_r \cap wC(\Pi^\vee)^\circ \neq \emptyset$ for some reflection $r \in W(S(\Pi^\vee))$ and $w \in W(S(\Pi^\vee))$. Then $rwC(\Pi^\vee) = wC(\Pi^\vee)$. But then the regularity of $C(\Pi^\vee)$ implies that $w^{-1}rw = 1$ and so $r = 1$. Hence $H_r \cap C(\Pi^\vee)^\circ = \emptyset$. Q.E.D.

Take $\Pi^\vee = \{\alpha_i^\vee \mid i \in I\} \subseteq V^\vee$, and let $S(\Pi^\vee)$ be a set of reflections s_i, $i \in I$, in $\mathrm{GL}(V)$ each with coroot $\alpha_i^\vee$ in $\Pi^\vee$. Suppose that $C(\Pi^\vee)$ is a polyhedral cone. Let $\Sigma^\vee(W(S(\Pi^\vee)))$ be the set of coroots of the reflections in $W(S(\Pi^\vee))$. To each $\alpha^\vee \in \Sigma^\vee(W(S(\Pi^\vee)))$ such that $H_{\alpha^\vee} \cap C(\Pi^\vee)^\circ = \emptyset$, either $\alpha^\vee(C(\Pi^\vee)^\circ) > 0$ or $\alpha^\vee(C(\Pi^\vee)^\circ) < 0$. Let

$$(8)\quad \Sigma^{\vee+}(W(S(\Pi^\vee))) = \{\alpha^\vee \in \Sigma^\vee(W(S(\Pi^\vee))) \mid \alpha^\vee(C(\Pi^\vee)^\circ) > 0\}.$$

The elements of $\Sigma^{\vee+}(W(S(\Pi^\vee)))$ will be said to be *positive* with respect to $C(\Pi^\vee)$. Because $\Pi^\vee \subseteq \Sigma^{\vee+}(W(S(\Pi^\vee)))$, the following proposition follows from Proposition 2.1.

Proposition 2.2. *A polyhedral cone $C(\Pi^\vee)$ with base $\Pi^\vee$ is a regular chamber if and only if*

$$(9)\qquad C(\Pi^\vee) = \bigcap_{\alpha^\vee \in \Sigma^{\vee+}(W(S(\Pi^\vee)))} D_{\alpha^\vee}.$$

To each $\beta^\vee \in W(S(\Pi^\vee))^\vee\Pi^\vee$, $s_{\beta^\vee} = s_{w^\vee\alpha^\vee} = ws_{\alpha^\vee}w^{-1}$ is in $W(\Pi^\vee))$. So for all $H_{\beta^\vee}$ such that $\beta^\vee \in W(S(\Pi^\vee))^\vee\Pi^\vee$ and $H_{\beta^\vee} \cap C(\Pi^\vee)^\circ = \emptyset$, either $\beta^\vee(C(\Pi^\vee)^\circ) > 0$ or $s_{\beta^\vee}\beta^\vee(C(\Pi^\vee)) > 0$. Set $\Sigma^\vee(\Pi^\vee) = \{\beta^\vee \in \Sigma^\vee(W(S(\Pi^\vee))) \mid H_{\beta^\vee} \cap C(\Pi^\vee)^\circ = \emptyset\}$ and set $\Sigma^{\vee+}(\Pi^\vee) = \Sigma^\vee(\Pi^\vee) \cap \Sigma^{\vee+}(W(S(\Pi^\vee)))$. Then $C(\Pi^\vee)$ is a chamber of

$W(S(\Pi^\vee))$ if and only if $\Sigma^\vee(\Pi^\vee) = W(S(\Pi^\vee))\Pi^\vee$. This is equivalent to having $D_{\beta^\vee} \supseteq C(\Pi^\vee)$ for $\beta^\vee \in \Sigma^{\vee +}(\Pi^\vee)$. But $\Pi^\vee \subseteq \Sigma^\vee(\Pi^\vee)$; so the following proposition follows.

Proposition 2.3. *A polyhedral cone $C(\Pi^\vee)$ with base $\Pi^\vee$ is a chamber for $W(S(\Pi^\vee))$ if and only if*

$$C(\Pi^\vee) = \bigcap_{\beta^\vee \in \Sigma^{\vee +}(\Pi^\vee)} D_{\beta^\vee}. \tag{10}$$

2.3. Dihedral Groups

The argument which we present is directed towards the utilization of Theorem 3.1 which establishes that $(W(S(\Pi^\vee)), S(\Pi^\vee))$ is a Coxeter system if each $C(\Pi^\vee_{ij})$ is a regular chamber, $\Pi^\vee_{ij}$ being any pair contained in $\Pi^\vee$. Thus the case where $W(S(\Pi^\vee))$ is a dihedral group requires special attention.[2]

Theorem 2.4. *Let $S = \{r, s\}$ where r and s are reflections in $\mathrm{GL}(V)$. Respectively, let $\alpha^\vee, \alpha$ and $\beta^\vee, \beta$ be coroot and root pairs for r and s. Let $\Pi^\vee = \{\alpha^\vee, \beta^\vee\}$, and let $C(\Pi^\vee)$ be the dihedral cone given by $C(\Pi^\vee) = D_{\alpha^\vee} \cap D_{\beta^\vee} \cap T$ where T is a $W(S)$-invariant subset of V and $S = S(\Pi^\vee)$. The following conditions on the roots and coroots of r and s are necessary and sufficient for $C(\Pi^\vee)$ to be a chamber for the action of $W(S)$ on T.*

$$\langle \alpha^\vee, \beta \rangle \leq 0 \text{ and } \langle \beta^\vee, \alpha \rangle \leq 0, \tag{11}$$

$$\langle \alpha^\vee, \beta \rangle = 0 \text{ if and only if } \langle \beta^\vee, \alpha \rangle = 0, \tag{12}$$

$$\langle \alpha^\vee, \beta \rangle \langle \beta^\vee, \alpha \rangle = 4\cos^2 \frac{\pi}{n}, \tag{13}$$

${}^{\vee}_{\alpha}n \in \mathbb{Z} \setminus \{0\}$, when $\langle \alpha^\vee, \beta \rangle \langle \beta^\vee, \alpha \rangle \leq 4$. Furthermore, $W(S(\Pi^\vee))$ is finite if and only if (13) holds. If $C(\Pi^\vee)$ is a chamber, then it is a regular chamber.

Proof. Since $D_{\alpha^\vee} \cap D_{\beta^\vee}$ is a chamber for the action of $W(S(\Pi^\vee))$ on V if and only if $D_{\alpha^\vee} \cap D_{\beta^\vee} \cap T$ is also a chamber for the action of $W(S(\Pi^\vee))$ on T, we take $T = V$. Thus $C(\Pi^\vee) = D_{\alpha^\vee} \cap D_{\beta^\vee}$. Let $V_0 = H_{\alpha^\vee} \cap H_{\beta^\vee}$. Then V_0 is the fixed subspace for the action of $W(S)$ on V, and $V_o \subseteq C(\Pi^\vee)$. Clearly $W(S)$ acts faithfully on V/V_0 and $C(\Pi^\vee)/V_0$ is a chamber of $W(S)$ on V/V_0 if and only if $C(\Pi^\vee)$ is a chamber on V. Without loss of generality, we may assume that $V_0 = 0$. Then $\dim V = 2$, and $C(\Pi^\vee)$ is bounded by the half lines $K_{\alpha^\vee} = H_{\alpha^\vee} \cap$

[2] This result clarifies a result stated by Vinberg [6].

$C(\Pi^\vee)$ and $K_{\beta^\vee} = H_{\beta^\vee} \cap C(\Pi^\vee)$. Set $C_s(\Pi^\vee) = C(\Pi^\vee) \cup sC(\Pi^\vee)$. Since $C(\Pi^\vee) \cap sC(\Pi^\vee) = K_{\beta^\vee}$, $C_s(\Pi^\vee)$ is the sector in V that is bounded by $K_{\alpha^\vee}$ and $sK_{\alpha^\vee}$.

Consider first that $C(\Pi^\vee)$ is a chamber and that $\langle \alpha^\vee, \beta \rangle \geq 0$. Let $\mathbb{R}^+$ be the set of positive real numbers. Then (4) implies that $\mathbb{R}^+\beta \subseteq C(\Pi^\vee)$. Hence $-\mathbb{R}^+\beta = s\mathbb{R}^+\beta \subseteq sC(\Pi^\vee)$. Because $C_s(\Pi^\vee)$ contains $\mathbb{R}\beta = \mathbb{R}^+\beta \cup -\mathbb{R}^+\beta$, the angle θ_s from $K_{\alpha^\vee}$ to $sK_{\alpha^\vee}$ satisfies $\theta_s \geq \pi$. But $sH_{\alpha^\vee} \cap C(\Pi^\vee)^o = \emptyset$; so $H_{\alpha^\vee} \cap sC(\Pi^\vee)^o = \emptyset$. Therefore $\theta_s = \pi$. Hence $H_{\alpha^\vee} \supseteq \mathbb{R}\beta$, which is equivalent to $\langle \alpha^\vee, \beta \rangle = 0$. Because $H_{\alpha^\vee}$ is a wall of $C_s(\Pi^\vee)$, $V = C_s(\Pi^\vee) \cup sC_s(\Pi^\vee) = C(\Pi^\vee) \cup sC(\Pi^\vee) \cup rC(\Pi^\vee) \cup rsC(\Pi^\vee)$. Consequently $W(S)$ is a fours group; so $rs = sr$. This implies $\mathbb{R}\alpha \subseteq H_{\beta^\vee}$; thus $\langle \beta^\vee, \alpha \rangle = 0$. Likewise $\langle \alpha^\vee, \beta \rangle = 0$ is a consequence of $\langle \beta^\vee, \alpha \rangle \geq 0$. This establishes (11) and (12). The condition (13) is established at the end of this argument.

Now consider that (11), (12) and (13) hold. If $\langle \alpha^\vee, \beta \rangle = \langle \beta^\vee, \alpha \rangle = 0$, then $W(S)$ must be a fours group, in which case, $C(\Pi^\vee)$ is a regular chamber. So consider that $\langle \alpha^\vee, \beta \rangle < 0$ and $\langle \beta^\vee, \alpha \rangle < 0$. Replace the pair $\beta^\vee, \beta$ by the pair $c\beta^\vee, c^{-1}\beta$ where $c^2 = \frac{\langle \alpha^\vee, \beta \rangle}{\langle \beta^\vee, \alpha \rangle}$. Then $\langle \alpha^\vee, \beta \rangle = \langle \beta^\vee, \alpha \rangle$, and $C(\Pi^\vee)$ remains unchanged along with $\langle \alpha^\vee, \beta \rangle \langle \beta^\vee, \alpha \rangle$. Let $\phi : V^\vee \to V$ be the correlation that is defined by $\phi : \alpha^\vee \mapsto \alpha$and $\phi : \beta^\vee \mapsto \beta$. Let $f : V \times V \to \mathbb{R}$ be the bilinear form that is given by setting $f(x, y) = \langle \phi^{-1}(x), y \rangle$. Then f is $W(S)$-invariant and symmetric. Also $\langle \alpha^\vee, \beta \rangle = f(\alpha, \beta)$. By (4), $f(\alpha, \alpha) = f(\beta, \beta) = 2$; set $a = f(\alpha, \beta)$. The discriminant of f is $4 - a^2 = 4 - \langle \alpha^\vee, \beta \rangle \langle \beta^\vee, \alpha \rangle$. So f is indefinite, degenerate or positive definite according as $a^2 > 4$, $a^2 = 4$, or $a^2 < 4$. Let $u = sr$, and set $U = \langle u \rangle$. Since $|W(S)| > 4$, $u^2 \neq 1$. The discriminant of the characteristic polynomial of u is $a^2(4 - a^2)$. So u has 2, 1, or 0 eigenspaces according as f is indefinite, degenerate or positive definite. In the first two cases, u has real eigenvalues; so $|u| = \infty$. Then u and u^2 have the same eigenspaces. These must be the isotropic lines of f.

When $\langle \alpha^\vee, \beta \rangle \langle \beta^\vee, \alpha \rangle > 4$, f is indefinite, its isotropic lines divide V into four sectors V_1, V_2, V_3, V_4, which are permuted by the group $W(S)/U$. These lines are interchanged by r and s; hence they are the eigenspaces for u. As $C_s(\Pi^\vee) \cap sC_s(\Pi^\vee) = uK_{\alpha^\vee} = tK_{\alpha^\vee}$, $C_s(\Pi^\vee)$ is contained in one of these sectors, say, V_1. It follows then that $V_1 = \bigcup_{n=-\infty}^{n=\infty} u^n C_s(\Pi^\vee)$ and that U acts regularly on $\{u^n C_s(\Pi^\vee) \mid n \in \mathbb{Z}\}$. From this, it follows that $W(S)$ acts regularly on $\{wC(\Pi^\vee) \mid w \in W(S)\}$. Therefore $C(\Pi^\vee)$ is a regular chamber.

The situation is similar when $\langle \alpha^\vee, \beta \rangle \langle \beta^\vee, \alpha \rangle = 4$and f is degenerate. The difference is that in this case there two sectors V_1 and V_2 which are separated by the unique isotropic line. This forces $\mathbb{R}\alpha = \mathbb{R}\beta$.

Next suppose that $\langle\alpha^{\vee},\beta\rangle\,\langle\beta^{\vee},\alpha\rangle < 4$, in which case f is positive definite and $W(S)$ is finite. Then f gives rise to a scalar product[3] where $a = \alpha\cdot\beta = 2\cos\theta$ and θ is the angle between the half lines $\mathbb{R}^{+}\alpha$ and $\mathbb{R}^{+}\beta$. The difference $\theta_0 = \Pi - \theta$ is the angle between the half lines $K_{\alpha^{\vee}}$ and $K_{\beta^{\vee}}$ and hence θ_0 is the angle of the sector $C(\Pi^{\vee})$. So $2\theta_0$ is the angle of the sector $C_s(\Pi^{\vee})$, which is also the angle of the rotation u. Let n be the least positive integer such that $C_s(\Pi^{\vee}) \cap u^{n}C_s(\Pi^{\vee}) \neq \emptyset$. Then $C_s(\Pi^{\vee})$ is a chamber for U if and only if $2\theta n = 2\pi$. This is equivalent to having $\langle\alpha^{\vee},\beta\rangle\langle\beta^{\vee},\alpha\rangle = f(\alpha,\beta)^2 = a^2 = 4\cos^2\frac{\pi}{n}$ where $n \in \mathbb{Z}\setminus\{0\}$. Clearly $C_s(\Pi^{\vee})$ is a chamber for U if and only if $C(\Pi^{\vee})$ is a chamber for $W(S)$. This proves that $C(\Pi^{\vee})$ is a chamber as well as showing that (13) is a consequence of $C(\Pi^{\vee})$ being a chamber. Since $|\mathcal{C}(W(S))| = |W(S)|$, $C(\Pi^{\vee})$ is also regular.

Finally, note that is finite if and only if u has no real eigenvalues, which is equivalent to (13) Also we have shown that (12), (11) and (13) imply that $C(\Pi^{\vee})$ is regular and that these conditions are implied when $C(\Pi^{\vee})$ is a chamber, in which case it must be regular. Q.E.D.

§3. Characterizations

3.1. Characterization of Linear Coxeter groups

The next result is due to J. Tits [5]. This argument was developed from his result which establishes the contragredient representation of a Coxeter group (*cf.* Bourbaki [1, V, §4.4] or Humphreys [4, p. 126]).

Theorem 3.1. *Let S be a set of reflections s_i, $i \in I$, in* $\mathrm{GL}(V)$ *and let $\alpha_i^{\vee}, \alpha_i$ be a paired coroot and root of s_i. Set $\Pi^{\vee} = \{\alpha_i^{\vee} \mid i \in I\}$ and $\Pi = \{\alpha_i \mid i \in I\}$. Let T be a $W(S)$-invariant subset of V. Suppose that $C(\Pi^{\vee})$ is a chamber for the action of $W(S(\Pi^{\vee}))$ on T such that $C(\Pi^{\vee}_{ij})$ is a regular chamber for $W(S(\Pi_{ij}))$ for each pair $\Pi^{\vee}_{\iota j} = \{\alpha_i^{\vee},\alpha_j^{\vee}\} \subseteq \Pi^{\vee}$. Then $(W(S),S)$ is a Coxeter system, and $W(S)$ is a linear Coxeter group acting on T.*

Proof. The proof of Theorem 3.1 as we have stated it is obtained from Tits [5, Lemme 1]. Tits' argument is centered about the proof of the following statement[4]:

[3] *cf.* Bourbaki [1, V, §2.3].

[4] Actually by replacing w by sw,the second statement becomes a consequence of the first; so the argument is directed to proving the first statement. Also Tits' statement does not require that s be a reflection.

(P) *Let $w \in W(S)$. Then, given $s \in S$ with coroot $\alpha_s^\vee$, either $wC(\Pi^\vee) \subseteq sD_{\alpha_s^\vee}$ and $\ell(sw) = \ell(w) - 1$ or $wC(\Pi^\vee) \subseteq D_{\alpha_s^\vee}$ and $\ell(sw) = \ell(w) + 1$.*

where $\ell(w)$ is the number of factors from S in a shortest expression of w as a product of elements of S. The argument is by induction on $\ell(w)$. Assuming that *(P)* holds for each dihedral group $W(S(\Pi_{ij}^\vee))$, $i, j \in I$, Tits argues by induction on $\ell(w)$ that *(P)* holds for $W(S)$. Either Lemma 1 of [1, V, §4.5] or the description of the action of $W(S(\Pi_{ij}^\vee))$ on its chambers given in Theorem 2.4 can be used to establish *(P)* for the subgroups $W(S(\Pi_{ij}^\vee))$. The condition *(P)* for the group $W(S)$ immediately implies the regularity of its chambers in the following way. Suppose that $w(C(\Pi^\vee) = C(\Pi^\vee)$ for some $w \in W(S)$. Then $wC(\Pi^\vee) \subseteq D_{\alpha_i^\vee}$ for all $i \in I$. So by *(P)*, $\ell(s_{\alpha_j^\vee} w) = \ell(w) + 1$ for all $s_{\alpha_j^\vee} \in S$. But this fails when $w \neq 1$ since there exist $\alpha_j^\vee \in \Pi^\vee$ such that $\ell(s_{\alpha_j^\vee} w) < \ell(w)$. Because $W(S)$ can be regarded as a Coxeter group acting on the chamber system $\mathcal{C}(W(S))$ the above argument also shows that this action is effective. Hence $(W(S), S)$ is a Coxeter system. Q.E.D.

Let $S = \{s_i \mid i \in I\}$ be a set of reflections of a reflection group W. Let $\alpha_i^\vee$ and α_i respectively be paired coroots and roots for s_i, $i \in I$. Set $\Pi^\vee = \{\alpha_i^\vee \mid i \in I\}$ and $\Pi = \{\alpha_i \mid i \in I\}$. We say that the sets $\Pi^\vee$ and Π have the *Cartan property* if every pair $(\alpha_i^\vee, \alpha_j)$, $i, j \in I$, $i \neq j$, satisfies the conditions (11), (12) and (13) of Theorem 2.4. A direct application of Theorem 3.1 and Theorem 2.4 gives the following corollary.

Corollary 3.2. *Let S be a set of reflections s_i, $i \in I$, in $\mathrm{GL}(V)$ and let $\alpha_i^\vee, \alpha_i$ be a coroot and root of s_i. Set $\Pi^\vee = \{\alpha_i^\vee \mid i \in I\}$ and $\Pi = \{\alpha_i \mid i \in I\}$. Suppose that $C(\Pi^\vee)$ is a polyhedral cone in a $W(S)$-invariant subset T of V. If $C(\Pi^\vee)$ is a chamber for the action of $W(S)$ on T and if $\Pi^\vee$ and Π have the Cartan property, then $W(S)$ is a linear Coxeter group.*

Theorem 3.3. *Let S be a set of reflections s_i, $i \in I$, in $\mathrm{GL}(V)$ and let $\alpha_i^\vee$ and α_i, respectively, be a paired coroot and root of r_i. Set $\Pi^\vee = \{\alpha_i^\vee \mid i \in I\}$ and $\Pi = \{\alpha_i \mid i \in I\}$ so that $S = S(\Pi^\vee)$. Let $C(\Pi^\vee)$ be a chamber for the action of $W(S)$ on a $W(S)$-invariant subset T, and let $\Pi^\vee$ be a base for $C(\Pi^\vee)$. Then the sets $\Pi^\vee$ and Π have the Cartan property, and $W(S(\Pi^\vee))$ is a linear Coxeter group acting on T.*

Proof. For each pair $\Pi_{ij}^\vee = \{\alpha_i^\vee, \alpha_j^\vee\} \subseteq \Pi^\vee$, we argue that $C(\Pi_{ij}^\vee)$ is a chamber for $W(S(\Pi_{ij}^\vee))$. By (10), $C(\Pi^\vee) = \bigcap \{D_{\alpha^\vee} \mid \alpha^\vee \in \Sigma^{\vee+}(\Pi^\vee)\}$. It is required to show that $H_{\alpha^\vee} \cap C(\Pi_{ij}^\vee)^\circ = \emptyset$ for $\alpha^\vee \in \Sigma^{\vee+}(\Pi_{ij}^\vee)$. So suppose that for some $\alpha^\vee \in \Sigma^{\vee+}(\Pi_{ij}^\vee)$, $H_{\alpha^\vee} \cap C(\Pi_{ij}^\vee)^\circ \neq \emptyset$. Now

$C(\Pi^\vee) \subseteq C(\{\alpha_k^\vee, \alpha\})$ where $k = i$ or j. For definiteness, suppose $k = i$. Let $V_0 = H_{\alpha_i^\vee} \cap H_{\alpha_j^\vee}$; then $H_{\alpha^\vee} \supseteq V_0$ and $H_{\alpha_j^\vee} \cap C(\{\alpha^\vee, \alpha_i^\vee\}) = V_0$. Hence $H_{\alpha_j^\vee} \cap C(\Pi^\vee)^\circ = \emptyset$ inasmuch as $C(\Pi^\vee)^\circ \subseteq C(\{\alpha^\vee, \alpha_k^\vee\})$. In particular, this implies that $F^\circ_{\alpha_j^\vee}(\Pi^\vee) \cap C(\Pi^\vee) = \emptyset$. But $\Pi^\vee$ is a base; so we have a contradiction. Therefore, $C(\Pi_{ij}^\vee)$ is a chamber for $W(S(\Pi_{ij}^\vee))$. By Theorem 2.4, it is a regular chamber and $\Pi_{ij}^\vee$ and $\Pi_{ij} = \{\alpha_i, \alpha_j\}$ have the Cartan property. Thus also $\Pi^\vee$ and Π have the Cartan property. Corollary 3.2 implies that $W(S(\Pi^\vee))$ is a linear Coxeter group. Q.E.D.

