COMMUTATORS AND CONJUGACY IN GROUPS.

A thesis submitted for the degree of Doctor of Philosophy at the University of Keele, in 1974,

by

DAVID RODNEY.

DECLARATION

The material in this thesis is claimed as original except where explicitly stated otherwise. This thesis has not been submitted previously for a higher degree of this or any other University.

ACKNOWLEDGEMENTS

I wish to express my gratitude to my supervisor, Dr. Hans Liebeck, for the tremendous guidance he has given me during the past three years.

I wish to thank the Science Research Council, whose maintenance grant has supported me during the course of my research.

Finally, I wish to thank Mrs. Doreen Large for her patience and excellent typing.

CONTENTS

ABSTRACT of the thesis, "Commutators and Conjugacy in Groups", by David Rodney, University of Keele, 1974.

It is well known that the commutator subgroup G', of a group G need not coincide with the set of commutators of G, $\mathcal{K}(G)$.

We are primarily concerned with investigating the class of groups $\mathcal{C}$, defined by, $G \in \mathcal{C}$ if and only if $G' = \mathcal{K}(G)$. Firstly we consider groups with a finite cyclic commutator subgroup. I. D. Macdonald showed that such a group need not be generated by a commutator. We show that, even if the commutator subgroup is generated by a commutator, the group need not belong to the class $\mathcal{C}$.

Next we consider a nilpotent of class two group G such that G' is finite and can be generated by three elements. We show that $G \in \mathcal{C}$. We extend these results to G being a finite metabelian group and we show that if G' is elementary abelian of rank 3, then $G \in \mathcal{C}$. We also show that if S is an elementary abelian of rank 2 Sylow subgroup of a finite group G, such that $S \subseteq G'$, then $S \subseteq \mathcal{K}(G)$, the set of commutators of elements of G. For all the results mentioned in the last two paragraphs we give examples to show that the results are not readily extendable.

Next we show that the unipotent groups of matrices belong to the class $\mathcal{C}$.

The remainder of the thesis is concerned with finite groups and we make extensive use of character theory. W. Burnside gives a necessary and sufficient condition, in terms of group characters, for an element of a finite group to be a commutator. We make a generalisation of this result and prove that if G is a finite group with irreducible characters $\chi^1, \ldots, \chi^h$ and conjugacy classes $C_1, \ldots, C_h$, then there exist $g_i \in C_{\lambda(i)}$ for $1 \leq i \leq n$ such that $g_1 g_2 \ldots g_n \in \mathcal{K}(G)$ if and only if

$$\sum_{j=1}^{h} \chi^j(g_1)\, \chi^j(g_2) \ldots \chi^j(g_n)/(\chi^j(1))^n \neq 0.$$

As a corollary we show that $g_1 g_2 \ldots g_n \in \mathcal{K}(G)$ if and only if for all r_i such that $(r_i, |g_i|) = 1$ there exist $x_i \in G$ for $1 \leq i \leq n$ such that $g_1^{x_1} \ldots g_{i-1}^{x_{i-1}} (g_i^{r_1})^{x_i} g_{i+1}^{r_{i+1}} \ldots g_n^{x_n} \in \mathcal{K}(G)$. This is a generalisation of a result of K. Honda.

It is unknown whether or not every element of a non-abelian finite simple group is a commutator. We show that three of the sporadic simple groups have this property and we give a list of references, where the truth of this conjecture can be shown, for other simple groups.

One of the difficulties in tackling the above conjecture concerning simple groups is the lack of knowledge concerning the number of conjugacy classes in a simple group. Non-abelian finite simple groups seems to have few conjugacy classes with respect to their order and we finish by investigating a related situation that occurs frequently in simple groups.

Let G be a finite group with an abelian subgroup M such that any two non-identity elements of M are conjugate within G. This situation was first investigated by A. Fomyn and we extend his results. Let G have irreducible characters $\chi^1, \chi^2, \ldots, \chi^h$ and let θ be a non-principal character of M. It is easily seen that $(\chi^i|_M, \theta)_M = f_i$ is independent of θ. Our main result is the following: Suppose that $f_i = 1$ for $2 \leq i \leq h$, then M is a Sylow 2-subgroup of G and,

either $G/O_{2'}(G) \cong PSL(2, 2^n)$

or $|M| = 2$, $G = G' \rtimes M$, G' is abelain and $g^m = g^{-1}$ for every $g \in G'$,

where $1 \neq m \in M$.

We also investigate the situation when $M \lhd G$. Here there is a close relationship between $I(\theta)$ and $C_G(m)$, where $1 \neq m \in M$. Indeed, if M is a normal Sylow subgroup of G, then we show that to each θ there exists an m such that $I(\theta) = C_G(m)$ and vica-versa. Whilst we are proving this we obtain information concerning the f_i's. Finally we consider the rather restricted case that M is a normal Sylow subgroup of G such that G/M is abelain. We obtain a classification of such groups.

NOTATION AND TERMINOLOGY

If G is any group then,

G' is the commutator subgroup of G, $[a, b] = a^{-1} b^{-1} ab$,

Z(G) is the centre of G and

$\mathcal{K}(G)$ is the set of commutators of elements of G.

$\mathcal{C}$ is the class of groups G such that $G' = \mathcal{K}(G)$.

d(G) is the minimal cardinality of any generating set of G.

Suppose H is a subgroup of G. Then,

$H \triangleleft G$ means H is a normal subgroup of G,

$N_G(H)$ denotes the normalizer of H in G and

$C_G(H)$ denotes the centralizer of H in G.

Suppose $\{g_i | i \in A\}$ is a set of elements of G, where A is any index set. Then,

$\langle g_i | i \in A \rangle$ denotes the subgroup of G generated by the $\{g_i\}$.

$g_i \sim_G g_j$ means that g_i is conjugate in G to g_j. If the group, G, under discussion cannot be mistaken then the G may be omitted.

$\langle g_i | i \in A \rangle^G$ denotes the normal closure of the $\{g_i\}$ in G.

If G is a finite group, and π is a set of primes, then $O_\pi(G)$ is the largest normal subgroup of G whose order is divisible only by primes in π.

Let π' denote the complementary set of primes to π. Then, $O_{\pi'}(G)$ is the largest normal subgroup of G whose order is coprime to the primes in π.

If H and K are any two groups, then,

$H \times K$ is the direct product of H and K,

$H \lambda K$ is a split extension of H by K and

$H \wr K$ is the ordinary wreath product of H with K.

Hom(H, K) is the set of homomorphisms from H to K.

Let G be a finite group.

When we refer to an irreducible character of G we mean an irreducible character over the complex numbers.

$\chi^1, \chi^2, \ldots, \chi^h$ denote the irreducible characters of G,

$C_1, \ldots, C_h$ denote the conjugacy classes of G and χ_j^i is the value of χ^i taken on C_j.

χ^1 is the principal character of G and $C_1 = 1$. Ker $(\chi) = \{g \in G | \chi(g) = \chi(1)\}$, the kernel of the character χ.

Irr (G) is the set of irreducible characters of G.

F(G) is the group algebra of G over the field F and $\hat{C}_i$ is the class sum of C_i in F(G).

If H is a subgroup of G and $\theta \in$ Irr(H), then θ^* is the character of G obtained by inducing θ up to G.

If $H \lhd G$ and $g \in G$, then θ^g is the irreducible character of H defined by, $\theta^g(h) = \theta(ghg^{-1})$, where $h \in H$.

$I(\theta) = \{g \in G | \theta^g = \theta\}$, the inertial group of θ.

GL(n, F), SL(n, F) and PSL(N, F), are respectively, the general linear, special linear and projective special linear groups of degree n over the field F.

Sp(n, F) is the Sympletic group of degree n over the field F and STL(n, F) is the group of upper unipotent matrices of degree n over the field F.

C_n is the cyclic group of order n.

If K is a field containing the field F, then G(K, F) is the Galois group of K over F.

$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{Z}$ are, respectively, the complex, real and rational and integral numbers.

If $\alpha, \beta \in \mathbb{Z}$, then (α, β) is the highest common factor of α and β and $\alpha | \beta$ means that α divides β.

$\alpha = \alpha_p \alpha_{p'}$, where α_p is a power of the prime number p and $(\alpha_p, \alpha_{p'}) = 1$.

Our notation is, hopefully, standard and has been drawn from the books of J. Dixon [6], W. Feit [9] and D. Gorenstein [16].

Chapter 1. Introduction and Review

It is well known that the commutator subgroup of an arbitary group need not consist entirely of commutators. The majority of this thesis is taken up with proofs that certain classes of groups are contained in the class $\mathcal{C}$, the class of groups whose commutator subgroups consist entirely of commutators.

Conversely, we also investigate conditions necessary to a group that belongs to $\mathcal{C}$.

It has been conjectured that all finite simple groups belong to $\mathcal{C}$ and we demonstrate the truth of this for various simple groups. A direct proof of the above conjecture is beyond our means at the present. In the final chapter we obtain results concerning finite groups with a small number of conjugacy classes. These are the sort of results that will be useful in trying to prove the conjecture.

We are primarily concerned with finite groups, though we do show that certain classes of infinite groups are contained in $\mathcal{C}$.

Trivially, is G is an abelian group, then $G \in \mathcal{C}$. If not abelian, the least complicated structure a group G can have is that of the commutator subgroup G' being cyclic. In [32], I. D. Macdonald considered such groups and he showed that such a group need not be generated by a commutator. Indeed, Macdonald shows, by example, that given a natural number n there exists a group G such that G' is cyclic of finite order and G' cannot be generated by less that n commutators.

In Chapter 2 we continue the study of groups with a cyclic commutator subgroup. We show that if G is a group with a finite cyclic commutator subgroup then, even if G' is generated by a commutator, it is not necessarily true that $G \in \mathcal{C}$. We give examples that demonstrate this. (It is from Chapter 2 that the author's paper [39] is derived.)

There are several ways we may increase the complexity of the groups under consideration.

In [31], I. D. Macdonald considered the following subgroup of the commutator subgroup. Let G be a group. Then we define the subgroup H(g), where $g \in G$ by,

$$H(g) = \langle [g, x] \mid x \in G \rangle.$$

Macdonald proves the following result.

Theorem. Let each subgroup H(g) of the group G consist of commutators of the form $[g, x]$, and let G be such that the minimal condition holds for the subgroups H(g). Then a non-trivial element of each subgroup $\langle g \rangle^G$ lies in the centre of G, provided that $g \neq 1$.

Corollary. Under the hypotheses of the theorem G is a ZA group. (By a ZA group is meant a group with an ascending central series which eventually exhausts the group.). Macdonald also shows that neither of the following two conditions implies the other:

(i) G' consists of commutators.

(ii) For each $g \in G$, H(g) consists of the commutators $[g, x]$ as x varies in G.

Whereas many finite non-nilpotent groups satisfy (i), by the above corollary no finite non-nilpotent group satisfies (ii). (e.g. The Alternating groups A_n, where $n \geq 5$ (c.f. N. Itô [27].) Macdonald gives an example of a finite nilpotent of class two group G such that G does not satisfy (i). Such a group necessarily satisfies (ii).

The example given by Macdonald, of a finite class two nilpotent group G such that $G \notin \mathfrak{G}$ is a generalisation of an example in R. D. Carmichael's book [4. p.39]. If H denotes the example in [4], then d(H') = 4. In Chapter 3 we show that this example is in some sense minimal and we prove the following result.

Theorem 3.1. Let G be nilpotent of class two such that G' is finite and $d(G') \leq 3$. Then $G \in \mathcal{C}$. From here we try to generalise to G being metabelian. We are able to prove the following.

Theorem 3.2. Let G be a finite group such that G' is elementary abelian of order p^3. Then $G \in \mathcal{C}$. It may be true that Theorem 3.2 extends to G' being a rank 3 abelian p-group but we have been unable to verify or disprove this. Another possible line of approach is to consider a Sylow subgroup S of a finite group G and to investigate $S \cap \mathcal{K}(G)$. We discuss this in Chapter 3. Various people have considered particular classes of groups and have shown them to belong to the class $\mathcal{C}$. We list several of them.

In [43], [44] and [45] R. C. Thompson shows that $GL(n, F) \in \mathcal{C}$ and $PSL(n, F) \in \mathcal{C}$, where n is any natural number and F is an arbitrary field.

In [34], O. Ore considers the symmetric groups. If S_n is the symmetric group on n symbols, then $S'_n \cong A_n$, the alternating group on n symbols. Ore shows that $S_n \in \mathcal{C}$. Let S be the infinite symmetric group. Ore shows that $S \in \mathcal{C}$, by showing that any one-to-one correspondence of an infinite set to itself is a commutator.

N. Itô in [27], shows that $A_n \in \mathcal{C}$, if $n \geq 5$. (Since $A_n' \cong A_n$ for $n \geq 5$, this is a strengthening of Ore's work and, indeed, Ore claims that this result is true though he does not prove it.)

Following the path of permutation groups we come to the work of C. V. Holmes [21]. He considers the related idea of monomial substitutions. Let H be a group and S a set. A monomial substitution over H is a linear transformation mapping each element x of S in a one-to-one manner onto some element of S multiplied by an element of H, the multiplication being formal. If substitution u maps x_i into $h_j x_j$ while substitution v maps x_j into $h_k x_k$, then the substitution uv maps x_i into $h_j h_k x_k$.

Suppose that S is an infinite set. Then the set of all such monomial substitutions is the infinite complete monomial group generated by the given group H and the given set S. The commutator subgroup of the infinite complete monomial group is itself and Holmes shows that every element is expressible as the product of at most two commutators.

Qin Jian-Min, in [36], considers the orthogonal groups over the complex numbers, denoted by $O(n, \mathbb{C})$. The matrices of determinant one in $O(n, \mathbb{C})$, form the subgroup $SO(n, \mathbb{C})$. Qin Jian-Min proves the following:

Theorem. Every element of $SO(2, \mathbb{C})$ is a commutator of $O(2, \mathbb{C})$, and every element of $SO(n, \mathbb{C})$ is a commutator of $SO(n, \mathbb{C})$, when $n \geq 3$.

Similar results are obtained by H. Toyama in [47]. Let $SU(n, \mathbb{C})$ denote the unimodular unitary group of degree n over $\mathbb{C}$ and $USp(n, \mathbb{C})$ denote the unitary symplectic group of degree n over $\mathbb{C}$. Toyama proves the following:

Theorem. Every element of $SU(n, \mathbb{C})$, $USp(n, \mathbb{C})$ and $SO(n, \mathbb{R})$ except for $SO(2, \mathbb{R})$ can be expressed as a commutator of two suitably chosen elements belonging to that group.

Xu Ch'eng-Hao [53] continues this work and he shows that $Sp(2n, \mathbb{C}) \in \mathcal{C}$.

Information concerning the above linear groups may be obtained from [6]. Ts'eng K'en-Ch'eng and Hsu Ch'eng-Hao, in [48], show that the Suzuki groups, discovered by M. Suzuki in [42], belong to the class $\mathcal{C}$.

Finally, Ts'eng K'en Cheng and Liu Chiung Sheng, in [49], show that the two Mathieu groups M_{11} and M_{12} belong to the class $\mathcal{C}$. (We have been unable to track this paper down and we have obtained this information from Maths. Review Vol. 36 #2700)

Along these lines we show, in Chapter 4, that the unipotent groups over any field belong to the class $\mathcal{C}$.

We now describe a result known to W. Burnside and developments from it.

Suppose G is a finite group, with irreducible characters $\chi^1, \chi^2, \ldots, \chi^h$ over $\mathbb{C}$. Let $g \in G$. Then, $g \in \mathcal{K}(G)$ if and only if $\sum_{i=1}^{h} \chi^i(g)/\chi^i(1) \neq 0$. (c.f. [3.p.319].)

As a corollary of this K. Honda proves, in [22], that in a finite group G, $g \in \mathcal{K}(G)$ if and only if every generator of $\langle g \rangle$ is a commutator.

In [14] P. X. Gallagher generalises the character inequality. He also extends the class of groups under consideration to compact groups.

So let G be a compact group. We let $\{\chi^i\}$ be the irreducible characters over $\mathbb{C}$ and let $f_i = \chi^i(1)$. Gallagher proves the following results.

Theorem. Suppose $|G : G'|$ is finite.
If $\sum_{f_i \geq 2} f_i^{(2-2n)} < |G : G'|$, then each element of G' may be written as a product of n commutators.

Theorem. Suppose $|G : G'|$ is finite and assume there is a finite or infinite sequence of elements $\{\tau_n\}$ such that for each character χ^i with $f_i \geq 2, \chi^i(\tau_n) = 0$ for some n. Then each element of G' may be approximated arbitrarily closely by products $[\tau_1, l_1][\tau_2, l_2] \ldots [\tau_n, l_n]$, $l_1, \ldots l_n \in G$.

Lemma. Let $\sigma, \tau_1, \ldots \tau_n, l_1 \ldots l_n \in G$. Then,

$$\int \ldots \int \chi^i(\sigma[\tau_1, l_1] \ldots [\tau_n, l_n]) dl_n \ldots dl_1 = f_i^{-n} \chi^i(\tau_1 \ldots \tau_n \sigma) \overline{\chi}(\tau_1) \ldots \overline{\chi}(\tau_n)$$

and

$$\int \ldots \int \chi^i(\sigma[\tau_1, l_1] \ldots [\tau_n, l_n]) dl_n d\tau_n \ldots dl_1 d\tau_1 = f_i^{-2n} \chi(\sigma).$$

(Information concerning the above Haar integrals may be found in [33].)

Gallagher shows, as an easy consequence of the lemma, that $\sigma \in G$ is a product of m commutators if and only if $\sum_{\chi^i} f_i^{1-2m} \chi^i(\sigma) \neq 0$.

Applying this work to finite groups Gallagher proves the following results.

Theorem. Let G be a finite group such that $4^n \geq |G'|$. Then each element of G' may be written as a product of n commutators

Theorem. In a finite group G each element of G' may be written as a product $[\tau_1, l_1] \ldots [\tau_n, l_n]$, where $\tau_1, \ldots, \tau_n$ are zeros of irreducible characters. Gallagher continued this work in [15]. He proves the following results.

Theorem. Let G be a finite group. If $(n + 2)!\, n! > 2|G'| - 2$ then each element of G' is a product of n commutators.

Theorem. If G is a finite p-group, with $|G'| = p^\alpha$, and if $n(n + 1) > \alpha$, then each element of G' is a product of n commutators.

We investigate the result of Burnside and the work of Honda in Chapter 5 and we make some small generalisations of their results.

As we have already mentioned it is an open question whether or not every element of a non-abelian finite simple group is a commutator. Three reasons for believing the truth of this conjecture are:

(i) Many finite simple groups are known to have this property. (See the list earlier in this chapter as well as Chapter 6.)

(ii) The value taken by a non-identity element g of a non-abelian finite simple group on a non-principal character tends to be very small in absolute size when compared to the degree of the character. Consequently, the character inequality $\sum \chi^i(g)/\chi^i(1) \neq 0$ is likely to hold.

(iii) An element of g of a group G is a commutator if and only if there exists an $h \in G$ such that gh is conjugate to h. Intuitively, the smaller the number of conjugacy classes G has, the more likely this is to happen. We observe that the number of conjugacy classes in a non-abelian finite simple group tends to be in some sense "small" in comparison with the order of the group.and thus leads us to expect that every element is a commutator.

The latter two reasons show the way progress may be made on this problem. We have been unable to make any progress with regards to (ii).

However, in Chapter 7, we consider finite groups with "few" conjugacy classes and we obtain several results. We consider the following situation. Let G be a finite group with / an abelian subgroup M such that any two non-identity elements of M are conjugate within G. This work was initiated by A. Fomyn in [12] and we generalise his results. A considerable amount of work has been done in this area, the most significant contribution probably being that of G. Higman in [20].

To end this review we mention a few properties of the class $\mathcal{C}$. Suppose G_1, $G_2 \in \mathcal{C}$. Then it is readily seen that $G_1 \times G_2 \in \mathcal{C}$. It is also apparent that if $H_1 \triangleleft G_1$, then $G_1/H_1 \in \mathcal{C}$. However, if H_2 is a subgroup of G_2 this does not imply that $H_2 \in \mathcal{C}$. e.g. N. Itô, in [27], shows that the Alternating groups A_n, for $n \geq 5$, belong to $\mathcal{C}$. Given a finite group $G \notin \mathcal{C}$ we can embed G in A_n for n sufficiently large.

Finally, we observe that if $G_1 \in \mathcal{C}$ and G_1 is isoclinic to G_3, then $G_3 \in \mathcal{C}$. This is a direct consequence of the definition of isoclinism which is:

Groups A and B are isoclinic if,

(i) $A/Z(A) \tilde{=} B/Z(B)$

(ii) $A' \tilde{=} B'$ and

(iii) If $a_1Z(A)$ and $a_2Z(A)$ correspond to $b_1Z(B)$ and $b_2Z(B)$ respectively under the isomorphism given in (i), then $[a_1, a_2]$ corresponds to $[b_1, b_2]$ under the isomorphism given in (ii).

Throughout this work we make extensive use of the commutator identities,

$$[ab, c] = [a, c]^b [b, c] \quad \text{and}$$

$$[a, bc] = [a, c] [a, b]^c,$$

without any reference to them.

CHAPTER 2 GROUPS WITH A CYCLIC COMMUTATOR SUBGROUP

In this chapter we investigate groups with a cyclic commutator subgroup. In [2] I. D. Macdonald shows that a finite cyclic derived subgroup G' of an arbitary group G need not be generated by a commutator. This leads one to ask whether a finite cyclic derived subgroup that is generated by a commutator consists entirely of commutators. We show that this is not necessarily true and give examples that demonstrate the fact. However, we prove the following theorem.

Theorem 2.1 Let G' be cyclic of finite order and assume $4 \nmid |G'|$. Suppose $G' = \langle c \rangle$, where $c = [a, b]$. Let μ and ν be integers such that $c^a = c^\mu$ and $c^b = c^\nu$. If one of the following four conditions fails to hold for every prime divisor p of $|G'|$, then G' consists of commutators.

I $\mu - 1 \equiv 0(p)$, $\nu - 1 \equiv 0(p)$; II $\mu - 1 \equiv 0(p)$, $\nu - 1 \not\equiv 0(p)$;

III $\mu - 1 \not\equiv 0(p)$, $\nu - 1 \equiv 0(p)$; IV $\mu - 1 \not\equiv 0(p)$, $\nu - 1 \not\equiv 0(p)$.

As a corollary we obtain the following generalisation of a result in [2].

Corollary 2.2. If G' is cyclic and either G is nilpotent or G' is infinite, then G' consists of commutators.

Before we can give the proof of the theorem we need to prove the following two lemmas.

Lemma 2.3 Let $m = m_1 m_2 \dots m_n$, where $m_i \in \mathbb{Z}$ for $1 \leq i \leq n$ and $(m_i, m_j) = 1$ if $i \neq j$. Given integers ξ_i, ζ_i for $1 \leq i \leq n$ such that $\alpha\xi_i + \beta\zeta_i + \gamma \equiv 0(m_i)$, then there exists integers ξ and ζ such that $\alpha\xi + \beta\zeta + \gamma \equiv 0(m)$.

Proof Let $\delta = (\alpha, \beta) = k\alpha + l\beta$ for integers k and l. Then (δ, m_i) divides γ. Since the m_i are coprime, it follows that (δ, m) divides γ. Consequently, there exist integers r and s such that $r\delta + sm = \gamma$. Letting $\xi = -rk$ and $\zeta = -rl$ we have that $\alpha\xi + \beta\zeta + \gamma \equiv 0(m)$.