3.2. The Tits Cone

In this section, all linear Coxeter groups will be regarded as acting on V. We consider a linear Coxeter group $W(S)$ where S is the set of reflections $S = \{s_i \mid i \in I\}$, and $C(\Pi^\vee)$ is a regular chamber such that $\Pi^\vee = \{\alpha_i^\vee \mid i \in I\}$, $\alpha_i^\vee$ being a coroot of s_i. For $\emptyset \subset J \subseteq I$, set $V_J = \bigcap_{j \in J} H_{\alpha_j^\vee}$; then $V_\emptyset = V$ and $\Pi_\emptyset^\vee = \emptyset$. Set $F_J = C(\Pi^\vee) \cap V_J$ and

$$(14) \qquad F_J^\circ(\Pi^\vee) = C(\Pi \setminus \Pi_J^\vee)^\circ \cap V_J$$

where $\emptyset \subseteq J \subseteq I$. The subset $F_J^\circ(\Pi^\vee)$ is called a *facet* of $C(\Pi^\vee)$ provided that it is nonempty. Then $C(\Pi^\vee) = \bigcup_{\emptyset \subseteq J \subseteq I} F_J^\circ(\Pi^\vee)$. The subspace V_j is said to be the *support* of $F_J(\Pi^\vee)$ and $F_J^\circ(\Pi^\vee)$. The subgroup $W_J = \langle s_j \mid j \in J\rangle$ is called a *parabolic* subgroup of $W(S)$. Set $\Pi_J^\vee = \{\alpha_j^\vee \in \Pi^\vee \mid j \in J\}$. Theorem 3.1 implies that W_J is a linear Coxeter group for which $C(\Pi_J^\vee)$ is a chamber. Since W_J leaves fixed V_J, it also leaves fixed $F_J(\Pi^\vee)$. If $\emptyset \subseteq J \subset K \subseteq I$, then $V_J \supseteq V_K$. Let J^* be the subset of I such that $H_{\alpha_j^\vee} \supseteq V_J$ for $j \in J^*$. Then J^* is the maximal subset of I such that $V_{J^*} = V_J$. Hence $\alpha_j^\vee(F_J^\circ(\Pi^\vee)) = 0$ for all $j \in J^*$. So $F_J^\circ(\Pi^\vee) = V_J \cap C(\Pi^\vee \setminus \Pi_J^\vee)^\circ = V_{J^*} \cap C(\Pi^\vee \setminus \Pi_{J^*}^\vee)^\circ = F_{J^*}^\circ(\Pi^\vee)$. Let $\mathcal{M}(\Pi^\vee)$ be the set of such maximal subsets J^* of I. Thus the set $\mathcal{F}(C(\Pi^\vee))$ of facets contained in $C(\Pi^\vee)$ is given by $\mathcal{F}(C(\Pi^\vee)) = \{F_J^\circ(\Pi^\vee) \mid J \in \mathcal{M}(\Pi^\vee)\}$. It is clear that the facets in $\mathcal{F}(C(\Pi^\vee))$ are mutually disjoint and that $C(\Pi^\vee) = \bigcup \{F_J^\circ(\Pi^\vee) \mid F_j(\Pi^\vee) \in \mathcal{F}(\mathcal{C}(\Pi^\vee))\}$.

Set

$$(15) \qquad T(W(S)) = \bigcup_{w \in W(S)} wC(\Pi^\vee).$$

Denote the complement of the envelope of the convex hull of $T(W(S))$ by $T(W(S))^\circ$. The set $T(W(S))$ is convex. Consequently $T(W(S))$ is called a *Tits cone*. For $w \in W(S)$ and $\emptyset \subset J \subseteq I$, $wF_J^\circ(\Pi^\vee)$ is a facet of $wC(\Pi^\vee)$ with support wV_J. The corresponding parabolic subgroup is wW_Jw^{-1}. Designate $\mathcal{F}(W(S))$ to be the set of facets of the chambers of $W(S)$. By (15),

$$T(W(S)) = \bigcup \mathcal{F}(W(S)). \tag{16}$$

Standard arguments[5] give the next two propositions and, together with (16), show that two chambers in $\mathcal{C}(W(S))$ can intersect only in a common facet and that the decomposition (16) is a partition of $T(W(S))$.

Proposition 3.4. *Let $F_J^\circ(\Pi^\vee)$, $F_K^\circ(\Pi) \in \mathcal{F}(C(\Pi^\vee))$ and take $w \in W(S)$. Then if $F_J^\circ(\Pi^\vee) \cap wF_K^\circ(\Pi^\vee) \neq \emptyset$, $J = K$ and $w \in W_J$. In particular, for $wF_J^\circ(\Pi^\vee) \in \mathcal{F}(W(S))$,*

$$wW_Jw^{-1} = \{u \in W(S) \mid uwF_J^\circ(\Pi^\vee) = wF_J^\circ(\Pi^\vee)\}.$$

Proposition 3.5. *$T(W(S))$ is convex.*

Proposition 3.6. *Let $W(S)$ be any linear Coxeter group acting on V. Let $C(\Pi^\vee)$ be a chamber for $W(S)$ with a base $\Pi^\vee$. Then $W(S)$ is finite if and only if $-C(\Pi^\vee) \subseteq T(W(S))$ and thus if and only if $T(W(S)) = V$.*

Proof. The convex hull of $C(\Pi^\vee) \cup -C(\Pi^\vee)$ is V. So $T(W(S)) = V$ if and only if $-C(\Pi^\vee) \subseteq T(W(S))$. Let $\Pi^\vee = \{\alpha_i^\vee \mid i \in I\}$ where $S = \{s_i \mid i \in I\}$ and $\alpha_i^\vee$ is a coroot of s_i. It is well-known[6] that a linear Coxeter group $W(S)$ with a finite set S of generating reflections is finite if and only if $-C(\Pi^\vee) \subseteq T(W(S))$. Of course, if $W(S)$ is finite, then S is finite. Therefore, it remains to show that if $-C(\Pi^\vee)$ is a chamber for $W(S)$, then S is finite. So assume that there exists $w_0 \in W(S)$ such that $w_0C(\Pi^\vee) = -C(\Pi^\vee)$. Then $w_0C(\Pi^\vee) \subseteq s_iD_{\alpha_i^\vee} = -D_{\alpha_i^\vee}$ for all $i \in I$. However, by *(P)* of §3.1, this occurs only if s_i appears in a reduced expression of w_0 as a product of reflections in S. Since $\ell(w) < \infty$, this implies that S is finite. Q.E.D.

If W_J is finite, then $F_J^\circ(\Pi^\vee)$ is said to have *finite type.* Set $\mathcal{E}(W(S))$ to be the subset of $\mathcal{F}(W(S))$ consisting of facets of finite type. Clearly $\mathcal{E}(W(S))$ is $W(S)$-invariant. Finally set

$$E(W(S)) = \bigcup \mathcal{E}(W(S)) \tag{17}$$

[5] *cf.* [1, V, §4.6]. This argument is an induction based on the mutual disjointness of the facets in $\mathcal{F}(C(\Pi^\vee))$.

[6] *cf.* [1, Ex. 2, p.130]. This exercise pertains to the present situation since *(P) of* §3.1 is available.

Define the *star* of a facet $wF_J^{\circ}(\Pi^{\vee})$ to be the subset

$$\operatorname{st} wF_J^{\circ}(\Pi^{\vee}) = \{uF_K^{\circ}(\Pi^{\vee}) \in \mathcal{F}(W(S)) \mid uF_K(\Pi^{\vee}) \supseteq wF_J^{\circ}(\Pi^{\vee})\}$$

of $\mathcal{F}(W(S))$. It is clear that $uC(\Pi^{\vee}) = uF_{\emptyset}^{\circ}(\Pi^{\vee}) \supseteq uF_K(\Pi^{\vee})$. Therefore the facets in $\operatorname{st} wF_J^{\circ}(\Pi^{\vee})$ are those that are contained in a chamber $uC(\Pi^{\vee}) = C(u^{\vee}\Pi^{\vee})$ for which $u^{\vee}\Pi^{\vee} \supseteq w^{\vee}\Pi_J^{\vee}$. Set

$$(18) \qquad \mathcal{C}(wF_J^{\circ}(\Pi^{\vee})) = \{C \in \mathcal{C}(W(S)) \mid C^{\circ} \in \operatorname{st} wF_J^{\circ}(\Pi^{\vee})\}.$$

Each chamber $C \in \mathcal{C}(wF_J^{\circ}(\Pi^{\vee}))$ has the form $C = uwC(\Pi^{\vee})$ for some $u \in W(S)$. In particular, we may take $u = 1$ since clearly $wC(\Pi^{\vee})$ is in $\mathcal{C}(wF_J^{\circ}(\Pi^{\vee}))$. Any two chambers $v_1wC(\Pi^{\vee})$ and $v_2wC(\Pi^{\vee})$ in $\mathcal{C}(wF_J^{\circ}(\Pi^{\vee}))$ intersect in $F_{12} = v_1wC(\Pi^{\vee}) \cap v_2wC(\Pi^{\vee})$ where $F_{12}^{\circ} \in \operatorname{st} wF_J^{\circ}(\Pi^{\vee})$. For $wF_J^{\circ}(\Pi^{\vee}) \in \mathcal{F}(W(S))$, set

$$(19) \qquad N(wF_J^{\circ}(\Pi^{\vee})) = \bigcup \mathcal{C}(wF_J^{\circ}(\Pi^{\vee})).$$

Theorem 3.7. *Let $F^{\circ} = F_J^{\circ}(\Pi^{\vee}) \in \mathcal{F}(W(S))$ where $\Pi^{\vee} = \{\alpha_i^{\vee} \mid i \in I\}$, and let $uC(\Pi^{\vee}) = C(u^{\vee}\Pi^{\vee}) \in \mathcal{C}(F^{\circ})$ where $u \in W(S)$, Set $J_u = \{j \in I \mid u^{\vee}\alpha_j^{\vee}(F^{\circ}) = 0\}$ and $K_u = I \setminus J_u = \{j \in I \mid u^{\vee}\alpha_k^{\vee}(F^{\circ}) > 0\}$. Set $\Gamma^{\vee} = \bigcup \{u^{\vee}\Pi_{K_u}^{\vee} \mid C(u^{\vee}\Pi^{\vee}) \in \mathcal{C}(F^{\circ})\}$. Then the following holds.*

(i) *$uC(\Pi_{J_u}^{\vee}) \in \mathcal{C}(W_J)$. When $C' \in \mathcal{C}(W_J)$, then $C' \cap C(\Gamma^{\vee}) \in \mathcal{C}(F^{\circ})$, and $\mathcal{C}(\mathcal{F}^{\circ}) = \{uC(\Pi^{\vee}) \mid u \in W_J\}$.*

(ii) *$N(F^{\circ}) = C(\Gamma^{\vee}) \subseteq T(W_J)$, and $\Gamma^{\vee}$ is a base for the polyhedral cone $C(\Gamma^{\vee})$ where $\Gamma^{\vee} = \bigcup \{(u^{\vee}\Pi_{K_u}^{\vee}) \mid u \in W_J\}$.*

(iii) *$F^{\circ} \subseteq N(F^{\circ})^{\circ}$ if and only if $F^{\circ} \in \mathcal{E}(W(S))$.*

Proof. (i) The hyperplanes $H_{u^{\vee}\alpha_j^{\vee}}$, $\alpha_j^{\vee} \in \Pi_{J_u}^{\vee}$ are hyperplanes of reflections $r_{u^{\vee}\alpha_j^{\vee}} \in W_J$. Clearly $uC(\Pi_{J_u}^{\vee})$ is a polyhedral cone. It is a chamber for W_J, for otherwise there would exist $H_r \in \mathcal{H}(W_J)$ such that $H_r \cap uC(\Pi_{J_u}^{\vee})^{\circ} \neq \emptyset$ in contradiction to $H_r \cap uC(\Pi^{\vee})^{\circ} = \emptyset$. On the other hand, if $C' \in \mathcal{C}(W_J)$. Then $C' \supseteq V_J \supseteq F^{\circ}$; hence it contains a chamber $C_1 \in \mathcal{C}(F^{\circ})$. Since the chambers in $\mathcal{C}(F^{\circ})$ belong to distinct chambers of the stabilizer of F°, which is W_J, C' contains only one chamber of $W(S)$. This forces $C' \cap C(\Gamma^{\vee}) \in \mathcal{C}(F^{\circ})$. Clearly $C(\Pi^{\vee}) \in \mathcal{C}(F^{\circ})$; so $\Pi^{\vee} = \Pi_{J_1}^{\vee} \cup \Pi_{K_1}^{\vee}$ and $\mathcal{C}(\mathcal{F}^{\circ}) = \{uC(\Pi^{\vee}) \mid u \in W_J\}$ inasmuch as $\mathcal{C}(W_J) = \{uC(\Pi_{J_1}^{\vee}) \mid u \in W_J\}$.

(ii) Now $\Gamma^{\vee} = \bigcup \{(u^{\vee}\Pi_{K_u}^{\vee}) \mid uC(\Pi^{\vee}) \supseteq F^{\circ}\}$. But because $F^{\circ} \not\subseteq H_{u^{\vee}\alpha_k^{\vee}}$ for $u^{\vee}\alpha_{\vee} \in \Gamma^{\vee}$, $F^{\circ} \subseteq D_{u^{\vee}\alpha^{\vee}}^{\circ}$. But then $uC(\Pi^{\vee}) \subseteq D_{u^{\vee}\alpha^{\vee}}^{\circ}$ for $uC(\Pi^{\vee}) \in \mathcal{C}(F^{\circ})$. Thus $N(F^{\circ}) \subseteq C(\Gamma^{\circ})$. However, $T(W(S)) \subseteq T(W_J)$ and the set $\mathcal{C}(W_J)$ partitions $T(W_J)$. Then the set $\{C' \cap C(\Gamma^{\circ}) \mid C' \in \mathcal{C}(W_J)\}$ partitions $C(\Gamma^{\circ})$ into the set $\mathcal{C}(F^{\circ})$. Thus $N(F^{\circ}) = C(\Gamma^{\circ})$.

Now $\bigcup_{u^\vee\alpha_k^\vee\in\Gamma^\vee} F^{\mathrm{o}}_{u^\vee\alpha_k^\vee}(\Gamma^\vee)$ is the envelope $B(\Gamma^\vee)$ of $C(\Gamma^\vee)$, and each $F^{\mathrm{o}}_{u^\vee\alpha_k^\vee}(\Gamma^\vee)$ contains the face $F^{\mathrm{o}}_{u^\vee\alpha_k^\vee}(uC(\Pi^\vee)$ of $uC(\Pi^\vee)\in \operatorname{st} F^{\mathrm{o}}$. Consequently $F^{\mathrm{o}}_{u^\vee\alpha_k^\vee}(\Gamma^\vee)\neq\emptyset$; so for each $u^\vee\alpha_k^\vee\in\Gamma^\vee$, $F^{\mathrm{o}}_{u^\vee\alpha_k^\vee}(\Gamma^\vee)$ is a face of $C(\Gamma^\vee)$, and thus $\Gamma^\vee$ is a base.

(iii) Because $F^{\mathrm{o}}\subseteq V_J$, it is contained in the Tits cone $T(W_J)$ of W_J. But $F^{\mathrm{o}}\subseteq T(W_J)^{\mathrm{o}}$ if and only if $T(W_J)=V$. It follows from Proposition 3.6 that $T(W_J)=V$ if and only if W_J is finite, in which case $F^{\mathrm{o}}\in\mathcal{E}(W(S))$. So it remains to show that $F^{\mathrm{o}}\subseteq N(F^{\mathrm{o}})^{\mathrm{o}}$ if and only if $T(W_J)=V$. Now $T(W_J)\supseteq T(W(S))$. So $F^{\mathrm{o}}\not\subseteq T(W_J)^{\mathrm{o}}$ is equivalent to both $T(W_J)\neq V$ and $F^{\mathrm{o}}\not\subseteq N(F^{\mathrm{o}})^{\mathrm{o}}$. On the other hand, $F^{\mathrm{o}}\subseteq T(W_J)^{\mathrm{o}}$ is equivalent to $T(W_J)=V$ and thus to having the envelope of $C(\Gamma^\vee)$ being contained in the walls $H_{\gamma^\vee}$, $\gamma\in\Gamma^\vee$, of $C(\Gamma^{\mathrm{o}})$. But $u^\vee\alpha_k^\vee(F^{\mathrm{o}})>0$ for all $u^\vee\alpha_k^\vee\in\Gamma^\vee$. This means that $F^{\mathrm{o}}\not\subseteq C(\Gamma^\vee)^{\mathrm{o}}=N(F^{\mathrm{o}})^{\mathrm{o}}$. Q.E.D.

Corollary 3.8. *Let $W(S)$ be a linear Coxeter group acting on V, and let $T(W(S))^{\mathrm{o}}$ be the interior of its Tits cone $T(W(S))$. Then $E(W(S))=T(W(S))^{\mathrm{o}}$.*

Proof. By virtue of Theorem 3.7, it follows that $F^{\mathrm{o}}\subseteq N(F^{\mathrm{o}})^{\mathrm{o}}=C(\Gamma^\vee)^{\mathrm{o}}$ if and only $F^{\mathrm{o}}\in\mathcal{E}(W(S))$ where $\Gamma^\vee$ is defined by (3.7). But $C(\Gamma^\vee)^{\mathrm{o}}\subseteq T(W(S))$. So $F^{\mathrm{o}}\subseteq T(W(S))^{\mathrm{o}}$ if $F^{\mathrm{o}}\in\mathcal{E}(W(S))$. On the other hand, if $F^{\mathrm{o}}\not\subseteq T(W(S))^{\mathrm{o}}$, then $F^{\mathrm{o}}\not\supseteq E(W(S))$, and it follows that $F^{\mathrm{o}}\not\subseteq T(wW_Jw^{-1})^{\mathrm{o}}$ where wW_Jw^{-1} is the subgroup of $W(S)$ that fixes F^{o}. As we argued in Theorem 3.7, this implies that W_J is infinite and so $F^{\mathrm{o}}\notin\mathcal{E}(W(S))$. Then $F^{\mathrm{o}}\not\subseteq E(W(S))$, and by (16), $T(W(S))^{\mathrm{o}}=E(W(S))$. Q.E.D.

3.3. Reflection Subgroups

A Coxeter group is given by a Coxeter system $(W(S),S)$, which specifies its presentation, and $W(S)$ may always be represented as a linear Coxeter group[7] by means of the contragredient representation. The involutions in $W(S)$ that correspond to the reflections in this representation are those that belong to the set R of the conjugates of the elements of S. Independently by M. Dyer [3] and V.V. Deodhar [2] showed that a subgroup of a Coxeter group that is generated by these involutions is again a Coxeter group. Also J. Tits has noted that Theorem 3.1 is applicable to this problem. Here we offer a direct proof that a reflection subgroup of a linear Coxeter group is a linear Coxeter group. This immediately implies that it is a Coxeter group. The importance of a direct proof lies in the geometrical insight which it provides, which is

[7] *cf.* Bourbaki [1].

useful when investigating particular reflection subgroups which can be identified by an explicit construction of the base of a chamber.

In this section, we work with a given linear Coxeter group $W = W(S)$ and a reflection subgroup W_0. We take $T = E(W)$ to be the underlying set T that is used to define the chambers of W and W_0 by means of (1).

Theorem 3.9. *Let W be a linear Coxeter group acting on V with a regular chamber $C(\Pi^\vee)$ that has a base $\Pi^\vee$. Let W_0 be a reflection subgroup of W that is generated by a set of reflections. Then W_0 is a linear Coxeter group with a chamber $C(\Pi_0^\vee)$ that contains $C(\Pi^\vee)$.*

Proof. Set

$$C_0 = \left(\bigcap_{\gamma^\vee \in \Sigma_0^{\vee +}} D_{\gamma^\vee} \right) \cap E(W). \tag{20}$$

It follows from Corollary 3.8 that $E(W) = T(W)^\circ$; so $C(\Pi^\vee)^\circ \neq \emptyset$. Because $C_0 \supseteq C(\Pi^\vee)^\circ$, it follows from (10) that C_0 is a chamber for W_0. By virtue of Theorem 3.3, it remains to show that C_0 has a base. Let $\Pi_0^\vee$ be the subset of $\Sigma_0^{\vee +}$ consisting of those coroots $\gamma^\vee$ such that $H_{\gamma^\vee}$ is a wall of a chamber $w_{\gamma^\vee} C(\Pi^\vee)$ of W that is contained in C_0; then $\gamma^\vee = w_{\gamma^\vee} \alpha_i^\vee$ for some $\alpha_i^\vee \in \Pi^\vee$ and

$$F_{\gamma^\vee}^\circ(\Pi_0^\vee) = H_{\gamma^\vee} \cap C(\Pi_0^\vee \setminus \{\gamma^\vee\})^\circ \supseteq H_{\gamma^\vee} \cap C(w_{\gamma^\vee}\Pi^\vee \setminus \{w_{\gamma^\vee}\alpha_i^\vee\})^\circ \neq \emptyset.$$

Therefore $\Pi_0^\vee$ is a base. By virtue of (20), $C(\Pi_0^\vee) \supseteq C_0$.

So it suffices to show that $C_0 \supseteq C(\Pi_0^\vee)$. Let B_0 be the envelope $C_0 \setminus C_0^\circ$ of C_0. By virtue of Theorem 3.4, $B_0 = \bigcup\{wF_J^\circ(\Pi) \in \mathcal{F}(W) \mid wF_J^\circ(\Pi) \subseteq B_0\}$. Take $wF_J^\circ(\Pi^\vee) \in \mathcal{F}(W)$ where $wF_J^\circ(\Pi^\vee) \subseteq B_0$. Then by Theorem 3.7, $N(wF_J^\circ(\Pi^\vee))$ is polyhedral cone, and as $T(W) = E(W)$, $wF^\circ(\Pi^\vee) \subseteq N(wF^\circ(\Pi^\vee))^\circ$. So as $wF_J^\circ(\Pi^\vee) \subseteq B_0$, $C_0 \cap N(wF_J^\circ(\Pi^\vee))^\circ \neq \emptyset$. Hence $C_0 \cap N(wF_J^\circ(\Pi^\vee))$ is a polyhedral cone $C(\Lambda_0^\vee)$ where $\Lambda_0^\vee \subseteq \Sigma^\vee$.

As $wF_J^\circ(\Pi^\vee) \subseteq B_0$, it follows from Theorem 3.7 that $wF_J^\circ(\Pi^\vee) \not\subseteq C(\Lambda_0^\vee)^\circ$. This means that $wF_J^\circ(\Pi^\vee)$ is contained in the envelope of $C(\Lambda_0^\vee)$. Because $wF_J^\circ(\Pi^\vee) \in \mathcal{E}\,(W\,(S))$, the parabolic subgroup wW_Jw^{-1} is finite. Therefore $\Lambda_0^\vee$ is finite and $C(\Lambda_0^\vee)$ has a base $\Pi^\vee(wF_J^\circ(\Pi^\vee))$. Let $\Pi_0^\vee(wF_J^\circ(\Pi^\vee))$ denote the subset of $\Pi^\vee(wF_J^\circ(\Pi^\vee))$ which consists of those $\gamma^\vee \in \Sigma_0^{\vee +}$ such that $H_{\gamma^\vee} \supseteq wF_J^\circ(\Pi^\vee)$. Then $\Pi_0^\vee(wF_J^\circ(\Pi^\vee)) \subseteq \Sigma_0^\vee$, and $C_0 \cap N(wF_J^\circ(\Pi^\vee)) = C(\Pi_0^\vee(wF_J^\circ(\Pi^\vee))) \cap N(wF_J^\circ(\Pi^\vee))$. Since $H_{\gamma^\vee} \cap N(wF_J^\circ(\Pi^\vee))^\circ \neq \emptyset$ for $\gamma^\vee \in \Pi_0^\vee(wF_J^\circ(\Pi^\vee))$, it follows that $\Pi_0^\vee(wF_J^\circ(\Pi^\vee)) \subseteq \Pi_0^\vee$. Set $\Pi_1^\vee = \bigcup_{wF_J^\circ(\Pi^\vee) \subseteq B_0} \Pi_0^\vee(wF_J^\circ(\Pi^\vee))$. Then $\Pi_1^\vee \subseteq$

$\Pi_0^\vee$ and $C(\Pi_1^\vee) \supseteq C(\Pi_0^\vee)$. By virtue of Corollary 3.2 and Theorem 3.3, $\Pi_1^\vee$ inherits the Cartan property from $\Pi_0^\vee$. Therefore $\Pi_1^\vee$ is a base for the polyhedral cone $C(\Pi_1^\vee)$, and $C(\Pi_1^\vee) = \bigcap_{wF_J^\circ(\Pi^\vee)\subseteq B_0} C(\Pi^\vee(wF_J^\circ(\Pi^\vee)))$. Since $B_0 = \bigcup\{wF_J^\circ(\Pi) \mid wF_J^\circ(\Pi) \subseteq B_0\}$, B_0 is contained in the envelope of $C(\Pi_1^\vee)$. Since C_0 is the convex hull of B_0, we now have $C_0 \supseteq C(\Pi_1^\vee) \supseteq C(\Pi_0^\vee)$. Q.E.D.

References

[1] Bourbaki, N., *Éléments de Mathématique, Groupes et algèbres de Lie,* Chapitres 4, 5, 6, Masson, Paris, 1981.

[2] Deodhar, V.V., A note on subgroups generated by reflections in Coxeter groups, *Arch. Math.*, **53** (1989), 543–546.

[3] Dyer, M., Reflection subgroups of Coxeter systems, *J. Algebra*, **135** (1990), 57–73.

[4] Humphreys, J.E., *Reflection Groups and Coxeter Groups,* Cambridge Univ. Press, 1990.

[5] Tits, Jacques, *Groupes et géométries de Coxeter,* Inst. Haute Études Sci. (mimeographed notes), Paris, 1961.

[6] Vinberg, E.B, Discrete linear groups generated by reflections, *Math. USSR-Ivz.*, **5** (1971) (Amer. Math. Sci. Trans.), 1083–1119.

Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, IL 61801
U.S.A.

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 437–448

The Isaacs character correspondence and isotypies between blocks of finite groups

Atumi Watanabe

§1. Introduction

Let $S$ and $G$ be finite groups such that $S$ acts on $G$ via automorphism and $(|S|, |G|) = 1$. It is well known that in this situation there is a natural bijection $\pi(G, S)$ from the set $\mathrm{Irr}_S(G)$ of $S$-invariant irreducible characters of $G$ onto the set $\mathrm{Irr}(C_G(S))$ of irreducible characters of $C_G(S)$. When $S$ is solvable, this is obtained by G. Glauberman and when $|G|$ is odd this is obtained by I. M. Isaacs. Moreover it is shown in [Wo1] that when $S$ is solvable and $|G|$ is odd these are equal. Let $p$ be a prime. In [Wa] we showed that the Glauberman character correspondence gives an isotypy between an $S$-invariant $p$-block $B$ of $G$ and a $p$-block of $C_G(S)$ if a defect group of $B$ is centralized by $S$. In [H] H. Horimoto proved that the Isaacs character correspondence gives a perfect isometry between an $S$-invariant $p$-block $B$ of $G$ and a $p$-block of $C_G(S)$ under the same assumption as in the Glauberman correspondence case (see Theorem 3.2 for the detail). The purpose of this paper is to show that the perfect isometry is an isotypy (Theorem 3.6).

Let $(\mathcal{K}, \mathcal{R}, \mathcal{F})$ be a $p$-modular system such that $\mathcal{K}$ is algebraically closed. Here we state the definition of isotypies between blocks, where a block means a $p$-block. Let $B$ be a block of $G$ with defect group $D$ and (D, B_D) be a maximal $B$-subpair of $G$. We denote by $\mathbf{Br}_B(G)$ the Brauer category of $B$. $\mathbf{Br}_B(G)$ is the category whose objects are $B$-subpairs of $G$ and whose morphisms are defined in the following way: For $B$-subpairs $(Q, b)$ and (R, b') $\mathrm{Mor}((Q, b), (R, b'))$ is the set of all cosets $gC_G(Q)$ of $G$ such that ${}^g(Q, b) \subseteq (R, b')$ (see [B-O], §1). We denote by $\mathbf{Br}_{B,D}(G)$ the full subcategory of $\mathbf{Br}_B(G)$ whose objects are the $B$-subpairs $(Q, b)$ such that $(Q, b) \subseteq (D, B_D)$. We note that for any $Q \leq D$ there exists a unique block $b$ such that $(Q, b) \subseteq (D, B_D)$, and we set $b =$

Received May 28, 1999.
Revised June 5, 2000.

B_Q. Let $\mathrm{CF}(G, \mathcal{K})$ be the $\mathcal{K}$-vector space of $\mathcal{K}$-valued class functions on G and let $\mathrm{CF}(G, B, \mathcal{K})$ be the subspace of $\mathrm{CF}(G, \mathcal{K})$ of class functions α such that α is a $\mathcal{K}$-linear combination of χ's in $\mathrm{Irr}(B)$. Let $\mathrm{CF}_{p'}(G, B, \mathcal{K})$ be the subspace of $\mathrm{CF}(G, B, \mathcal{K})$ of class functions vanishing on the p-singular elements of G. Let $(x, \mathbf{b})$ be a B-Brauer element of G. The decomposition map

$$d_G^{(x,\mathbf{b})} : \mathrm{CF}(G, B, \mathcal{K}) \to \mathrm{CF}_{p'}(C_G(x), \mathbf{b}, \mathcal{K})$$

is defined by $d_G^{(x,\mathbf{b})}(\alpha)(y) = \alpha(xye_{\mathbf{b}})$ for any p'-element y of $C_G(x)$, where $e_{\mathbf{b}}$ is the block idempotents of $\mathcal{R}C_G(x)$ corresponding to $\mathbf{b}$. Finally let H be a second finite group and B' be a block of H with D as a defect group. Let (D, B'_D) be a maximal B'-subpair of H and for any subgroup Q of D let (Q, B'_Q) be the B'-subpair of H such that $(Q, B'_Q) \subseteq (D, B'_D)$.

Definition ([B, 4.6]). With the above notations (G, B) and (H, B') are *isotypic* if the following conditions hold :

(i) The inclusion of D into G and H induces an equivalence of the Brauer categories $\mathbf{Br}_{B,D}(G)$ and $\mathbf{Br}_{B',D}(H)$.

(ii) There exists a family of perfect isometries

$$\{R^Q : \mathcal{R}_{\mathcal{K}}(C_G(Q), B_Q) \to \mathcal{R}_{\mathcal{K}}(C_H(Q), B'_Q)\}_{\{Q(cyclic) \leq D\}}$$

such that for any $x \in D$

$$(*) \qquad d_H^{(x,B'_{\langle x\rangle})} \circ R^{\langle 1\rangle} = (R^{\langle x\rangle})_{p'} \circ d_G^{(x,B_{\langle x\rangle})},$$

where $(R^{\langle x\rangle})_{p'}$ is the $\mathcal{K}$-linear map from $\mathrm{CF}_{p'}(C_G(x), B_{\langle x\rangle}, \mathcal{K})$ onto $\mathrm{CF}_{p'}(C_H(x), B'_{\langle x\rangle}, \mathcal{K})$ induced by $R^{\langle x\rangle}$ and we regard $R^{\langle 1\rangle}$ as a $\mathcal{K}$-linear map from $\mathrm{CF}(G, B, \mathcal{K})$ onto $\mathrm{CF}(H, B', \mathcal{K})$. In the above $R^{\langle 1\rangle}$ is called an *isotypy* between B and B', and $(R^Q)_{\{Q(cyclic) \leq D\}}$ is called the *local system* of $R^{\langle 1\rangle}$. See [B, §1] for the definition of perfect isometries between blocks.

§2. Isaacs character correspondence

In this section we recall the definition of the Isaacs correspondence and state some results in [I1], [Wo1, 2] which are used in the next section. Let G be a finite group. For normal subgroups $L \leq K$ of G such that K/L is abelian, and for G-invariant irreducible characters θ of K and ϕ of L, if θ is fully ramified with respect to K/L and ϕ is an irreducible constituent of θ_L, then (G, K, L, θ, ϕ) is called a character five.

Theorem 2.1 ([I1, Theorem 9.1 ; Corollary 6.4]). *Let (G, K, L, θ, ϕ) be a character five. Assume that either $|G : K|$ or $|K : L|$ is odd. Let $\Psi^{(K/L)}$ be the character of G/K defined with respect to the form $\ll, \gg_\phi$ on K/L, and view $\Psi^{(K/L)}$ as a character of G. Then there exists a conjugacy class $\mathcal{U}$ of subgroups $U \leq G$ such that*

(a) $(\Psi^{(K/L)}(x))^2 = \pm|C_{K/L}(x)|$ *for* $x \in G$;

(b) $UK = G$ *and* $U \cap K = L$;

(c) U^a *is G-conjugate to U for all* $a \in \mathrm{Aut}(G)$ *such that* $K^a = K$, $L^a = L$ *and* $\phi^a = \phi$;

(d) *the equation* $\chi_U = (\Psi^{(K/L)})_U\xi$, *for* $\chi \in \mathrm{Irr}(G|\theta)$ *and* $\xi \in \mathrm{Irr}(U|\phi)$ *defines a* 1-1 *correspondence between these sets of characters, and*

(e) *if* $|G : K|$ *is odd,* $\chi \in \mathrm{Irr}(G|\theta)$ *and* $\xi \in \mathrm{Irr}(U|\phi)$, *then* $\chi_U = (\Psi^{(K/L)})_U\xi$ *if and only if* (χ_U, ξ) *is odd.*

For the definition of $\Psi^{(K/L)}$ in the above, see [I1], page 619, Theorem 6.3 and the above of Theorem 9.1. $\Psi^{(K/L)}$ is determined by the form $\ll, \gg_\phi$ on K/L and the action of G/K on K/L.

Hypothesis 2.2. Let S act on G via automorphism such that $(|S|, |G|) = 1$. Let $C = C_G(S)$ and let Γ be the semi-direct product GS.

Lemma 2.3 ([I1, Corollary 10.7]; [Wol, Corollary 4.3]). *Assume Hypothesis* 2.2 *with $|G|$ odd. Let $[G, S]'C \leq H \leq G$ such that H is S-invariant. Then there exists a bijection $\sigma(G, H, S) : \mathrm{Irr}_S(G) \to \mathrm{Irr}_S(H)$ such that for $\chi \in \mathrm{Irr}_S(G)$, $\sigma(G, H, S)(\chi)$ is the unique S-invariant irreducible character α of H with (χ_H, α) odd.*

Definition ([I1, §10]). Assume Hypothesis 2.2 with $|G|$ odd. If $C < G$, then let

$$G = G_0 > G_1 > G_2 > G_3 > \cdots > G_n = C$$

by $G_{i+1} = [G_i, S]'C$, for $i \geq 0$. The Isaacs character correspondence $\pi(G, S) : \mathrm{Irr}_S(G) \to \mathrm{Irr}(C)$ is the composition map

$$\sigma(G_{n-1}, C, S)\sigma(G_{n-2}, G_{n-1}, S) \cdots \sigma(G_2, G_1, S)\sigma(G, G_1, S)$$

if $C < G$, otherwise $\pi(G, S)$ is the identity map.

The following lemmas play big roles in this paper.

Lemma 2.4 ([Wol, Theorem 4.6]). *Assume Hypothesis* 2.2 *with $|G|$ odd. Let $K = [G, S]$, $L = K'$, and $U = LC$. Assume that $U \leq H \leq G$ is S-invariant. Let $\chi \in \mathrm{Irr}_S(G)$ and $\psi = \sigma(G, H, S)(\chi)$. Then*

(a) $\sigma(G, U, S)(\chi) = \sigma(H, U, S)(\psi)$, *and*

(b) $\pi(G,S)(\chi) = \pi(H,S)(\psi)$.

Lemma 2.5 ([Wo2, Lemma 2.5]). *Assume Hypothesis* 2.2 *and* $N \lhd \Gamma$ *and* $N \leq G$. *Let* $\chi \in \mathrm{Irr}_S(G)$, $\theta \in \mathrm{Irr}_S(N)$, $T = T_G(\theta)$ *the inertial subgroup of* θ *in* G, $\mu = \pi(G,S)(\chi)$, *and* $\nu = \pi(N,S)(\theta)$. *Then*

(a) $(\chi_N, \theta) \neq 0$ *if and only if* $(\mu_{N\cap C}, \nu) \neq 0$,

(b) $T \cap C = T_C(\nu)$ *and* $\pi(G,S)(\psi^G) = (\pi(T,S)(\psi))^C$ *for* $\psi \in \mathrm{Irr}_S(T|\theta)$.

Lemma 2.6 ([Wo1, Lemma 4.9]). *Assume Hypothesis* 2.2 *with* $|G|$ *odd. Let* U *be a normal subgroup of* S *and* $H = C_G(U)$. *Then* $\pi(G,U)$ *maps* $\mathrm{Irr}_S(G)$ *onto* $Irr_S(H)$ *and* $\pi(G,S) = \pi(H,S/U)\pi(G,U)$.

§3. Isotypies obtained from Isaacs character correspondences

Since the Isaacs character correspondence is defined in the case $|G|$ is odd, we set the following hypothesis. Then G is solvable by the Feit-Thompson's theorem.

Hypothesis 3.1. Let S and G be finite groups such that S acts on G, $(|S|,|G|) = 1$ and that $|G|$ is odd. Put $C = C_G(S)$.

Theorem 3.2 ([H, Theorem 1, (a)]). *Under the above hypothesis, let* B *be an* S*-invariant block of* G *such that a defect group* D *of* B *is centralized by* S. *Then there exists a block* b *of* C *such that* $\mathrm{Irr}(b) = \{\pi(G,S)(\chi) | \chi \in \mathrm{Irr}(B)\}$ *and* $\pi(G,S)$ *gives a perfect isometry* R *between* B *and* b. *Moreover* D *is a defect group of* b.

In the above theorem the assumption for B implies that $\chi \in \mathrm{Irr}(B)$ is S-invariant by [Wa, Proposition 1]. We call b the *Isaacs correspondent of* B. We will show that the perfect isometry R in the above theorem is an isotypy .

Lemma 3.3. *Let* (G,K,L,θ,ϕ) *be a character five such that* K *is a* p'*-group and* $|G|$ *is odd. Let* $\Psi^{(K/L)}$ *be the character of* G/K *defined with respect to the form* $\ll,\gg_\phi$ *on* K/L. *Let* Q *be a* p*-subgroup of* C, $\theta^* = \pi(K,Q)(\theta)$ *and* $\phi^* = \pi(L,Q)(\phi)$. *Then the following hold.*

(i) $(C_G(Q), C_K(Q), C_L(Q), \theta^*, \phi^*)$ *is a character five.*

(ii) *Suppose that* Q *is a cyclic group generated by* x *and let* $\Psi^{(C_K(x)/C_L(x))}$ *be the character of* $C_G(x)/C_K(x)$ *defined with respect to the form* $\ll,\gg_{\phi^*}$ *on* $C_K(x)/C_L(x)$. *If* K/L *is a* q*-group for a prime* q, *then there exists a sign* $\epsilon_x = \pm 1$ *such that*

$$\Psi^{(K/L)}(x\rho) = \epsilon_x \Psi^{(C_K(x)/C_L(x))}(\rho)$$

for all $\rho \in C_G(x)_{p'}$.