Lemma 2.4 Let $c = [a, b]$, $c^a = c^\mu$ and $c^b = c^\nu$, where $\mu, \nu \in \mathbb{Z}$ and neither μ nor ν equals 1. If α, β, γ, δ, ε and ϕ are non-negative integers, then $[a^\alpha b^\beta c^\gamma, a^\delta b^\varepsilon c^\phi] = c^\lambda$, where

$$\lambda = \gamma(\mu^\delta \nu^\varepsilon - 1) - \phi(\mu^\alpha \nu^\beta - 1) + \left(\frac{\mu^\alpha - 1}{\mu - 1}\right)\left(\frac{\nu^\varepsilon - 1}{\nu - 1}\right)\nu^\beta - \left(\frac{\mu^\delta - 1}{\mu - 1}\right)\left(\frac{\nu^\beta - 1}{\nu - 1}\right)\nu^\varepsilon .$$

Proof:
$$\begin{aligned}
[a^\alpha b^\beta c^\gamma, a^\delta b^\varepsilon c^\phi] &= [a^\alpha b^\beta c^\gamma, c^\phi][a^\alpha b^\beta c^\gamma, a^\delta b^\varepsilon]^{c^\phi} \\
&= [a^\alpha b^\beta, c^\phi]^{c^\gamma}[c^\gamma, c^\phi][a^\alpha b^\beta, a^\delta b^\varepsilon]^{c^\gamma c^\phi}[c^\gamma, a^\delta b^\varepsilon]^{c^\phi} \\
&= [a^\alpha b^\beta, c^\phi][a^\alpha, a^\delta b^\varepsilon]^{b^\beta}[b^\beta, a^\delta b^\varepsilon][c^\gamma, a^\delta b^\varepsilon] \\
&= [a^\alpha b^\beta, c^\phi][a^\alpha, b^\varepsilon]^{b^\beta}[a^\alpha, a^\delta]^{b^{\beta+\varepsilon}}[b^\beta, b^\varepsilon][b^\beta, a^\delta]^{b^\varepsilon}[c^\gamma, a^\delta b^\varepsilon] \\
&= [a^\alpha b^\beta, c^\phi][a^\alpha, b^\varepsilon]^{b^\beta}[b^\beta, a^\delta]^{b^\varepsilon}[c^\gamma, a^\delta b^\varepsilon] . \qquad (2.4.1)
\end{aligned}$$

Now,
$$\begin{aligned}
[a^\alpha b^\beta, c^\phi] &= [a^\alpha b^\beta, c^{(\phi-1)}][a^\alpha b^\beta, c]^{c^{(\phi-1)}} \\
&= [a^\alpha b^\beta, c^{(\phi-1)}][a^\alpha b^\beta, c] \\
&= [a^\alpha b^\beta, c]^\phi . \qquad (2.4.2)
\end{aligned}$$

Secondly
$$\begin{aligned}
[c, a^\delta] &= [c, a^{(\delta-1)}]\{[c, a]\}^{a^{(\delta-1)}} \\
&= [c, a^{(\delta-1)}]\{c^{(\mu-1)}\}^{\mu^{(\delta-1)}} \\
&= c^{(\mu-1)(1+\mu+\ldots+\mu^{(\delta-1)})} \\
&= c^{(\mu^\delta - 1)} . \qquad (2.4.3)
\end{aligned}$$

Similarly
$$[c, b^\varepsilon] = c^{(\nu^\varepsilon - 1)} . \qquad (2.4.4)$$

Finally,

$$\begin{aligned}
[a^{\alpha}, b^{\varepsilon}] &= [a^{\alpha}, b^{\varepsilon-1}][a^{\alpha}, b]^{b^{(\varepsilon-1)}} \\
&= [a^{\alpha}, b^{\varepsilon-1}]\{[a, b]^{a^{(\alpha-1)}}[a^{\alpha-1}, b]\}^{b^{(\varepsilon-1)}} \\
&= [a^{\alpha}, b^{\varepsilon-1}]\{[a, b]^{a^{(\alpha-1)}}[a, b]^{a^{(\alpha-2)}} \ldots [a, b]\}^{b^{(\varepsilon-1)}} \\
&= [a^{\alpha}, b^{\varepsilon-1}]\{c^{\mu^{(\alpha-1)}} c^{\mu^{(\alpha-2)}} \ldots c\}^{\nu^{(\varepsilon-1)}} \\
&= [a^{\alpha}, b^{\varepsilon-1}]\ c^{\{(\mu^{\alpha}-1)/(\mu-1)\}\ \nu^{(\varepsilon-1)}} \\
&= c^{\{(\mu^{\alpha}-1)/(\mu-1)\}(1+\nu+ \ldots +\nu^{(\varepsilon-1)})} \\
&= c^{\{(\mu^{\alpha}-1)/(\mu-1)\}\{(\nu^{\varepsilon}-1)/(\nu-1)\}} \qquad (2.4.5)
\end{aligned}$$

Consequently,

$$\begin{aligned}
[a^{\alpha}b^{\beta}, c^{\phi}] &= [a^{\alpha}b^{\beta}, c]^{\phi}, \qquad \text{by} \qquad (2.4.2) \\
&= \{[a^{\alpha}, c]^{b^{\beta}}, [b^{\beta}, c]\}^{\phi} \\
&= \{c^{(1-\mu^{\alpha})\nu^{\beta}}\ c^{(1-\nu^{\beta})}\}^{\phi}, \qquad \text{by (2.4.3) and} \qquad (2.4.4) \\
&= c^{\phi(1-\mu^{\alpha}\nu^{\beta})}\ . \qquad (2.4.6)
\end{aligned}$$

Similarly,

$$[c^{\gamma}, a^{\delta}b^{\varepsilon}] = c^{\gamma(\mu^{\delta}\nu^{\varepsilon}-1)}\ . \qquad (2.4.7)$$

Finally,

$$\begin{aligned}
[a^{\alpha}, b^{\varepsilon}]^{b^{\beta}} &= \{c^{\{(\mu^{\alpha}-1)/(\mu-1)\}\{(\nu^{\varepsilon}-1)/(\nu-1)\}}\}^{b^{\beta}}, \qquad \text{by} \qquad (2.4.5) \\
&= c^{\{(\mu^{\alpha}-1)/(\mu-1)\}\{(\nu^{\varepsilon}-1)/(\nu-1)\}\nu^{\beta}}\ . \qquad (2.4.8)
\end{aligned}$$

In a similar fashion,

$$[b^{\beta}, a^{\delta}]^{b^{\varepsilon}} = c^{-\{(\mu^{\delta}-1)/(\mu-1)\}\{(\nu^{\beta}-1)/(\nu-1)\}\nu^{\varepsilon}} \qquad (2.4.9)$$

Substituting (2.4.6), (2.4.7), (2.4.8) and (2.4.9) into (2.4.1) we see that

$$\left[a^{\alpha}b^{\beta}c^{\gamma},\ a^{\delta}b^{\varepsilon}c^{\phi}\right] = c^{\lambda}, \text{ where}$$

$$\lambda = \gamma(\mu^{\delta}\nu^{\varepsilon}-1) - \phi(\mu^{\alpha}\nu^{\beta}-1) + \left(\frac{\mu^{\alpha}-1}{\mu-1}\right)\left(\frac{\nu^{\varepsilon}-1}{\nu-1}\right)\nu^{\beta} - \left(\frac{\mu^{\delta}-1}{\mu-1}\right)\left(\frac{\nu^{\beta}-1}{\nu-1}\right)\nu^{\varepsilon}.$$

q.e.d.

Proof of Theorem 2.1. It suffices to show that the group $\langle a, b\rangle$ belongs to $\mathfrak{C}$. So we assume $G = \langle a, b\rangle$. Now $c^{\lambda} \in K(G)$ if and only if there exist non-negative integers α, β, γ, δ, ε and ϕ such that

$$\left[a^{\alpha}b^{\beta}c^{\gamma},\ a^{\delta}b^{\varepsilon}c^{\phi}\right] = c^{\lambda}.$$

If $\mu = 1$, then $[a^{\alpha}, b] = c^{\alpha}$ for all integers α, which implies $G \in \mathfrak{C}$. Similarly, if $\nu = 1$ then $G \in \mathfrak{C}$. Thus we need only consider the case $\mu \neq 1$ and $\nu \neq 1$. By Lemma 2.4, the proof is reduced to the following: given $\lambda \in \mathbb{Z}$, $1 \leq \lambda \leq |G'|$, we must find non-negative integers α, β, γ, δ, ε and ϕ such that

$$\gamma(\mu^{\delta}\nu^{\varepsilon}-1) - \phi(\mu^{\alpha}\nu^{\beta}-1) + \left(\frac{\mu^{\alpha}-1}{\mu-1}\right)\left(\frac{\nu^{\varepsilon}-1}{\nu-1}\right)\nu^{\beta} - \left(\frac{\mu^{\delta}-1}{\mu-1}\right)\left(\frac{\nu^{\beta}-1}{\nu-1}\right)\nu^{\varepsilon} \equiv \lambda(|G'|). \quad (2.1.1)$$

The proof continues on the following lines: given λ, we find suitable values of α, β, δ and ε, depending on which of the conditions I to IV is assumed not to hold for all prime divisors p of $|G'|$, and for each p we find integers $\gamma^{(p)}$ and $\phi^{(p)}$ such that

$$\gamma^{(p)}(\mu^{\delta}\nu^{\varepsilon}-1) - \phi^{(p)}(\mu^{\alpha}\nu^{\beta}-1) + \left(\frac{\mu^{\alpha}-1}{\mu-1}\right)\left(\frac{\nu^{\varepsilon}-1}{\nu-1}\right)\nu^{\beta} - \left(\frac{\mu^{\delta}-1}{\mu-1}\right)\left(\frac{\nu^{\beta}-1}{\nu-1}\right)\nu^{\varepsilon} \equiv \lambda(|G'|_p).$$

Then, by Lemma 2.3, we claim the existence of γ and ϕ such that the congruence (2.1.1) holds.

There are four cases to consider. For brevity of notation let us denote the left hand side of (2.1.1) by $f(\gamma, \phi)$ after α, β, δ and ε have been chosen.

Case 1 For each p, condition I does not hold. Let $\alpha = \varepsilon = 0$, $\beta = \delta = 1$. Then, $f(\gamma, \phi) = \gamma(\mu - 1) - \phi(\nu - 1) - 1$. Now for each prime divisor p of $|G'|$ either $\mu - 1 \not\equiv 0(p)$ or $\nu - 1 \not\equiv 0(p)$ by assumption. Consequently, there exist $\gamma^{(p)}$ and $\phi^{(p)}$ such that $f(\gamma^{(p)}, \phi^{(p)}) \equiv \lambda(|G'|_p)$ for each prime divisor p of $|G'|$. By Lemma 2.3, there exist γ and ϕ such that $f(\gamma, \phi) \equiv \lambda(|G'|)$ as required.

Case 2 For each p, condition II does not hold. By a result of K. Honda [4], c is a commutator if and only if every generator of $\langle c \rangle$ is a commutator. Thus by induction on $|G'|$, it suffices to show that for each prime divisor q of $|G'|$, $c^q = [a_q, b_q]$ for some $a_q, b_q \in G$, and for each prime divisor of $|\langle a_q, b_q \rangle'|$ condition II does not hold. (Clearly the induction starts when $|G'|$ is prime.)

Let $\alpha = 1$, $\beta = \delta = 0$ and $\varepsilon = q$. Then,

$$f(\gamma, \phi) = \gamma(\nu^q - 1) - \phi(\mu - 1) + \left(\frac{\nu^q - 1}{\nu - 1}\right).$$

For each p such that III or IV holds, let $\gamma^{(p)} = 0$ and choose $\phi^{(p)}$ such that

$$f(\gamma^{(p)}, \phi^{(p)}) = -\phi^{(p)}(\mu - 1) + \left(\frac{\nu^q - 1}{\nu - 1}\right) \equiv q(|G'|_p). \qquad (2.1.2)$$

For each p such that I holds let $\phi^{(p)} = 0$. Then we have

$$\begin{aligned} f(\gamma^{(p)}, \phi^{(p)}) &= \gamma^{(p)}(\nu^q - 1) + \left(\frac{\nu^q - 1}{\nu - 1}\right) \\ &= (1 + \nu + \nu^2 + \ldots + \nu^{q-1})(\gamma^{(p)}(\nu - 1) + 1) \\ &= (1 + (1+k) + \ldots + (1+k)^{q-1})(\gamma^{(p)}k + 1), \\ &\qquad \text{where } k = \nu - 1 \\ &= (q + \tfrac{1}{2}q(q-1)k + k^2 h(k))(\gamma^{(p)}k + 1), \\ &\qquad \text{where } h(k) \text{ is a polynomial in } k \\ &= q + \gamma^{(p)}k(q + \tfrac{1}{2}q(q-1)k + k^2 h(k)) + \tfrac{1}{2}q(q-1)k + k^2 h(k). \end{aligned}$$

Thus we have $f(\gamma^{(p)}, \phi^{(p)}) \equiv q(|G'|_p)$ if we can find $\gamma^{(p)}$ such that

$$\gamma^{(p)}k(q + \tfrac{1}{2}q(q-1)k + k^2h(k)) + \tfrac{1}{2}q(q-1)k + k^2h(k) \equiv O(|G'|_p)$$

We can do this if and only if

$$d = (k(q + \tfrac{1}{2}q(q-1)k + k^2h(k)),\ |G'|_p) \mid (\tfrac{1}{2}q(q-1)k + k^2h(k)).$$

Because p satisfies condition I and $k = \nu - 1$ we have that $p|k$.

If $q \neq p$ then $d = (k, |G'|_p)$ and

$$(k, |G'|_p) \mid (\tfrac{1}{2}q(q-1)k + k^2h(k)).$$

If $q = p \neq 2$ then $d = (kp, |G'|_p)$ and

$$(kp, |G'|_p) \mid (\tfrac{1}{2}p(p-1)k + k^2h(k)).$$

Finally, if $q = p = 2$, then, since we assume that $4 \nmid |G'|$, we have that $d = 2$ and $2 \mid (k + k^2h(k))$.

Therefore we can find $\gamma^{(p)}$ and $\phi^{(p)}$ such that

$$f(\gamma^{(p)}, \phi^{(p)}) = \gamma^{(p)}(\nu^q-1) + (\frac{\nu^q-1}{\nu-1}) \equiv q(|G'|_p). \qquad (2.1.3)$$

By applying Lemma 2.3 to the congruences (2.1.2) and (2.1.3) we deduce that there exist γ and ϕ such that $f(\gamma, \phi) \equiv q(|G'|)$ and so c^q is a commutator. Since $\alpha = 1$, $\beta = \delta = 0$ and $\varepsilon = q$ we have that $c^q = [ac^\gamma, b^q c^\phi]$. Now $c^{ac^\gamma} = c^\mu$ and $c^{b^q c^\phi} = c^{\nu^q}$, so for each prime divisor of $|\langle ac^\gamma, b^q c^\phi \rangle'|$ condition II does not hold, completing the induction.

Case 3 For each p, condition III does not hold. Let $\alpha = q$, $\beta = \delta = 0$ and $\varepsilon = 1$ giving

$$f(\gamma, \phi) = \gamma(\nu-1) - \phi(\mu^q-1) + (\frac{\mu^q-1}{\mu-1}).$$

The proof follows by an argument analogous to the one used in Case 2.

Case 4 For each p condition IV does not hold. The proof is, once again, on the same lines to the ones used in Case 2. Let $\alpha = \beta = 1$, $\delta = 0$ and $\varepsilon = q$, where q is a prime divisior of $|G'|$. Then,

$$f(\gamma, \phi) = \gamma(\nu^q-1) - \phi(\mu\nu-1) + (\frac{\nu^q-1}{\nu-1})\nu.$$

For each p such that II or III holds let $\gamma^{(p)} = 0$ and choose $\phi^{(p)}$ such that

$$f(\gamma^{(p)}, \phi^{(p)}) = -\phi^{(p)}(\mu\nu-1) + (\frac{\nu^q-1}{\nu-1})\nu \equiv q(|G'|_p).$$

For each p such that I holds let $\phi^{(p)} = 0$. Then we have

$$f(\gamma^{(p)}, \phi^{(p)}) = \gamma^{(p)}(\nu^q-1) + (\frac{\nu^q-1}{\nu-1})\nu$$

$$= (1+\nu+ \ldots +\nu^{q-1})(\gamma^{(p)}(\nu-1) + \nu)$$

$$= (1+(1+k) + \ldots + (1+k)^{q-1})(\gamma^{(p)}k + k + 1),$$

where $k = \nu - 1$

$$= (q+\tfrac{1}{2}q(q-1)k + k^2h(k))(\gamma^{(p)}k + k + 1),$$

where h(k) is a polynomial in k

$$= q + \gamma^{(p)}k(q+\tfrac{1}{2}q(q-1)k + k^2h(k))$$

$$+ k(q+\tfrac{1}{2}q(q-1)k + k^2h(k)) + \tfrac{1}{2}q(q-1)k + k^2h(k).$$

So $f(\gamma^{(p)}, \phi^{(p)}) \equiv q(|G'|_p)$ if we can find $\gamma^{(p)}$ such that

$$\gamma^{(p)}k(q+\tfrac{1}{2}q(q-1)k + k^2h(k)) + k(q+\tfrac{1}{2}q(q-1)k + k^2h(k)) + \tfrac{1}{2}q(q-1)k + k^2h(k) \equiv 0(|G'|_p).$$

Similarly to Case 2 we can do this if an only if

$$d = (k(q+\tfrac{1}{2}q(q-1)k + k^2h(k)), |G'|_p) \mid (k(q+\tfrac{1}{2}q(q-1)k + k^2h(k)) + \tfrac{1}{2}q(q-1)k + k^2h(k)).$$

Now d certainly divides $k(q+\frac{1}{2}q(q-1)k + k^2h(k))$ and so we have to show that d divides $(\frac{1}{2}q(q-1)k + k^2h(k))$. This was established in Case 2. As in Case 2 this implies that c^q is a commutator. Moreover $c^q = [abc^\gamma, b^q c^\phi]$ and it is easily seen that for each prime divisor of $|\langle abc^\gamma, b^q c^\phi\rangle'|$, condition II does not hold. q.e.d.

Proof of Corollary 2.2 By a result of [3], G' is generated by a commutator. Suppose first that G' is finite and G is nilpotent. By an argument in [3] we may assume that G is finite.

Now G being finite nilpotent implies that G is the direct product of its Sylow p-subgroup and consequently $G \in \mathfrak{C}$ is and only if $S_p \in \mathfrak{C}$, where S_p is any Sylow p-subgroup of G.

If $p \nmid 2$ then, by Theorem 2.1, $S_p \in \mathfrak{C}$.

If $p = 2$ let $(S_2)' = \langle c \rangle$, $c = [a, b]$ and $c^a = c^\mu$.

It suffices to show that $c^2 \in K(S_2)$.

If $\mu \equiv 3(4)$ we consider $[c, a] = c^{\mu-1}$. By the aforementioned result of Honda, $c^{\mu-1} \in K(S_2)$ implies that $c^2 \in K(S_2)$.

If $\mu \equiv 1(4)$ we consider $[a^2, b] = c^{\mu+1}$ and similarly conclude that $c^2 \in K(S_2)$.

This completes the proof of the case that G' is finite and G is nilpotent.

Next we suppose that G' is infinite. Let $G' = \langle c \rangle$ and $c = [a, b]$. Now $c^a = c$ or $c^a = c^{-1}$. If $c^a = c$ then $[a^\alpha, b] = c^\alpha$ for all integers α and consequently $G \in \mathfrak{C}$. Similarly of $c^b = c$ then $G \in \mathfrak{C}$. If $c^a = c^b = c^{-1}$ we consider $[b, ab \ldots ab]$ where there are α occurences of ab in the commutator $[b, ab \ldots ab]$.

Now $[b, ab \ldots ab] = [b, y]\,[b, ab]^y$,

where $y = (ab)^{\alpha-1}$

$= [b, y]\,[b, a]^{by}$

$= [b, y]\,(c^{-1})^{by}$

$= [b, y]\,c$

$= c^\alpha$, by an obvious induction.

Consequently $G \in \mathfrak{C}$, which completes the proof of the corollary.

We give examples to show that the theorem cannot be greatly extended. First we exhibit a class of groups G in which all of the conditions I to IV arise and G is disjoint from the class $\mathfrak{C}$.

Let p be a prime. From [40, pp 249-251] we know that there exist $p + 1$ distinct primes $\{q_i : 1 \leq i \leq p + 1\}$ such that $q_i \equiv 1(p)$ for each i. The multiplicative group of non-zero elements of $GF(q_j)$, the Galois field with q_j elements, is isomorphic to the cyclic group C_{q_j-1}, of order $q_j - 1$ [1, pp 49-51]. By our choice of q_j, the mapping that sends every element of C_{q_j-1} to its p th power is a homomorphism with a non-trivial kernel. Consequently for each prime q_j there exists an w_j such that $w_j \not\equiv 1(q_j)$ and $w_j^p \equiv 1(q_j)$. We define G to be the group generated by a and b subject to the following relations:

$[a, b] = c$, $|\langle c \rangle| = pq_1q_2 \ldots\ldots q_{p+1}$,

$c^a = c^r$ and $c^b = c^s$ where $r, s \in \mathbb{Z}$ are determined by

$r \equiv 1(p)$ $s \equiv 1(p)$, $r \equiv 1(q_1)$ $s \equiv w_1(q_1)$,

$r \equiv w_2(q_2)$ $s \equiv 1(q_2)$ and $r \equiv w_j(q_j)$ $s \equiv w_j^{(j-2)}(q_j)$ for $3 \leq j \leq p+1$.

We show that $c^p \notin K(G)$. By Lemma 2.2 $c^p \in K(G)$ if and only if there exist non-negative integers α, β, γ, δ, ε and ϕ such that

$$\gamma(r^\delta s^\varepsilon - 1) - \phi(r^\alpha s^\beta - 1) + \left(\frac{r^\alpha - 1}{r-1}\right)\left(\frac{s^\varepsilon - 1}{s-1}\right)s^\beta - \left(\frac{r^\delta - 1}{r-1}\right)\left(\frac{s^\beta - 1}{s-1}\right)s^\varepsilon \equiv p(|G'|) \qquad (2.1.4)$$

We denote the left hand side of (2.1.4) by f and the four terms of f by x_1, x_2, x_3 and x_4 respectively. Now $f \equiv p(|G'|)$ implies that $f \equiv 0(p)$, $f \equiv p(q_1)$, $f \equiv p(q_2)$, ... $f \equiv p(q_p)$ and $f \equiv p(q_{p+1})$ simultaneously. Now $x_1 \equiv x_2 \equiv 0(p)$ for every choice of α, β, γ, δ, ε and ϕ. Furthermore, $x_3 - x_4 \equiv 0(p)$ if and only if $\alpha\varepsilon - \delta\beta \equiv 0(p)$. Since $f = x_1 - x_2 + x_3 - x_4$, we require this congruence. If $\alpha \equiv \delta \equiv 0(p)$, then $f \equiv 0(q_2)$. So we may suppose that $\alpha \not\equiv 0(p)$. If $\beta \equiv 0(p)$, we must have $\varepsilon \equiv 0(p)$ to ensure that $\alpha\varepsilon - \delta\beta \equiv 0(p)$, but this implies $f \equiv 0(q_1)$, so $\beta \not\equiv 0(p)$. By our choice of primes $\{q_j : 1 \leq j \leq p+1\}$, there exist q_k such that $r^\alpha s^\beta \equiv 1(q_k)$. We show $f \equiv 0(q_k)$, which gives the desired contradiction. If $\delta \equiv 0(p)$, we must have $\varepsilon \equiv 0(p)$, to ensure that $\alpha\varepsilon - \delta\beta \equiv 0(p)$, but this implies $f \equiv 0(q_k)$. So we may assume that $\delta \not\equiv 0(p) \not\equiv \varepsilon$. Consequently there exists $\lambda \in \mathbb{Z}$ such that $\delta \equiv \lambda\alpha(p)$.