Proof. (i) Since θ is G-invariant, by [I2, Theorem 13.14] and [Wol, Theorem 5.1] θ^* the unique constituent of $\theta_{C_K(Q)}$ such that p does not divide $(\theta_{C_K(Q)}, \theta^*)$. Therefore θ^* is $C_G(Q)$-invariant. Similarly ϕ^* is $C_G(Q)$-invariant. Since θ is a unique constituent of ϕ^K as ϕ is fully ramified with respect to K/L, θ^* is a unique constituent of $(\phi^*)^{C_K(Q)}$ by Lemma 2.5. Hence $(C_G(Q), C_K(Q), C_L(Q), \theta^*, \phi^*)$ is a character five. Here we show $\ll, \gg_\phi = \ll, \gg_{\phi^*}$ on $C_K(Q)/C_L(Q)$ without the assumption ϕ is fully ramified with respect to K/L, where $C_K(Q)/C_L(Q)$ is identified with a subgroup of K/L. Let $y \in C_K(Q)$ and $\hat{\phi}$ be an extension of ϕ to $\langle L, y\rangle$. We can show that $\hat{\phi}$ is Q-invariant by a theorem of Glauberman([I2, Lemma 13.8]). Then $\pi(\langle L, y\rangle, Q)(\hat{\phi})$ is an extension of ϕ^* to $\langle C_L(Q), y\rangle$ by Lemma 2.5 because $\langle C_L(Q), y\rangle/C_L(Q)$ is cyclic. For $z \in C_K(Q)$ let $(\hat{\phi})^z = \lambda\hat{\phi}$ where λ is a linear character of $\langle L, y\rangle$ so that $L \subseteq \mathrm{Ker}\lambda$. Then we see easily $\pi(\langle L, y\rangle, Q)((\hat{\phi})^z) = \pi(\langle L, y\rangle, Q)(\lambda\hat{\phi}) = \lambda\pi(\langle L, y\rangle, Q)(\hat{\phi})$ where λ is regarded as a character of $\langle C_L(Q), y\rangle$. So we have $(\pi(\langle L, y\rangle, Q)(\hat{\phi}))^z = \pi(\langle L, y\rangle, Q)((\hat{\phi})^z) = \lambda\pi(\langle L, y\rangle, Q)(\hat{\phi})$. Hence $\ll y, z \gg_\phi = \lambda(y) = \ll y, z \gg_{\phi^*}$.

(ii) Let $E = K/L$, $E_1 = C_E(x)$ and $E_2 = [E, x]$. Then $E = E_1 \times E_2$. Since $E_1 = C_K(x)L/L$, E_1 and $C_K(x)/C_L(x)$ are $C_G(x)/C_K(x)$-isomorphic when $C_G(x)/C_K(x)$ acts on them. Suppose that $1 < E_1 < E$. Then by the algorithm for computation of $\Psi^{(E)}$,

$$\Psi^{(E)}(x\rho) = \Psi^{(E_1)}(x\rho)\Psi^{(E_2)}(x\rho)$$

for all $\rho \in C_G(x)_{p'}$. Since $C_{E_2}(x\rho)$ is the identity group, by [I1, Corollary 6.4], $\Psi^{(E_2)}(x\rho) = \pm 1$ and hence we have $\Psi^{(E_2)}(x\rho) = \Psi^{(E_2)}(x)$ for $\rho \in C_G(x)_{p'}$ because $x\rho$ is a $2'$-element. On the other hand since $\ll, \gg_\phi = \ll, \gg_{\phi^*}$ on $E_1 \cong C_K(x)/C_L(x)$, by [I1, Theorem 6.3] and by the algorithm for computation of $\Psi^{(E)}$ we have $\Psi^{(E_1)} = \Psi^{(C_K(x)/C_L(x))}$ as characters of $C_G(x)/C_K(x)$. Moreover $x \in \mathrm{Ker}\Psi^{(C_K(x)/C_L(x))}$ by [I1, Corollary 6.4] because x is a $2'$-element. So if we put $\epsilon_x = \Psi^{(E_2)}(x)$, we have $\Psi^{(E)}(x\rho) = \epsilon_x\Psi^{(C_K(x)/C_L(x))}(\rho)$ for all $\rho \in C_G(x)_{p'}$. Next suppose that $E_1 = E$. Then we have $\Psi^{(E)}(x\rho) = \Psi^{(E)}(\rho) = \Psi^{(C_K(x)/C_L(x))}(\rho)$ for all $\rho \in C_G(x)_{p'}$ by the same argument as in the above. So we may assume E_1 is the identity group. Then by [I1, Corollary 6.4] again, $\Psi^{(E)}(x\rho) = \Psi^{(E)}(x) = \pm 1$ for all $\rho \in C_G(x)_{p'}$. On the other hand $\Psi^{(C_K(x)/C_L(x))}(\rho) = 1$ for all $\rho \in C_G(x)_{p'}$. So if we put $\epsilon_x = \Psi^{(E)}(x)$, then we have $\Psi^{(E)}(x\rho) = \epsilon_x\Psi^{(C_K(x)/C_L(x))}(\rho)$ for all $\rho \in C_G(x)_{p'}$. This completes the proof of (ii). Q.E.D.

Lemma 3.4. *Assume Hypothesis 3.1. Let B be an S-invariant block of G such that a defect group D of B is centralized by S and let*

b be the Isaacs correspondent of B. Let (Q, B_Q) be an S-invariant B-subpair of G such that $Q \subseteq D$ and a defect group of B_Q is centralized by S and let b_Q be the Isaacs correspondent of B_Q. Then b_Q is associated with b in the sense of Brauer.

Proof. We prove by induction on $|G|$. Let $K = O_{p'}(G)$ and ζ^* be an irreducible character of $C_K(S)$ covered by b. We may assume that ζ^* is Q-invariant because Q is contained in a defect group D of b. Let $\zeta \in \mathrm{Irr}_S(K)$ have the Isaacs correspondent ζ^*, and let $H = T_G(\zeta)$, $T_G(\zeta)$ is the stabilizer of ζ in G. Then B covers ζ by Lemma 2.5 and H is S-invariant. By Lemma 2.5 again, $Q \leq T_C(\zeta^*) = H \cap C$, *i.e.*, ζ is SQ-invariant. Let $\zeta_1 = \pi(K, Q)(\zeta)$ and $\zeta_2 = \pi(C_K(Q), S)(\zeta_1)$. Then we have $\zeta_2 = \pi(K, SQ)(\zeta) = \pi(C_K(S), Q)(\zeta^*)$ by Lemma 2.6. And $T_{C_G(Q)}(\zeta_1) = H \cap C_G(Q)$ and $T_{C_C(Q)}(\zeta_2) = H \cap C_G(Q) \cap C_C(Q) = C \cap H \cap C_G(Q)$. Moreover by the assumption, B_Q covers ζ_1 because B covers ζ. Hence b_Q covers ζ_2 by Lemma 2.5 since b_Q is the Isaacs correspondent B_Q. Let $\tilde{b}_Q$ be a block of $C \cap H \cap C_G(Q)$ such that $\tilde{b}_Q$ is the Clifford correspondent of b_Q and similarly let $\tilde{B}_Q$ be a block of $H \cap C_G(Q)$ such that $\tilde{B}_Q$ is the Clifford correspondent of B_Q. Since ζ and hence ζ_1 is S-invariant and B_Q is S-invariant, $\tilde{B}_Q$ is S-invariant. Let $\tilde{B} = (\tilde{B}_Q)^H$. Then $\tilde{B}$ covers ζ and we have $\tilde{B}^G = ((\tilde{B}_Q)^{C_G(Q)})^G = B$. Hence B is the Clifford correspondent of $\tilde{B}$. Moreover since ζ, and B is S-invariant, $\tilde{B}$ is S-invariant. Here we show that a defect group of $\tilde{B}$ is centralized by S. S acts on the defect groups of $\tilde{B}$. By a theorem of Glauberman there exists a defect group $\tilde{D}$ of $\tilde{B}$ which is S-invariant. So when S acts on the defect groups of B, D and $\tilde{D}$ are fixed elements. So D are $\tilde{D}$ are C-conjugate by a theorem of Glauberman. So $\tilde{D}$ is centralized by S. Similarly a defect group of $\tilde{B}_Q$ is centralized by S. By Lemma 2.5 and the assumption, $\tilde{b}_Q$ is the Isaacs correspondent of $\tilde{B}_Q$. Now let $\tilde{b}$ be the Isaacs correspondent of $\tilde{B}$. $\tilde{b}$ covers ζ^* by Lemma 2.5. Here assume $H < G$. By the induction hypothesis $\tilde{b}_Q$ is associated with $\tilde{b}$. On the other hand since b is the Isaacs correspondent B, b is the Clifford correspondent of $\tilde{b}$. These imply $(b_Q)^C = (\tilde{b}_Q)^C = ((\tilde{b}_Q)^{H \cap C})^C = (\tilde{b})^C = b$. Thus we assume ζ is G-invariant. Hence B is of maximum defect and D is a Sylow p-subgroup of G because G is solvable. Now we can show that a p-complement of G is S-invariant by using a theorem of Glauberman. So $[G, S]$ is a p'-group. Hence $G = KC$. From this $K \cap C$ is the maximal normal p'-subgroup of C. Since ζ^* is C-invariant, b is the unique p-block of C which covers ζ^*. Now $(b_Q)^C$ covers ζ^* because b_Q covers ζ_2 and $\zeta_2 = \pi(C_K(S), Q)(\zeta^*)$. So $b = (b_Q)^C$. This completes the proof. Q.E.D.

Under Hypothesis 3.1 let B be an S-invariant block of G with the Isaacs correspondent b. Let D be a common defect group of B and b and (D, B_D) be an S-invariant maximal B-subpair. Let (Q, B_Q) be a B-subpair contained in (D, B_D). Then B_Q is S-invariant and a defect group of B_Q is centralized by S as we proved in [Wa, §3]. We prove it again for the self-containedness. Let $(Q, B_Q) \ntriangleleft (R, B_R)$ be B-subpairs contained in (D, B_D). If B_R is S-invariant, then B_Q is S-invariant. So we can show that B_Q is S-invariant by the induction on $|D : Q|$. Next we show that a defect group of B_Q is centralized by S for any $Q \leq D$. In fact we show that a defect group of $(B_Q)^T$ is centralized by S where T is the inertial group of B_Q in $N_G(Q)$. Let U be a defect group of $(B_Q)^T$. Since $(B_Q)^T$ is associated with B, $Q^v \leq U^v \leq D$ for some $v \in G$. So we have $C_\Gamma(Q) \geq S^{v^{-1}}$ and $C_\Gamma(Q) \geq S$. Since $C_\Gamma(Q) = SC_G(Q)$, by the Schur-Zassenhaus theorem there exists an element $u \in C_G(Q)$ such that $S^{v^{-1}} = S^u$. Then $v^{-1}u^{-1} \in C$. Hence we have $U^{u^{-1}} \leq D^{v^{-1}u^{-1}} \subseteq C$. Thus $U^{u^{-1}}$ is a defect group of $(B_Q)^T$ centralized by S. Now let b_Q be the Isaacs correspondent of B_Q. By Lemma 3.4 (Q, b_Q) is a b-subpair of C.

Proposition 3.5. *With the above notations we have the following.*

(i) *(D, b_D) is a maximal b-subpair of C and $(Q, b_Q) \subseteq (D, b_D)$ for any $Q \leq D$.*

(ii) *The Brauer categories $\mathbf{Br}_{B,D}(G)$ and $\mathbf{Br}_{b,D}(C)$ are equivalent.*

Proof. (i) By Lemma 3.4 and Theorem 3.2, it is evident that (D, b_D) is a maximal b-subpair of C. We prove the latter of (i) by the induction on $|D : Q|$. Assume $Q \lhd R \leq D$ and $(R, b_R) \subseteq (D, b_D)$. Then $(B_R)^{RC_G(Q)} = B_Q$ and R fixes B_Q. So we see that R stabilizes b_Q because the map $\pi(C_G(Q), S)$ is an $N_C(Q)$-map. Now B_Q as a block of $RC_G(Q)$ is S-invariant and a defect group of B_Q is centralized by S as we saw in the above. So by Lemma 2.5, b_Q as a block of $RC_C(Q)$ is the Isaacs correspondent of B_Q. Hence by Lemma 3.4, we have $(b_R)^{RC_C(Q)} = b_Q$ and hence $(Q, b_Q) \subseteq (R, b_R) \subseteq (D, b_D)$.

(ii) Let $Q \leq D$ and let $(Q, B_Q)^x \subseteq (D, B_D)$ for $x \in G$. Then $(B_Q)^x = B_{Q^x}$. Since $Q^x \leq D \leq C$, we can show $x \in C_G(Q)C$ by the Schur-Zassenhaus theorem. So we may assume $x \in C$. Then $(b_Q)^x$ is the Isaacs correspondent of $(B_Q)^x$ and hence we have $(b_Q)^x = b_{Q^x}$. Conversely if $(Q, b_Q)^y \leq (D, b_D)$ for $y \in C$ then we have $(b_Q)^y = b_{Q^y}$, hence $(B_Q)^y = B_{Q^y}$ because $(b_Q)^y$ is the Isaacs correspondent of $(B_Q)^y$. This implies that $\mathbf{Br}_{B,D}(G)$ and $\mathbf{Br}_{b,D}(C)$ are equivalent. This completes the proof of the proposition. Q.E.D.

With the notations in the just above of Proposition 3.5, let R^Q be the perfect isometry from $\mathcal{R}_{\mathcal{K}}(C_G(Q), B_Q)$ onto $\mathcal{R}_{\mathcal{K}}(C_C(Q), b_Q)$ for $Q \leq D$ and let $R = R^{\langle 1\rangle}$. We are now in a position to prove our main theorem.

Theorem 3.6. *Assume Hypothesis 3.1 and let B be an S- invariant block of G such that a defect group D of B is centralized by S and b be the Isaacs correspondent of B. Then R is an isotypy between B and b with local system $(\pm R^Q)_{\{Q(\mathrm{cyclic}) \leq D\}}$, where R^Q is as in the just above.*

Proof. We prove by induction on $|G|$. Since the Brauer categories $\mathbf{Br}_{B,D}(G)$ and $\mathbf{Br}_{b,D}(C)$ are equivalent by Proposition 3.5, it suffices to prove

$$(1) \qquad \pm(R^{\langle x\rangle})_{p'} \circ d_G^{(x,B_x)} = d_C^{(x,b_x)} \circ R$$

for any $x \in D$, where $B_x = B_{\langle x\rangle}$ and $b_x = b_{\langle x\rangle}$. Let H be a normal p'-subgroup of G and let ζ be an S-invariant irreducible character of H covered by B. We put $\pi(H,S)(\zeta) = \zeta^*$. By Lemma 2.5, b covers ζ^*. Let $T = T_G(\zeta)$ and $\tilde{B}$ be a block of T such that $\tilde{B}$ covers ζ and that $\tilde{B}$ corresponds to B by the Clifford theorem (then we say that$\tilde{B}$ and B are *Clifford induction equivalent.*) From the argument in the proof of Lemma 3.4, $\tilde{B}$ is S-invariant and a defect group of $\tilde{B}$ is centralized by S. Let $\tilde{b}$ be the Isaacs correspondent of $\tilde{B}$. By Lemma 2.5 $T_C(\zeta^*) = T \cap C = C_T(S)$ and $\tilde{b}$ covers ζ^*. Moreover we see $\tilde{b}$ and b are Clifford induction equivalent by Lemma 2.5 again because b is the Isaacs correspondent of B. Let $\tilde{D}$ be a defect group of $\tilde{b}$. Then $\tilde{D}$ is a defect group of B. Since $\tilde{D}$ and D are S-invariant, they are conjugate by an element of C by a theorem of Glauberman. So we may assume $\tilde{D} = D$. In fact let $g \in C$. $(D^g, (B_D)^g)$ is an S-invariant maximal B-subpair of G with $D^g \subseteq C$ and $(Q^g, (B_Q)^g) \subseteq (D^g, (B_D)^g)$ for any $Q \leq D$. On the other hand by the definition of Isaacs correspondence, $(b_Q)^g$ is the Isaacs correspondent of $(B_Q)^g$, and $(R^Q)^g$ is the perfect isometry from $\mathcal{R}_{\mathcal{K}}(C_G(Q^g), (B_Q)^g)$ onto $\mathcal{R}_{\mathcal{K}}(C_C(Q^g), (b_Q)^g)$. Moreover we can see that (1) holds for (x, B_x) if and only if (1) holds for $(x, B_x)^g$, that is, $\pm((R^{\langle x\rangle})^g)_{p'} \circ d_G^{(x^g,(B_x)^g)} = d_C^{(x^g,(b_x)^g)} \circ R$ for all $x \in D$. Thus we may assume $\tilde{D} = D$.

Let $(D, \tilde{B}_D)$ be an S-invariant maximal $\tilde{B}$-subpair of T. By [F-H], p 3471, Remark, $(\tilde{B}_D)^{C_G(D)}$ is defined and it is Clifford induction equivalent to $\tilde{B}_D$. And $(\tilde{B}_D)^{C_G(D)}$ is S-invariant because $\tilde{B}_D$ is S-invariant. Hence $(\tilde{B}_D)^{C_G(D)}$ and B_D are $N_C(D)$-conjugate by a theorem of Glauberman. So we may assume $(\tilde{B}_D)^{C_G(D)} = B_D$ if necessary by replacing ζ with $N_C(C)$-conjugate of it. Now let $Q \leq D$ and $\zeta_1 =$

$\pi(H,Q)(\zeta)$. Then $T_{C_G(Q)}(\zeta_1) = T \cap C_G(Q)$. Let $\zeta_2 = \pi(C_H(Q),S)(\zeta_1)$. By Lemma 2.6 we have $\zeta_2 = \pi(C_H(S),Q)(\zeta^*)$, and hence we have also $T_{C_C(Q)}(\zeta_2) = T \cap C \cap C_G(Q)$. Let $(Q,\tilde{B}_Q) \subseteq (D,\tilde{B}_D)$ and $\tilde{b}_Q$ be the Isaacs correspondent of $\tilde{B}_Q$. Then $\tilde{B}_Q$ covers ζ_1, and $\tilde{b}_Q$ covers ζ_2 by Lemma 2.5. Therefore $(\tilde{B}_Q)^{C_G(Q)}$ is defined and this is Clifford induction equivalent to $\tilde{B}_Q$. By [F-H], p 3471, Remark, $(Q,(\tilde{B}_Q)^{C_G(Q)}) \subseteq (D,(\tilde{B}_D)^{C_G(D)}) = (D,B_D)$ because $(Q,\tilde{B}_Q) \subseteq (D,\tilde{B}_D)$, and hence we have $B_Q = (\tilde{B}_Q)^{C_G(Q)}$. So Lemma 2.5 implies $b_Q = (\tilde{b}_Q)^{C_C(Q)}$, that is, $\tilde{b}_Q$ and b_Q are Clifford induction equivalent. Here we assume $T < G$. By the induction hypothesis (1) holds for $\tilde{B}$. On the other hand $\tilde{B}$ and B are isotypic by the induction of characters, similarly $\tilde{b}$ and b are also isotypic by [F-H], p 3471, Remark. So combining these facts with Lemma 3.5 we can see that (1) holds for B. Hence we may assume $T = G$. In particular we may assume that B is of maximum defect and hence a Sylow p-subgroup of G is centralized by S.

Let $K = [G,S]$ and θ be an S-invariant irreducible character of K covered by B. By a theorem of Glauberman we have $G = CK$ and we have also $C \cap K \subseteq K'$. From the above arguments K is a p'-group and θ is G-invariant. Moreover we may assume $C < G$. Let $\Gamma = SG$ the semi direct product of G by S, K/L be a chief factor group of Γ and $X = LC$. Then $G = XK$, $X \cap K = L$ and $X < G$. Besides a Sylow p-subgroup of X also is centralized by S. So the Isaacs correspondence gives a bijection between $\mathrm{Bl}_S(X)$ and $\mathrm{Bl}(C)$ by Theorem 3.2. Let B_X be an S-invariant block of X with Isaacs correspondent b. We note D is a defect group of B_X. On the other hand, since $X \supseteq CK'$, by Lemma 3.4, there exists a perfect isometry R' from $\mathcal{R}_{\mathcal{K}}(G,B)$ onto $\mathcal{R}_{\mathcal{K}}(X,B_X)$ such that for $\chi \in \mathrm{Irr}(B)$ $R'(\chi)$ is the unique S-invariant irreducible character α of X with (α,χ_X) odd. Moreover R is the composition of R' and the perfect isometry from $\mathcal{R}_{\mathcal{K}}(X,B_X)$ onto $\mathcal{R}_{\mathcal{K}}(C,b)$. Now let $Q \leq D$. $C_X(Q)$ is S-invariant and a Sylow p-subgroup of $N_X(Q)$, and hence that of $C_X(Q)$ is centralized by S from the Schur-Zassenhaus theorem. Moreover $C_X(Q) = C_C(Q)[C_X(Q),S] = C_C(Q)C_L(Q) \geq C_C(Q)[C_G(Q),S]'$. Let B'_Q be an S-invariant block of $C_X(Q)$ with Isaacs correspondent b_Q. By the same reason as in the above there exists a perfect isometry R'^Q from $\mathcal{R}_{\mathcal{K}}(C_G(Q),B_Q)$ onto $\mathcal{R}_{\mathcal{K}}(C_X(Q),B'_Q)$ such that for $\mu \in \mathrm{Irr}(B_Q)$, $R'^Q(\mu)$ is the unique S-invariant irreducible character β of $C_X(Q)$ with $(\beta,\mu_{C_X(Q)})$ odd. And R^Q is the composition of R'^Q and the perfect isometry from $\mathcal{R}_{\mathcal{K}}(C_X(Q),B'_Q)$ onto $\mathcal{R}_{\mathcal{K}}(C_C(Q),b_Q)$. Since a Sylow p-subgroup of X is centralized by S and $b = (b_Q)^C$, $(B'_Q)^X$ has b as the Isaacs correspondent by Lemma 3.4. So we have $(B'_Q)^X = B_X$. Let

$(Q, \mathbf{b})$ be a B_X-subpair contained in (D, B'_D). Since $(Q, b_Q) \subseteq (D, b_D)$ by Proposition 3.5, $\mathbf{b}$ has b_Q as the Isaacs correspondent. So $\mathbf{b} = B'_Q$. Thus by the induction hypothesis for X and B_X, it suffices to show

$$(2) \qquad \pm(R'^{\langle x\rangle})_{p'} \circ d_G^{(x,B_x)} = d_X^{(x,B'_x)} \circ R'$$

for all $x \in D$ where $B'_x = B'_{\langle x\rangle}$,

Now let ϕ be an S-invariant irreducible character of L covered by B_X. Then it is clear ϕ is a constituent of θ_L. Moreover since θ is G-invariant and K/L is abelian, $T_K(\phi)$ is normal in Γ. Hence $T_K(\phi) = L$ or $T_K(\phi) = K$ because K/L is a chief factor of Γ. We assume $T_K(\phi) = L$ for a while. At first we show $X = T_G(\phi)$ as follows. Since θ is G-invariant, we have $G = T_G(\phi)K$ and $T_G(\phi) \cap K = L$. Since $T_G(\phi)$ is S-invariant, we have $T_G(\phi) = T_C(\phi)[T_G(\phi), S] \leq XT_K(\phi) = X$. The fact that $|T_G(\phi)| = |X|$ implies $X = T_G(\phi)$. From this $\xi \leftrightarrow \xi^G$ defines a one-to-one correspondence between $\mathrm{Irr}(X|\phi)$ and $\mathrm{Irr}(G|\theta)$ preserving the actions of S on them. Therefore in particular B_X and B are Clifford induction equivalent and $R'(\xi^G) = \xi$ for $\xi \in \mathrm{Irr}(B_X)$. Let $Q \leq D$, $\theta^* = \pi(K,Q)(\theta)$ and $\phi^* = \pi(L,Q)(\phi)$. Then B_Q covers θ^* and B'_Q covers ϕ^*. Besides θ^* is $C_G(Q)$-invariant and $T_{C_K(Q)}(\phi^*) = C_L(Q)$. Since $C_G(Q) = C_X(Q)C_K(Q)$, from the same argument as for B_X and B, B'_Q and B_Q are Clifford induction equivalent and $R'^Q(\eta^{C_G(Q)}) = \eta$ for $\eta \in \mathrm{Irr}(B'_Q)$. So we have $(R'^{\langle x\rangle})_{p'} \circ d_G^{(x,B_x)} = d_X^{(x,B'_x)} \circ R'$ from [F-H], p 3471, Remark since $(Q, B'_Q) \subseteq (D, B'_D)$ for any $Q \leq D$. Thus (2) holds.