So $\alpha\varepsilon - \delta\beta \equiv 0(p)$ implies that $\alpha\varepsilon - \lambda\alpha\beta \equiv 0(p)$ and $\varepsilon \equiv \lambda\beta(p)$.

Thus $r^\delta s^\varepsilon \equiv r^{\lambda\alpha} s^{\lambda\beta} \equiv (r^\alpha s^\beta)^\lambda \equiv 1(q_k)$, which implies $x_1 \equiv x_2 \equiv 0(q_k)$.

Now $x_3 - x_4 = \left(\frac{r^\alpha - 1}{r-1}\right)\left(\frac{s^\varepsilon - 1}{s-1}\right)s^\beta - \left(\frac{r^\delta - 1}{r-1}\right)\left(\frac{s^\beta - 1}{s-1}\right)s^\varepsilon \equiv 0(q_k)$ if and only if

$(r^\alpha - 1)(s^\varepsilon - 1)s^\beta - (r^\delta - 1)(s^\beta - 1)s^\varepsilon \equiv 0(q_k)$

Now, $(r^\alpha - 1)(s^\varepsilon - 1)s^\beta - (r^\delta - 1)(s^\beta - 1)s^\varepsilon$

$= r^\alpha s^{\varepsilon+\beta} - r^\alpha s^\beta - s^{\varepsilon+\beta} + s^\beta - r^\delta s^{\varepsilon+\beta} + r^\delta s^\varepsilon + s^{\varepsilon+\beta} - s^\varepsilon$

$\equiv s^\varepsilon - 1 + s^\beta - s^\beta + 1 - s^\varepsilon \ (q_k)$

$\equiv 0 \ (q_k)$.

So, $f \equiv 0(q_k)$ which implies $c^p \notin K(G)$.

The constraint $4 \nmid |G'|$. If condition I is assumed not to arise in G, then the constraint $4 \nmid |G'|$ may be dropped. This is easily seen by referring to the proof of Theorem 2.1. However, the constraint is needed for each of the other three cases, as we now demonstrate.

Since we are demonstrating the fact that the prime 2 acts differently from other primes, we obtain explicit examples of groups rather than a whole class, as in the previous example.

Let $G = \langle a,b \mid [a,b] = c, c^{60} = 1, c^a = c^{29}, c^b = c^{11} \rangle$.

Because $60 = 4.3.5$, $29 - 1 \equiv 0(2)$, $11-1 \equiv 0(2)$, $29-1 \not\equiv 0(5)$, $11-1 \equiv 0(5)$, $29-1 \not\equiv 0(3)$ and $11-1 \not\equiv 0(3)$, G is such that condition II does not hold for each prime divisor of $|G'|$. A similar argument to that of the previous example shows that $c^2 \notin \mathcal{K}(G)$.

By symmetry, $4 \nmid |G'|$ is essential when condition III is assumed not to arise for each prime divisor of $|G'|$.

In a similar fashion one can show that if

$$G = \langle a,b \mid [a,b] = c, c^{60} = 1, c^a = c^{19}, c^b = c^{11} \rangle,$$

then $c^2 \notin \mathcal{K}(G)$. This shows that $4 \nmid |G'|$ is an essential constraint when condition IV is assumed not to hold for each prime divisor of $|G'|$.

Chapter 3 METABELIAN GROUPS

If not cyclic the least complicated structure the commutator subgroup can have is abelian and it is to such groups that we now turn our attention. There is a relatively well known example of a nilpotent of class two group G of order 256 such that G' is elementary abelian of order 16 and $G \notin \mathcal{C}$ (c.f. R. Carmichael [4 p.39]). We will show that this group is in many ways, minimal with respect to not belonging to the class $\mathcal{C}$. Indeed we obtain the following result:

Theorem 3.1 Let G be nilpotent of class 2 such that G' is finite and $d(G') \leq 3$. Then G' consists of commutators.

Proof: By an argument in [3] it suffices to assume that G is finite. Now G is finite nilpotent if and only if G is the direct product of its sylow-p-subgroups. Thus it suffices to consider G a p-group.

Let $G = \langle a_i | 1 \leq i \leq n \rangle$. If $c_{ij} = [a_i, a_j]$, then, because G' is an abelian p-group, we may select a minimal generating set from the c_{ij}'s. We consider the various possibilities that may arise in turn:

Case 1 $G' = \langle c_{12} \rangle$

Here we have that $c_{12}^{\alpha} = [a_1, a_2^{\alpha}]$ for all integers α.

Case 2 $G' = \langle c_{12}, c_{13} \rangle$.

Then, $c_{12}^{\alpha} c_{13}^{\beta} = [a_1, a_2^{\alpha} a_3^{\beta}]$, for all integers α and β.

Case 3 $G' = \langle c_{12}, c_{34} \rangle$.

Thus $c_{ij} = c_{12}^{\alpha_{ij}} c_{34}^{\beta_{ij}}$.

Let $(i, j) \in \{(1, 3), (1, 4), (2, 3), (2, 4)\}$.

If $\alpha_{ij} \neq 0(p)$, then there exists $\omega \in \mathbb{Z}$ such that

$$c_{ij}^{\omega} = c_{12}^{\alpha_{ij}\omega} c_{34}^{\beta_{ij}\omega} \quad \text{and} \quad \alpha_{ij}\omega \equiv 1(|c_{12}|).$$

Consequently $G' = \langle c_{ij}, c_{34} \rangle$, which is a presentation of the form discussed in Case 2.

Similarly, if $\beta_{ij} \not\equiv 0(p)$ we are reduced to Case 2.

Consequently, we may assume that for

$$(i, j) \in \{(1, 3), (1, 4), (2, 3), (2, 4)\}, \alpha_{ij} \equiv \beta_{ij} \equiv 0(p).$$

We consider $[a_1a_3, a_2^{\alpha}a_4^{\beta}] = c_{12}^{\alpha}c_{14}^{\beta}c_{23}^{-\alpha}c_{34}^{\beta}$

$$= c_{12}^{\alpha(1-\alpha_{23}) + \beta\alpha_{14}} c_{34}^{-\alpha\beta_{23} + \beta(1+\beta_{14})}.$$

Let $p^m = \max\{|c_{12}|, |c_{34}|\}$.

Then, for any integers r and s, $c_{12}^{r} c_{34}^{s} \in \mathcal{K}(G)$ if there exist solutions to the equations

$$\left.\begin{aligned} (1 - \alpha_{23})\alpha + \alpha_{14}\beta &\equiv r(p^m) \\ -\beta_{23}\alpha + (1 + \beta_{14})\beta &\equiv s(p^m) \end{aligned}\right\} \qquad (3.1.1)$$

Because $\alpha_{23} \equiv \beta_{23} \equiv \alpha_{14} \equiv \beta_{14} \equiv 0(p)$ we have that

$$\begin{vmatrix} 1 - \alpha_{23} & \alpha_{14} \\ -\beta_{23} & 1 + \beta_{14} \end{vmatrix} \not\equiv 0(p).$$

Therefore there exist solutions to the equations (3.1.1), completing the proof for Case 3.

Case 4 $\qquad G' = \langle c_{12}, c_{13}, c_{14} \rangle$.

Then $c_{12}^{\alpha} c_{13}^{\beta} c_{14}^{\gamma} = [a_1, a_2^{\alpha}a_3^{\beta}a_4^{\gamma}]$, for all integers α, β and γ.

Case 5 $\qquad G' = \langle c_{12}, c_{13}, c_{23} \rangle$.

We have to show that $c_{12}^{r} c_{13}^{s} c_{23}^{t} \in \mathcal{K}(G)$ for $r, s, t, \in \mathbb{Z}$.

Let $r = \bar{r}\, p^{\lambda}$, $s = \bar{s}\, p^{\mu}$ and $t = \bar{t}\, p^{\zeta}$, where $(\bar{r}, p) = (\bar{s}, p) = (\bar{t}, p) = 1$. We may assume without loss of generality that $\mu = \min\{\lambda, \mu, \zeta\}$. We consider $[a_1a_2^{\alpha}, a_2^{r}a_3^{s}] = c_{12}^{r} c_{13}^{s} c_{23}^{\alpha s}$. Since $(\bar{s}, p) = 1$, there exists $\bar{\alpha}$ such that $\bar{\alpha}\,\bar{s} \equiv \bar{t}(|c_{23}|)$. Let $\alpha = \bar{\alpha} p^{(\zeta-\mu)}$. Then $[a_1a_2^{\alpha}, a_2^{r}a_2^{s}] = c_{12}^{r} c_{13}^{s} c_{23}^{t}$, as required.

Case 6 $\qquad G' = \langle c_{12}, c_{34}, c_{13} \rangle$.

Let $c_{ij} = c_{12}^{\alpha_{ij}} c_{34}^{\beta_{ij}} c_{13}^{\gamma_{ij}}$.

Similarly to Case 3 we need only consider the case where the following restrictions hold:

(i) $\alpha_{14} \equiv 0(p)$. (Otherwise a reduction to Case 5.)

(ii) $\alpha_{23} \equiv 0(p)$. (Otherwise a reduction to Case 4.)

(iii) $\beta_{14} \equiv 0(p)$. (Otherwise a reduction to Case 4.)

(iv) $\beta_{23} \equiv 0(p)$. (Otherwise a reduction to Case 5.)

Let $p^m = \max\{|c_{12}|, |c_{34}|, |c_{13}|\}$.

Given $r, s, t \in \mathbb{Z}$, we show that we can find $\alpha, \beta, \gamma \in \mathbb{Z}$ such that $[a_1a_3, a_2^{\alpha}a_3^{\beta}a_4^{\gamma}] = c_{12}^{r} c_{34}^{s} c_{13}^{t}$.

Now $[a_1a_3, a_2^{\alpha}a_3^{\beta}a_4^{\gamma}] = c_{12}^{\alpha} c_{13}^{\beta} c_{14}^{\gamma} c_{23}^{-\alpha} c_{34}^{\gamma}$

$= c_{12}^{(1-\alpha_{23})\alpha + \alpha_{14}\gamma} c_{34}^{(1+\beta_{14})\gamma - \beta_{23}\alpha} c_{13}^{\beta + \gamma_{14}\gamma - \gamma_{23}\alpha}$.

So, we need to show the existence of solutions to the equation

$$\left.\begin{aligned} (1 - \alpha_{23})\alpha \qquad\qquad + \alpha_{14}\gamma &\equiv r(p^m) \\ - \beta_{23}\alpha \qquad + (1+\beta_{14})\gamma &\equiv s(p^m) \\ - \gamma_{23}\alpha + \beta \qquad + \gamma_{14}\gamma &\equiv t(p^m) \end{aligned}\right) \qquad (2.1.2)$$

Because $\alpha_{14} \equiv \alpha_{23} \equiv \beta_{14} \equiv \beta_{23} \equiv 0(p)$ we have that

$$\begin{vmatrix} 1 - \alpha_{23} & 0 & \alpha_{14} \\ - \beta_{23} & 0 & (1+\beta_{14}) \\ - \gamma_{23} & 1 & \gamma_{14} \end{vmatrix} \not\equiv 0(p), \text{ and, consequently,}$$

we may solve the equations (2.1.2) completing the proof for Case 6.

Case 7 $\qquad G' = \langle c_{12}, c_{34}, c_{15} \rangle$.

Let $c_{ij} = c_{12}^{\alpha_{ij}} c_{34}^{\beta_{ij}} c_{15}^{\gamma_{ij}}$.

Similarly to Cases 3 and 6 we need only consider the case where

$\alpha_{13} \equiv \alpha_{14} \equiv \alpha_{35} \equiv \alpha_{45} \equiv \beta_{23} \equiv \beta_{24} \equiv \beta_{35} \equiv \beta_{45} \equiv \gamma_{13} \equiv \gamma_{14} \equiv \gamma_{23} \equiv \gamma_{24} \equiv 0(p)$ (Otherwise a reduction to Case 6), $\beta_{13} \equiv \beta_{14} \equiv 0(p)$ (Otherwise a reduction to Case 4) and $\beta_{25} \equiv 0(p)$ (otherwise a reduction to Case 5).

Let $p^m = \max\{|c_{12}|, |c_{34}|, |c_{15}|\}$ and consider

$$[a_1^{\alpha}a_2^{\beta}a_3^{\gamma}, a_4a_5] = c_{14}^{\alpha}\, c_{15}^{\alpha}\, c_{24}^{\beta}\, c_{25}^{\beta}\, c_{34}^{\gamma}\, c_{35}^{\gamma}$$

$$= c_{12}^{\alpha_{14}\alpha+(\alpha_{24}+\alpha_{25})\beta+\alpha_{35}\gamma}\; c_{34}^{\beta_{14}\alpha+(\beta_{24}+\beta_{25})\beta+(1+\beta_{35})\gamma}\; c_{15}^{(1+\gamma_{14})\alpha+(\gamma_{24}+\gamma_{25})\beta+\gamma_{35}\gamma}.$$

So, given $r, s, t \in \mathbb{Z}$, there exist $\alpha, \beta, \gamma \in \mathbb{Z}$ such that

$[a_1^{\alpha}a_2^{\beta}a_3^{\gamma}, a_4a_5] = c_{12}^{r}\, c_{34}^{s}\, c_{15}^{t}$ if we can solve the following equations:

$$\left.\begin{aligned}
\alpha_{14}\,\alpha + (\alpha_{24} + \alpha_{25})\,\beta + \alpha_{35}\gamma &\equiv r(p^m)\\
\beta_{14}\,\alpha + (\beta_{24} + \beta_{25})\,\beta + (1+\beta_{35})\gamma &\equiv s(p^m)\\
(1+\gamma_{14})\alpha + (\gamma_{24} + \gamma_{25})\,\beta + \gamma_{35}\gamma &\equiv t(p^m)
\end{aligned}\right\} \quad (2.1.3)$$

If $\alpha_{24} + \alpha_{25} \not\equiv 0(p)$ then

$$\begin{vmatrix} \alpha_{14} & \alpha_{24}+\alpha_{25} & \alpha_{35} \\ \beta_{14} & \beta_{24}+\beta_{25} & 1+\beta_{35} \\ 1+\gamma_{14} & \gamma_{24}+\gamma_{25} & \gamma_{35} \end{vmatrix} \not\equiv 0(p),$$ and solutions exist to the equations (2.1.3)

So we are left to consider the case $\alpha_{24} + \alpha_{25} \equiv 0(p)$. We consider

$[a_1^{\alpha}a_2^{\beta}a_3^{\gamma}a_5, a_1a_4a_5] = c_{12}^{\delta}\, c_{34}^{\varepsilon}\, c_{15}^{\phi}$, where

$\delta = \alpha_{14}\alpha + (\alpha_{24} + \alpha_{25} - 1)\beta - (\alpha_{13} - \alpha_{35})\gamma - \alpha_{45}$,

$\varepsilon = \beta_{14}\alpha + (\beta_{24} + \beta_{25})\beta + (1 - \beta_{13} + \beta_{35})\gamma - \beta_{45}$ and

$\phi = (1 + \gamma_{14})\alpha + (\gamma_{24} + \gamma_{25})\beta - (\gamma_{13} - \gamma_{35})\gamma - 1 - \gamma_{45}$.

So given $r, s, t \in \mathbb{Z}$ there exist $\alpha, \beta, \gamma \in \mathbb{Z}$ such that

$[a_1^{\alpha}a_2^{\beta}a_3^{\gamma}a_5, a_1a_4a_5] = c_{12}^{r}\, c_{34}^{s}\, c_{15}^{t}$ if we can solve the following equations:

$$\left.\begin{aligned}
\alpha_{14}\alpha + (\alpha_{24}+\alpha_{25}-1)\beta - (\alpha_{13}-\alpha_{35})\gamma &\equiv r+\alpha_{45}(p^m)\\
\beta_{14}\alpha + (\beta_{24}+\beta_{25})\beta + (1-\beta_{13}+\beta_{35})\gamma &\equiv s+\beta_{45}(p^m)\\
(1+\gamma_{14})\alpha + (\gamma_{24}+\gamma_{25})\beta - (\gamma_{13}-\gamma_{35})\gamma &\equiv t+1+\gamma_{45}(p^m)
\end{aligned}\right\} \quad (2.1.4)$$

Because $\alpha_{24} + \alpha_{25} \equiv 0(p)$,

$$\begin{vmatrix} \alpha_{14} & \alpha_{24}+\alpha_{25}-1 & -\alpha_{13}+\alpha_{35} \\ \beta_{14} & \beta_{24}+\beta_{25} & 1-\beta_{13}+\beta_{35} \\ (1+\gamma_{14}) & \gamma_{24}+\gamma_{25} & -\gamma_{13}+\gamma_{35} \end{vmatrix} \not\equiv 0(p),$$

and, consequently, there exist solutions to the equations (2.1.4), completing the proof for Case 7.

Case 8 $\quad G' = \langle c_{12}, c_{34}, c_{56} \rangle$.

Let $\quad c_{ij} = c_{12}^{\alpha_{ij}} c_{34}^{\beta_{ij}} c_{56}^{\gamma_{ij}}$.

For $(i,j) \in \{(1,3), (1,4), (1,5), (1,6), (2,3), (2,4), (2,5), (2,6) (3,5), (3,6), (4,5), (4,6)\}$

we need only consider $\alpha_{ij} \equiv \beta_{ij} \equiv \gamma_{ij} \equiv 0(p)$, otherwise we have a reduction to Case 7.

Let $p^m = \max\{|c_{12}|, |c_{34}|, |c_{56}|\}$. Similarly to before, given $r, s, t \in \mathbb{Z}$ we show that there exist $\alpha, \beta, \gamma \in \mathbb{Z}$ such that $[a_1a_3a_5, a_2^{\alpha}a_4^{\beta}a_6^{\gamma}] = c_{12}^{r} c_{34}^{s} c_{56}^{t}$. As before this reduces to showing that there exist solutions to the equations

$$\left.\begin{aligned} (1 - \alpha_{23} - \alpha_{25})\alpha + (\alpha_{14} - \alpha_{45})\beta + (\alpha_{16} + \alpha_{36})\gamma &\equiv r(p^m) \\ -(\beta_{23} + \beta_{25})\alpha + (1 + \beta_{14} - \beta_{45})\beta + (\beta_{16} + \beta_{36})\gamma &\equiv s(p^m) \\ -(\gamma_{23} + \gamma_{25})\alpha + (\gamma_{14} - \gamma_{45})\beta + (1 + \gamma_{16} + \gamma_{36})\gamma &\equiv t(p^m) \end{aligned}\right\} \quad (2.1.5)$$

Once again the corresponding determinant takes a non-zero value modulo p and, therefore, solutions to (2.1.5) exist. q.e.d.

We now give two examples of groups that demonstrate the fact that no generalisation of Theorem 3.1. is easily obtainable.

Let $G_1 = \langle a_i \mid 1 \leq i \leq 4, a_i^2 = 1, G_1 \text{ is class 2 nilpotent}, [a_2,a_4] = [a_3,a_4] = 1 \rangle$

and $G_2 = \langle b_i \mid 1 \leq i \leq 4, b_i^2 = 1, G_2 \text{ is class 2 nilpotent}, [b_1,b_2] = [b_3,b_4] = 1 \rangle$.

Now G_1 is the aforementioned example from [4] and it is quite easy to show (c.f. I. D. Macdonald [3]) that $[a_1,a_4][a_2,a_3] \notin \mathcal{H}(G_1)$. However, one can easily demonstrate that $G_2 \in \mathcal{C}$.

Theorem 3.1 is essentially a statement related to finite p-groups. By assuming the groups concerned to be nilpotent of class two we were able to deal with groups of arbitrary exponent. If, however, we only assume the groups to be metabelian such that the derived subgroup is a p-group, then we are only able to handle some cases where the derived subgroup is elementary abelian.

Theorem 3.2 Let G be a finite group such that G' is elementary abelian of order p^3. Then $G \in \mathcal{G}$.

Proof. Let S be a Sylow p-subgroup of G. Because $G' \subseteq S$, we have that $S \lhd G$. So, by the Schur-Zassenhaus Theorem [16, pp 220-224], $G = S \lambda K$, where K is a complement to S in G. Again because $G' \subseteq S$, we have that K is abelian.

By Theorem 5.2.3 of [16] we make the following crucial observation:

$$G' = [G', K] \times C_{G'}(K) \tag{3.2.1}$$

We continue by considering, in turn, the various possibilities arising from (3.2.1).

Case 1 $$G' = [G', K] \tag{3.2.2}$$

Let $G' = \langle a_1, a_2, a_3 \rangle$, where $a_i = [b_i, k_i]$, $b_i \in G'$, $k_i \in K$ for $1 \leq i \leq 3$. We may assume that $K = \langle k_1, k_2, k_3 \rangle$.

Suppose $C_{G'}(\langle k_1, k_2 \rangle) = \langle 1 \rangle$. Then once again by Theorem 5.2.3. of [16], $G' = [G', \langle k_1, k_2 \rangle]$. Because K is abelian $[G', \langle k_1, k_2 \rangle] = \langle [G', \langle k_1 \rangle], [G', \langle k_2 \rangle] \rangle$. Let $g \in G'$. Then $g = g_1 g_2$, for some $g_i \in [G', \langle k_i \rangle]$, $1 \leq i \leq 2$. Let $h \in G'$. Then $[h, k_1^n] = [h, k_1][h^{k_1}, k_1^{n-1}] = \ldots = [h, k_1][h^{k_1}, k_1] \ldots [h^{k_1^{n-1}}, k_1] = [hh^{k_1} \ldots h^{k_1^{n-1}}, k_1]$. Thus $g_1 = [h_1, k_1]$, for some $h_1 \in G'$. Similarly, $g_2 = [h_2, k_2]$ for some $h_2 \in G'$. So, $g = g_1 g_2 = [h_1, k_1][h_2, k_2] = [k_1 h_2, k_2 h_1^{-1}]$, which implies that $G \in \mathcal{G}$.

We now consider the case $C_{G'}(\langle k_1, k_2 \rangle) \neq \langle 1 \rangle$. By symmetry we may assume that $C_{G'}(\langle k_1, k_3 \rangle) \neq \langle 1 \rangle \neq C_{G'}(\langle k_2, k_3 \rangle)$.

If $C_{G'}(\langle k_r, k_s \rangle) \cap \langle C_{G'}(\langle k_r, k_t \rangle), C_{G'}(\langle k_s, k_t \rangle) \rangle \neq \langle 1 \rangle$, for $r, s, t \in \{1, 2, 3\}$ and r, s, t pairwise different, then $C_{G'}(\langle k_r, k_s, k_t \rangle) = C_{G'}(K) \neq \langle 1 \rangle$.

But, from (3.2.1) and (3.2.2) we reach the conclusion $C_{G'}(K) = \langle 1 \rangle$, a contradiction. Consequently, $G' = C_{G'}(\langle k_1, k_2 \rangle) \times C_{G'}(\langle k_1, k_3 \rangle) \times C_{G'}(\langle k_2, k_3 \rangle)$. Let $C_{G'}(\langle k_1, k_2 \rangle) = \langle g_1 \rangle$, $C_{G'}(\langle k_1, k_3 \rangle) = \langle g_2 \rangle$ and $C_{G'}(\langle k_2, k_3 \rangle) = \langle g_3 \rangle$ where,

$$\langle g_1 \rangle \cong \langle g_2 \rangle \cong \langle g_3 \rangle \cong C_p.$$

Now $K \subseteq N_G(C_{G'}\langle k_1, k_2 \rangle)$, so $g_1^{k_3} = g_1^{r_1}$, for some $r_1 \in \mathbb{Z}$.

If $r_1 = 1$, then $k_3 \in C_G(C_{G'}(\langle k_1, k_2 \rangle))$ and consequently, $C_{G'}(\langle k_1, k_2, k_3 \rangle) = C_{G'}(K) \neq \langle 1 \rangle$, contradicting (3.2.2). So, $g_1^{k_3} = g_1^{r_1}$, where $r_1 \neq 1$. In a similar fashion,

$g_2^{k_2} = g_2^{r_2}$ and $g_3^{k_1} = g_3^{r_3}$, where r_2 and r_3 are positive integers not equal to one.

Thus,

$g_1^{r_1 - 1} = [g_1, k_3]$, $g_2^{r_2 - 1} = [g_2, k_2]$ and $g_3^{r_3 - 1} = [g_3, k_1]$.

Now there exist λ_i such that $(r_i - 1)\lambda_i \equiv 1(p)$ for $1 \leq i \leq 3$.

Consequently,

$g_1 = [g_1^{\lambda_1}, k_3]$, $g_2 = [g_2^{\lambda_2}, k_2]$ and $g_3 = [g_3^{\lambda_3}, k_1]$.

Let $g \in G'$. Then $g = g_1^{\alpha} g_2^{\beta} g_3^{\gamma}$, where $\alpha, \beta, \gamma \in \mathbb{Z}$.

So,

$$g = [g_1^{\lambda_1}, k_3]^{\alpha} [g_2^{\lambda_2}, k_2]^{\beta} [g_3^{\lambda_3}, k_1]^{\gamma} = [g_1^{\lambda_1 \alpha} g_2^{\lambda_2 \beta} g_3^{\lambda_3 \gamma}, k_1 k_2 k_3].$$

This completes the proof for Case 1.

Case 2 $\quad G' = S' \cong C_p \times C_p \times C_p$.

S induces a group of automorphisms on S', by conjugation. So there exists a homomorphism ϕ of S into GL(3, p). Since S is a p-group we may consider $\phi(S) \subseteq STL(3, p)$ which is, by Theorem 1.4A of [6], a Sylow p-subgroup of GL(3, p). Because S' is abelian, $\phi(S)$ is an abelian group. By Theorem 1.2 of [6], $|STL(3, p)| = p^3$. By Lemma 1.3 of [6], STL(3, p) is nilpotent of class 2 and consequently, either $|\phi(S)| = p$ or $|\phi(S)| = p^2$.

Let $S' = \langle g_1, g_2, g_3 \rangle$, where we may assume that $g_i \in \mathcal{H}(G)$ for $1 \leq i \leq 3$. By considering [7] we see that it suffices to show that $g_1 g_2^{\alpha} g_3^{\beta} \in \mathcal{H}(S)$ and $g_2 g_3^{\beta} \in \mathcal{H}(S)$, where $\alpha, \beta \in \mathbb{Z}$. We consider the various possibilities for the structure of $\phi(S)$ in turn.

(i) $|\phi(S)| = p^2$.

So $\phi(S) = \left\langle \begin{bmatrix} 1 & \gamma & 0 \\ 0 & 1 & \delta \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\rangle$ where $\gamma, \delta \in \mathbb{Z}$.

Various situations arise, depending on the values of γ, δ and p.

Because $\mathcal{H}(S)$ is a characteristic subset of S it suffices to show that the element under consideration is conjugate to a commutator.

(a) $\gamma \equiv 0(p)$.

If $\delta \equiv 0(p)$, then $|\phi(S)| = p$. So $\delta \not\equiv 0(p)$.

By considering how $\phi(S)$ acts upon S' we see that

$g_1 \sim g_1 g_3$, $g_2 \sim g_2 g_3^{\delta}$ and $g_3 \in Z(S)$. Because $S' = \langle g_1, g_2, g_3 \rangle$, S is nilpotent of class 3 and $S/\langle g_3 \rangle$ is nilpotent of class 2. By Theorem 3.1, $S/\langle g_3 \rangle \in \mathfrak{C}$. So $g_1 g_2^{\alpha} \langle g_3 \rangle \in \mathcal{H}(S/\langle g_3 \rangle)$ and consequently,

$$g_1 g_2^{\alpha} g_3^{\lambda} \in \mathcal{H}(S) \text{ for some } \lambda \in \mathbb{Z}.$$

Now $g_1 g_2^{\alpha} g_3^{\lambda} \sim g_1 g_2^{\alpha} g_3^{\lambda} \cdot g_3 \sim \ldots \sim g_1 g_2^{\alpha} g_3^{\lambda+r}$, where $r \in \mathbb{Z}$. So $g_1 g_2^{\alpha} g_3^{\beta} \in \mathcal{H}(S)$, where $\alpha, \beta \in \mathbb{Z}$.

Now $g_2 \sim g_2 g_3^{\delta} \sim g_2 g_3^{2\delta} \ldots \sim g_2 g_3^{r\delta}$, where $r \in \mathbb{Z}$. Since $\delta \not\equiv 0(p)$ we have $g_2 \sim g_2 g_3^{\beta}$, where $\beta \in \mathbb{Z}$ and consequently, $g_2 g_3^{\beta} \in \mathcal{H}(S)$.

(b) $\gamma \not\equiv 0(p)$ and $p \neq 2$.

Now $\begin{bmatrix} 1 & \gamma & 0 \\ 0 & 1 & \delta \\ 0 & 0 & 1 \end{bmatrix}^{r_1} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}^{r_2} = \begin{bmatrix} 1 & r_1\gamma & r_1(r_1-1)\gamma\delta/2 + r_2 \\ 0 & 1 & r_1\delta \\ 0 & 0 & 1 \end{bmatrix}$

By selecting suitable r_1 and r_2 we have $g_1 \sim g_1 g_2^{\alpha} g_3^{\beta}$, where $\alpha, \beta \in \mathbb{Z}$ and consequently, $g_1 g_2^{\alpha} g_3^{\beta} \in \mathcal{H}(S)$. To show that $g_2 g_3^{\beta} \in \mathcal{H}(S)$ we observe that $\exists\ s \in S$ such that $s^{-1} g_1 s = g_1 g_2 g_3^{\beta}$ and consequently, $[g_1, s] = g_2 g_3^{\beta}$.

(c) $p = 2$ and $\gamma \equiv 1(2)$.

Let $s_1, s_2 \in S$ be such that s_1 and s_2 induce the automorphisms given by the matrices $\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & \delta\\ 0 & 0 & 1\end{pmatrix}$ and $\begin{pmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$ respectively.

Then $g_1^{s_1} = g_1g_2$, $g_1^{s_2} = g_1g_3$, $g_1^{s_2s_1} = g_1g_2g_3$ and $[g_1, s_2s_1] = g_2g_3$. Consequently, $S \in \mathcal{C}$.

(ii) $|\phi(S)| = p$.

There are two possibilities to consider.

(a) $\phi(S) = \left\langle \begin{pmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} \right\rangle$

$S/\langle g_3\rangle$ is nilpotent of class 2 and by a similar argument to that used in (i)(a) we may conclude that $g_1g_2^{\alpha}g_3^{\beta} \in \mathcal{K}(S)$, where $\alpha, \beta \in \mathbb{Z}$. It remains to show that $g_2g_3^{\beta} \in \mathcal{K}(S)$, where $\beta \in \mathbb{Z}$. Let $g_2 = [s_1, s_2]$ and $g_3 = [g_1, s_3]$ where $s_1, s_2, s_3 \in S$. Now $[g_1, s_1] \in Z(S)$, so $[g_1, s_1] = g_3^{\lambda}$, where $\lambda \in \mathbb{Z}$. If $\lambda \not\equiv 0(p)$, then $[s_1, s_2g_1^{\mu}] = g_2g_3^{-\lambda\mu}$ and for suitable choice of μ we have $[s_1, s_2g_1^{\mu}] = g_2g_3^{\beta}$, where $\beta \in \mathbb{Z}$. Thus it remains to consider the case $\lambda \equiv 0(p)$, i.e. $[g_1, s_1] = 1$. Similarly we may assume that $[g_1, s_2] = 1$.

We note that $[s_3, s_2]^{g_1} = [s_3^{g_1}, s_2] = [s_3g_3, s_2] = [s_3, s_2]$ and similarly, $[s_3, s_1]^{g_1} = [s_3, s_1]$.

Let $[s_3, s_1] = g_1^{\omega_1}g_2^{\omega_2}g_3^{\omega_3}$ and $[s_3, s_2] = g_1^{\omega_4}g_2^{\omega_5}g_3^{\omega_6}$, where $\omega_i \in \mathbb{Z}$ for $1 \leq i \leq 6$.

We consider $g = [s_3s_1^{\lambda}s_2^{\mu}, s_1^{\gamma}s_2^{\delta}g_1^{\varepsilon}]$, where $\lambda, \mu, \gamma, \delta, \varepsilon \in \mathbb{Z}$.

Because $[g_1, s_1] = [g_1, s_2] = 1$ and $Z(s) = \langle g_2, g_3\rangle$ we have that $\langle s_1, s_2\rangle \subseteq C_s(S')$. Using this fact it is easily seen that

$$g = [s_3, s_1]^{\gamma}[s_3, s_2]^{\delta}[s_3, g_1]^{\varepsilon}[s_1, s_2]^{\lambda\delta}[s_2, s_1]^{\mu\gamma}$$
$$= (g_1^{\omega_1}g_2^{\omega_2}g_3^{\omega_3})(g_1^{\omega_4}g_2^{\omega_5}g_3^{\omega_6})^{\delta}g_3^{-\varepsilon}g_2^{\lambda\delta - \mu\gamma}$$

We choose γ and δ such that, either $\gamma \notin O(p)$ or $\delta \notin O(p)$ and $\omega_1\gamma + \omega_4\delta \equiv O(p)$.

We then choose γ, μ and ε such that $g = s_2 s_3^{\beta}$, where $\beta \in \mathbb{Z}$.

(b) $\phi(S) = \left\langle \begin{vmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{vmatrix} \right\rangle$

Let $g_1 = [s_1, s_2]$ where $s_1, s_2 \in S$.

Suppose $g_1^{s_1} = g_1 g_2^{\lambda}$, where $\lambda \notin O(p)$. Consequently, $g_2^{s_1} = g_2 g_3^{\lambda}$.

Then, $[s_1, s_2 g_1^{\alpha} g_2^{\beta}] = g_1 (g_2^{\alpha} g_3^{\beta})^{\lambda}$

and $[s_1, g_1 g_2^{\beta}] = (g_2 g_3^{\beta})^{\lambda}$, where $\alpha, \beta \in \mathbb{Z}$.

Similarly, $g_1^{s_2} = g_1 g_2^{\lambda}$ where $\lambda \notin O(p)$ implies $S \in \mathfrak{C}$, so it only remains for us to consider the case $g_1^{s_1} = g_1^{s_2} = g_1$.

Now there exists $s \in S$ such that $g_1^{s} = g_1 g_2$ and $g_2^{s} = g_2 g_3$.

Let $[s, s_2] = g_1^{\omega_1} g_2^{\omega_2} g_3^{\omega_3}$, where $\omega_i \in \mathbb{Z}$ for $1 \leq i \leq 3$.

Then, $[s s_1^{-\omega_1+1}, s_2 g_1^{\lambda} g_2^{\mu}] = g_1 g_2^{\omega_2 - \lambda} g_3^{\omega_3 + \mu}$

and $[s s_1^{-\omega_1}, s_2 g_1^{\lambda} g_2^{\mu}] = g_2^{\omega_2 - \lambda} g_3^{\omega_3 + \mu}$.

By suitable choices of λ and μ we have that $g_1 g_2^{\alpha} g_3^{\beta} \in \mathfrak{K}(S)$ and $g_2 g_3^{\beta} \in \mathfrak{K}(S)$ where $\alpha, \beta \in \mathbb{Z}$.

This concludes the proof of Case 2.

Case 3 $\qquad [G', K] \neq G' \neq S'$

By Theorem 5.3.5 of [16] we have,

$$S = [S, K]\, C_S(K) \qquad (.3.2.3)$$

Now $K \trianglelefteq N_G([S, K])$ and $[s_1, k]^{s_2} = [s_1 s_2, k][s_2, k]^{-1}$, where $s_1, s_2 \in S$ and $k \in K$. Therefore

$$[S, K] \lhd G \qquad (3.2.4).$$

By considering (3.2.3) and (3.2.4), remembering that G' is abelian, we see that

$$S' = \langle [[S, K], C_S(K)], C_S(K)' \rangle \tag{3.2.5}$$

Because of (3.2.4) we have that

$$[[S, K], C_S(K)] \subseteq [S, K]. \tag{3.2.6}$$

By Theorem 5.3.6 of [16],

$$[S, K] = [[S, K], K].$$

So,

$$[[S, K], C_S(K)] \subseteq [G', K]. \tag{3.2.7}$$

By Theorem 5.2.3 of [16],

$$G' = [G', K] \times C_{G'}(K) \tag{3.2.8}$$

Noting that $C_S(K)' \subseteq C_{G'}(K)$ we have, by considering (3.2.5), (3.2.7) and (3.2.8),

$$S' = [[S, K], C_S(K)] \times C_S(K)'. \tag{3.2.9}$$

Again by Theorem 5.2.3 of [16] we have,

$$S' = [S', K] \times C_{S'}(K). \tag{3.2.10}$$

Now $C_S(K)' \subseteq C_{S'}(K) \subseteq C_{G'}(K)$, $[S', K] \subseteq [G', K]$ and by (3.2.7) $[[S, K], C_S(K)] \subseteq [G', K]$.

So by (3.2.8) we have,

$$C_S(K)' = C_{S'}(K) \tag{3.2.11}$$

If $[[S, K], C_S(K)] \neq [S', K]$, then there exist $x \in [[S, K], C_S(K)]$ and $y \in [S', K]$ such that $1 \neq xy \in C_{S'}(K)$. But $\langle [[S, K], C_S(K)], [S', K] \rangle \subseteq [G', K]$ and, by (3.2.8), $[G', K] \cap C_{G'}(K) = \langle 1 \rangle$, a contradiction.

Therefore,

$$[[S, K], C_S(K)] = [S', K]. \tag{3.2.12}$$

We consider the various possibilities for the structure of S' in turn.

(i) $$C_{S'}(K) \cong C_p, \quad [S', K] = \langle 1 \rangle.$$

By (3.2.10), $$S' \cong C_p. \tag{3.2.13}$$

Because $G = S \lambda K$, $G' = \langle [S, K], S' \rangle$.

Recalling that, by Theorem 5.3.6 of [6], $[S, K] = [[S, K], K]$, we see that

$[S, K] = [G', K] \cong C_p \times C_p$.

So, by (3.2.8), $C_{G'}(K) \cong C_p$. (3.2.14)

Let $g \in G'$. Then $g = g_1 g_2$, where $g_1 \in [G', K]$ and $g_2 \in C_{G'}(K)$.

Again by Theorem 5.3.6 of [6] we have $[G', K] = [[G', K], K]$.

So $g_1 = [s_1, k_1][s_2, k_2] = [k_2 s_1, k_1 s_2^{-1}]$, where $k_1, k_2 \in K$ and $s_1, s_2 \in [G', K]$.

By (3.2.11), (3.2.13) and (3.2.14) we have,

$$C_{G'}(K) = C_{S'}(K) = C_S(K)'.$$

So $g_2 = [s_3, s_4]$, where $s_3, s_4 \in C_S(K)$.

Consequently $g = g_1 g_2 = [k_2 s_1 s_3, k_1 s_2^{-1} s_4]$.

(ii) $$C_{S'}(K) \cong [S', K] \cong C_p.$$

Because $C_S(K) \subseteq N_S([S', K])$ and S is a p-group, we have that

$[C_S(K), [S', K]] \subsetneq [S', K]$.

Since $[S', K] = C_p$,

$$[C_S(K), [S', K]] = \langle 1 \rangle. \quad (3.2.15)$$

Now $G' = \langle [S, K], S' \rangle$. So, by (3.2.10), $G' = \langle [S, K], C_{S'}(K) \rangle$. By Theorem 5.3.6 of [6], $[S, K] = [[S, K], K]$. So $G' = \langle [G', K], C_{S'}(K) \rangle$.

Because $C_{S'}(K) \cong C_p$, $[G', K] = \langle g_1 \rangle \times [S', K] \cong C_p \times C_p$. Let $g \in G'$.

Then $g = g_1^{\alpha} g_2 g_3$, where $g_2 \in [S', K]$, $g_3 \in C_{S'}(K)$ and $\alpha \in \mathbb{Z}$.

Suppose $\alpha \neq 0$.

Now, as in (i), $g_1^{\alpha} g_2 = [k_1 s_1, k_2 s_2]$, where $k_1, k_2 \in K$ and $s_1, s_2 \in [G', K]$.

By (3.2.11), $g_3 = [s_3, s_4]$, where $s_3, s_4 \in C_S(K)$.

Now, $[k_1 s_1 s_3, k_2 s_2 s_4] = [k_1 s_1 s_3, s_4][k_1 s_1 s_3, k_2 s_2]^{s_4}$

$= [k_1, s_4]^{s_1 s_3}[s_1 s_3, s_4][k_1 s_1, k_2 s_2]^{s_3 s_4}[s_3, k_2 s_2]^{s_4}$

$= [s_1, s_4][s_3, s_4][k_1 s_1, k_2 s_2][s_3, s_2]$, by (3.2.15), (3.2.12)

and because $s_3, s_4 \in C_S(K)$.

By (3.2.12), $[s_1, s_4][s_3, s_2] = g_2^{\mu}$, where $\mu \in \mathbb{Z}$.

So, $[k_1 s_1 s_3, k_2 s_2 s_4] = g_1^{\alpha} g_2 g_3 g_2^{\mu}$.

By (3.2.12) there exists $s \in C_S(K)$ such that $g_1^s = g_1 g_2^\lambda$, where $\lambda \in \mathbb{Z}$ and $\lambda \not\equiv 0(p)$. Consequently, there exists $\zeta \in \mathbb{Z}$ such that $\mu + \zeta\lambda\alpha \equiv 0(p)$. Then, $[k_1 s_1 s_3,\ k_2 s_2 s_4]^{s^\zeta} = g_1^\alpha g_2 g_3$, as required.

If $\alpha = 0$ it suffices to show that $S \in \mathcal{C}$. This was shown to be true in Case 2.

(iii) $$C_{S'}(K) = C_p \times C_p$$

Let $H_1 = C_S(K) \times H_2$, where H_2 is a finite p-group such that $H_2' \cong C_p$. By Case 2, $H_1 \in \mathcal{C}$, which implies that $C_S(K) \in \mathcal{C}$.

By (3.2.8), $[G', K] \cong C_p$, so $[G', K] \in \mathcal{C}$.

Let $g \in G'$. Then $g = g_1 g_2$, where $g_1 \in C_{S'}(K)$ and $g_2 \in [G', K]$.

Now $g_1 = [s_1, s_2]$, where $s_1, s_2 \in C_S(K)$ and $g_2 = [s_3, k]$, where $s_3 \in [G', K]$ and $k \in K$.

Consequently, $g = [s_1, s_2][s_3, k] = [s_1 s_3, k s_2]$, because $\langle 1 \rangle = [C_S(K), [G', K]] \subsetneq [G', K]$.

(iv) $C_{S'}(K) = 1$. Then $S' = [S, K]$. Therefore $G' = [G', K]$, a contradiction. q.e.d.

Instead of assuming that G' is a p-group we now assume that $S \subseteq G'$.

Theorem 3.3 Let G be a finite group with a Sylow p-subgroup $S \cong C_p \times C_p$ such that $S \subseteq G'$.

Then, $$S \subseteq \mathcal{K}(G).$$

Proof By Theorem 7.4.4 of [16] we see that $S \subseteq N_G(S)'$. So it suffices to assume that $S \lhd G$. We assume G to be a minimal counter-example and we obtain a contradiction.

Let $S = \langle c_1 \rangle \times \langle c_2 \rangle$, where we assume $c_1 \notin \mathcal{K}(G)$. Now G induces a p'-group of automorphisms upon S and, consequently by Theorem 2.3 of [15], $S = [S, G] \times C_S(G)$. By the Focal Subgroup Theorem (c.f. Theorem 7.3.4 of [16]).

$$[S, G] = S \cap G' = S. \quad \text{So } C_S(G) = \langle 1 \rangle.$$

Thus, there exists $g_1 \in G$ such that $c_1^{g_1} \neq c_1$.

If g_1 induces a fixed point free automorphism upon S, then it immediately follows that $S \subseteq \mathcal{K}(G)$. So we only need to consider the case where

$C_S(g_1) \neq 1$. Without loss of generality we may assume that $c_2^{g_1} = c_2$.
Let $c_1^{g_1} = c_1^r c_2^w$, for $r,w \in \mathbb{Z}$.
Suppose that $[c_1, g] \in \langle [c_1, g_1] \rangle \ \forall g \in G$. Now, $[c_1^\lambda, g_1] = [c_1, g_1]^\lambda$, $\lambda \in \mathbb{Z}$ and consequently, $\langle [c_1, g_1] \rangle \subseteq \mathcal{K}(G)$. Therefore $c_1 \notin \langle [c_1, g_1] \rangle$.
By Proposition 12.2 of [35], G has a proper normal subgroup K such that $|G/K| \mid |S/\langle [c_1, g_1] \rangle|$. Therefore $|G/K| = p$. So G/K is abelian and, therefore, $G' \subseteq K$. But $S \subseteq G'$ and, consequently, $|G/K|$ is a p'-number, a contradiction. So we may assume that there exists $g_2 \in G$ such that,

$$S = \langle [c_1, g_1], [c_1, g_2] \rangle.$$

Because S is abelian normal subgroup of G the mapping $\phi(g_2)$ defined by

$\phi(g_2) : s \mapsto [s, g_2]$, where $s \in S$, is an endomorphism of S.
Moreover $\phi(g_2)(S) \subseteq \mathcal{K}(G)$. So, if $[c_2, g_2] \notin \langle [c_1, g_1] \rangle$, then $\phi(g_2)(S) = S \subseteq \mathcal{K}(G)$.
By the minimality of G we may assume that $G = \langle S, g_1, g_2 \rangle$. If $[c_2, g_2] = 1$, then $c_2 \in Z(G)$ and $C_S(G) \neq \langle 1 \rangle$, a contradiction. So $[c_2, g_2] \neq 1$.
Therefore, $[c_2, g_2] = [c_1, g_2]^\alpha$ for some $\alpha \in \mathbb{Z}$, where $(\alpha, p) = 1$.
So, there exists $\beta \in \mathbb{Z}$ such that $[c_2, g_2]^\beta = [c_1, g_2]$.
But $[c_2, g_2]^\beta = [c_2^\beta, g_2]$ and if we substitute c_2^β for c_2 above we may assume that $[c_1, g_2] = [c_2, g_2]$. Let $c_1^{g_2} = c_1^t c_2^u$; then $c_2^{g_2} = c_1^{t-1} c_2^{u+1}$, where $t, u \in \mathbb{Z}$.
If $g_1 g_2$ induces a fixed point free automorphism upon S, then $S \subseteq \mathcal{K}(G)$.
So we may assume that $C_S(g_1 g_2) \neq \langle 1 \rangle$.
Now,

$$c_1^{g_2 g_1} = (c_1^t c_2^u)^{g_1} = (c_1^r c_2^w)^t c_2^u = c_1^{rt} c_2^{wt+u}$$

and

$$c_2^{g_2 g_1} = (c_1^{t-1} c_2^{u+1})^{g_1} = (c_1^r c_2^w)^{t-1} c_2^{u+1} = c_1^{r(t-1)} c_2^{w(t-1)+u+1}.$$

Since $C_S(g_1 g_2) \neq \langle 1 \rangle$, there exist $\lambda, \mu \in \mathbb{Z}$ such that $(c_1^\lambda c_2^\mu)^{g_2 g_1} = c_1^\lambda c_2^\mu$.