Next suppose $T_K(\phi) = K$. Then $G = T_G(\phi)$ and $T_{C_K(Q)}(\phi^*) = C_K(Q)$ for any $Q \leq D$. Since $K^\perp = \{c \in K| \ll c,\ y \gg_\phi = 1\ \forall\ y \in K\}$ is normal in Γ by [I1, Lemma 2.1], $K^\perp = K$ or $K^\perp = L$. At first we discuss the case $K^\perp = K$. Then ϕ is extendible to K, by [I1, Theorem 2.7]. Moreover B_X and B are isomorphic by [I1, Lemma 10.5] and $R'(\chi) = \chi_X$ for $\chi \in \mathrm{Irr}(B)$. In the proof of Lemma 3.3, (i) we proved that $\ll,\gg_\phi = \ll,\gg_{\phi^*}$ on $C_K(Q)/C_L(Q) \subseteq K/L$. So $C_K(Q)^\perp = \{c \in C_K(Q)| \ll c,\ y \gg_\phi = 1\, \forall\, y \in C_K(Q)\} = C_K(Q)$. Hence by [I1, Theorem 2.7] again, ϕ^* is extendible to $C_K(Q)$. Since $C_G(Q) = C_X(Q)C_K(Q)$ and $C_L(Q) = C_X(Q) \cap C_K(Q)$, by applying [I1, Theorem 10.5] for $C_G(Q)$ and B_Q, we see B_Q and B'_Q are isomorphic, and $R'^Q(\gamma) = \gamma_{C_X(Q)}$ for $\gamma \in \mathrm{Irr}(B_Q)$. On the other hand $(Q, B'_Q) \subseteq (D, B'_D)$ for any $Q \leq D$ and by Proposition 3.5 the inclusion of D into G and X induces an equivalence of the Brauer categories $\mathbf{Br}_{B,D}(G)$ and $\mathbf{Br}_{B_X,D}(X)$. The proof of Proposition 3.5, (ii) implies also that for any $x, y \in D$, B-Brauer pairs (x, B_x) and (y, B_y) are G-conjugate if and only if (x, B'_x)

and (y, B'_y) are C-conjugate. Moreover if $x \in D$ and $\mathbf{b}$ is a block of $C_G(x)$ associated with B, then $(x, \mathbf{b})$ is C-conjugate to (y, B_y) for some $y \in D$. So we can see that, $(R'^{\langle x \rangle})_{p'} \circ d_G^{(x,B_x)} = d_X^{(x,B'_x)} \circ R'$ for all $x \in D$. Thus (2) holds for all $x \in D$.

Thus our proof is reduced to the case $K^{\perp} = L$. Then (G, K, L, θ, ϕ) is a character five by [I1, Theorem 2.7]. This time we will use Theorem 2.1 for this character five. Since $K = [G, S]$ and S fixes ϕ, we can see $X \in \mathcal{U}$ in Theorem 2.1. In fact an S-invariant member of $\mathcal{U}$ coincides with X. By Theorem 2.1, (d) and (e), we have

$$\chi_X = (\Psi^{(K/L)})_X R'(\chi) \tag{3}$$

for $\chi \in \mathrm{Irr}(B)$. Then we say that B and B_X are *fully ramified equivalent* with respect to (G, K, L, θ, ϕ). Let $Q \leq D$, $\theta^* = \pi(K, Q)(\theta)$ and $\phi^* = \pi(L, Q)(\phi)$. By lemma 3.3, (i), $(C_G(Q), C_K(Q), C_L(Q), \theta^*, \phi^*)$ is an S-invariant character five. So by [H, Proposition 4, (a)], the equation

$$\psi_{C_X(Q)} = (\Psi^{(C_K(Q)/C_L(Q))})_{C_X(Q)} \psi' \tag{4}$$

for $\psi \in \mathrm{IBr}(C_G(Q)|\theta^*)$ and $\psi' \in \mathrm{IBr}(C_X(Q)|\phi^*)$ defines a 1-1 correspondence between these sets. Since B_Q covers θ^* and B'_Q covers ϕ^*, and B_Q and B'_Q have the same Isaacs correspondent b_Q, by Theorem 2.1, (d) and (e), we see that B_Q and B'_Q are fully ramified equivalent with respect to $(C_G(Q), C_K(Q), C_L(Q), \theta^*, \phi^*)$. We note $\varphi' = R'^Q(\varphi)$ for $\varphi \in \mathrm{IBr}(B_Q)$. Now let $x \in D$ and let $\chi \in \mathrm{Irr}(B)$ and $\xi = R'(\chi)$. Putting $Q = \langle x \rangle$ from (4) we have

$$\chi(x\rho) = \sum_{\psi \in \mathrm{IBr}(C_G(x)|\theta^*)} d^x_{\chi\psi} \psi(\rho) = \sum_{\psi} d^x_{\chi\psi} \Psi^{(C_K(x)/C_L(x))}(\rho) \psi'(\rho)$$

for $\rho \in C_X(x)_{p'}$ where $d^x_{\chi\psi}$ is the generalized decomposition number. Recalling that K/L is a chief factor of Γ and hence K/L is a q-group for a prime number q, we have the following from (3) and Lemma 3.3, (ii)

$$\begin{aligned}
\chi(x\rho) &= \Psi^{(K/L)}(x\rho)\xi(x\rho) \\
&= \epsilon_x \Psi^{(C_K(x)/C_L(x))}(\rho) \sum_{\psi \in \mathrm{IBr}(C_G(x)|\theta^*)} d^x_{\xi\psi'} \psi'(\rho) \\
&= \sum_{\psi} \epsilon_x \Psi^{(C_K(x)/C_L(x))}(\rho) d^x_{\xi\psi'} \psi'(\rho),
\end{aligned}$$

where $\epsilon_x = \pm 1$. From this and the fact $\Psi^{(C_K(x)/C_L(x))}(\rho) \neq 0$ by Theorem 2.1, (a), we have

$$\sum_{\varphi \in \mathrm{IBr}(B_x)} d^x_{\chi\varphi} R'^{\langle x \rangle}(\varphi)(\rho) = \epsilon_x \sum_{\nu \in \mathrm{IBr}(B'_x)} d^x_{\xi\nu} \nu(\rho)$$

for all $\rho \in C_X(x)_{p'}$. Thus we have $(R'^{\langle x \rangle})_{p'} \circ d_G^{(x,B_x)} = \epsilon_x d_X^{(x,B'_x)} \circ R'$. This completes the proof of the theorem. Q.E.D.

References

[B] M. Broué, Isométries parfaites, types de blocs, catégories dérivés, Astérisque, **181–182** (1990), 61-92.

[B-O] M. Broué and J.B. Olsson, Subpairs multiplicities in finite groups, J. reine angew. Math., **371** (1986), 125–143.

[F-H] P. Fong and M. E. Harris, On perfect isometries and isotypies in alternating groups, Trans. Amer. Math. Soc., **349** (1997), 3469–3516.

[H-K] A. Hida and S. Koshitani, Morita equivalent blocks in non-normal subgroups and p-radical blocks in finite groups, J. London Math. Soc., (2) **59** (1999), 541–556.

[H] H. Horimoto, On a correspondence between blocks of finite groups induced from the Isaacs character correspondence, Hokkaido Math. J., **30** (2001), 65–74.

[I1] I.M. Isaacs, Characters of solvable and symplectic groups, Amer.J. Math., **95** (1973), 594–635.

[I2] I.M. Isaacs, *Character theory of finite groups*, Academic Press, New York, 1976.

[Wa] A. Watanabe, The Glauberman character correspondence and perfect isometries for blocks of finite groups, J. Algebra, **216** (1999), 548–565.

[Wo1] T.R. Wolf, Character correspondence in solvable groups, Illinois J. Math., **22** (1978), 327–340.

[Wo2] T.R. Wolf, Character correspondences induced by subgroups of operator groups, J. Algebra, **57** (1979), 502–521.

Department of Mathematics
Faculty of Science, Kumamoto University
Kumamoto 860-8555, Japan

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 449–451

Either 71 : 35 or $L_2(71)$ is a maximal subgroup of the Monster

Hiroyoshi Yamaki

§1. Introduction

Let $\mathbb{M}$ be the Monster simple group. Then

$$|\mathbb{M}| = 2^{46}.3^{20}.5^{9}.7^{6}.11^{2}.13^{3}.17.19.23.29.31.41.47.59.71.$$

By [2] 71 : 35 is the normalizer of a Sylow 71-subgroup and 59 : 29 is the normalizer of a Sylow 59-subgroup of $\mathbb{M}$.

The purpose of this note is to prove:

Theorem 1. *Either* 71 : 35 *or* $L_2(71)$ *is a maximal subgroup of* $\mathbb{M}$.

Theorem 2. *Either* 59 : 29 *or* $L_2(59)$ *is a maximal subgroup of* $\mathbb{M}$.

Remark. 71 : 35 is a maximal subgroup of $L_2(71)$ and 59 : 29 is a maximal subgroup of $L_2(59)$. However we do not know whether $L_2(71)$ or $L_2(59)$ is involved in $\mathbb{M}$ or not (See [6]). Since $|L_2(71)| = 72.71.35$ and $|L_2(59)| = 60.59.29$, these are surprisingly small groups in comparison with $\mathbb{M}$.

Theorems 1 and 2 are closely related to the prime graphs of finite groups. Let $G$ be a finite group and $\Gamma(G)$ the prime graph of $G$. $\Gamma(G)$ is the graph such that the vertex set is the set of prime divisors of $|G|$, and two distinct vertices $p$ and $r$ are joined by an edge if and only if there exists an element of order $pr$ in $G$. Let $n(\Gamma(G))$ be the number of connected components of $\Gamma(G)$. It has been proved that $n(\Gamma(G)) \leq 6$ in [7], [4], [5].

Supported in part by Grant-in-Aid for Scientific Research (No.12640030), Japan Society for the Promotion of Science.

Received December 17, 1999.

Revised June 17, 2000.

§2. The proof of Theorems

We will give a proof of Theorem 1. Theorem 2 can be proved by the same way just replacing 71 by 59.

Lemma 1. *The* 71*-signalizer of* $\mathbb{M}$ *is trivial.*

Proof. The list of maximal p-local subgroups of $\mathbb{M}$ in [2] is complete if one adds $7^2 : SL(2,7)$ which is missing (See [6]). The result follows immediately. Q.E.D.

Lemma 2. $L_2(71)$ *is the only possible finite simple group involved in* $\mathbb{M}$ *whose order is divisible by* 71.

Proof. Lemma 2 can be proved using the classification of the prime graph components of finite simple groups in [7], [5], [4] since $\{71\}$ is a connected component of the prime graph of a simple group involved in $\mathbb{M}$ whose order is divisible by 71. Q.E.D.

Next important lemma was essentially proved by Gruenberg and Kegel (See [7]) before the classification of finite simple groups. Applying the classification of finite simple groups we have:

Lemma 3. *Let* G *be a finite group with* $n(\Gamma(G)) \geq 2$*. Then one of the following holds.*

1. G *is a Frobenius group or a* 2*-Frobenius group.*
2. G *has a chain of normal subgroups* $G \rhd L \rhd N \rhd 1$ *such that* N *and* G/L *are nilpotent* π*-groups and* L/N *is a non abelian simple group where* π *is the connected component of* $\Gamma(G)$ *containing* 2.

Proof. See [1]. Q.E.D.

As is well known $\Gamma(\mathbb{M})$ has four connected components (See [3], [7]) and $\{71\}$ is a connected component of $\Gamma(\mathbb{M})$. Let G be a maximal subgroup of $\mathbb{M}$ whose order is divisible by 71. It follows that $n(\Gamma(G)) \geq 2$ and $\{71\}$ is a connected component of $\Gamma(G)$. We can apply Lemma 3.

Suppose that G is a Frobenius group. Then the Frobenius kernel is of order 71 and G is contained in $71 : 35$.

Suppose that G is a 2-Frobenius group. Then G has a chain of normal subgroups: $G \rhd H \rhd K \rhd 1$ such that H is a Frobenius group with kernel K and G/K is also a Frobenius group with kernel H/K. It follows that $|K| = 71$. Since $71 : 35$ is the normalizer of a Sylow 71-subgroup in $\mathbb{M}$, G/K cannot be a Frobenius group, a contradiction.

Suppose that G has a chain of normal subgroups $G \rhd L \rhd N \rhd 1$ such that N and G/L are nilpotent π-groups and L/N is a non-abelian simple group where π is the connected component of $\Gamma(G)$ containing 2. Since

π does not contain 71, $(L:N)$ is divisible by 71. Lemma 1 yields $N=1$. It follows from Lemma 2 that L is $L_2(71)$ and $G=L$ or $G=PGL(2,71)$. Since $\mathbb{M}$ does not contain $71:70$, we have $G=L=L_2(71)$. The proof of Theorem 1 is complete.

Remark. The argument breaks down for the prime divisors of $|\mathbb{M}|$ less than 59 (See [2], [6]).

We have actually proved:

Theorem 3. *Let G be a maximal subgroup of $\mathbb{M}$ whose order is divisible by 71. Then G is isomorphic to $71:35$ or $L_2(71)$.*

Theorem 4. *Let G be a maximal subgroup of $\mathbb{M}$ whose order is divisible by 59. Then G is isomorphic to $59:29$ or $L_2(59)$.*

References

[1] N. Chigira, N. Iiyori and H. Yamaki, Non-abelian Sylow subgroups of finite groups of even order, Invent. Math., **139** (2000), 525–539.

[2] J. Conway, R.T. Curtis, S. Norton, R. Parker and R. Wilson, Atlas of finite groups, Clarendon Press, Oxford, 1985.

[3] N. Iiyori and H. Yamaki, A conjecture of Frobenius, Sugaku Expositions, Amer. Math. Soc., **9** (1996), 69–85.

[4] N. Iiyori and H. Yamaki, Prime graph components of the simple groups of Lie type over the fields of even characteristic, J. Algebra, **155** (1993), 335–343, Corrigenda, **181** (1996) 659.

[5] A. S. Kondrat'ev, Prime graph components of finite simple groups, Math. USSR Sbornik, **67** (1990), 235–247.

[6] S. Norton, Anatomy of the Monster : I, The Atlas of finite groups: Ten years on, Ed. by R. Curtis and R. Wilson, London Math. Soc. Lecture Note Series, **249**, 198–214, Cambridge Univ. Press, Cambridge 1998.

[7] J. S. Williams, Prime graph components of finite groups, J. Algebra, **69** (1981), 487–513.

Department of Mathematics
Faculty of Science, Kumamoto University
Kumamoto 860-8555 Japan
e-mail: yamaki@gpo.kumamoto-u.ac.jp

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 453–464

Radical subgroups of the sporadic simple group of Suzuki

Satoshi Yoshiara

Abstract.

For the sporadic Suzuki simple group, the radical $p$-subgroups for $p = 2$ and 3 are classified and the simplicial complex of their chains is shown to be homotopically equivalent to a $p$-local geometry. Further investigation of the related complexes for $p = 2$ gives a counterexample to Conjecture 1 in [4].

§1. Introduction and Notation

In this note, the poset $\mathcal{B}_p(Suz)$ of radical $p$-subgroups of the sporadic simple group of Suzuki, denoted $Suz$, is determined up to conjugacy for $p = 2$ and 3. Then we have a homotopy equivalence equivariant with group action between the simplicial complex $\Delta(\mathcal{B}_p^{cen}(Suz))$ of chains of centric radical p-subgroups of $Suz$ and a $p$-local geometry of $Suz$. The latter is a well known complex of dimension 2: for $p = 2$ one of the remarkable examples of geometries which are almost buildings (GABs) arising from sporadic simple groups ([8] and §4); and for $p = 3$ the truncation at points of a flag-transitive extended generalized quadrangle (EGQs) which appears as the residue of the extended dual polar space of the Monster ([6] and §5). Further examination leads the author to modify the conjecture given in [4, §4, Conjecture 1].

To give precise expositions, recall the following terminologies for a finite group $G$ and a prime $p$: a nontrivial $p$-subgroup $P$ of $G$ is called *radical* (resp. *centric*), if $O_p(N_G(P)) = P$ (resp. every $p$-element of $C_G(P)$ lies in $Z(P)$). The poset of nontrivial $p$-subgroups of $G$ with respect to inclusion is denoted $\mathcal{S}_p(G)$. We use $\mathcal{B}_p(G)$, $\mathcal{B}_p^{con}(G)$ and $\mathcal{B}_p^{cen}(G)$ to denote the subposets of $\mathcal{S}_p(G)$ consisting of radical $p$-subgroups, radical $p$-subgroups $P$ with *$p$-constrained* normalizer $N = N_G(P)$ (that

Received March 26, 1999.
Revised May 18, 2000.

is, $C_{\bar{N}}(O_p(\bar{N})) \leq O_p(\bar{N})$ with $\bar{N} = N/O_{p'}(N))$ and centric radical p-subgroups, respectively. For a poset X, the *order complex*, denoted $\Delta(X)$, is the simplicial complex with X as the set of vertices and the chains of elements of X as the simplices.

The inclusion gives a G-homotopy equivalence of $\Delta(\mathcal{B}_p(G))$ with $\Delta(\mathcal{S}_p(G))$ (e.g. [2, 6.6.1]) and $\mathcal{B}_p(G) \supseteq \mathcal{B}_p^{con}(G) \supseteq \mathcal{B}_p^{cen}(G)$ for every G and p [4, §4]. If G is a finite group of Lie type in characteristic p, then $\mathcal{B}_p(G) = \mathcal{B}_p^{con}(G) = \mathcal{B}_p^{cen}(G)$ and $\Delta(\mathcal{B}_p(G))$ coincides with the barycentric subdivision of the *building* of G (e.g. [2, 6.6.1]). In [4], we verified analogues of these facts for some sporadic simple groups: if $\mathcal{B}_p(G) = \mathcal{B}_p^{con}(G) = \mathcal{B}_p^{cen}(G)$ then $\Delta(\mathcal{B}_p(G))$ is G-homotopically equivalent to a complex Δ, which is one of p-local geometries of G.

While buildings are defined in a unified way for groups of Lie type, there is no canonical definition of p-local geometry for sporadic G. It just means a G-simplicial complex in which some stabilizers of vertices are p-local subgroups. Some sporadic has no or more than one such complexes constructed in ad hoc manner, though, in general, there is the best one among them in the sense that it satisfies some local axioms similar to those for buildings.

Partially motivated by searching for a unified definition of "the best" p-local geometry of a sporadic simple group G, we gave the following conjecture [4, §4, Conjecture 1] as a generalization of the observations in [4]: for sporadic G having a p-local geometry Δ, $\mathcal{B}_p^{cen}(G) = \mathcal{B}_p^{con}(G)$ and $\Delta(\mathcal{B}_p^{cen}(G))$ (or $\Delta(\mathcal{B}_p^{con}(G))$) is G-homotopically equivalent to Δ.