Thus, $rt\,\lambda + r(t-1)\mu \equiv \lambda(p)$

and $(wt+u)\lambda + (w(t-1) + u+1)\mu \equiv \mu(p)$

i.e.
$$\left.\begin{aligned} (rt-1)\lambda + r(t-1)\mu &\equiv 0(p) \\ (wt+u)\lambda+(w(t-1)+u)\mu &\equiv 0(p) \end{aligned}\right\} \qquad (3.3.1)$$

The simultaneous equations (3.3.1) have a non-trivial solution if and only if,

$$\begin{vmatrix} rt - 1 & r(t-1) \\ wt + u & w(t-1) + u \end{vmatrix} \equiv 0(p).$$

i.e. $(rt - 1)(w(t-1) + u) - (wt + u)(r(t-1)) \equiv 0(p)$.

This reduces to,

$$u(r-1) - w(t-1) \equiv 0(p) \qquad (3.3.2)$$

If $u \equiv 0(p)$, then $[c_1, g_2] = c_1^{t-1}$.

Because $S = \langle [c_1, g_1], [c_1, g_2] \rangle$, $t - 1 \not\equiv 0(p)$.

Consequently, by considering $[\lambda]$, $c_1 \in \mathcal{K}(G)$, a contradiction.

So we may assume that $u \not\equiv 0(p)$.

If $r \equiv 1(p)$, then g_1 induces a p-automorphism upon S. So $r \not\equiv 1(p)$.

So there exists $\zeta \in \mathbb{Z}$ such that $\zeta(r-1) \equiv (t-1)\ (p)$.

We consider $\zeta((r-1) + w)$.

By (3.3.2),

$$\zeta((r-1) + w) \equiv \zeta(w(t-1)/u + w)\ (p).$$

But $\zeta((r-1) + w) \equiv t - 1 + \zeta w(p)$, by construction.

Therefore, $t - 1 \equiv \zeta w(t-1)/u\ (p)$.

Thus, either $t \equiv 1(p)$ or $\zeta w/u \equiv 1(p)$.

If $t \equiv 1(p)$, then, by (3.3.2), $u(r-1) \equiv 0(p)$.

But neither $u \equiv 0(p)$ nor $(r-1) \equiv 0(p)$ so we have a contradiction.

Finally, if $\zeta w/u \equiv 1(p)$, then $\zeta w \equiv u(p)$.

But this implies $[c_1, g_1]^{\zeta} = [c_1, g_2]$, our final contradiction.

This completes the proof of Theorem 3.3.

We now consider possible generalisations of the preceding three theorems. We give a list of conjectures and possible lines of investigation together with

any relevant comments.

Conjecture 3.4. Let G be a finite group such that G' is an abelian p-group of rank three. Then $G \in \mathcal{C}$.

Conjecture 3.5. Let G be a finite group with an abelian Sylow subgroup S of rank three such that $S \subseteq G'$. Then $S \subseteq \mathcal{K}(G)$.

As can be seen from the proofs of Theorem 3.2 and Theorem 3.3, the fact that the relevant subgroups have exponent p is most extensively used and it is not at all clear whether the methods used in these proofs can be adapted to handle the case where the subgroups have exponent p^{α}, where α is a positive integer. It ought to be possible to, either extend Theorem 3.3 to the case where S is elementary abelian of rank three, or find a counter-example.

Another possible approach is to increase the rank of the relevant subgroup, whilst maintaining the exponent equals p condition. From the example following the proof of Theorem 3.1 we see that there exists a group G such that G' is elementary abelian of rank four and $G \notin \mathcal{C}$. However, the group exhibited is a p-group and if we make the restriction that the Sylow p-subgroup is abelian, then matters are not so clear. So a natural question to ask is:

Let G be a finite group with an abelian Sylow p-subgroup such that G' is an elementary abelian p-group of rank r. What is the largest value that r can take that guarantees that $G \in \mathcal{C}$?

We give the following example as a first approximation to this bound.

Example 3.6. Let $G = C_p \wr (C_q \times C_q \times C_q)$, where p and q are different primes. We show that $G \notin \mathcal{C}$.

Now G' is an elementary abelian p-group of rank (q^3-1). So, if $p \neq 2$ we can put $q = 2$ and $r < 7$. However, if $p = 2$, then putting $q = 3$ gives $r < 26$ and whilst the first bound appears reasonable, the second one does not.

So let G be generated by the q^3 elements $\{a_{ijk} | 1 \leq i, j, k \leq q\}$ and the three elements $\{b_i | 1 \leq i \leq 3\}$, where the $\{b_i\}$ act upon the $\{a_{ijk}\}$ by the b_t permuting the t th subscript of a_{ijk} cyclically in a canonical fashion. Let $g \in \mathcal{K}(G)$. Then,

$$g = \left[b_1^{r_1} b_2^{r_2} b_3^{r_3} \prod_{i,j,k} a_{ijk}^{\alpha_{ijk}}, b_1^{s_1} b_2^{s_2} b_3^{s_3} \prod_{l,m,n} a_{lmn}^{\beta_{lmn}} \right]$$

$$= \left(\prod_{l,m,n} \left[b_1^{r_1} b_2^{r_2} b_3^{r_3}, a_{lmn} \right]^{\beta_{lmn}} \right) \left(\prod_{i,j,k} \left[a_{ijk}, b_1^{s_1} b_2^{s_2} b_3^{s_3} \right]^{\alpha_{ijk}} \right)$$

$$= \left(\prod_{l,m,n} \left(a_{l'm'n'}^{-1} a_{lmn} \right)^{\beta_{lmn}} \right) \left(\prod_{i,j,k} \left(a_{ijk}^{-1} a_{i'j'k'} \right)^{\alpha_{ijk}} \right),$$

where $l' = l + r_1$, $m' = m + r_2$, $n' = n + r_3$,

$i' = i + s_1$, $j' = j + s_2$, $k' = k + s_3$ and all addition is done modulo q.

Consequently,

$$g = \left(\prod_{l,m,n} a_{lmn}^{\gamma_{lmn}} \right) \left(\prod_{i,j,k} a_{ijk}^{\delta_{ijk}} \right),$$

where $\gamma_{lmn} = \beta_{lmn} - \beta_{l'm'n'}$

and $\delta_{ijk} = \alpha_{i'j'k'} - \alpha_{ijk}$.

Finally we have,

$$g = \prod_{ijk} a_{ijk}^{\varepsilon_{ijk}}, \quad \text{where } \varepsilon_{ijk} = \gamma_{ijk} + \delta_{ijk}.$$

It is easily seen that

$$\sum_{u=0}^{p-1} \sum_{v=0}^{p-1} \varepsilon_{wxy} = 0, \tag{3.6.1}$$

where $w = i + r_1 u + s_1 v$, $x = j + r_2 u + s_2 v$ and $y = k + r_3 u + s_3 v$.

We now demonstrate that $g = [a_{ijk}, b_1][a_{ijk}, b_2][a_{ijk}, b_3] \notin \mathcal{K}(G)$.

Now $g = \prod_{l,m,n} a_{lmn}^{\varepsilon_{lmn}}$,

where $\varepsilon_{ijk} = -3$, $\varepsilon_{i+1jk} = \varepsilon_{ij+1k} = \varepsilon_{ijk+1} = 1$ and all other ε_{ijk} equal zero.

If $g \in \mathcal{K}(G)$, then by (3.6.1) there exist $\{u_i\}$ and $\{v_i\}$ where $1 \leq i \leq 3$, such that,

$$r_1u_1 + s_1v_1 = 0, \quad r_2u_1 + s_2v_1 = 0, \quad r_3u_1 + s_3v_1 = 1, \tag{3.6.2}$$

$$r_1u_2 + s_1v_2 = 0, \quad r_2u_2 + s_2v_2 = 1, \quad r_3u_2 + s_3v_2 = 0, \tag{3.6.3}$$

$$r_1u_3 + s_1v_3 = 1, \quad r_2u_3 + s_2v_3 = 0 \quad \text{and} \quad r_3u_3 + s_3v_3 = 0. \tag{3.6.4}$$

From (3.6.2) we may assume, without loss of generality, that $r_3 \neq 0 \neq u_i$.

If $v_1 \neq 0$ then, considering the first two equations of (3.6.2) gives

$$\begin{bmatrix} r_1 & s_1 \\ r_2 & s_2 \end{bmatrix} \begin{bmatrix} u_1 \\ v_1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

This has a non trivial solution if and only if

$$\begin{vmatrix} r_1 & s_1 \\ r_2 & s_2 \end{vmatrix} = 0.$$

This contradicts the first two equations of (3.6.4).

So we may assume that $v_1 = 0$.

By (3.6.2), $r_1 = r_2 = 0$.

The first two equations of (3.6.3) now imply that $s_1 = 0$. But $r_1 = s_1 = 0$ implies $r_1u_3 + s_1v_3 = 0$ contradicting (3.6.4). Consequently $g \notin \mathcal{K}(G)$.

Finally, on a slightly different tack, we consider another line of possible advancement.

In Theorem 3.3 we assumed that in a finite group G, a Sylow subgroup S was contained in G'. If we drop this restriction we can still ask questions of the form:

Let G be a finite group with Sylow subgroup S. What conditions must we impose on either G or S or $S \cap G'$ to ensure that $S \cap G' \subseteq \mathcal{K}(G)$?

As an example of possible results of this nature we prove the following theorem.

Theorem 3.7 Let G be a finite group with a cyclic Sylow p-subgroup S. Then, either $S \subseteq \mathcal{K}(G)$ or $S \cap G' = \langle 1 \rangle$.

Proof. Let $S = \langle s \rangle$. Then, by applying the Focal Subgroup Theorem [16 Theorem 7.3.4] we see that,

$$S \cap G' = \langle [s, n] \mid n \in N_G(S) \rangle .$$

For $n \in N_G(S)$, let $s^n = s^{r_n}$, where $r_n \in \mathbb{Z}$.

Then $s^{(r_n-1)} = [s, n]$ and moreover, $s^{(r_n-1)\lambda} = [s, n]^\lambda = [s^\lambda, n]$, where $\lambda \in \mathbb{Z}$.

If there exists an $n \in N_G(S)$ such that $(r_n-1, p) = 1$ we may conclude that $S \subseteq \mathcal{K}(G)$. Suppose $r_n - 1 = O(p)$ for every $n \in N_G(S)$. So. either $n \in C_G(S)$ or n induces automorphism whose order is divisible by p. The latter possibility is ruled out because S is a Sylow subgroup of G. Therefore $N_G(S) = C_G(S)$. By the well known theorem of Burnside [16Theorem 7.4.3], S has a normal complement H. Because G/H is abelian $G' \subseteq H$ and $S \cap G' = \langle 1 \rangle$.

We show that this result does not extend to S being a Hall subgroup.

Let $G = \langle a, b \mid a^{15} = b^2 = 1, \ a^b = a^4 \rangle$.

Then $\langle a \rangle$ is a Hall subgroup, but $G' = \langle a^3 \rangle$.

It would be very useful for such an investigation to have some results analogous to the Focal Subgroup Theorem and other related results (c.f. [16 Chapter 7]). Such results appear difficult to obtain because there is no obvious way of tackling such questions. The proof of the Focal Subgroup Theorem and most results related to it rely on the *TRANSFER HOMOMORPHISM.* This is of very little use in the questions we are considering. As a final comment we give the following conjecture.

Conjecture 3.8 Let G be a finite group with an abelian Sylow subgroup S. Then $S \cap \mathcal{K}(G) = S \cap \mathcal{K}(N_G(S))$.

Chapter 4. UNIPOTENT GROUPS

R.C. Thompson in [43], [44] and [45] considered the linear groups GL(n, F) and SL(n, F) over an arbitrary commutative field F. He shows that GL(n, F) and PSL(n, F) belong to the class $\mathcal{C}$.

We prove an analogous result for the unipotent group of matrices STL(n ,F).

Theorem 4.1 STL(n, F) $\in \mathcal{C}$, where n is an integer greater than one and F is an arbitrary commutative field.

Proof. Let $A \in \mathcal{K}(\mathrm{STL}(n, F))$. Then $A = [B, C]$, where $B, C \in \mathrm{STL}(n, F)$. Let $B = (b_{ij})$ and $C = (c_{ij})$. If $B^{-1} = (d_{ij})$ and $C^{-1} = (e_{ij})$, then because B and C are elements of STL(n, F),

$$\sum_{k=i}^{j} d_{ik}\, b_{kj} = \delta_{ij} = \sum_{k=i}^{j} c_{ik}\, e_{kj} \quad . \tag{4.1.1}$$

where δ_{ij} is the Kronecker delta symbol.

Suppose $B^{-1}C^{-1} = (f_{ij})$ and $BC = (g_{ij})$

Again because both $B^{-1}C^{-1}$ and BC are both elements of STL(n, F) we have,

$$f_{ij} = d_{ij} + e_{ij} + \sum_{k=i+1}^{j-1} d_{ik}\, e_{kj} \quad \text{if } i < j, \tag{4.1.2}$$

$$g_{ij} = b_{ij} + c_{ij} + \sum_{k=i+1}^{j-1} b_{ik}\, c_{kj} \quad \text{if } i < j, \tag{4.1.3}$$

$$f_{ii} = g_{ii} = 1 \text{ for } 1 \leq i \leq n \quad \text{and} \quad f_{ij} = g_{ij} = 0 \text{ if } i > j.$$

So if $A = (a_{ij})$, we have,

$$a_{ij} = \begin{cases} f_{ij} + g_{ij} + \sum_{k=i+1}^{j-1} f_{ik}\, g_{kj} & \text{if } i < j, \\ 1 & \text{if } i = j, \\ 0 & \text{if } i > j. \end{cases} \tag{4.1.4}$$

From (4.1.4),

$a_{ii+1} = f_{ii+1} + g_{ii+1} + o$

$= d_{ii+1} + e_{ii+1} + 0 + b_{ii+1} + c_{ii+1} + 0$, by (4.1.2) and (4.1.3).

But, from (4.1.1),

$$d_{ii+1} + b_{ii+1} = 0 = e_{ii+1} + c_{ii+1}.$$

Therefore,

$$a_{ii+1} = 0 \quad \text{for } 1 \leqslant i \leqslant n - 1.$$

Let $A' \in \mathfrak{N}(STL(n, F))$. Then it is easily seen, that if $AA' = (h_{ij})$, that $h_{ii+1} = 0$ for $1 \leqslant i \leqslant n - 1$.

Consequently, if $T = (t_{ij})$ $STL(n, F)'$, then $t_{ii+1} = 0$ for $1 \leqslant i \leqslant n - 1$.

We show that every element (u_{ij}) of STL(n, F) which has the property $u_{ii+1} = 0$ for $1 \leqslant i \leqslant n - 1$ is a commutator in STL(n, F). The proof proceeds by induction upon n.

The exact form of our induction hypothesis is:

given $A = (a_{ij})$, where $A \in STL(n, F)$ and $a_{ii+1} = 0$ for $1 \leqslant i \leqslant n-1$, there exist matrices B and C belonging to STL(n, F) such that $A = [B, C]$. Furthermore, if $B = (b_{ij})$ and $C = (c_{ij})$, we can select B and C such that $b_{ii+1} \neq 0 \neq c_{ii+1}$ for $1 \leqslant i \leqslant n-1$.

The latter part of the inductive hypothesis is there to enable the inductive argument to be completed.

The induction clearly starts because

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -\beta \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}, \text{ for every } \alpha, \beta \in F.$$

We assume that the hypothesis is true for unipotent groups of matrices of rank less than r, and that $n = r$. Let $A = (a_{ij})$ be an element of STL(r, F) such that $a_{ii+1} = 0$ for $1 \leqslant i \leqslant r-1$.

Then, $A = (a_{ij}) = \begin{pmatrix} 1 & 0 & a_{13} & \cdots & a_{1r} \\ 0 & & & & \\ \vdots & & & & \\ 0 & & \bar{A} & & \end{pmatrix}$

where $\bar{A} = (\bar{a}_{ij})$ is an element of STL(r-1, F) such that $\bar{a}_{ii+1} = 0$ for $1 \leq i \leq r-2$ and

$$\bar{a}_{ij} = a_{i+1j+1} \quad \text{for} \quad 1 \leq i, j \leq r-1. \tag{4.1.5}$$

By induction there exist $\bar{B} = (\bar{b}_{ij})$ and $\bar{C} = (\bar{c}_{ij})$, elements of STL(r-1, F) such that $\bar{A} = [\bar{B}, \bar{C}]$ and $\bar{b}_{ii+1} \neq 0 \neq \bar{c}_{ii+1}$ for $1 \leq i \leq r-2$.

Consequently the remainder of the proof is reduced to finding suitable b_{1j} and c_{1j} for $2 \leq j \leq r$ with $b_{12} \neq 0 \neq c_{12}$ such that

$$\begin{pmatrix} 1 & 0 & a_{13} & \cdots & a_{1r} \\ 0 & & & & \\ \vdots & & \bar{A} & & \\ 0 & & & & \end{pmatrix} = \begin{pmatrix} 1 & b_{12} & \cdots & b_{1r} \\ 0 & & & \\ \vdots & & \bar{B} & \\ 0 & & & \end{pmatrix}^{-1} \begin{pmatrix} 1 & c_{12} & \cdots & c_{1r} \\ 0 & & & \\ \vdots & & \bar{C} & \\ 0 & & & \end{pmatrix}^{-1} \begin{pmatrix} 1 & b_{12} & \cdots & b_{1r} \\ 0 & & & \\ \vdots & & \bar{B} & \\ 0 & & & \end{pmatrix}$$

$$\begin{pmatrix} 1 & c_{12} & \cdots & c_{1r} \\ 0 & & & \\ \vdots & & \bar{C} & \\ 0 & & & \end{pmatrix}$$

We let $B = (b_{ij}) = \begin{pmatrix} 1 & b_{12} & \cdots & b_{1r} \\ 0 & & & \\ \vdots & & \bar{B} & \\ 0 & & & \end{pmatrix}$ and $C = (c_{ij}) = \begin{pmatrix} 1 & c_{12} & \cdots & c_{1r} \\ 0 & & & \\ \vdots & & \bar{C} & \\ 0 & & & \end{pmatrix}$

So $b_{i+1\ j+1} = \bar{b}_{ij}$ and $c_{i+1\ j+1} = \bar{c}_{ij}$ for $1 \leq i \leq j \leq r-1$. (4.1.6)

Suppose $A' = (a'_{ij}) = [\bar{B}, \bar{C}]$.

Let $j \geq 3$. Then, by (4.1.4),

$$a'_{1j} = f_{1j} + g_{1j} + \sum_{k=2}^{j-1} f_{1k}\, g_{kj}.$$

where $B^{-1}C^{-1} = (f_{ij})$ and $BC = (g_{ij})$.

If $B^{-1} = (d_{ij})$ and $C^{-1} = (e_{ij})$, then, by (4.1.2) and (4.1.3),

$$a'_{1j} = d_{1j} + e_{1j} + \sum_{k=2}^{j-1} d_{1k}\, e_{kj} + b_{1j} + c_{1j} + \sum_{k=2}^{j-1} b_{1k}\, c_{kj} + \sum_{k=2}^{j-1} f_{1k}\, g_{kj}.$$

By (4.1.4),

$$b_{1j} + d_{1j} = -\sum_{k=2}^{j-1} b_{1k}\, d_{kj} \quad \text{and} \quad c_{1j} + e_{1j} = -\sum_{k=2}^{j-1} c_{1k}\, e_{kj}.$$

Therefore,

$$a'_{1j} = \sum_{k=2}^{j-1} (d_{1k}\, e_{kj} + b_{1k}\, c_{kj} - b_{1k}\, d_{kj} - c_{1k}\, e_{kj} + f_{1k}\, g_{kj}). \qquad (4.1.7)$$

We need to show that a'_{1j} can be constructed equal to a_{1j}, for $3 \leq j \leq r$, in such a way that $b_{12} \neq 0 \neq c_{12}$.

We show this by induction upon j.

By (4.1.7),

$$a'_{13} = d_{12}\, e_{23} + b_{12}\, c_{23} - b_{12}\, d_{23} - c_{12}\, e_{23} + f_{12}\, g_{23}$$

$$= d_{12}\, e_{23} + b_{12}\, c_{23} - b_{12}\, d_{23} - c_{12}\, e_{23} + (d_{12} + e_{12})(b_{23} + c_{23}),$$

by (4.1.2) and (4.1.3).

By (4.1.1), $d_{12} = -b_{12}$, $d_{23} = -b_{23}$, $e_{12} = -c_{12}$ and $e_{23} = -c_{23}$.

Consequently,

$$a'_{13} = b_{12}\, c_{23} + b_{12}\, c_{23} + b_{12}\, b_{23} + c_{12}\, c_{23} - (b_{12} + c_{12})(b_{23} + c_{23})$$

$$= b_{12}\, c_{23} - c_{12}\, b_{23}.$$

Now $c_{23} = \bar{c}_{12} \neq 0$ and $b_{23} = \bar{b}_{12} \neq 0$.

Therefore there exist $b_{12}, c_{12} \in F$ such that $b_{12} \neq 0 \neq c_{12}$ and $a_{13} = b_{12} c_{23} - c_{12} b_{23}$. So the induction starts. By considering (4.1.7) we see that a'_{1j} is independent of b_{1k} and c_{1k} (and consequently d_{1k} and e_{1k}) for $k \geqslant j$. We assume that b_{1k} and c_{1k} have been chosen for $2 \leqslant k \leqslant j - 2$ such that $a'_{1k} = a_{1k}$ for $3 \leqslant k \leqslant j - 1$. We show that there exist b_{1j-1} and c_{1j-1} such that $a'_{ij} = a_{1j}$ and in doing so we complete the proof of the theorem.

By (4.1.7),

$$a'_{1j} = d_{1j-1} e_{j-1j} + b_{1j-1} c_{j-1j} - b_{1j-1} d_{j-1j} - c_{1j-1} e_{j1j} + f_{1j-1} g_{j-1j} + X_1, \qquad (4.1.8)$$

where X_1 is a constant expression only involving terms whose values have already been fixed.

By (4.1.2) and (4.1.3),

$$f_{1j-1} g_{j-1j} = (d_{1j-1} + e_{1j-1})(b_{j-1j} + c_{j-1j}) + X_2, \qquad (4.1.9)$$

where X_2 is similarly a constant term.

By (4.1.1),

$$d_{j-1j} = -b_{j-1j}, \quad e_{j-1j} = -c_{j-1j}, \qquad (4.1.10)$$

$$d_{1j-1} = -b_{1j-1} + X_3 \quad \text{and} \quad e_{1j-1} = -c_{1j-1} + X4, \qquad (4.1.11)$$

where X_3 and X_4 are also constant terms.

Substituting (4.1.9), (4.1.10) and (4.1.11) into (4.1.8) we have,

$$a'_{ij} = b_{ij-1} c_{j-1j} + b_{1j-1} c_{j-1j} + b_{1j-1} b_{j-1j} + c_{1j-1} c_{j-1j} - (b_{1j-1} + c_{1j-1})(b_{j-1j} + c_{j-1j}) + X_5, \text{ where } X_5 \text{ is a constant.}$$

$$= b_{1j-1} c_{j-1j} - c_{1j-1} b_{j-1j} + X_5.$$

Because $c_{j-1j} = \bar{c}_{j-2j-1} \neq 0$ and $b_{j-1j} = \bar{b}_{j-2j-1} \neq 0$, there exist b_{ij-1} and c_{1j-1} such that $a'_{1j} = a_{1j}$.

Chapter 5 CHARACTER THEORY

In previous chapters have have considered particular classes of groups and in doing so we have found various sufficient conditions for an element of a group under consideration to be a commutator. We now turn our attention to the problem of finding necessary and sufficient conditions for a group element to be a commutator. The character theory of finite groups plays a major role in this discussion and, consequently, all groups considered in this chapter will be finite.

Throughout this chapter we adopt the following notation.

G is a finite group.

$\mathbb{C}(G)$ is the group algebra of G over the complex number $\mathbb{C}$. $C_1, C_2, \ldots, C_h$ are the conjugancy classes of G and $C_1 = \langle 1 \rangle$. $\hat{C}_i = \sum_{g \in C_1} g$ is the class sum of C_i in $\mathbb{C}(G)$. $\chi^1, \chi^2, \ldots \chi^h$ are the irreducible characters of G over $\mathbb{C}$, denoted by Irr(G). $\chi^i{}_j$ is the value χ^i takes on C_j for $1 \leq i, j \leq h$.

The original result of this nature was given by Burnside in [3 , p 319] when he states that a necessary and sufficient condition for an element of C_j to be a commutator is that,

$$\sum_{i=1}^{h} \chi^i{}_j / \chi^i{}_1 \neq 0.$$

This work was generalised by P. X. Gallagher in [14]. Gallagher considers compact groups and obtains results by the use of the Haar Integral. For comparison with our result we will consider only the realisation of his results in terms of finite groups. Gallagher shows that a necessary and sufficient condition for an element of C_j to be a product of n commutators is that,

$$\sum_{i=1}^{h} \chi^i{}_j / (\chi^i{}_1)^{2n-1} \neq 0.$$

K. Honda, in [2], obtained Burnside's result independently and, as a consequence, showed that $g \in \mathcal{K}(g)$ if and only if $g^r \in \mathcal{K}(G)$, where $r \in \mathbb{Z}$ and $\langle g \rangle = \langle g^r \rangle$.

We obtain the following generalisation of Burnside's result.

Theorem 5.1. Let $C_{\lambda(j)}$ for $1 \leq j \leq n$ be a collection of conjugacy classes of G, repetition of classes being allowed. Then, there exist $x_j \in C_{\lambda(j)}$ for $1 \leq i \leq n$ such that $\prod_{j=1}^{n} x_j \in \mathcal{K}(G)$ if and only if

$$\sum_{i=1}^{h} \prod_{j=1}^{n} \chi^i{}_{\lambda(j)} / (\chi^i{}_1)^n \neq 0.$$

Proof From [9.p28] we know that $\{\hat{C}_i \mid 1 \leq i \leq h\}$ is a basis of $Z(\mathbb{C}(G))$. Consequently,

$$\hat{C}_{\lambda(1)} \hat{C}_{\lambda(2)} \cdots \hat{C}_{\lambda(n)} \hat{C}_j = \hat{C}_{\lambda(1)} \cdots \hat{C}_{\lambda(n-1)} \sum_{k(n)=1}^{h} \alpha_{jk(n)} \hat{C}_{k(n)}$$

$$= \hat{C}_{\lambda(1)} \cdots \hat{C}_{\lambda(n-2)} \sum_{k(n)=1}^{h} \sum_{k(n-1)=1}^{h} \alpha^{(n)}_{jk(n)} \alpha^{(n-1)}_{k(n)k(n-1)} \hat{C}_{k(n-1)}$$

$$= \sum_{k(n)=1}^{h} \cdots \sum_{k(1)=1}^{h} \alpha^{(n)}_{jk(n)} \alpha^{(n-1)}_{k(n)k(n-1)} \cdots \alpha^{(1)}_{k(2)k(1)} \hat{C}_{k(1)}, \tag{5.1.1}$$

where $\alpha^{(i)}_{jk(i)} \in \mathbb{C}$, for $1 \leq i \leq n$ and $1 \leq j \leq h$.

We define ω_i on $Z(\mathbb{C}(G))$ for $1 \leq i \leq h$ by,

$$\omega_i(\hat{C}_j) = |C_j| \chi^i{}_j / \chi^i{}_1 \quad \text{and extending}$$

linearly over $Z(\mathbb{C}(G))$. By [9. p28] we have that ω_i is a homomorphism of $Z(\mathbb{C}(G))$ into $\mathbb{C}$.

Consequently,

$$\omega_i(\hat{C}_{\lambda(1)} \hat{C}_{\lambda(2)} \cdots \hat{C}_{\lambda(n)} C_j) = \omega_i(\hat{C}_{\lambda(1)}) \omega_i(\hat{C}_{\lambda(2)}) \cdots \omega_i(\hat{C}_{\lambda(n)}) \omega_i(\hat{C}_j)$$

But, by (5.1.1)

$$\omega_i(\hat{C}_{\lambda(1)} \hat{C}_{\lambda(2)} \cdots \hat{C}_{\lambda(n)} \hat{C}_j) = \sum_{k(n)=1}^{h} \cdots \sum_{k(1)=1}^{h} \alpha^{(n)}_{jk(n)} \alpha^{(n-1)}_{k(n)k(n-1)} \cdots$$

$$\alpha^{(1)}_{k(2)k(1)} \omega_i(\hat{C}_{k(1)}) .$$

Therefore,

$$\omega_i(\hat{C}_{\lambda(1)})\ \omega_i(\hat{C}_{\lambda(2)})\ \cdots\ \omega_i(\hat{C}_{\lambda(n)})\,\omega_i(\hat{C}_j)$$

$$= \sum_{k(n)=1}^{h} \cdots \sum_{k(1)=1}^{h} \alpha^{(n)}_{jk(n)}\ \alpha^{(n-1)}_{k(n)k(n-1)}\ \cdots\ \alpha^{(1)}_{k(2)k(1)}\ \omega_i(\hat{C}_{k(1)})$$

Applying the definition of ω_i we obtain,

$$\Big(\prod_{r=1}^{n} |C_{\lambda(r)}|\chi^i_{\lambda(r)}\Big)\big(|C_j|\chi^i{}_j\big) \,/\, (\chi^i{}_1)^{n+1}$$

$$= \sum_{k(n)=1}^{h} \cdots \sum_{k(1)=1}^{h} \alpha^{(n)}_{jk(n)}\ \alpha^{(n-1)}_{k(n)k(n-1)} \cdots\ \alpha^{(1)}_{k(2)k(1)}\ |C_{k(1)}|(\chi^i{}_{k(1)} \,/\, \chi^i{}_1). \tag{5.1.2}$$

We multiply both sides of (5.1.2) by $\bar{\chi}^i{}_j$ and then sum over j, obtaining,

$$\Big(\prod_{r=1}^{n} |C_{\lambda(r)}|\chi^i{}_{\lambda(r)}\Big)\Big(\sum_{j=1}^{h} |C_j|\chi^i{}_j\ \bar{\chi}^i{}_j\Big) \,/\, (\chi^i{}_1)^n$$

$$= \sum_{j=1}^{h} \sum_{k(n)=1}^{h} \cdots \sum_{k(1)=1}^{h} \alpha^{(n)}_{jk(n)}\ \alpha^{(n-1)}_{k(n)k(n-1)} \cdots \alpha^{(1)}_{k(2)k(1)} |C_{k(1)}|\chi^i{}_{k(1)}\ \bar{\chi}^i{}_j.$$

From [9.p14] we see that $\sum_{j=1}^{h} |C_j|\chi^i{}_j\ \bar{\chi}^i{}_j = |G|$ (5.1.3)

Therefore, if we sum (5.1.3) over i, we obtain,

$$|G| \sum_{i=1}^{h} \Big(\prod_{r=1}^{n} |C_{\lambda(r)}|\ \chi^i{}_{\lambda(r)}\Big) \,/\, (\chi^i{}_1)^n$$

$$= \sum_{j=1}^{h} \sum_{k(n)=1}^{h} \cdots \sum_{k(1)=1}^{h} \alpha^{(n)}_{jk(n)}\ \alpha^{(n-1)}_{k(n)k(n-1)} \cdots\ \alpha^{(1)}_{k(2)k(1)}\ |C_{k(1)}|\Big(\sum_{i=1}^{h} \chi^i{}_{k(1)}\bar{\chi}^i{}_j\Big). \tag{5.1.4}$$

Now, by [9.p16], $\sum_{i=1}^{h} \chi^i{}_{k(1)}\ \bar{\chi}^i{}_j = \dfrac{|G|}{|C_{k(1)}|}\ \delta_{k(1)j}$, where $\delta_{k(1)j}$ is the Kronecker delta symbol.

Consequently, we can reduce (5.1.4) to,

$$\sum_{i=1}^{h} \Big(\prod_{r=1}^{n} |C_{\lambda(r)}|\chi^i{}_{\lambda(r)}\Big) \,/\, (\chi^i{}_1)^n = \sum_{k(n)=1}^{h} \cdots \sum_{k(1)=1}^{h} \alpha^{(n)}_{k(1)k(n)}\ \alpha^{(n-1)}_{k(n)k(n-1)}$$

$$\alpha^{(1)}_{k(2)k(1)}. \tag{5.1.5}$$

Now $\alpha^{(j)}_{ik(j)} \neq 0$ if and only if there exist $x_i \in C_i$ and $x_j \in C_{\lambda(j)}$ such that $x_j x_i \in C_{k(j)}$, where $1 \leq i \leq h$, $1 \leq j \leq n$ and $1 \leq k_{(j)} \leq h$.

So $\alpha^{(n)}_{k(1)k(n)}\ \alpha^{(n-1)}_{k(n)k(n-1)} \cdots \alpha^{(1)}_{k(2)k(1)} \neq 0$ if and only if there exist $y_1 \in C_{k(1)}$, $x_n \in C_{\lambda(n)}$ such that $x_n y_1 \in C_{k(n)}$ and $y_j \in C_{k(j)}$ and $x_{j-1} \in C_{\lambda(j-1)}$ such that $x_{j-1} y_j \in C_{k(j-1)}$ for $2 \leq j \leq n$.

We may select $y_n = x_n y_1$ by taking suitable conjugate values of y_n and x_{n-1}. Similarly we may select $y_j = x_j x_{j+1} \cdots x_n y_1$ by taking suitable conjugate values of y_j and x_{j-1} for $2 \leq j \leq n$.

Therefore,

$\alpha^{(n)}_{k(1)k(n)}\ \alpha^{(n-1)}_{k(n)k(n-1)} \cdots \alpha^{(1)}_{k(2)k(1)} \neq 0$ if and only if $x_1 x_2 \cdots x_n y_1 \in C_{k(1)}$. But $y_1 \in C_{k(1)}$, so $\alpha^{(n)}_{k(1)k(n)}\ \alpha^{(n-1)}_{k(n)k(n-1)} \cdots \alpha^{(1)}_{k(2)k(1)} \neq 0$ if and only if $x_1 x_2 \cdots x_n = [y_1, \bar{g}]$ for some $g \in G$. Consequently by considering (5.1.5) we have that $x_1 x_2 \cdots x_n \in \mathcal{K}(G)$ if and only if $0 \neq \sum_{i=1}^{h} (\chi^i(x_1) \cdots \chi^i(x_n) / (\chi^i_1)^n$. This completes the proof of the Theorem.

We obtain the following corollary which corresponds to the corollary Honda obtained from Burnside's result.

Corollary 5.2. Let G be a finite group and $x_i \in G$ for $1 \leq i \leq n$. Suppose that $x_1 x_2 \cdots x_n \in \mathcal{K}(G)$ and that there exists an x_j such that $(|x_k|, |x_j|) = 1$ if $k \neq j$. Then for every $r \in \mathbb{Z}$ such that $(r, |x_j|) = 1$ there exist $g_i \in G$ for $1 \leq i \leq n$ such that

$$x_1^{g_1} x_2^{g_2} \cdots (x_j^r)^{g_j} \cdots x_n^{g_n} \in \mathcal{K}(G).$$

Proof. By Theorem 5.1 $x_1 \cdots x_n \in \mathcal{K}(G)$ implies that

$$\sum_{i=1}^{h} \chi^i(x_1)\, \chi^i(x_2) \cdots \chi^i(x_n) / (\chi^i_1)^n \neq 0.$$

Let $|G| = m$ ... and consider the Galois group, $G(\mathbb{Q}(\sqrt[m]{1}), \mathbb{Q})$. Let $r \in \mathbb{Z}$ such that $(|x_j|, r) = 1$. Let ω_k be a primitive $|x_k|$th roof of unity, for $1 \leq k \leq n$. Then because $(|x_j|, |x_k|) = 1$ if $k \neq j$, there exists $\sigma \in G(\mathbb{Q}(\sqrt[m]{1}), \mathbb{Q})$ such that $\sigma(\omega_j) = \omega_j^r$ and $\sigma(\omega_k) = \omega_k$ if $k \neq j$.

If we define $(\chi^i)^\sigma$ by $(\chi^i)^\sigma(g) = (\chi^i(g))^\sigma$ for every $g \in G$ then it is easily seen that $(\chi^i)^\sigma$ is an irreducible character of G and σ induces a permutation upon the $\{\chi^i \mid 1 \leq i \leq h\}$.

Consequently,

$$\sum_{i=1}^{h} ((\chi^i)^\sigma(x_i) \ldots (\chi^i)^\sigma(x_n)) / ((\chi^i_1)^\sigma)^n \neq 0.$$

But, by our choice of σ, $(\chi^i)^\sigma(x_j) = \chi^i(x_j^r)$, $(\chi^i)^\sigma(x_k) = \chi^i(x_k)$ if $j \neq k$ and $(\chi^i_1)^\sigma = \chi^i_1$.

Therefore,

$$\sum_{i=1}^{h} \chi^i(x_1) \ldots \chi^i(x_{j-1}) \chi^i(x_j^r) \chi^i(x_{j+1}) \ldots \chi^i(x_n) / (\chi^i_1)^n \neq 0.$$

By Theorem 5.1 there exist g_i for $1 \leq i \leq n$ such that

$x_1^{g_1} \ldots (x_j^r)^{g_j} \ldots x_n^{g_n} \in \mathcal{K}(G)$.

As a rather elementary example we examine how this work applies to finite nilpotent of class 2 groups. We first of all prove the following result.

Lemma 5.2. Let G be a finite nilpotent of class 2 p-group such that $G \notin \mathcal{C}$. Then the number of conjugacy classes G possesses is a multiple of p.

Proof. Let $g \in G' \setminus \mathcal{K}(G)$.

We consider $H = G/\langle g \rangle$. This is well defined because $g \in Z(G)$. Suppose H has k conjugacy classes and let $\{h_i \mid 1 \leq i \leq k\}$ be representatives from each class. We consider $\{h_i g^j \mid 1 \leq i \leq k, 1 \leq j \leq |g|\}$. It is easily seen that every conjugacy class of G is represented in this set.

Suppose $h_i g^j \sim_G h_{i'} g^{j'}$. Then $h_i \sim_H h_{i'}$ and consequently, $i = i'$.

Now $g \in Z(G)$, so $h_i g^j \sim_G h_i g^{j'}$ implies that

$$h_i \sim_G h_i g^{(j-j')} \sim_G h_i g^{2(j-j')} \sim_G \cdots \sim_G h_i g^{\alpha(j-j')},$$

where $\alpha \in \mathbb{Z}$.

Now $h_i \sim_G h_i g^{(j-j')}$ implies that $g^{(j-j')} \in \mathcal{K}(G)$. So by Corollary 5.2 (or, originally from [22]), $j-j' = 0(p)$. Therefore, $\{h_i g^l \mid 1 \leq l \leq |g|\}$ give representatives of $j-j'$ conjugacy classes and the proof is complete.

e.g. Suppose G is a finite nilpotent of class 2 group such that $G \notin \mathcal{C}$.

Let $g \in G' \setminus \mathcal{K}(G)$ and suppose $|g| = p$, for some prime p.

Let $H = G/\langle g \rangle$ and suppose H possesses k conjugacy classes. By referring to the proof of Lemma 5.2 it is easily seen that G possesses pk conjugacy classes.

Let $\{\chi^i \mid 1 \leq i \leq pk\} = \mathrm{Irr}(G)$. Now $g \in Z(G)$ implies that $\chi^i(g) = \omega^{\alpha(i)} \chi^i_1$, where ω is a primitive p th root of unity and $\alpha(i) \in \mathbb{Z}$.

By Theorem 5.1, $\sum_{i=1}^{pk} \chi^i(g) / \chi^i_1 = 0$.

$$\text{i. e. } \sum_{i=1}^{pk} \omega^{\alpha(i)} = 0.$$

Because ω is a primitive p th root of unity, we may number the $\{\chi^i\}$ such that

$$\omega^{\alpha(i)} = \omega^r, \text{ where } rk+1 \leq i \leq (r+1)k.$$

Thus, in the nilpotent of class 2 case we obtain detailed information concerning the values taken by a non-commutator inside the commutator subgroup.

Chapter 6. Simple Groups

In [34], O. Ore conjectured that every element of a non-abelian finite simple group is a commutator. As he commented, the techniques required to prove such a result do not appear to be readily available. One likely avenue of progress seems to lie with the character relationships discussed in Chapter 5. Although we cannot prove the necessary result for an arbitrary non-abelian finite simple group, we show, by examining character tables, that several such groups do indeed consist of commutators.

We consider the various character tables in turn and we make the necessary calculations. Since the calculations are routine we content ourselves with only presenting the character tables of three of the so called "sporadic" simple groups. We give references to other character tables and we claim that in all of them the conjecture can be verified after a short calculation.

We recall that if G is a finite group, $g \in G$ and $\chi^1, \chi^2, \ldots, \chi^h$ are the irreducible characters of G, then $g \in \mathcal{K}(G)$ if and only if $\sum_{i=1}^{h} \chi^i(g)/\chi^i(1) \neq 0$. Let χ^1 be the principal character of G, then $g \in \mathcal{K}(G)$ if and only if $1 + \sum_{i=2}^{h} \chi^i(g)/\chi^i(1) \neq 0$.

When we investigate the character table of the group under consideration it will usually be observed that on a non-principal character χ a non-identity element g of G takes a value insignificant in absolute value when compared with $\chi(1)$. Thus $\sum_{i=2}^{h} \chi^i(g)/\chi^i(1)$ will be far less than 1 in absolute value and consequently, $1 + \sum_{i=2}^{h} \chi^i(g)/\chi^i(1)$ will not equal zero, as required. Therefore, whenever the desired conclusion is apparent by inspection, we will omit any calculations.

Our presentation of character tables is standard and follows [9, §7]. When necessary we will make the pertinent calculations at the end of the character tables.

I. Janko's group of order 175,560

We present the character table obtained by J. McKay in [30, pp.89-100] of the group discovered by Z. Janko in [28].

Class	1	2	3	4	5	6	7
Character							
χ^1	1	1	1	1	1	1	1
χ^2	56	0	2	2+4c2	2+4c1	-1	-1
χ^3	56	0	2	2+4c1	2+4c2	-1	-1
χ^4	76	4	1	1	1	0	0
χ^5	76	-4	1	1	1	0	0
χ^6	77	5	-1	2	2	1	1
χ^7	77	-3	2	2c1	2c2	1	1
χ^8	77	-3	2	2c2	2c1	1	1
χ^9	120	0	0	0	0	2c2+2c3+2c5	2c4+2c6+2c9
χ^{10}	120	0	0	0	0	2c1+2c7+2c8	2c2+2c3+2c5
χ^{11}	120	0	0	0	0	2c4+2c6+2c9	2c1+2c7+2c8
χ^{12}	133	5	1	-2	-2	0	0
χ^{13}	133	-3	-2	1+2c2	1+2c1	0	0
χ^{14}	133	-3	-2	1+2c1	1+2c2	0	0
χ^{15}	209	1	-1	-1	-1	0	0

Class	8	9	10	11	12	13	14	15
Character								
χ^1	1	1	1	1	1	1	1	1
χ^2	-1	2c3	2c6	1	0	0	0	0
χ^3	-1	2c6	2c3	1	0	0	0	0
χ^4	0	1	1	-1	-1	-1	-1	1
χ^5	0	1	1	-1	1	1	-1	-1
χ^6	1	-1	-1	0	0	0	0	-1
χ^7	1	2c3	2c6	0	2c2	2c4	0	0
χ^8	1	2c6	2c3	0	2c4	2c2	0	0
χ^9	2c1+2c7+2c8	0	0	-1	0	0	1	0
χ^{10}	2c4+2c6+2c9	0	0	-1	0	0	1	0
χ^{11}	2c2+2c3+2c5	0	0	-1	0	0	1	0
χ^{12}	0	1	1	1	0	0	0	-1
χ^{13}	0	1+2c6	1+2c3	1	2c2	2c4	0	0
χ^{14}	0	1+2c3	1+2c6	1	2c4	2c2	0	0
χ^{15}	0	-1	-1	0	1	1	-1	1

In the above table $\alpha c\beta$ denotes $\alpha \cos(2\pi\beta/5)$, where $\alpha, \beta \in \mathbb{Z}$.

Let G denote the group under consideration. It is easily seen that

$\sum_{i=1}^{15} \chi^i(g)/\chi^i(1) \neq 0$ for every $g \in G$ and, consequently G consists of commutators.

However, as an example, we do the necessary calculations for the second conjugacy class. If g is an element of the second conjugacy class, then,

$$\sum_{i=1}^{15} \chi^i(g)/\chi^i(1) = 1 + \frac{0}{56} + \frac{0}{56} + \frac{4}{76} - \frac{4}{76} + \frac{5}{77} - \frac{3}{77} - \frac{3}{77}$$
$$+ \frac{0}{120} + \frac{0}{120} + \frac{0}{120} + \frac{5}{133} - \frac{3}{133} - \frac{3}{133} + \frac{1}{209}$$
$$= 1 - 23/1463 \neq 0.$$

Therefore, $g \in \mathcal{K}(G)$.