However, further investigation of $\mathcal{B}_2(Suz)$ reveals that the former part of the above conjecture (and hence also Conjecture 2 in [4]) is *false*: in fact, $\mathcal{B}_2^{con}(Suz)$ consists of $\mathcal{B}_2^{cen}(Suz)$ *and* two conjugacy classes; moreover, the GAB of Suz is *not* even homotopically equivalent to $\Delta(\mathcal{B}_2^{con}(Suz))$, while it *is* to $\Delta(\mathcal{B}_2^{cen}(Suz))$. Thus the above conjecture should be modified as follows by ignoring the former part.

Conjecture: For sporadic G, $\Delta(\mathcal{B}_p^{cen}(G))$ is G-homotopically equivalent to a certain p-local geometry Δ.

The modified conjecture seems to hold for every finite simple group and every prime, if we take as Δ a variant of the best p-local geometry in the sense above. Thus the author dares to propose the following as a uniform definition of p-local geometries:

> For a finite group G and a prime divisor p of its order, a G-simplicial complex Δ is called a *p-local geometry*, if
> (a) it is G-homotopically equivalent to $\Delta(\mathcal{B}_p^{cen}(G))$, and
> (b) no proper subcomplex of Δ satisfies the condition (a).

§2. Maximal 2-local subgroups of *Suz*

We follow the notation in §1 as well as the standard terminologies on group theory (e.g. [1] and [5]). Throughout the note, set $G := Suz$. We only consider the primes $p = 2$ and 3, as $|G|_p \leq p^2$ for other primes.

There are two classes $2A$ and $2B$ of involutions of G. The product of commuting distinct two $2A$-involutions is a $2A$-involution [5, Table III]. Thus every maximal 2-local subgroup is contained in the normalizer of a $2A$ or $2B$-pure elementary abelian subgroup. It is shown in [5] that the normalizer of a $2A$-pure elementary abelian subgroup is conjugate to a subgroup of one of the following three groups.

$C_G(z) \cong 2_-^{1+6} \cdot U_4(2)$ (z, a $2A$-involution)
$N_G(F_2) \cong 2^{2+8} : (A_5 \times S_3)$ (F_2, a $2A$-pure 2^2-group)
$N_G(F_3) \cong 2^{4+6} : (3 \cdot A_6)$ (F_3, a $2A$-pure 2^4-group)

In [7], it is shown that a $2B$-pure elementary abelian subgroup is of order at most 4, and that its normalizer is conjugate to a subgroup of $N_G(F_2)$ or one of the following two groups:

$N_G(F_4) \cong (A_4 \times L_3(4)).2$ (F_4, a $2B$-pure 2^2-group)
$N_G(F_5) \cong (E_4 \times 3^2 : Q_8).S_3$ (F_5, a $2B$-pure 2^2-group)

Details of the structure $N_G(F_i)$ $(i = 4, 5)$ are given below with the latter classification, because they are not contained in [5] but required later.

The centralizer of a $2B$-involution u has a subgroup $\langle u, v\rangle \times L$ of index 2, where $\langle u, v\rangle$ is a $2B$-pure 2^2-subgroup and $C_G(u)^\infty = L \cong L_3(4)$ [5, 2.5]. Every element of order 3 of L is a $3C$-element, as it commutes with the $2B$-involution u [5, Table V]. For a $3C$-element x of L, $C_G(x) = C_G(M) = M \times A$, where M is a $3C$-pure 3^2-subgroup containing x and $A \cong A_6$. As $\langle u, v\rangle \leq C_G(x)$, $\langle u, v\rangle \leq A$.

Let $D := \langle u, v, t\rangle \cong D_8$ be a Sylow 2-subgroup of A containing $\langle u, v\rangle$. We may take $t^2 = 1$, $v^t = uv$, $Z(D) = \langle u\rangle$. Two 2^2-subgroups $F_4 := \langle u, v\rangle$ and $F_5 := \langle u, t\rangle$ of D are $2B$-pure, as they commute with the $3C$-element x. The normalizers in $A \cong A_6$ of F_i $(i = 4, 5)$ are S_4: we denote $N_A(F_4) = F_4 \langle x, t\rangle$ and $N_A(F_5) = F_5 \langle y, v\rangle$ with x and y elements of order 3 inverted by t and v, respectively. Thus $N_G(F_i)$ is a nontrivial split extension of $C_G(F_i)$ by S_3 $(i = 4, 5)$. In particular, $O_2(N_G(F_i)) \leq C_G(F_i)$ $(i = 4, 5)$. We have $(C_G(u) \geq)$ $C_G(F_4) = F_4 \times L \cong 2^2 \times L_3(4)$. Thus $O_2(N_G(F_4)) = F_4 \in \mathcal{B}_2(G)$. However, $N_G(F_4)$ is not 2-constrained nor centric, because of $L \cong L_3(4)$.

To determine the structure of $C_G(F_5)$, we examine the action of t on L. As M is a 3-subgroup of $C_G(u)$, it lies in L, and so it is a Sylow 3-subgroup of $L \cong L_3(4)$. Since $[t, v] \neq 1$, we have $C_G(u) = ((\langle u, v\rangle \times L) \langle t\rangle$. As $|C_G(g)|_2 = 2^2$ for an element g of order 7 of L, the involution t does not centralize L. Thus t induces a unitary automorphism of $L \cong L_3(4)$, as $C_L(t) \geq M \cong 3^2$. Then $C_L(t) = MQ \cong U_3(2^2)$ with $Q \cong Q_8$ acting fixed point freely on M. Inside $C_G(u)$, we have $C_G(F_5) = F_5 \times (M.Q)$. Then $O_2(N_G(F_5)) = F_5 \in \mathcal{B}_2(G)$, which is not 2-centric because of Q. The normalizer $N_G(F_5)$ is solvable, and so 2-constrained.

The complement $\langle x, t\rangle \cong S_3$ acts on L with a non-normal subgroup $\langle t\rangle$ inducing a unitary automorphism. Thus its normal subgroup $\langle x\rangle$ centralizes L. Then $N_G(F_4) = (F_4 \langle x\rangle \times L)\langle t\rangle$, where $F_4 \langle x\rangle \cong A_4$.

The quotient group $\overline{N_G(F_5)} = N_G(F_5)/F_5$ is a direct product of $\overline{M.Q} \cong 3^2 Q_8$ with $\overline{\langle y, t\rangle} \cong S_3$, because $\overline{\langle y, t\rangle}$ acts on $\overline{M.Q}$, while t centralizes $M.Q$. However, $N_G(F_5)$ is not a direct product of $(F_5 \times M.Q)$ with $\langle y, t\rangle$ as we see below. The group $Q \cong Q_8$ acts on $A = C_G(M)' \cong A_6$, while it centralizes a Sylow 2-subgroup $\langle u, t, v\rangle$ of A. Note $[Q, A] \neq 1$: because $Q \in C_G(A)$ would imply that a Sylow 2-subgroup of the centralizer of an element of order 5 of A (which is a $5A$-element by [5, Table V]) is Q_8, while G has a subgroup $A_5 \times A_6$ and a Sylow 2-subgroup of A_6 is D_8. Thus $[Q : C_Q(A)] = 2$ and $Q/C_Q(A)$ corresponds to an odd permutation of S_6. Then $MC_Q(A)$ is normal in $N_G(F_5)$, and $N_G(F_5)/MC_Q(A)$ is a split extension by $\langle y, v\rangle \cong S_3$ of its permutation module $\mathbf{F}_2^3$.

The involution of $C_Q(A) \cong 4$ centralizes a $5A$-element of A, and so it lies in the class $2A$ [5, Table V]. As $(Q \leq)\ L \cong L_3(4)$ has a single class of involutions, every involution of L lies in the class $2A$. Involutions of $N_G(F_4) \setminus (F_4 \langle x\rangle \times L)$ are conjugate to t, and those of $(F_4 \langle x\rangle \times L) \setminus L$ are conjugate to u or ul with l an involution of L. They are $2B$-involutions, as the product of commuting distinct $2A$-involutions lies in $2A$. Hence L is a subgroup of $N_G(F_4)$ generated by $2A$-involutions.

Lemma 1. *If E is a $2B$-pure elementary abelian subgroup of G, then $N_G(E)$ is contained in $N_G(F_i)$ $(i = 4, 5)$ or $N_G(F_2)$ up to conjugacy.*

Proof. Let u be the above $2B$-involution of F_i $(i = 4, 5)$. We may assume $u \in E$ and $|E| = 4$, and hence $E \leq C_G(u) = (F_4 \times L)\langle t\rangle$. If $E \leq F_4 \times L$, then $E = F_4$ or $E = \langle u, gl\rangle$ for an involution $l \in L$ and $g \in F_4$. In the latter case, the subgroup of $C_G(E)$ generated by $2A$-involutions is $C_L(l)$, a Sylow 2-subgroup of L, and thus $Z(C_L(l)$ is conjugate to F_2 [5, 2.5]. Then $N_G(E) \leq N_G(F_2)$ up to conjugacy.

Note that if glt with $g \in F_4$, $l \in L$ is an involution, then $1 = (glt)^2 = gl.tgt.tlt = gg^t.ll^t \in F_4 \times L$, and hence $g \in \langle u\rangle$ and lt is an involution in Lt. Since $Aut(L_3(4)) \setminus L_3(4)$ has a single class of involutions, glt is conjugate to gt under L. Thus if $E \not\leq F_4 \times L$, then $E = \langle u, t\rangle = F_5$ up to conjugacy. Q.E.D.

§3. Radical 2-subgroups of *Suz*

We freely use the notation in §2. We also set $U_i := O_2(N_G(F_i))$ $(i = 1, \dots, 5)$, where $F_1 = \langle z \rangle$. Then

$$U_1 \cong 2_-^{1+6},\ U_2 \cong 2^{2+8},\ U_3 \cong 2^{4+6},\quad U_4 = F_4 \cong 2^2 \text{ and}$$
$$U_5 = F_5 \cong 2^2;$$

and they are radical 2-subgroups of G, as we remarked. No two of them are conjugate in view of their normalizers. From the discussions of §2, we may take $F_1 \leq F_2 \leq F_3$ and $\langle F_4, F_5 \rangle = F_4 F_5 \cong D_8$.

Proposition 2. *There are exactly* 10 *classes of radical* 2*-subgroups of* G *with the following representatives*:

R	$R \cong$	$Z(R)$	$N_G(R)$
U_5	2^2	2^2	$(U_5 \times 3^2 {:} Q_8) {:} S_3$
U_4	2^2	2^2	$(U_4 {:} 3 \times L_3(4)).2$
U_{45}	D_8	2	$U_4.2 \times 3^2 {:} Q_8$
U_3	2^{4+6}	2^4	$U_3 {:} (3 \cdot A_6)$
U_2	2^{2+8}	2^2	$U_2 {:} (A_5 \times S_3)$
U_{23}	$2^2[2^8 2^2]$	2^2	$U_2(2^2 {:} 3 \times S_3) = U_3(3.S_4)$
U_1	2_-^{1+6}	2	$U_1 \cdot U_4(2)$
U_{12}	$2^2[2^8.2^2]$	2	$U_1 \cdot 2^4 A_5 = U_2 : (A_5 \times 2)$
U_{13}	$2^3[2.2^6.2^2]$	2	$U_1 \cdot 2_+^{1+4}(3 \times S_3) = U_3 {:} (3 \times S_4)$
U_{123}	*Sylow*	2	$U_{123}.3$

Furthermore, we may take $U_{45} = U_4 U_5$ *with* $N_G(U_{45}) = N_G(U_4) \cap N_G(U_5)$, $U_{ij} = U_i U_j$ $(i, j \in \{1, 2, 3\})$ *with* $N_G(U_{ij}) = N_G(U_i) \cap N_G(U_j)$, *and* $U_{123} = U_1 U_2 U_3$ *with* $N_G(U_{123}) = \cap_{i=1}^3 N_G(U_i)$.
In particular, $\mathcal{B}_2^{cen}(G)$ *consists of* 7 *conjugacy classes of* $U_X (\emptyset \neq X \subseteq \{1, 2, 3\})$; *while* $\mathcal{B}_2^{con}(G)$ *consists of those classes together with* 2 *further classes of* U_5 *and* U_{45}.

Proof. Let U be any radical 2-subgroup of G. If $N_G(U) \leq N_G(F_5)$ but $U \neq F_5 = U_5$, then $U/U_5 \in \mathcal{B}_2(N_G(F_5)/F_5)$ by [4, 1.9]. We saw $N_G(F_5)/F_5 \cong (3^2 Q_8) \times S_3$ in §2. By Lemma [3, 3.2] $\mathcal{B}_2((3^2 Q_8) \times S_3)$ consists of three conjugacy classes with representatives Q_8 in the first direct factor, 2 in the second direct factor, and $Q_8 \times 2$. In the first and the last cases, we may take $U = U_5 \times Q$ and $U = (U_5 \times Q) \langle v \rangle$ respectively. Then the central involution of Q is a unique $2A$-involution of U, because $L \cap U = Q$ and $2A$-involutions of $N_G(F_5)$ lie in L. Hence up to conjugacy $N_G(U) \leq C_G(z)$. In the second case, $U = U_5 \langle v \rangle \cong D_8$ with center $\langle u \rangle$, and hence $N_G(U) \leq C_G(u) \leq N_G(U_4)$.

Assume $N_G(U) \leq N_G(U_4)$ but $U \neq U_4$. Then U/U_4 is a radical 2-subgroup of $N_G(U_4)/U_4 \cong (Z_3 \times L_3(4)).2$. If $U \cap L \neq 1$, $N_G(U)$

$(\leq N_G(U_4) \leq N_G(L))$ normalizes a $2A$-pure subgroup $\Omega_1(Z(U \cap L)) \neq 1$. If $U \cap L = 1$, we may take $U = U_4 \langle t \rangle$, and hence $U = U_4 \langle t \rangle = \langle F_4, F_5 \rangle \cong D_8$. Conversely, the normalizer of $U_{45} := \langle F_4, F_5 \rangle$ lies in the centralizer of a $2B$-involution u of $Z(U_{45})$. Inside $C_G(u) = (U_4 \times L)\langle t \rangle$, we see $C_G(U_{45}) = \langle u \rangle \times C_L(t)$ and $N_G(U_{45}) = U_{45} \times C_L(t) \cong D_8 \times (3^2 : Q_8)$, and hence U_{45} is a radical subgroup but not centric. The normalizer $N_G(U_{45})$ is solvable and so 2-constrained.

Assume now that $N_G(U) \leq N_G(U_3)$ but $U \neq U_3$. Then $U/U_3 \in \mathcal{B}_2(N_G(U_3)/U_3) = \mathcal{B}_2(3A_6)$. The action of $N_G(U_3)/O_{2,3}(N_G(U_3)) \cong A_6$ on $Z(U_3) = F_3 \cong 2^4$ is equivalent to the restriction to $Sp_4(2)'$ of the action of $Sp_4(2) \cong S_6$ on its natural module. Then the subspace $C_{F_3}(U) = Z(U)$ fixed by a unipotent radical U/U_3 is a totally isotropic 1 or 2-subspace. In the former case, $N_G(U) \leq C_G(z)$ up to conjugacy. In the latter case, $Z(U)$ is conjugate to F_2 by [5, 2.4], and thus $N_G(U) \leq N_G(U_2)$ up to conjugacy.

Assume that $N_G(U) \leq N_G(U_2)$. As $\mathcal{B}_2(N_G(U_2)/U_2) = \mathcal{B}_2(A_5 \times S_3)$, U/U_2 is one of the following by [3, 3.2]: the trivial group, a 2^2-subgroup of A_5, 2 of S_3, or $2^2 \times 2$. In the latter two cases, as S_3 is faithful on $Z(U_2) = F_2 \cong 2^2$, U contains an involution which flips two involutions in F_2. Thus $Z(U)$ has a unique involution, and $N_G(U) \leq C_G(z)$ up to conjugacy. In the second case, $Z(U) = F_2$ and $N_G(U) \leq N_G(F_2)$. Then $N_G(U)/U_2 \cong A_4 \times S_3$ and $O_2(N_G(U)) = U \in \mathcal{B}_2(G)$. Hence we have one new radical group U_{23} $(\leq C_G(F_2) \cong 2^{2+8} : A_5)$ with $U_{23}/U_2 \cong 2^2$. In fact $U_{23} = \langle U_2, U_3 \rangle$.

Finally assume that $N_G(U) \leq C_G(z)$ but $U \neq U_1$. Since U_1 is an extraspecial group, $Z(U) = Z(U_1) = \langle z \rangle$ for every $U/U_1 \in \mathcal{B}_2(C_G(z)/U_1)$. Then $N_G(U) \leq C_G(z)$ and $U \in \mathcal{B}_2(G)$. As $C_G(z)/U_1 \cong \Omega_6^-(2)$ is of Lie rank 2, including U_1, there are exactly 4 classes of radical 2-subgroups of G with centers conjugate to $\langle z \rangle$. The subgroups U_1, U_1U_2, U_1U_3 and $U_1U_2U_3$ are their representatives, because the images of the last three in $C_G(z)/U_1$ are the unipotent radicals fixing a singular 1, 2-subspaces and its flag, respectively, of the natural module $U_1/\langle z \rangle$ for $\Omega_6^-(2)$.

We obtained 10 classes of radical subgroups. No two of them are conjugate, in view of their structures. The normalizers and generators of representatives are calculated inside maximal 2-locals containing them. Q.E.D.

§4. Homotopy equivalence for $p = 2$

Let $\mathcal{F}$ be the poset of the conjugates of F_i $(i = 1, 2, 3)$ with respect to inclusion $\leq$. The order complex $\Delta(\mathcal{F})$ is called *the GAB of $G = Suz$* (which is the most famous 2-local geometry of G, and so is denoted by

$\mathcal{L}_2(G)$ later). This looks different from that given in [8, Def.6.2] (denoted $(\mathcal{G}, I)$ there), but using the flag-transitivity of $\mathcal{G}$ it is immediate to verify that the following map gives an isomorphism of $(\mathcal{G}, I)$ with $(\mathcal{F}, \leq)$: $\tau : \mathcal{G} \ni x \mapsto Z(O_2(K_x)) \in \mathcal{F}$, where K_x denotes the kernel of the action of the stabilizer of x in G on the residue at x. More precisely, τ sends a 'point', 'line' or 'cross' [8, §6] to a conjugate of F_1, F_2 or F_3, respectively, and a flag is mapped to a chain.

In the following, we sometimes identify $\mathcal{G}$ with $\mathcal{F}$ via the map τ, and use terms, points, lines and crosses. For each nonempty subset X of $\{1,2,3\}$, $F_X := \{F_i | i \in X\}$ is a flag of type X, because we take $F_1 < F_2 < F_3$. We may verify that the stabilizer of F_X in G is $N_G(U_X)$ and that U_X is the O_2-part of the kernel of the action of $N_G(U_X)$ on the residue of the flag F_X.

Recall that the *barycentric subdivision* $\tilde{\Delta}$ of a simplicial complex Δ is a complex with the simplices of Δ as its vertices and the chain $(\sigma_1 \subset \sigma_2 \subset \ldots \subset \sigma_n)$ of simplices of Δ as the simplices. The geometric realization of Δ and its barycentric subdivision $\tilde{\Delta}$ are the same. In particular, they are homotopically equivalent.

From the above remarks and Proposition 2, we have:

Proposition 3. *The order complex $\Delta(\mathcal{B}_2^{cen}(G))$ of the poset of centric radical 2-subgroups of G is isomorphic to the barycentric subdivision of the GAB $\mathcal{L}_2(G)$ of G. Consequently $\Delta(\mathcal{B}_2^{cen}(G))$ is G-homotopically equivalent to the 2-local geometry $\mathcal{L}_2(G)$.*

Since $\mathcal{B}_2^{cen}(G)$ is a proper subset of $\mathcal{B}^{con}(G)$ (Proposition 2), the former part of Conjecture 1 in [4] (see also introduction) does not hold, but from Proposition 3 the latter part holds for $\Delta(\mathcal{B}_2^{cen}(G))$. To examine the homotopy equivalence of $\Delta(\mathcal{B}_2^{con}(G))$ with the 2-local geometry of G, we calculate their Euler characteristics.

A radical subgroup conjugate to U_X ($X \subseteq \{1,2,3\}$ or $X \subseteq \{4,5\}$) is called to be *of type* X. The sequence of types of terms in a chain is called the *type* of that chain. We have $U_X < U_Y$ for $X \subset Y \subseteq \{1,2,3\}$ or $X \subset Y \subseteq \{4,5\}$ by Proposition 2. Furthermore,

Lemma 4. *Up to conjugacy the following inclusions hold:*

$U_4 < U_2$ and $U_4 < U_3$, but $U_4 \not\leq U_1$;
$U_5 \not\leq U_i$ for every $i = 1,2,3$;
$U_5 < U_{13}$ but $U_5 \not\leq U_{12}$ and $U_5 \not\leq U_{23}$;
$U_{45} \not\leq U_X$ for every proper subset X of $\{1,2,3\}$.