II. The Mathieu Group, M_{24}.

We exhibit the character table obtained by J. Todd in [46] of the quintuply transitive Mathieu group M_{24}, of degree 24 and order 244,823,040.

Class	1	2	3	4	5	6	7	8	9	10	11	12	13
Character													
χ^1	1	1	1	1	1	1	1	1	1	1	1	1	1
χ^2	23	7	5	3	3	2	2	1	1	1	0	0	0
χ^3	45	-3	0	0	1	α	$\bar{\alpha}$	-1	0	1	0	0	$-\alpha$
χ^4	45	-3	0	0	1	$\bar{\alpha}$	α	-1	0	1	0	0	$-\bar{\alpha}$
χ^5	231	7	-3	1	-1	0	0	-1	1	0	β	$\bar{\beta}$	0
χ^6	231	7	-3	1	-1	0	0	-1	1	0	$\bar{\beta}$	β	0
χ^7	252	28	9	2	4	0	0	0	1	-1	-1	-1	0
χ^8	253	13	10	3	1	1	1	-1	-2	0	0	0	-1
χ^9	483	35	6	-2	3	0	0	-1	2	-1	1	1	0
χ^{10}	770	-14	5	0	-2	0	0	0	1	0	0	0	0
χ^{11}	770	-14	5	0	-2	0	0	0	1	0	0	0	0
χ^{12}	990	-18	0	0	2	α	$\bar{\alpha}$	0	0	0	0	0	α
χ^{13}	990	-18	0	0	2	$\bar{\alpha}$	α	0	0	0	0	0	$\bar{\alpha}$
χ^{14}	1035	-21	0	0	3	2α	$2\bar{\alpha}$	-1	0	1	0	0	0
χ^{15}	1035	-21	0	0	3	$2\bar{\alpha}$	2α	-1	0	1	0	0	0
χ^{16}	1035	27	0	0	-1	-1	-1	1	0	1	0	0	-1
χ^{17}	1265	49	5	0	1	-2	-2	1	1	0	0	0	0
χ^{18}	1771	-21	16	1	-5	0	0	-1	0	0	1	1	0
χ^{19}	2024	8	-1	-1	0	1	1	0	-1	0	-1	-1	1
χ^{20}	2277	21	0	-3	1	2	2	-1	0	0	0	0	0
χ^{21}	3312	48	0	-3	0	1	1	0	0	1	0	0	-1
χ^{22}	3520	64	10	0	0	-1	-1	0	-2	0	0	0	1
χ^{23}	5313	49	-15	3	-3	0	0	-1	1	0	0	0	0
χ^{24}	5544	-56	9	-1	0	0	0	0	1	0	-1	-1	0
χ^{25}	5796	-28	-9	1	4	0	0	0	-1	-1	1	1	0
χ^{26}	10395	-21	0	0	-1	0	0	1	0	0	0	0	0

Class	14	15	16	17	18	19	20	21	22	23	24	25	26
Character													
χ^1	1	1	1	1	1	1	1	1	1	1	1	1	1
χ^2	0	0	0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
χ^3	$-\overline{\alpha}$	-1	-1	1	-1	1	3	5	0	$\overline{\alpha}$	α	-3	0
χ^4	$-\alpha$	-1	-1	1	-1	1	3	5	0	α	$\overline{\alpha}$	-3	0
χ^5	0	1	1	0	0	3	0	-9	1	0	0	-1	-1
χ^6	0	1	1	0	0	3	0	-9	1	0	0	-1	-1
χ^7	0	-1	-1	0	0	0	0	12	2	0	0	4	1
χ^8	-1	0	0	1	1	1	1	-11	-1	1	1	-3	0
χ^9	0	0	0	0	0	3	0	3	-2	0	0	3	0
χ^{10}	0	γ	$\overline{\gamma}$	1	1	-2	-7	10	0	0	0	2	-1
χ^{11}	0	$\overline{\gamma}$	γ	1	1	-2	-7	10	0	0	0	2	-1
χ^{12}	$\overline{\alpha}$	1	1	1	-1	-2	3	-10	0	$\overline{\alpha}$	α	6	0
χ^{13}	α	1	1	1	-1	-2	3	-10	0	α	$\overline{\alpha}$	6	0
χ^{14}	0	0	0	-1	1	-1	-3	-5	0	$-\overline{\alpha}$	$-\alpha$	3	0
χ^{15}	0	0	0	-1	1	-1	-3	-5	0	$-\alpha$	$-\overline{\alpha}$	3	0
χ^{16}	-1	0	0	0	2	3	6	35	0	-1	-1	3	0
χ^{17}	0	0	0	0	0	-3	8	-15	0	1	1	-7	-1
χ^{18}	0	0	0	-1	-1	-1	7	11	1	0	0	3	0
χ^{19}	1	0	0	0	0	0	8	24	-1	1	1	8	-1
χ^{20}	0	0	0	0	2	-3	6	-19	1	-1	-1	-3	0
χ^{21}	-1	0	0	0	-2	0	-6	16	1	1	1	0	0
χ^{22}	1	1	1	0	0	0	-8	0	0	-1	-1	0	0
χ^{23}	0	0	0	0	0	-3	0	9	-1	0	0	1	1
χ^{24}	0	1	1	0	0	0	0	24	-1	0	0	-8	1
χ^{25}	0	0	0	0	0	0	0	36	1	0	0	-4	-1
χ^{26}	0	-1	-1	0	0	3	0	-45	0	0	0	3	0

In the above table, $\alpha = \frac{1}{2}(-1 + i\sqrt{7})$, $\beta = \frac{1}{2}(-1 + i\sqrt{15})$ and $\gamma = \frac{1}{2}(-1 + i\sqrt{23})$.

$\sum_{i=1}^{26} \chi^i(g)/\chi^i(1) = 1 + {}^{5377}/_{11385}$ if g is an element of the second conjugacy class.

$\sum_{i=1}^{26} \chi^i(g)/\chi^i(1) = 1 + {}^{38}/_{1449}$ if g is an element of the twentyfirst conjugacy class.

The required inequality obviously holds for all other conjugacy classes and, consequently, the Mathieu group M_{24} consists of commutators.

III. The Higman-Sims group of order $1100.8! = 44,352,000$.

We present the character table obtained by J. S. Frame in [13] of the simple group discovered by D. G. Higman and C. C. Sims in [19].

Class	1	2	3	4	5	6	7	8	9	10	11	12
Character												
χ^1	1	1	1	1	1	1	1	1	1	1	1	1
χ^2	22	0	0	1	2	4	0	6	2	2	0	0
χ^3	77	0	0	0	2	5	1	13	5	1	1	-1
χ^4	175	-1	-1	0	0	4	0	15	-1	3	-1	1
χ^5	231	0	0	0	1	6	-2	7	-1	-1	-1	-1
χ^6	1056	0	0	-1	1	-6	2	32	0	0	0	0
χ^7	825	0	0	-1	0	6	-2	25	1	1	1	1
χ^8	770	0	0	0	0	5	1	34	2	-2	-2	0
χ^9	1925	0	0	0	0	-1	-1	5	5	-3	1	1
χ^{10}	1925	0	0	0	0	-1	-1	5	-3	1	1	-1
χ^{11}	3200	-1	-1	1	0	-4	0	0	0	0	0	0
χ^{12}	1408	0	0	1	-2	4	0	0	0	0	0	0
χ^{13}	2750	0	0	-1	0	5	1	-50	2	2	0	0
χ^{14}	1750	1	1	0	0	-5	-1	-10	6	2	-2	0
χ^{15}	693	0	0	0	-2	0	0	21	5	1	1	-1
χ^{16}	154	0	0	0	-1	1	1	10	6	-2	0	0
χ^{17}	1386	0	0	0	1	0	0	-6	-2	-2	0	0
χ^{18}	2520	1	1	0	0	0	0	24	-8	0	0	0
χ^{19}	154	0	0	0	-1	1	1	10	-2	2	0	2
χ^{20}	154	0	0	0	-1	1	1	10	-2	2	0	-2
χ^{21}	770	0	0	0	0	5	1	-14	-2	-2	0	0
χ^{22}	770	0	0	0	0	5	1	-14	-2	-2	0	0
χ^{23}	896	α	$\bar{\alpha}$	0	1	-4	0	0	0	0	0	0
χ^{24}	896	$\bar{\alpha}$	α	0	1	-4	0	0	0	0	0	0

Class	13	14	15	16	17	18	19	20	21	22	23	24
Character												
χ^1	1	1	1	1	1	1	1	1	1	1	1	1
χ^2	0	-1	2	-2	-2	-2	0	-6	-1	-1	1	-3
χ^3	-1	0	-3	1	1	1	-1	5	0	0	-2	2
χ^4	1	-1	5	1	11	2	0	15	0	0	0	0
χ^5	-1	1	1	1	-9	0	0	15	0	0	2	6
χ^6	0	-1	-4	0	0	0	0	0	0	0	2	6
χ^7	1	1	-5	-1	9	0	0	-15	0	0	0	0
χ^8	0	0	0	0	-10	-1	1	-14	1	1	-1	-5
χ^9	1	-1	5	1	-19	-1	-1	5	0	0	0	0
χ^{10}	-1	-1	5	1	1	1	1	-35	0	0	0	0
χ^{11}	0	1	-5	-1	-16	2	0	0	0	0	0	0
χ^{12}	0	-1	-7	1	16	-2	0	0	0	0	0	8
χ^{13}	0	0	0	0	-10	-1	1	10	0	0	0	0
χ^{14}	0	0	0	0	10	1	-1	-10	0	0	0	0
χ^{15}	-1	0	3	-1	9	0	0	21	1	1	1	-7
χ^{16}	0	1	4	0	10	1	1	-2	-2	-2	0	4
χ^{17}	0	0	6	-2	18	0	0	6	1	1	-1	11
χ^{18}	0	0	0	0	0	0	0	24	-1	-1	-1	-5
χ^{19}	-2	1	4	0	-10	-1	-1	-10	0	0	0	4
χ^{20}	2	1	4	0	-10	-1	-1	-10	0	0	0	4
χ^{21}	0	0	0	0	10	1	-1	-10	β	$\overline{\beta}$	1	-5
χ^{22}	0	0	0	0	10	1	-1	-10	$\overline{\beta}$	β	1	-5
χ^{23}	0	1	1	1	16	-2	0	0	0	0	0	-4
χ^{24}	0	1	1	1	16	-2	0	0	0	0	0	-4

If g is an element of the eight conjugacy class, then $\sum_{i=1}^{24} \chi^i(g)/\chi^i(1)$

$= 1 + {}^{5381}/6325.$

If g is an element of the 17th conjugacy class, then $\sum_{i=1}^{24} \chi^i(g)/\chi^i(1) = 1 - {}^6/_{175}$.

If g is an element of the twentieth conjugacy class, then $\sum_{i=1}^{24} \chi^i(g)/\chi^i(1) = 1 - {}^6/_{25}$.

It is apparent that the required inequality holds for the other conjugacy classes and, consequently, the Higman-Sims group consists of commutators.

We conclude this chapter by giving references to character tables of various simple groups. From these tables it can be verified that all the groups consist of commutators. We only give references to groups where, as far as we know, no verification of the conjecture under consideration has been explicitly stated. We firstly consider various "sporadic" simple groups. The character tables of the other four Mathieu groups M_{23}, M_{22}, M_{12} and M_{11} can be obtained from [46]. (In [49] it is shown that both M_{22} and M_{11} consist of commutators. However, we have been unable to obtain this paper so we include the above reference for the sake of completeness.)

The character tables of the finite simple groups of Ree (c.f. [37] and[38]) are presented by H. N. Ward in [51].

The character table of the simple group of order 448, 345, 497, 600, presented by M. Suzuki in[2 p.113] was obtained by D. Wright in [52].

The character table of the simple group M(22) of order $2^{17}.3^9.5^2.7.11.23$, discovered by B. Fischer in [11], is presented by D. C. Hunt in [23].

The character table of the simple group ·3 of order $2^{10}.3^7.5^3.7.11.23$, discovered by J. Conway in [5], is presented by D. Fendel in [10].

The character table of the Hall-Janko group of order 604, 800, is presented by M. Hall, Jr. and D. Wales in [18].

Finally, the charcter table of the Higman-Janko-McKay group of order $2^7.3^5.5.17.19$ can be found in [17].

With regards to infinite families of simple groups, in [41], B.Srinivasan gives the character tables for the finite symplectic groups Sp(4,q), where q is odd. In [8] H. Enomoto handles the characteristic two case and he gives the character tables for $Sp(4,2^n)$, where $n \in \mathbb{Z}$.

Chapter 7 CONJUGACY IN GROUPS

The proof of the conjecture that every non-abelian finite simple group consists of commutators appears to be very difficult to obtain. The kind of knowledge required for such a proof does not appear to be readily accessible. It would be a great help if information concerning the number of conjugacy classes in a non-abelian finite simple group could be obtained. From an empirical point of view, such groups appear to have "few" conjugacy classes. Consequently, in this final chapter we turn our attention to finite groups in which we make assumptions concerning the conjugacy classes. Although the results we obtain are not themselves statements concerning commutators, they are the sort of results that will come in very useful in trying to prove the above conjecture.

Throughout this chapter we assume that G is a finite group which contains a subgroup M of order p^n such that any two non-identity elements of M are conjugate within G. We make extensive use of the character theory of finite groups and we adopt the notation of Chapter 5.

This work was initiated by A. Fomyn in [12]. His work was written in Russian and, in extending his results, we have used different techniques which simplify his proofs. Consequently, we will prove everything from scratch without referring to his work. We will however state which results originated from Fomyn.

We assume, with Fomyn, that M is abelian. This is certainly the case when $M \trianglelefteq G$.

Let $1 \neq m \in M$ and $\theta \in \mathrm{Irr}(M)$, where $\theta \neq 1_M$, the principal character of M.

Theorem 7.1. $\chi^i_1 = (p^n-1)\, f_i + k_i$, where

$$f_i = (\chi^i|_M, \theta)_M = (\chi^i_1 - \chi^i(m)) / p^n \quad \text{and}$$

$$k_i = (\chi^i|_M, 1_M)_M = (\chi^i_1 + (p^n-1)\, \chi^i(m)) / p^n.$$

Proof $(\chi^i|_M, \theta)_M = \frac{1}{|M|} \sum_{g \in M} \chi^i(g)\, \overline{\theta}(g)$

$$= \frac{1}{|M|} (\chi^i_1 + \sum_{1 \neq g \in M} \chi^i(g)\, \overline{\theta}(g)), \text{ because } \theta(1) = 1.$$

Now $\chi^i(g)$ is constant for all non-identity elements of M.

Therefore,

$$(\chi^i|_M, \theta)_M = \frac{1}{|M|} (\chi^i_1 + \chi^i(m) \sum_{1 \neq g \in M} \overline{\theta}(g))$$

Because $\theta \neq 1_M$, $(1_M, \theta)_M = \sum_{g \in M} \overline{\theta}(g) = 0$.

Consequently, $\sum_{1 \neq g \in M} \overline{\theta}(g) = -1$.

Therefore,

$$(\chi^i|_M, \theta)_M = (\chi^i_1 - \chi^i(m)) / p^n = f_i, \text{ say.}$$

Similarly,

$$(\chi^i|_M, 1_M)_M = \frac{1}{|M|} \sum_{g \in G} \chi^i(g)\, \overline{1}_M(g)$$

$$= (\chi^i_1 + (p^n-1)\, \chi^i(m)) / p^n = k_i, \text{ say.}$$

Now $|\mathrm{Irr}(M)| = |\mathrm{Hom}(M, \mathbb{C})| = p^n$.

Because f_i is independent of θ we have the desired result that

$$\chi^i_1 = (p^n-1)\, f_i + k_i.$$

Fomyn obtained the result that $\chi^i_1 = (p^n-1)\, f_i + k_i$ though he did not observe either $(\chi^i|_M, \theta)_M = f_i$ or $(\chi^i|_M, 1_M)_M = k_i$. He also assumed that $\langle M \rangle^G = G$ and we do not

We now give a simplified verification of some formulae obtained by Fomyn.

Theorem 7.2.

(i) $\chi^i(m) = k_i - f_i$

(ii) $p^n \sum_{i=1}^{h} f_i \chi^i_1 = |G|$

(iii) $p^n \sum_{i=1}^{h} k_i \chi^i_1 = |G|$

(iv) $p^{2n} \sum_{i=1}^{h} f_i^2 = |G| + |C_G(m)|$

(v) $p^{2n} \sum_{i=1}^{h} k_i^2 = |G| + (p^n-1)^2 |C_G(m)|$

(vi) $p^{2n} \sum_{i=1}^{h} k_i f_i = |G| - (p^n-1)\,|C_G(g)|$

Proof. By Theorem 7.1,

$$k_i - f_i = (\chi^i_1 + (p^n-1)\,\chi^i(m)) / p^n - (\chi^i_1 - \chi^i(m)) / p^n = \chi^i(m).$$

By [9.p.16], $$\sum_{i=1}^{h} \chi^i_1 \chi^i(m) = 0. \qquad (7.2.1)$$

So, by Theorem 7.1,

$$\sum_{i=1}^{h} \chi^i_1 (\chi^i_1 - p^n f_i) = 0.$$

Now $\sum_{i=1}^{h} (\chi^i_1)^2 = |G|$, by [9.p.16].

So,

$$p^n \sum_{i=1}^{h} f_i \chi^i_1 = |G|.$$

By Theorem 7.2 (i), $\chi^i(m) = k_i - f_i$.

So, $$\sum_{i=1}^{h} \chi^i_1 (k_i - f_i) = 0, \qquad \text{by (7.2.1).}$$

Now $p^n \sum_{i=1}^{h} f_i \chi^i_1 = |G|$, by Theorem 7.2 (ii),

So $p^n \sum_{i=1}^{h} k_i \chi^i_1 = p^n \sum_{i=1}^{h} f_i \chi^i_1 = |G|.$

Now $m \sim {}_G m^{-1}$, so, by [9.p.16], $\sum_{i=1}^{h} (\chi^i(m))^2 = |C_G(m)|$. (7.2.2)

So, by Theorem 7.1,

$$|C_G(m)| = \sum_{i=1}^{h} (\chi^i_1 - p^n f_i)^2$$

$$= \sum_{i=1}^{h} (\chi^i_1)^2 - 2p^n \sum_{i=1}^{h} \chi^i_1 f_i + p^{2n} \sum_{i=1}^{h} f_i^2$$

$$= |G| - 2|G| + p^{2n} \sum_{i=1}^{h} f_i^2, \text{ by [9.p.16] and Theorem 7.2 (ii).}$$

Thus, $p^{2n} \sum_{i=1}^{h} f_i^2 = |G| + |C_G(m)|$.

By Theorem 7.1, $\chi^i(m) = (p^n k_i - \chi^i_1) / (p^n-1)$.

So, by (7.2.2),

$$|C_G(m)| = \sum_{i=1}^{h} ((p^n k_i - \chi^i_1) / (p^n-1))^2$$

$$= \frac{1}{(p^n-1)^2} (p^{2n} \sum_{i=1}^{h} k_i^2 - 2p^n \sum_{i=1}^{h} k_i \chi^i_1 + \sum_{i=1}^{h} (\chi^i_1)^2)$$

$$= \frac{1}{(p^n-1)^2} (p^{2n} \sum_{i=1}^{h} k_i^2 - |G|), \text{ by [9.p.16] and Theorem 7.2.(iii).}$$

Therefore, $p^{2n} \sum_{i=1}^{h} k_i^2 = |G| + (p^n-1)^2 |C_G(m)|$.

Finally, by Theorem 7.2 (i), $\chi^i(m) = k_i - f_i$.

So, by (7.2.2),

$$|C_G(m)| = \sum_{i=1}^{h} (k_i - f_i)^2 = \sum_{i=1}^{h} k_i^2 - 2 \sum_{i=1}^{h} k_i f_i + \sum_{i=1}^{h} f_i^2.$$

So, $2p^{2n} \sum_{i=1}^{h} k_i f_i = p^{2n} \sum_{i=1}^{h} k_i^2 + p^{2n} \sum_{i=1}^{h} f_i^2 - p^{2n} |C_G(m)|$

$$= |G| + (p^n-1)^2 |C_G(m)| + |G| + |C_G(m)| - p^{2n} |C_G(m)|,$$

By Theorem 7.2 (iv) and Theorem 7.2 (v).

Thus, $p^{2n} \sum_{i=1}^{h} k_i f_i = |G| - (p^n-1)\,|C_G(m)|$, as required.

Fomyn obtained the following corollaries to Theorem 7.2.

Corollary 7.3. If the order of a Sylow p-subgroup of $C_G(m)$ is not greater than $p^{(2n-1)}$, then it is a Sylow p-subgroup of G.

Proof. The proof follows immediately from Theorem 7.2 (iv).

Let χ^1 be the principal character of G.

Corollary 7.4. If f_i is an odd number for $2 \leq i \leq h$, then $p = 2$ and M is a Sylow 2-subgroup of G.

(Note that $f_i = 0$ if and only if $M \subseteq \mathrm{Ker}(\chi^i)$. So f_i being non-zero for $2 \leq i \leq h$ implies that $\langle M \rangle^G = G$.)

Proof. By Theorem 7.2 (v) and Theorem 7.2 (vi) we obtain,

$$p^{2n} \sum_{i=1}^{h} k_i(k_i - f_i) = (p^{2n} - p^n)\,|C_G(m)|.$$

Now χ^1 being the principal character implies that $k_1 = 1$ and $f_1 = 0$. So,

$$p^{2n} + p^{2n} \sum_{i=2}^{h} k_i(k_i - f_i) = (p^{2n} - p^n)\,|C_G(m)|. \qquad (7.2.3)$$

Since $p^{2n} - p^n$ is always even and $k_i(k_i - f_i)$ is even because f_i is odd we have that $p = 2$. The highest power of 2 to divide the left hand side of (7.2.3) is 2^{2n}. Consequently, the highest power of 2 to divide $|C_G(m)|$ is 2^n. By Corollary 7.3 a Sylow 2-subgroup of $C_G(m)$ is a Sylow 2-subgroup of G. Since $|M| = 2^n$ and $M \subseteq C_G(m)$, the proof is complete.

As a further corollary of Theorem 7.2 Fomyn obtained the following result.

Corollary 7.5. Suppose $f_i = 1$ for $2 \leq i \leq h$ and that G does not possess three pairwise non-equivalent irreducible representations of degree p^n-1. If G is a simple group, then $G \cong A_5$, the alternating group on 5 symbols.

We will extend the result, but before doing so we give a final corollary to Theorem 7.2.

Corollary 7.6. M is a normal subgroup of G if and only if

$$f_i k_i = 0 \quad \text{for } 1 \leq i \leq h$$

Proof. We observe that $M \triangleleft G$ is and only if $|Cl(m)| = p^n-1$, where $Cl(m)$ is the conjugacy class of G containing m. Noting that f_i and k_i are non-negative for $1 \leq i \leq h$ and $|Cl(m)|\ |C_G(m)| = |G|$, the result follows from Theorem 7.2(vi).

Theorem 7.7. Suppose $f_i = 1$, for $2 \leq i \leq h$.

Then $p = 2$, M is a Sylow 2-subgroup of G and

either (a) $G/O_2,(G) \cong PSL(2, 2^n)$

or (b) $|M| = 2$, $G = G' \rtimes M$, G' is abelian and $g^m = g^{-1}$ for every $g \in G'$.