Proof. The group $C_G(U_1)/U_1 \cong O_6^-(2) \cong SU_4(2)$ has two classes of involutions, called $2A$ and $2B$ (see e.g.[1]). In the natural unitary module $GF(4)^4$ for $SU_4(2)$, the subspace fixed by a $2A$ (resp. $2B$)-involution of $SU_4(2)$ is of dimension 3 (resp. 2). It is straightforward to verify that there are exactly two conjugacy classes of $2B$-pure 2^2-subgroups: a representative of one class fixes 1 isotropic point p and 3 isotropic lines though p; that of the other class fixes 5 isotropic points p_i $(= 1, \dots, 5)$ on an isotropic line l_1 and 5 isotropic lines l_i $(i = 1, \dots, 5)$, where l_2 and l_3 (resp. l_4 and l_5) though p_2 (resp. p_3).

We may assume that $F_1 = \langle z \rangle$ with a $2A$-involution of $C_Q(A) \leq L \cong L_3(4)$ (with notation in Section 2) centralized by $U_{45} \cong D_8$. Then U_Y lies in $C_G(F_1)$ for every $Y \subseteq \{4, 5\}$. Now $O_2(C_G(F_1)) = U_1 \cong 2_-^{1+6}$ contains $F_2 > Z(U_1) = F_1$, and hence every involution of U_1 is a $2A$-involution. In particular, $2B$-pure 2^2-subgroups U_i $(i = 4, 5)$ and so U_{45} of G intersect trivially with U_1, and each of them is isomorphic to its image in $C_G(F_1)/U_1 \cong SU_4(2)$. For a $2B$-involution $u \in Z(U_{45})$, we may verify that its image in $C_G(F_1)/F_1$ does not centralize a subgroup of order 9, and hence it is a $2B$-involution of $SU_4(2)$. Thus the images $\overline{U_i}$ $(i = 4, 5)$ are $2B$-pure 2^2-subgroups of $SU_4(2)$.

Since $C_G(U_5)$ does not contain a $2A$-pure 2^2-subgroup (see Section 2), U_5 is not contained in U_2, U_3 nor U_{23} up to conjugacy. On the other hand, from the explicit shapes of U_2 and U_3 (e. g. see W_2 and W_3 in [8, §3,4]), there is a $2B$-pure 2^2-subgroup contained in both of them. In view of $C_G(u)$, this should be U_5. Since the sets of isotropic points and lines correspond respectively to the 'crosses' and 'lines' incident to the 'point' F_1 [8, §6], the image $\overline{U_5} \leq U_2/F_1$ corresponds to a $2B$-pure subgroup of $SU_4(2)$ fixing 5 points and 5 lines. On the other hand, the image $\overline{U_4}$ corresponds to a $2B$-pure subgroup of $SU_4(2)$ fixing 1 point and 3 lines. Interpreting these informations in terms of inclusions of the corresponding stabilizers (subgroups of type X with $1 \in X \subseteq \{1, 2, 3\}$), we conclude the above inclusions. Q.E.D.

Proposition 5. (1) *The Euler characteristic of* $\mathcal{B}_2(G)$ *(that is, the alternating sum of numbers of* m*-chains for* $m = -1, \dots, 3$*) is* $2^{13}.514507 = 2^{13} \cdot 7 \cdot 31 \cdot 2371$.

(2) *The Euler characteristic of* $\Delta(\mathcal{B}_2^{con}(G))$ *is* $-2^{11}.823.1229$*, while that of* $\Delta(\mathcal{B}_2^{cen}(G))$ *(or* $\mathcal{L}_2(G)$*) is* $2^{10}.4091$*. Thus* $\Delta(\mathcal{B}_2^{con}(G))$ *is not homotopically equivalent to the* 2*-local geometry* $\mathcal{L}_2(G)$.

Proof. From the above lemma, the possible types of chains are: Sequences of properly increasing nonempty subsets of $\{1, 2, 3\}$; 45, (4, 45), (5, 45), (45, 123), (4, 45, 123), (5, 45, 123); 5, (5, 13), (5, 123); (5, 13, 123); 4, (4, 2), (4, 3), (4, 12), (4, 23), (4, 123), (4, 2, 12), (4, 2, 23), (4, 2, 123), (4, 3, 23), (4, 3, 13), (4, 3, 123); (4, 2, 12, 123), (4, 2, 23, 123), (4, 3, 13, 123), (4, 3, 23, 123). Denote by $n(X_1, \dots, X_m)$ the number of chains of type $(X_1, \dots, X_m)$.

Let χ be the Euler characteristic of $\Delta(\mathcal{B}_2^{cen}(G))$, that is, the alternating sum of $n(X_1, \dots, X_m)$'s with sign $(-1)^{m-1}$ for all nonempty sequences $X_1 \subset \cdots \subset X_m \subseteq \{1,2,3\}$ together with the additional term -1. Moreover, let $\chi(4)$ (resp. $\chi(5)$) be the alternating sum of the numbers of chains of type containing 4 (resp. 5) but not 45, and $\chi(45)$ be the alternating sum of the numbers of type containing a term of type 45:

Note that for $m > 1$, $n(X_1, \dots, X_m)$ equals $n(X_1, \dots, X_{m-1})$ times the number of subgroups of type X_m containing $U_{X_{m-1}}$. The latter number is easy to find if $X_{m-1} \subset \{1,2,3\}$, because the 2-local geometry $\mathcal{L}_2(G)$ has orders 2, 2 and 4. Then it is straightforward to verify: $\chi = 2^{10}.4091$, $\chi(5) = n(5)(1 - 9 - 9.3 + 9.3) = (-8)|G|/|N_G(F_5)| = -2^{10}.3^4.5^2.7.11.13$ and $\chi(45) = n(45)(1-1-1-9+9+9) = 8|G|/|N_G(U_{45})| = 2^{10}.3^5.5^2.7.11.13$. As for $\chi(4)$, the above remark yields the sums of terms $n(4,2,\dots) = n(4,2)(1 - 3 - 5 + 15 - 15 - 15) = (-8)n(4,2)$, $-n(4,12) + n(4,12,123) = 4n(4,12)$, $-n(4,23)+n(4,23,123) = 2n(4,23)$, and $-n(4,13)+n(4,13,123) = 2n(4,13)$.

To determine the numbers $n(4,2)$ etc., we need the following facts (the proofs are omitted, as they are straightforward): there are exactly 9 $2A$-involutions in $C_G(F_5)$: there are exactly 21×2 crosses (subgroups conjugate to F_3) in $L \cong L_3(4)$: there are two classes of lines (subgroups conjugate to F_2) in L, each line l of a class of length 3.5.7 is contained in exactly 5 crosses π with $U_4 \leq U_{l,\pi}$, and each line m of the other class of length $2^2.3.5.7$ is contained in exactly one cross μ with $U_4 \leq U_{m,\mu}$, where for example $U_{m,\pi}$ denotes the kernel of the action of the stabilizer of a flag (m,π) on the set of three points incident with (m,π). From these facts and the substructure of the residue at a point F_1 fixed by $\overline{U_i}$ $(i = 4,5)$ (see the proof of the previous lemma), we have: $n(4,2)/n(4) = 3.5.7$, $n(4,12)/n(4) = 3^2.5.7$, $n(4,23)/n(4) = 3.5.7 \times 5 + 2^2.3.5.7 \times 1$, $n(4,13)/n(4) = 3^2.5.7 \times 2$, $n(4,123)/n(4) = 3^2.5.7 \times (5+4)$. As $n(4) = [G : N_G(F_4)]$, we then calculate $\chi(4) = n(4)(1 - 3^4.5.7 + 2.3^4.5.7 - 8.3.5.7 + 8.3^2.5.7 - 2^5.3.7) = 2^{10}.3^4.5.11.13$. This yields the Euler characteristic of $\Delta(\mathcal{B}_2(G))$, because it is $\chi + \chi(4) + \chi(5) + \chi(45)$. Moreover, the Euler characteristic of $\Delta(\mathcal{B}_2^{con}(G))$ is given by $\chi + \chi(5) + \chi'(45)$, where $\chi'(45)$ is the alternating sum of numbers of chains of type containing 45 but not 5, so it is $n(45)(1 - 1 + 9 - 9) = 0$. Q.E.D.

§5. Radical 3-subgroups of G

There are three classes of elements of order 3 in G. It follows from [5, 2.2, 2.3] that a maximal 3-local subgroup of G is conjugate to one of the following four groups:

$N_G(T_1) \cong$ $3 \cdot U_4(3).2$, where T_1 is generated by a $3A$-element, and there is an involution inverting T_1 which induces a field automorphism on $C_G(T_1)/T_1 \cong U_4(3)$.

$N_G(T_2) \cong$ $3^{2+4} : 2(A_4 \times 2^2).2$, where T_2 is a 3^2-subgroup with two (resp. two) cyclic subgroups of type $3A$ (resp. $3B$).

$N_G(T_3) \cong$ $3^5 : M_{11}$, where $T_3 \cong 3^5$ consists of 11 (resp. 110) cyclic subgroups of type $3A$ (resp. $3B$).

$N_G(T_4) \cong$ $(3^2 : 4 \times A_6).2$, where T_4 is a $3C$-pure 3^2-subgroup.

Note that with notation in Section 2, $T_4 = M$ and $(M : C_Q(A)) \times A$ is a subgroup of $N_G(F_4)$ isomorphic to $3^2 : 4 \times A_6$. As the involutions of $C_Q(A)$ lie in the class $2A$, elements of order 3 of A are $3A$ or $3B$-elements. As the product of commuting distinct two $3A$-elements is either a $3A$ or $3B$-element [5, Table III], every $3A$-element of $N_G(F_4)$ lies in A. We also note that every 3^2-subgroup generated by $3A$-elements is conjugate to T_2. Thus we may assume $T_1 < T_2 < T_3$.

We set $V_i := O_3(N_G(T_i))$ $(i = 1, \dots, 4)$. Then $T_1 = V_1 \cong 3$, $V_2 \cong 3^{2+4}$, $T_3 = V_3 \cong 3^5$ and $T_4 = V_4 \cong 3^2$, $T_i = Z(V_i)$ and $N_G(T_i) = N_G(V_i)$ for $i = 1, \dots, 4$. Clearly, V_i is a radical 3-subgroup for every $i = 1, \dots, 4$.

Proposition 6. *There are exactly* 5 *classes of radical* 3*-subgroups of* G *with representatives* V_i $(i = 1, \dots, 4)$ *and a Sylow* 3*-subgroup* S. *In particular,* $\mathcal{B}_3^{cen}(G) = \mathcal{B}_3^{con}(G)$ *consists of* 3 *classes of subgroups* V_i $(i = 2, 3)$ *and* S.

Proof. Let V be any radical 3-subgroup of G. If $N_G(V) \leq N_G(T_4)$ but $V \neq T_4$, it follows from [4, Lemma 1.9] that V/T is a radical 3-subgroup of $N_G(T_4)/T_4 \cong (4 \times A_6).2$, which implies that $V/T \cong 3^2$. Then we have $V = T_4 \times T$, where T is a Sylow 3-subgroup of the A_6-subgroup $A = C_G(T_4)'$. It follows from the previous remarks that $T \cong 3^2$ is the subgroup of V generated by $3A$-elements in V. Thus $N_G(V) \leq N_G(T)$ and T is conjugate to T_2. Then up to conjugacy $N_G(V) \leq N_G(T_2)$. But then $V \cong 3^4$ would contain $O_3(N_G(T_2)) = V_2 \cong 3^{2+4}$ by [4, Lemma 1.9], which is a contradiction.

Assume that $N_G(V) \leq N_G(T_i)$ but $V \neq V_i$ for $i = 2$ or 3. Observe that the radical 3-subgroups of $N_G(T_2)/V_2 \cong 2(A_4 \times 2^2).2$ are Sylow 3-subgroups, and similarly those of $N_G(T_3)/V_3 \cong M_{11}$. Thus V is a Sylow 3-subgroup of G in these cases.

Finally, consider the case $N_G(V) \leq N_G(T_1)$ but $V \neq T_1$. Then V/T_1 is a radical 3-subgroup of $N_G(T_1)/T_1 \cong U_4(3).2$. Thus V/T_1 is the unipotent radical of the stabilizer of an isotropic point, line or a flag of the 3-dimensional unitary projective space over $GF(9)$. In the last case, V is a Sylow 3-subgroup of G. Then $(N_G(T_2) \cap N_G(T_1))/T_1 \cong 3^{1+4}2.(A_4 \times 2).2$ (resp. $(N_G(T_3) \cap N_G(T_1))/T_1 \cong 3^4 : M_{10})$ is a parabolic subgroup of

$U_4(3).2$ ($U_4(3)$ extended by a field automorphism) corresponding to an isotropic point (resp. line) with unipotent radical $T_2/T_1 \cong 3^{1+4}$ (resp. $T_3/T_1 \cong 3^4$). Thus in the former two cases, V is conjugate to T_2 or T_3. Q.E.D.

The EGQ $\mathcal{L}_3(G)$ of $G = Suz$ (which is a 3-local geometry) is usually defined as the order complex of the poset $\mathcal{T}$, the union of the conjugates of T_i $(i = 1, 2, 3)$ under G. Let $\mathcal{T}'$ be the subposet of $\mathcal{T}$ of conjugates of T_2 and T_3. Then $\Delta(\mathcal{T}')$ is the truncation of $\mathcal{L}_3(G)$ at the 'points'.

Proposition 7. *The complex $\Delta(\mathcal{B}_3^{cen}(G))$ is G-homotopically equivalent to the truncation of the EGQ $\mathcal{L}_3(G)$ at the conjugates of T_1.*

Proof. Let $\mathcal{P}$ be the union of $\mathcal{B}_3^{cen}(G)$ (consisting of conjugates of V_2, $V_3 = T_3$ and Sylow 3-subgroups) with the conjugates of $T_2 = Z(V_2)$. As a 3^2-subgroup of $M_{11} \cong N_G(T_3)/T_3$ fixes exactly two of 11 subgroups of type $3A$ of T_3, we may take $T_2 = Z(S)$ with S a Sylow 3-subgroup of G containing T_3.

We examine the subposet $\mathcal{P}_{>T_2} := \{X \in \mathcal{P} | T_2 < X\}$. Observe that V_2 has exactly two subgroups of type $3A$, which lie in $Z(V_2) = T_2$. Thus if $T_2 \leq V_2^g$ for $g \in G$, then the subgroup T_2^g generated by $3A$-elements of V_2^g coincides with T_2, and hence $g \in N_G(T_2) = N_G(V_2)$. As T_3 is generated by all $3A$-elements in S, we have $T_2 < S^g$ iff $T_2 < T_3^g$ for $g \in G$. The 5-transitivity of $N_G(T_3)/T_3 \cong M_{11}$ on the 11 subgroups of T_3 of type $3A$ implies that $T_2 < T_3^g$ iff $T_2^{g^{-1}} = T_2^h$ for some $h \in N_G(T_3)$, and thus $T_3^g = T_3^k$ for $k = hg \in N_G(T_2)$. Hence $\mathcal{P}_{>T_2}$ consists of S^k, T_3^k $(k \in N_G(T_2))$ together with V_2. For $k \in N_G(T_2) = N_G(V_2)$, there is no inclusion relation between V_2 and T_3^k; S^k contains V_2, as $S > V_2$; while S^k is the unique conjugate of S containing T_3^k. Thus the complex $\Delta(\mathcal{P}_{>T_2})$ is contractible to V_2. Then it follows from Theorem of Bouc [2, 6.6.5] that the inclusion of $\mathcal{B}_3^{cen}(G)$ to $\mathcal{P}$ gives a G-homotopy equivalence between their order complexes.

We will verify that the inclusion of $\mathcal{T}'$ into $\mathcal{P}$ is also a G-homotopy equivalence of $\Delta(\mathcal{T}')$ with $\Delta(\mathcal{P})$ by the same theorem. The subposet $\mathcal{P}_{<V_2} = \{X \in \mathcal{P} | X < V_2\}$ consists of a single element T_2 and so is contractible. The subposet $\mathcal{P}_{<S} = \{X \in \mathcal{P} | X < S\}$ consists of T_3 (the unique subgroup generated by 11 subgroups of type $3A$ in S), the $\binom{11}{2}$ conjugates of T_2 under $N_G(T_3)$, and V_2. (We see V_2 is the unique conjugate of V_2 contained in S as follows. Assume $S \geq V_2^g$ for some $g \in G$. Then $V_2^g \trianglelefteq S$ as $[S : V_2^g] = 3$, and then S acts on the set of two subgroups of V_2^g of type $3A$. Then the Sylow 3-subgroup S centralizes T_2^g generated by those subgroups, and thus $T_2 = Z(S)$ coincides with T_2^g. Then $g \in N_G(T_2) = N_G(V_2)$ and $V_2^g = V_2$.) We may collapse

$\Delta(\mathcal{P}_{<S})$ to the 1-simplex with vertices T_2, T_3 by simultaneously deleting T_2^g and (T_2^g, T_3) for all $g \in N_G(T_3)$ with $T_2^g \neq T_2$ as well as V_2 and (T_2, V_2). Thus $\Delta(\mathcal{P}_{<S})$ is contractible. Q.E.D.

Remark. Using similar methods to those in Section 3, the Euler characteristic of $\Delta(\mathcal{B}_3(G))$ (resp. $\Delta(\mathcal{B}_3^{cen}(G))$ and $\Delta(\mathcal{L}_3(G))$) is calculated to $-3^6.67843$ (resp. $-3^5.38587$ and $3^5.41.733$).

References

[1] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[2] D. Benson, *Representations and Cohomology II : Cohomology of groups and modules*, Cambridge studies in advanced mathematics, **31**, Cambridge U. Press, Cambridge, 1991.

[3] M. Sawabe, 2-Radical subgroups of the Conway simple group Co_1, *J. Algebra*, **211** (1999), 115–133.

[4] S.D. Smith and S. Yoshiara, Some homotopy equivalences for sporadic geometries, *J. Algebra*, **192** (1997), 326–379.

[5] R.A. Wilson, The complex Leech lattice and maximal subgroups of the Suzuki group, *J. Algebra*, **84** (1983), 151–188.

[6] R. Weiss and S. Yoshiara, A geometric characterization of the groups Suz and HS, *J. Algebra*, **133** (1990), 182–196.

[7] S. Yoshiara, On maximal subgroups of the Suzuki sporadic simple group, *Thesis for master's degree*, University of Tokyo, 1982.

[8] S. Yoshiara, A lattice theoretical construction of a GAB of the Suzuki sporadic simple group, *J. Algebra*, **112** (1988), 198–239.

Division of Mathematical Sciences
Osaka Kyoiku University
Kashiwara, Osaka 582-8582, Japan
e-mail: yoshiara@cc.osaka-kyoiku.ac.jp

Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 465–474

$|\mathrm{Hom}(A, G)|$ (III)

Tomoyuki Yoshida

§1. Introduction

For a finite group $G$, its *Frobenius number* h_n^{cyc} is the number of solutions of the equation $x^n = 1$ in $G$ and a *Sylow number* s_n^{cyc} is the number of cyclic subgroups of $G$ of order $n$. These numbers are named after Frobenius theorem and Sylow's theorem ([Yo 96]). The classical Frobenius theorem states that h_n^{cyc} is divisible by the greatest common divisor of $n$ and $|G|$. The following *transition formula* holds:

$$h_n^{\mathrm{cyc}} = \sum_{r|n} \varphi(r) s_r^{\mathrm{cyc}}, \quad (n \geq 1), \tag{1}$$

where $\varphi$ denotes the Euler function.

Now define the *zeta functions of Sylow and Frobenius types* by

$$\begin{aligned} S_G^{\mathrm{cyc}}(z) &:= \sum_{n=1}^{\infty} \frac{\varphi(n) s_n^{\mathrm{cyc}}}{n^z} = \sum_{g \in G} |g|^{-z}, \\ H_G^{\mathrm{cyc}}(z) &:= \sum_{n=1}^{\infty} \frac{h_n^{\mathrm{cyc}}}{n^z}. \end{aligned}$$

Then the transition formula can be presented by the *transition identity* between these functions as follows:

$$H_G^{\mathrm{cyc}}(z) = \zeta(z) S_G^{\mathrm{cyc}}(z), \tag{2}$$

where the transition function $\zeta(z)$ is Riemann's zeta function. Another expression of the transition formula (1) is given by the following cyclotomic identity:

$$\prod_{n=1}^{\infty} \left(\frac{1}{1 - t^n} \right)^{\sharp\{g \in G \mid |g| = n\}/n} = \exp\left(\sum_{n=1}^{\infty} \frac{h_n^{\mathrm{cyc}}}{n} t^n \right). \tag{3}$$

Received April 20, 1999.
Revised July 11, 2000.

Here we note that the number h_n^{cyc} equals the number of group homomorphisms from a cyclic group C_n of order n to the group G:

$$h_n^{\mathrm{cyc}} = h(C_n, G) := |\mathrm{Hom}(C_n, G)|.$$

The purpose of this paper is to generalize the above formulas (1), (2) to more general classes of groups

The most of notation and terminology in this paper are standard (cf. [Su 82]). The symbol $\Omega_1(A)$ for a group A denotes the subgroup generated by elements of prime order; C_n denotes a cyclic group of order n; ${C_p}^r$ denotes an elementary abelian p-group of order p^r.

§2. Frobenius numbers and Sylow numbers.

For any finite groups A and B, put

$$\begin{aligned} h(A,B) &:= |\mathrm{Hom}(A,B)|, \\ q(A,B) &:= \sharp\{A_1 \trianglelefteq A \mid A/A_1 \cong B\}, \\ s(A,B) &:= \sharp\{A_1 \subseteq B \mid A_1 \cong A\}. \end{aligned}$$

We call $h(A,B)$ (resp. $s(A,B)$) a *Frobenius* (resp. *Sylow*) *number*. The following lemma easily follows from the homomorphism theorem:

Lemma 2.1 (Transition formula). *For any finite groups A and G,*

$$\begin{aligned} h(A,G) &= {\sum_B}' \sharp\{A_1 \trianglelefteq A \mid A/A_1 \cong B\} \cdot |\mathrm{Aut}B| \cdot s(B,G) \\ &= \sum_{A_1 \trianglelefteq A} |\mathrm{Aut}(A/A_1)| \cdot s(A/A_1, G). \end{aligned}$$

where B runs over all isomorphism classes of finite groups.

Now, let μ (resp. μ_A^n) be the Möbius function of the lattice of subgroups (resp. normal subgroups) of a finite group A.

Lemma 2.2. *Assume that A is a finite nilpotent group with $B \le C \le A$. $A_{(p)}, B_{(p)}, C_{(p)}$ denote the Sylow p-subgroups of A, B, C, respectively.*

(i) $\mu_A^n(B,C) = \mu_{A/B}^n(1, C/B)$.

(ii) $\mu(B,C) = \prod_p \mu(B_{(p)}, C_{(p)}), \quad \mu_A^n(1,B) = \prod_p \mu_{A_{(p)}}^n(1, B_{(p)})$.

(iii) *If $\mu_A^n(1,B) \ne 0$, then B is a subgroup of $\Omega_1(Z(A))$.*

(iv) *When C is a p-group,*

$$\mu(B,C) = \begin{cases} (-1)^r p^{\binom{r}{2}} & \text{if } B \trianglelefteq C \text{ and } C/B \cong {C_p}^r \\ 0 & \text{else.} \end{cases}$$

(v) *When A is a p-group,*

$$\mu_A^n(1,B) = \begin{cases} \mu(1,B) = (-1)^r p^{\binom{r}{2}} & \text{if } C_p{}^r \cong B \leq \Omega_1(Z(A)) \\ 0 & \text{if } B \not\subseteq \Omega_1(Z(A)). \end{cases}$$

Proof. Refer to [St 97, Section 3.9, 10].

Proposition 2.3 (Inversion formula). *For any finite group A and G,*

$$s(A,G) = \frac{1}{|\mathrm{Aut}(A)|} \sum_{B \trianglelefteq A} \mu_A^n(1,B) h(A/B,G). \tag{4}$$

Proof. Submitting the identity (Lemma 2.1)

$$h(A/B,G) = {\sum_C}' q(A/B,C)|\mathrm{Aut}(C)|s(C,G)$$

to the right hand side of (4), we have

$$\begin{aligned} \text{RHS} &= \frac{1}{|\mathrm{Aut}(A)|} \sum_{B \trianglelefteq A} \mu_A^n(1,B) {\sum_C}' q(A/B,C)\,|\mathrm{Aut}(C)|\,s(C,G) \\ &= \frac{1}{|\mathrm{Aut}(A)|} {\sum_C}' \left(\sum_{B \trianglelefteq A} \mu_A^n(1,B) q(A/B,C) \right) |\mathrm{Aut}(C)|\,s(C,G). \end{aligned}$$

The inner summation is equal to

$$\begin{aligned} \sum_{B \trianglelefteq A} \cdots &= \sum_{B \trianglelefteq A} \mu_A^n(1,B) \cdot \sharp\{B_1/B \trianglelefteq A/B \mid A/B_1 \cong C\} \\ &= \sum_{\substack{B_1 \trianglelefteq A \\ :A/B_1 \cong C}} \sum_{\substack{B \trianglelefteq A \\ :B \subseteq B_1}} \mu_A^n(1,B) \\ &= \sum_{\substack{B_1 \trianglelefteq A \\ :A/B_1 \cong C}} \delta(1,B_1) = \begin{cases} 1 & \text{if } A \cong C \\ 0 & \text{else.} \end{cases} \end{aligned}$$

Hence the right hand side of (4) is equal to $s(A,G)$. Q.E.D.

Corollary 2.4 (Inversion formula for nilpotent groups). *For any finite nilpotent group A and for any finite group G,*

$$s(A,G) = \frac{1}{|\mathrm{Aut}(A)|} \sum_{B \leq \Omega_1(Z(A))} \mu(1,B) h(A/B,G). \tag{5}$$

§3. Zeta functions of Sylow type.

Let $\mathcal{A}$ be a family of finite groups closed under isomorphisms and quotient groups. Furthermore, let $w : \mathbb{N} \longrightarrow R$ be a mapping to a commutative complete topological ring R containing the rational number field $\mathbb{Q}$. Then the *zeta function of Sylow type* of the finite group G with respect to $\mathcal{A}$ and w is defined by

$$S(\mathcal{A}, w, G) := \sum_{A \in \mathcal{A}/\cong}{}' s(A, G) w(|A|) = \sum_{\substack{A \leq G \\ :A \in \mathcal{A}}}{}' w(|A|).$$

Note that $\mathcal{A}$ can be replaced by the finite (up to isomorphism) family consisting of those members of $\mathcal{A}$ which are involved in the group G.

Theorem 3.1 (Transition formula). *Assume that the family $\mathcal{A}$ consists of some nilpotent groups. Then the following holds*:

$$(6) \quad S(\mathcal{A}, w, G) = \sum_{C,B}{}' \frac{\mu(1,B) w(|B| \cdot |C|) |\mathrm{Ext}(C, B; \mathcal{A})|}{|\mathrm{Aut}(B)| \cdot |\mathrm{Aut}(C)| \cdot |\mathrm{Hom}(C, B)|} h(C, G),$$

where C (resp. B) runs over a complete set of representatives of $\mathcal{A}/\cong$ (resp. abelian groups such that $B = \Omega_1(B)$). Furthermore, $\mathrm{Ext}(C, B; \mathcal{A})$ *denotes the set of equivalence classes of central extensions*:

$$\mathrm{Ext}(C, B; \mathcal{A}) = \{1 \longrightarrow B \longrightarrow A (\in \mathcal{A}) \longrightarrow C \longrightarrow 1 (\text{c.e.})\}/\cong .$$

Proof. First, by the inversion formula,

$$\begin{aligned} S(\mathcal{A}, w, G) &= \sum_{A \in \mathcal{A}}{}' s(A, G) w(|A|) \\ &= \sum_{A \in \mathcal{A}}{}' \sum_{B \leq Z(A)} \mu(1, B) h(A/B, G) \frac{w(|A|)}{|\mathrm{Aut}(A)|} \\ &= \sum_{A \in \mathcal{A}}{}' \sum_{C \in \mathcal{A}}{}' \sum_{\substack{B \leq Z(A) \\ :A/B \cong C}} \mu(1, B) h(A/B, G) \frac{w(|A|)}{|\mathrm{Aut}(A)|} \\ &= \sum_{A \in \mathcal{A}}{}' \sum_{C \in \mathcal{A}}{}' \sum_{B:\text{abel}}{}' \sum_{B \rightarrowtail A \twoheadrightarrow C (\text{c.e.})} \frac{\mu(1, B) h(C, G) w(|A|)}{|\mathrm{Aut}(A)| \, |\mathrm{Aut}(B)| \, |\mathrm{Aut}(C)|}, \end{aligned}$$

where the most inner summation is taken over all central extensions:

$$1 \longrightarrow B \longrightarrow A (\in \mathcal{A}) \longrightarrow C \longrightarrow 1.$$

The equivalence of two such central extensions is defined by

$$\begin{aligned}(1 \to B \xrightarrow{\varphi} A \xrightarrow{\psi} C \to 1) &\sim (1 \to B \xrightarrow{\varphi'} A \xrightarrow{\psi'} C \to 1)\\ \Longleftrightarrow \exists \alpha &\in \mathrm{Aut}(A) \text{ s.t. } \alpha \circ \varphi = \varphi', \psi = \psi' \circ \alpha.\end{aligned}$$

By extension theory of groups, the number of such central extensions equivalent to a given $B \rightarrowtail A \twoheadrightarrow C$ is equal to

$$\frac{|\mathrm{Aut}(A)|}{|\mathrm{Hom}(C, B)|}.$$

Thus

$$\begin{aligned}&S(\mathcal{A}, w, G)\\ &= {\sum_{A \in \mathcal{A}}}' {\sum_{C \in \mathcal{A}}}' {\sum_{B:\text{abel}}}' \sum_{[B \rightarrowtail A \twoheadrightarrow C(\text{c.e.})]} \frac{\mu(1, B) h(C, G) w(|A|)}{|\mathrm{Hom}(C, B)|\,|\mathrm{Aut}(B)|\,|\mathrm{Aut}(C)|}\\ &= {\sum_{A \in \mathcal{A}}}' {\sum_{C \in \mathcal{A}}}' {\sum_{B:\text{abel}}}' \sum_{[B \rightarrowtail A \twoheadrightarrow C(\text{c.e.})]} \frac{\mu(1, B) h(C, G) w(|B| \cdot |C|)}{|\mathrm{Hom}(C, B)|\,|\mathrm{Aut}(B)|\,|\mathrm{Aut}(C)|}\\ &= {\sum_{C,B}}' \frac{\mu(1, B) w(|B| \cdot |C|) |\mathrm{Ext}(C, B; \mathcal{A})|}{|\mathrm{Aut}(B)|\,|\mathrm{Aut}(C)|\,|\mathrm{Hom}(C, B)|}\, h(C, G).\end{aligned}$$

Remark. For the class of finite nilpotent groups, (6) does not converge.

Applying Theorem 3.1 to the family $\mathcal{C}$ of cyclic groups, we have the formula (1) in Introduction. In this case,

$$|\mathrm{Ext}(C_n, C_m; \mathcal{C})| = \varphi(m)\varphi(n)\mathrm{gcd}(m, n)/\varphi(mn).$$

Next, applying Theorem 3.1 to the family $\mathcal{A}_p$ of abelian p-groups, we have the transition formula as follows:

$$\frac{H_G^{\mathrm{A}_p}(x)}{S_G^{\mathrm{A}_p}(x)} = \prod_{m=1}^{\infty} (1 - p^{-m} x)^{-1}, \tag{7}$$

where

$$\begin{aligned}H_G^{\mathrm{A}_p}(x) &:= \sum_{n=0}^{\infty} {\sum_{|A|=p^n}}' \frac{h(A, G)}{|\mathrm{Aut}(A)|} x^n,\\ S_G^{\mathrm{A}_p}(x) &:= \sum_{n \geq 0} {\sum_{|A|=p^n}}' s(A, G) x^n.\end{aligned}$$

This funny identity with $G=1, x=1$ implies P.Hall's strange formula:

$$\sum_A{}' \frac{1}{|\mathrm{Aut}(A)|} = \sum_A{}' \frac{1}{|A|}, \tag{8}$$

where A runs over all classes of abelian p-groups([Yo 92]).

§4. Partition identities.

Let $\mathcal{E}_p$ be the family of all elementary abelian p-groups. As is well-known, the following hold:

$$\begin{aligned}
&|\mathrm{Ext}({C_p}^s, {C_p}^r; \mathcal{E}_p)| = 1,\\
&\sharp\{B \subseteq {C_p}^n \mid |B| = p^r\} = \begin{bmatrix} n \\ r \end{bmatrix}_p := \frac{[p]_n}{[p]_r [p]_{n-r}},\\
&[p]_n = (p-1)(p^2-1)\cdots(p^n-1),\\
&|\mathrm{Aut}({C_p}^n)| = |\mathrm{GL}(n,p)| = p^{\binom{n}{2}}[p]_n,\\
&\mu(1, {C_p}^r) = (-1)^r p^{\binom{r}{2}}.
\end{aligned}$$

Thus Lemma 2.1 and Proposition 2.3 have the following forms:

$$\begin{aligned}
&(9) \quad h({C_p}^n, G) &=& \sum_{r=0}^{n} \begin{bmatrix} n \\ r \end{bmatrix}_p \cdot |\mathrm{GL}(r,p)|\, s({C_p}^r, G),\\
&(10) \quad s({C_p}^n, G) &=& \frac{1}{|\mathrm{GL}(n,p)|} \sum_{r=0}^{n} (-1)^r p^{\binom{r}{2}} \begin{bmatrix} n \\ r \end{bmatrix}_p h({C_p}^{n-r}, G).
\end{aligned}$$

We take the weight function w of the form $w(p^n) = f(n)x^n$, so that by Theorem 3.1, we have

$$\begin{aligned}
S^{\mathrm{E}_p}_{G,f}(x) &:= \sum_{n\geq 0} s({C_p}^n, G) f(n) x^n\\
&= \sum_{r,s\geq 0} \frac{(-1)^r p^{\binom{r}{2}} f(r+s) h({C_p}^s, G)}{|\mathrm{GL}(r,p)| \cdot |\mathrm{GL}(s,p)| \cdot p^{rs}} x^{r+s}\\
&= \sum_{n=0}^{\infty} \left(\sum_{r=0}^{\infty} \frac{f(r+n)}{[p]_r} (-p^{-n}x)^r \right) \frac{h({C_p}^n, G)}{|\mathrm{GL}(n,p)|} x^n. \qquad (11)
\end{aligned}$$

Case $f(n) = 1$. In this case, (11) gives

$$\begin{aligned}
S^{\mathrm{E}_p}_{G,1}(x) &= \sum_{n\geq 0} s({C_p}^n, G)\, x^n \\
&= \sum_{n=0}^{\infty} \left(\sum_{r=0}^{\infty} \frac{1}{[p]_r} (-p^{-n}x)^r \right) \frac{h({C_p}^n, G)}{|\mathrm{GL}(n,p)|} x^n \\
&= \prod_{r=1}^{\infty} (1 - p^{-r}x) \cdot \sum_{n=0}^{\infty} \left(\prod_{r=1}^{n} (1 - p^{-r}x)^{-1} \right) \frac{h({C_p}^n, G)}{|\mathrm{GL}(n,p)|} x^n. \qquad (12)
\end{aligned}$$

Here we used the q-binomial theorem:

$$\sum_{r=0}^{\infty} \frac{1}{[p]_r} (-p^{-n}x)^r = \prod_{r=1}^{\infty} (1 - p^{-n-r}x). \qquad (13)$$

Even if the group G is trivial, (12) gives a non-trivial formula called Cauchy's identity (1893) and then Euler's one:

$$\begin{aligned}
\prod_{r=1}^{\infty} (1 - p^{-r}x)^{-1} &= \sum_{n=0}^{\infty} \left(\prod_{i=1}^{n} (1 - p^{-i}x)^{-1} \right) \frac{x^n}{|\mathrm{GL}(n,p)|}, \qquad (14) \\
\prod_{r=1}^{\infty} (1 - p^{-r})^{-1} &= \sum_{n=0}^{\infty} \left(\prod_{i=1}^{n} (p^i - 1)^{-2} \right) p^n. \qquad (15)
\end{aligned}$$

Case $f(n) = p^{\binom{n}{2}}$. In this case, (11) gives

$$\begin{aligned}
S^{\mathrm{E}_p}_{G,f}(x) &:= \sum_{n\geq 0} s({C_p}^n, G) p^{\binom{n}{2}} x^n \\
&= \sum_{n=0}^{\infty} \left(\sum_{r=0}^{\infty} \frac{p^{\binom{n}{2}+\binom{r}{2}}}{[p]_r} (-x)^r \right) \frac{h({C_p}^n, G)}{|\mathrm{GL}(n,p)|} x^n, \\
&= \left(\sum_{r=0}^{\infty} \frac{p^{\binom{r}{2}}}{[p]_r} (-x)^r \right) \cdot \left(\sum_{n=0}^{\infty} \frac{h({C_p}^n, G)}{[p]_n} x^n \right), \\
&= \prod_{r=1}^{\infty} (1 + p^{-r}x)^{-1} \cdot \left(\sum_{n=0}^{\infty} \frac{h({C_p}^n, G)}{[p]_n} x^n \right). \qquad (16)
\end{aligned}$$

Here we used the q-binomial theorem. Hence, we conclude that

$$\frac{H^{\mathrm{E}_p}_{G,f}(x)}{S^{\mathrm{E}_p}_{G,f}(x)} = \prod_{r=1}^{\infty} (1 + p^{-r}x), \qquad (17)$$

where

$$H^{\mathrm{E}_p}_{G,f}(x) := \sum_{n=0}^{\infty} \frac{h(C_p{}^n, G)}{[p]_n} x^n. \qquad (|x| < p).$$

Remark. As rational functions over the complete p-adic number field, we have

$$(18) \qquad \frac{H^{\mathrm{E}_p}_{G,f}(x)}{S^{\mathrm{E}_p}_{G,f}(x)} = \prod_{r=0}^{\infty}(1 + p^r x)^{-1}.$$

A special value of $S^{\mathrm{E}_p}_{G,f}(x)$ is related with the Euler characteristic $\chi(\mathcal{S}_p(G))$ of the poset of non-trivial p-subgroups:

$$(19) \qquad \chi(\mathcal{S}_p(G)) := \sum_{A,B \neq 1} \mu(A, B) = -\sum_{B \neq 1} \mu(1, B),$$

where A, B run over all nontrivial p-subgroups and μ is the Möbius function of the subgroup lattice of G. Thus Lemma 2.2(iv) implies the following:

Lemma 4.1. *Under the above notation, the following holds:*

$$(20) \qquad S^{\mathrm{E}_p}_{G,f}(-1) = 1 - \chi(\mathcal{S}_p(G)).$$

For $n \geq 0$, we define the numbers χ'_n's by

$$\chi'_n := \sum_{r=0}^{n} (-1)^r p^{\binom{r}{2}} s(C_p{}^r, G).$$

Then $1 - \chi'_n$ is equal to the Euler characteristic of the poset of p-subgroups of G of order at most p^n. By the inversion formula (10), we have

$$(21) \qquad [p]_n \chi'_n = \sum_{r=0}^{n} (-1)^{n-r} p^{\binom{r+1}{2}} \begin{bmatrix} n \\ r \end{bmatrix}_p h_{n-r}.$$

Consider the following generating series associated to the series $\{\chi'_n\}_{n \geq 0}$:

$$X_G(t) := \sum_{n=0}^{\infty} \chi'_n (-t)^n.$$

Then we have

$$\begin{aligned} X_G(t) &= \sum_{n=0}^{\infty}\sum_{r=0}^{n}(-1)^r p^{\binom{r}{2}} s({C_p}^r, G)(-t)^n \\ &= (1+t)^{-1}\sum_{r=0}^{\infty} p^{\binom{r}{2}} s({C_p}^r, G)t^r \\ &= (1+t)^{-1} S_{G,f}^{\mathrm{E}_p}(t). \end{aligned}$$

Thus the transition identity (16) gives

$$X_G(t) = \prod_{n=0}^{\infty}(1+p^{-n}t)^{-1}\cdot H_{G,f}^{\mathrm{E}_p}(t). \tag{22}$$

Similarly, if we view $X_G(t)$ and $H_{G,f}^{\mathrm{E}_p}(t)$ as p-adic power series (18), we have

$$X_G(t) = \prod_{n=1}^{\infty}(1+p^{n}t)\cdot H_{G,f}^{\mathrm{E}_p}(t). \tag{23}$$

These formula gives a transition formula between $\{h_n\}$ and $\{\chi'_n\}$:

$$h_n = \sum_{r=0}^{n}(-1)^r p^{n-r}\begin{bmatrix} n \\ r \end{bmatrix}_p \chi'_r. \tag{24}$$

By (21) and (24), if p^n divides $|G|$, then

$$\chi'_n \equiv 0 \pmod{p^n} \quad \Longleftrightarrow \quad h_n \equiv 0 \pmod{p^n}. \tag{25}$$

The right hand side of this statement is valid by [Yo 93]. Thus we again have Brown's cohomological Sylow theorem ([Yo 96]):

$$\chi(\mathcal{S}_p(G)) \equiv 1 \pmod{|G|_p}. \tag{26}$$

References

[St 97] R.P. Stanley, Enumerative Combinatorics, Volume I, Cambridge University Press, 1997.

[Su 82] M. Suzuki, Group Theory, I, II, Springer, 1982.

[Yo 92] T. Yoshida, P.Hall's strange formula for abelian p-groups, *Osaka Math.J.,* **29** (1992), 421–431.

[Yo 93] T. Yoshida, |Hom(A,G)|, *J. Algebra,* **156** (1993), 125–156.

[Yo 96] T. Yoshida, Classical problems in group theory (I): Enumerating subgroups and homomorphisms, *Sugaku Expositions,* **9** (1996),169–184.

Department of Mathematics
Hokkaido University
Sapporo 060-0810, Japan
e-mail: yoshidat@math.sci.hokudai.ac.jp