Proof. As we noted above $\langle M \rangle^G = G$. Let $N \triangleleft G$. Since any two non-identity elements of M are conjugate within G,

either $N \cap M = \langle 1 \rangle$ or $M \subseteq N$. But $\langle M \rangle^G = G$, so, either $N \cap M = \langle 1 \rangle$ or $N = G$.

Suppose $N \cap M = \langle 1 \rangle$ and we consider $\zeta \in Irr(G/N)$.

Now $NM/N \cong M/M \cap N = M$. Suppose μ is a non-principal character of NM/N.

Because ζ is also an irreducible character of G, we see that

$(\zeta|_{NM/M}, \mu)_{NM/M} = 1$. (In other words our assumption that $f_i = 1$ for non-principal characters is quotient closed.)

Two cases arise, depending on whether or not G is solvable.

Suppose G is not solvable. By Corollary 7.4, M is a Sylow 2-subgroup of G.

Because $\langle M \rangle^G = G$, $G/O_2,(G)$ is a simple group. J. H. Walter in [50] classified non-abelian finite simple groups with an abelian Sylow 2-subgroup. From [50] we see that $G/O_2,(G)$ is isomorphic to one of the

following:

(i) $PSL(2, 2^m)$, $m > 1$.

(ii) $PSL(2, q)$, $q \equiv 3$ or 5 (modulo 8), $q > 3$.

(iii) A simple group H such that for each involution t of H, $C_H(t) = \langle t \rangle \times A$, where A is isomorphic to $PSL(2, q)$, with $q \equiv 3$ or 5 (modulo 8).

We give an argument of Fomyn to show that G possesses an irreducible character of degree $2^n - 1$. From Theorem 7.2 (ii),

$$2^n \sum_{i=2}^{h} \chi^i_1 = |G|.$$

But $\sum_{i=1}^{h} (\chi^i_1)^2 = |G|$ from [9. p.16].

So, $\sum_{i=2}^{h} \chi^i_1(\chi^i_1 - 2^n) = -1$.

Consequently there exists a χ^j where $2 \leq j \leq h$ such that $\chi^j_1 < 2^n$. But $f_i = 1$ for $2 \leq i \leq h$ implies that $\chi^i_1 \geq 2^n - 1$, by Theorem 7.1. So G possesses a χ^j where $2 \leq j \leq h$ such that $\chi^j_1 = 2^n - 1$. Of the three possibilities for the structure of $G/O_2,(G)$, in Case (ii), G has a Sylow 2-subgroup of order 4 (c.f. [6 p.9]). So, by the above argument G possesses an irreducible character of degree 3. From [7. p.228] we see that this implies q is equal to 5. But $PSL(2, 5) \cong PSL(2, 4)$, from [16 p.493]. So this exceptional occurence is contained in Case (i). (Note that $PSL(2, 5) \cong PSL(2, 4) \cong A_5$ and this is the case covered by Fomyn in Corollary 7.5.) Z. Janko and J. G. Thompson, in [29], show that for the groups in Case (iii), either $q = 5$, or $q = 3^{2r+1}$, where $r \geq 1$. Janko, in [28], considered the case $q = 5$ and showed that the group arising is the group named after him, Janko's group of order 175,560. A Sylow 2-subgroup of this group has order 8, but from the character table obtained by J. McKay in [30] we see that Janko's group does not possess an irreducible character of degree 7, contradicting the above argument. If $q = 3^{2r+1}$, where $r \geq 1$, then, from [29. Lemma 2.1], a

Sylow 2-subgroup of G has order 8. Now G has a subgroup $K \tilde{=} PSL(2, q)$, with $q \geq 27$. From [7.p.228] we see that PSL(2, q) possesses no non-principal character of degree less than $(q - 1)/2 \geq 13$. Therefore, if G possesses an irreducible character χ of degree 7, then $K \subseteq \mathrm{Ker}(\chi)$. But G is a simple group, so this is impossible. So we are reduced to considering Case (i). From [7. p.235] we see that $PSL(2, 2^m)$ obeys the conditions of the theorem, where $m \geq 1$. Moreover, the order of a Sylow 2-subgroup of $PSL(2, 2^m)$ equals 2^m from [6.p.9]. So we do indeed have that $G/O_{2'}(G) \tilde{=} PSL(2, 2^n)$.

If G is solvable, then because G/N satisfies the hypotheses of the theorem, where $N \lhd G$, we have that M has a normal 2-complement $O_{2'}(G)$. If m_1, m_2 are non-identity elements of M, then $m_1 \sim_G m_2$. Consequently $m_1N \sim_{G/N} m_2N$, where $N \lhd G$. Because $G/O_{2'}(G) \tilde{=} M$, we must have $M \tilde{=} C_2$.

Now $G = \langle M \rangle^G = \langle M, [M, O_{2'}(G)] \rangle$.

So, $O_{2'}(G) = [M, O_{2'}(G)] = G'$.

Suppose there exists χ^j such that $\chi^j_1 > 2$.

Now $\sum_{i=1}^{h} \chi^i_1 \chi^i(m) = 0$, from [9.p.16].

Since $|G : G'| = 2$, G has two linear characters χ^1 and χ^2 say.

Moreover, $\chi^1(m) = 1$ and $\chi^2(m) = -1$.

Consequently,

$$\sum_{i=3}^{h} \chi^i_1 \chi^i(m) = 0. \qquad (7.7.1)$$

By Theorem 7.1, $\chi^j(m) = \chi^j_1 - 2$ which is greater than zero by assumption. In order that (7.7.1) holds there must exist χ^r such that $\chi^r(m) < 0$, where $3 \leq r \leq h$.

But, again by Theorem 7.1, $f_r = (\chi^r_1 - \chi^r(m))/2$ and, if $\chi^r(m) < 0$, then $f_r \neq 1$ contradicting our initial assumption. So $\chi^i_1 = 2$ for $3 \leq i \leq h$.

By a result of I. M. Isaacs and D. S. Passman [25.Theorem II], G has a normal abelian subgroup of index 2. i.e. G' is abelian. Now M induces a group of

automorphisms upon G' and $(|M|, |G'|) = 1$. It is easily seen that Theorem 5.2.3 of [16] can be extended to cover this case and we have

$$G' = [G', M] \times C_{G'}(M).$$

But $G' = [G', M]$, from above. So $C_{G'}(M) = C_{G'}(\langle m \rangle) = \langle 1 \rangle$. Thus m induces a fixed point free automorphism upon G'. Let $g \in G'$ and suppose $g^m = h$. Because $m^2 = 1$, $h^m = g$. Thus $(gh)^m = hg = gh$, because G' is abelian. Since m induces a fixed point free automorphism, $h = g^{-1}$.

It would be nice if we were able to extend the previous theorem by letting the f_i's take a different set of values. In the solvable case progress may be possible, for it is easily seen that the assumption that $f_i > 0$ for $2 \leq i \leq h$ forces G to be a split extension of a group of odd order by an involution. However, in the non-solvable case matters are more difficult. If one examines the character tables of non-abelian finite simple groups one does not readily see any straightforward pattern for the f_i's that arise.

e.g. In Janko's group of order 175,560, by considering M to be a Sylow 2-subgroup, we obtain the following set of values for the f_i's:-

$$\{0,\ 7,\ 7,\ 9,\ 10,\ 9,\ 10,\ 10,\ 15,\ 15,\ 15,\ 16,\ 17,\ 17,\ 26\}.$$

By assuming that $f_i > 0$ for $2 \leq i \leq h$ we came to the conclusion that $\langle M \rangle^G = G$. We now consider the opposite case, that of M being a normal subgroup of G.

We recall that if $M \lhd G$, $\theta \in Irr(M)$ and $g \in G$, we may define $\theta^g \in Irr(M)$ by $\theta^g(h) = \theta(ghg^{-1})$, $h \in M$. Further we recall that the Inertial Group of θ, denoted by $I(\theta)$ is $\{g | g \in G,\ \theta^g = \theta\}$. Finally if H is a subgroup of G, $\chi \in Irr(G)$ and $\lambda \in Irr(H)$ such that λ is a constituent of χ restricted to H, then we write that $\lambda \in \chi|_M$.

We show that there is a very close relationship between $I(\theta)$ and $C_G(m)$, where we still assume that θ is a non-principal character of M and $1 \neq m \in M$.

We first prove an introductory result of independent interest.

Theorem 7.8. Let $M \lhd G$. Suppose that $\{f_i \mid 2 \leq i \leq r\}$ are the only non-zero f_i's. Then there exists $\zeta^i \in \mathrm{Irr}(I(\theta))$ such that $f_i = \zeta^i(1)$ for some i, $2 \leq i \leq r$. Conversely, given $\zeta^i \in \mathrm{Irr}(I(\theta))$ such that $\theta \in \zeta^i|_M$, then there exists an f_i such that $f_i = \zeta^i(1)$.

Proof. Let $\chi^i \in \mathrm{Irr}(G)$ be such that $M \nleq \mathrm{Ker}(\chi^i)$.

By Corollary 7.6 we see that $f_i \neq 0 = k_i$.

So $\chi^i|_M = f_i \sum_j \theta^j$, where $\{\theta^j\} = \mathrm{Irr}(M) \setminus \{1_M\}$.

By restricting χ^i to $I(\theta)$ we may select an $\zeta^i \in \mathrm{Irr}(I(\theta))$ such that $\zeta^i \in \chi^i|_{I(\theta)}$ and $\theta \in \zeta^i|_M$. Then, from [9. p.53] we see that $\zeta^{i*} = \chi^i$, where ζ^{i*} is the character of G obtained by inducing ζ^i up to G. Because $\zeta^i \in \mathrm{Irr}(I(\theta))$ we see that $\zeta^i|_M = \zeta^i(1)$. Consequently, by [9. p.53], $\zeta^i(1) = f_i$.

The proof of the converse follows by reversing the above argument.

Theorem 7.9. If $M \lhd G$, then $|C_G(m)| = |I(\theta)|$.

Proof. Select $\zeta \in \mathrm{Irr}(I(\theta))$ such that $\theta \in \zeta|_M$.

Then, by Theorem 7.8 and from [9. p.53] it is easily seen that,

$$\zeta^* = \chi^j \text{ and } \zeta(1) = f_j. \tag{7.9.1}$$

By [9. p.45],

$$\zeta^*(m) = \frac{1}{|I(\theta)|} \sum_{g \in G} \zeta(gmg^{-1}).$$

Because any two non-identity elements of M are conjugate within G we have,

$$\zeta^*(m) = \frac{|C_G(m)|}{|I(\theta)|} \sum_k \zeta(m_k), \tag{7.9.2}$$

where $\{m_k\}$ are the non-identity elements of M.

Now, $(\theta, 1_M)_M = \frac{1}{|M|} \sum_{h \in M} \theta(h) = 0$, by [9. p.14].

So, $\sum_k \theta(m_k) = -\theta(1) = -1$.

Therefore, $\sum_k \zeta(m_k) = \sum_k \zeta(1)\,\theta(m_k) = -\zeta(1)$.

By Theorem 7.2.(i) and (7.9.1) we have,

$$\zeta^*(m) = \chi^j(m) = -f_j = -\zeta(1).$$

Comparing with (7.9.2) we see that $|C_G(m)| = |I(\theta)|$.

Suppose we assume that M is a Sylow p-subgroup of G. By a result of Burnside [16 Theorem 7.1.1], two elements of M are conjugate within G if and only if they are conjugate within $N_G(M)$. So, in assuming that M is a Sylow p-subgroup it is reasonable to assume that $M \lhd G$.

Under these assumptions we prove the following theorem.

Theorem 7.10. Suppose M is a normal Sylow p-subgroup of G. Then, to each non-principal character $\theta^i \in \mathrm{Irr}(M)$ there exists $1 \neq m_i \in M$ such that

$$I(\theta^i) = C_G(m_i), \text{ and conversely.}$$

Proof. Suppose θ^i is a non-principal character of M. Let $M = \langle g_i \rangle \times \mathrm{Ker}(\theta^i)$, where $\theta(g_i) = \omega$, ω a primitive p th root of unity.

It is easily seen that $I(\theta^i) \subseteq N_G(\mathrm{Ker}(\theta^i))$ and that $g_i^{\,g} = g_i k$, where $g \in I(\theta)$ and $k \in \mathrm{Ker}(\theta^i)$. Consequently, $[M, I(\theta^i)] \subseteq \mathrm{Ker}(\theta^i)$. By [16 Theorem 5.2.3], g_i may be chosen such that $I(\theta^i) \subseteq C_G(g_i)$. This particular value of g_i is our desired m_i. By applying Theorem 7.9, we see that $I(\theta^i) = C_G(m_i)$.

Conversely, given $1 \neq m_i \in M$, we consider the following equation, which follows from [16 Theorem 5.2.3].

$$M = [M, C_G(m_i)] \times C_M(C_G(m_i))$$

Let $C_M(C_G(m_i)) = \langle m_i \rangle \times K_1$

and also let $K_2 = [M, C_G(m_i)] \times K_1$.

If we define θ^i by $\theta^i(m_i) = \omega$ and $\theta^i(k) = 1$ for each $k \in K_2$, then it is easily seen that $C_G(m_i) \subseteq I(\theta^i)$. By Theorem 7.9, we reach the desired conclusion that $C_G(m_i) = I(\theta^i)$.

We now obtain information concerning the relationship between $I(\theta)/M$ and the $\{f_i | 2 \leq i \leq h\}$.

Theorem 7.11. Suppose M is a normal Sylow p-subgroup of G and that $\{f_i | 2 \leq i \leq r\}$ are the only non-zero f_i's. Then $\{f_i | 2 \leq i \leq r\}$ are the degrees of the irreducible characters of $I(\theta)/M$.

Proof. We consider θ^*, the character of $I(\theta)$ obtained by inducing θ up to $I(\theta)$.

If $\zeta \in \mathrm{Irr}(I(\theta))$ is such that $\theta \in \zeta|_M$, then $\zeta|_M = \zeta(1)\theta$.

By the Frobenius Reciprocity Theorem [9. p.47],

$$(\zeta, \theta^*)_{I(\theta)} = (\zeta|_M, \theta)_M = \zeta(1).$$

By Theorem 7.8 we see that there are (r-1) such ζ's denoted by $\{\zeta^i | 2 \leq i \leq r\}$ and that $\zeta^i(1) = f_i$, where $2 \leq i \leq r$.

Let $\{\lambda_i\} = \mathrm{Irr}(I(\theta)/M)$. These are the characters of $I(\theta)$ that contain M in their respective kernels. By Theorem 7.10, there exists an $m \in M$ such that $I(\theta) = C_G(m)$. Moreover, by considering the proof of Theorem 7.10 we see that m may be chosen such that $\theta(m) = \omega$, a primitive p th root of unity.

Now the $\{\zeta^i | 2 \leq i \leq r\}$ are precisely the irreducible characters of $I(\theta)$ such that $\mathrm{Ker}(\theta) \subseteq \mathrm{Ker}(\zeta^i)$ and $\zeta^i(m) = \zeta^i(1)\omega$, for $2 \leq i \leq r$.

Now M is a normal Sylow p-subgroup of $I(\theta)$. So, by the Schur-Zassenhaus Theorem [16 Theorem 6.2.1], M has a complement K in $I(\theta)$. Noting this and also that $m \in Z(I(\theta))$ we see that there is a well defined bijection ϕ between the $\{\lambda_j\}$ and then $\{\zeta^i\}$, given by,

$$\phi : \lambda_j \to \zeta^j, \text{ where we define } \zeta^j \text{ by}$$

$$\zeta^j(kgm^\alpha) = \lambda_j(kgm^\alpha)\omega^\alpha, \text{ where } k \in K,\ g \in \mathrm{Ker}(\theta) \text{ and } \alpha \in \mathbb{Z}.$$

Recalling that $f_i = \zeta^i$ for $2 \leq i \leq r$ we see that the proof is complete.

We finish by applying this work to a rather restricted case.

Theorem 7.12. Suppose M is a normal Sylow p-subgroup of G and that G/M is abelian.

Suppose π = {set of prime divisors of p^n-1}.

Then, (i) G has a normal abelian Hall π'-subgroup.

(ii) $C_G(m) \lhd G$ and $G/C_G(m)$ is cyclic of order (p^n-1).

(iii) $C_G(m) = Z(G) \times M$.

Proof. By Corollary 7.6, $k_i f_i = 0$ for $1 \leq i \leq h$.

Now the non-zero k_i are the degrees of the irreducible characters of G/M. Because G/M is abelian these k_i equal 1. By considering Theorem 7.8, again noting that G/M is abelain we see that the non-zero f_i also equal one. By Theorem 7.1 we see that either $\chi^i(1) = 1$ or $\chi^i(1) = p^n-1$, for $1 \leq i \leq h$. By a theorem of I. M. Isaacs and D. S. Passman [26. Theorem 3.1], we see that G has a normal abelian Hall π'-subgroup H, $C_G(H) \lhd G$ with $G/C_G(H)$ cyclic of order (p^n-1) and that $C_G(H) = Z(G) \times B$, where $B \lhd G$, and $G/C_G(H)$ acts fixed point freely on B.

Now $m \in H$, so $C_G(m) \supseteq C_G(H)$.

But $|G : C_G(m)| = |G : C_G(H)| = (p^n-1)$.

Therefore, $C_G(m) = C_G(H)$.

Because M is a normal Sylow p-subgroup of G, M has a complement K in G.

Now $K \tilde{=} G/M$ which is abelian. Therefore B = M and the proof is complete.

The author would like to point out that since he obtained these results he has become aware of some results of I. M. Isaacs [24] and unpublished results of E. C. Dade and G. Glauberman that describe the relationships between the inertial groups and centralizers of elements in far greater generality.

BIBLIOGRAPHY

1. E. Artin, Galois Theory (University of Notre Dame, Indiana, 1959).

2. R. Brauer and C. Sah, Ed., Theory of Finite Groups (Bejamin, New York, 1969)

3. W. Burnside, Theory of Groups of Finite Order, 2nd edition(Dover,New York,1955)

4. R. D. Carmichael, Introduction to the Theory of Groups of Finite Order (Ginn and Co., Boston, U.S.A., 1937)

5. J. H. Conway, "A group of order 8, 315, 553, 613, 086, 720, 000", Bull. London Math. Soc. 1(1969), 79-88.

6. J. D. Dixon, The Structure of Linear Groups (Van Nostrand, London, 1971).

7. L. Dornhoff, Group Representation Theory Part A (Marcel Dekker Inc. New York, 1971).

8 H. Enomoto, "The characters of the finite symplectic group Sp(4,q), $q=2^f$", Osaka J. Math. 9(1972), 75-94.

9. W. Feit, Characters of Finite Groups (Benjamin, New York, 1967).

10. D. Fendel, "A Characterisation of Conway's Group . 3", J. of Algebra 24(1973), 159-196.

11. B. Fischer, "Finite groups generated by 3-transpositions", Invent.Math., to appear.

12. A. Fomyn, "On the degrees of irreducible complex representations of some finite groups", Ural Gos.Univ. Matematiskeskoi Zapiski 8 (1971), Tetrad 1, 111-120. (Russian).

13. J. S. Frame, "Computation of Characters of the Higman-Sims Group and its Automorphism group", J. of Algebra 20(1972), 320-349.

14. P. X. Gallagher, "Group Character and Commutators", Math.Zeit 79(1962), 122-126

15. ———————— , "The generation of the Lower Central Series", Canadian J. of Maths, 17(1965), 405-410.

16. D. Gorenstein, Finite Groups (Harper & Row, New York, 1968).

17. M. Hall Jr., Lecture Notes, Summer School on Group Theory and Computation, University College, Galway, Ireland, 1973.

18. M. Hall Jr., and D. Wales, "The Simple Group of Order 604, 800", J. of Algebra 9(1968), 417-450.

19. D. G. Higman and C. C. Sims, "A simple group of order 44, 352, 000", Math. Zeit. 105(1968), 110-113.

20. G. Higman, "Suzuki 2-groups", Illinois J. of Maths. 7(1963), 79-96.

21 C. V. Holmes, "Commutator Groups of Monomial Groups", Pacific J. of Maths. 10(1960), 1313-1318.

22. K. Honda, "On Commutators in Finite Groups", Commentarii Mathematici, Universitatis Sancti Pauli (Tokyo) 2(1953), 9-12.

23. D. C. Hunt, "Character tables of certain finite simple groups", Bull. Australian Math. Soc. 5(1971), 1-42.

24. I. M. Isaacs, "Fixed points and charcters in groups with non-coprime operator groups", Canadian J. of Maths. 20(1968), 1315-1320.

25. I. M. Isaacs and D. S. Passman, "Groups whose irreducible representations have degrees dividing p^e", Illinois J. of Maths. 8(1964), 446-457.

26. ———————————, "A characterization of groups in terms of the degrees of their characters, II", Pacific J. of Maths. 24(1968), 467-510.

27. N. Ito, "A theorem on the alternating group, $U_n(n \geq 5)$", Math.Japon. 2(1951), 59-60.

28. Z. Janko, "A new finite simple group with abelian 2-Sylow groups and its characterization", J. of Algebra 3(1966), 147-187.

29. Z. Janko and J. G. Thompson, "On a class of finite simple groups of Ree", J. of Algebra 4(1966), 274-292.

30. J. Leech Ed., Computational Problems in Abstract Algebra (Pergammon Press, Oxford, 1970).

31. I. D. Macdonald, "On a set of Normal Subgroups", Proc. of the Glasgow Math. Assoc. 5(1962), 137-146.

32. ———————, "On Cyclic Commutator Subgroups", J. London Math. Soc. 38(1963), 419-422.

33. L. Nachbin, The Haar Integral (Van Nostrand, New York, 1965).

34. O. Ore, "Some remarks on commutators", Proc. American Math. Soc.2(1951), 307-314.

35. D. S. Passman, Permutation Groups (Benjamin, New York, 1968).

36. Qin Jian-Min, "On Commutators in Orthogonal Groups", Acta Mathematica Sinica 15(1965), 708-719.

37. R. Ree, "A family of simple groups associated with the simple Lie algebra algebra of type (G_2)", Bull. American Math. Soc. 66(1960), 508-510.

38. ———————, "A family of simple groups associated with the simple Lie algebra of type (G_2)", American J. of Maths. 83(1961), 432-462.

39. D. M. Rodney, "On Cyclic Derived Subgroups", J. London Math. Soc.,to appear.

40. W. Sierpinski, Theory of Numbers (Warsaw, 1964).

41. B. Srinivasan, "The characters of the finite symplectic group Sp(4,q)", Trans. American Math. Soc. 131(1968), 488-525.

42. M. Suzuki, "On a class of Doubly Transitive Groups", Annals of Maths. 75(1962), 105-145.

43. R. C. Thompson, "Commutators in the Special and General Linear Groups", Trans. American Math. Soc. 101(1961), 16-33.

44. ———————, "Commutators of matrices with coefficients from the field of two elements", Duke. J. of Maths. 29(1962), 367-373.

45. ———————, "On Matrix Commutators", Portugaliae Mathematica 21 (1962), 143-153.

46. J. A. Todd, "A representation of the Mathieu group M_{24} as a collineation group", Annali di Matematica Pure ed Applicata 71(1966), 199-238.

47. H. Toyama, "On Commutators of Matrices", Kodai Math. Sem. Rep. Nos 5-6 (1949), 1-2.

48. Ts'eng K'en Cheng and Hsu Ch'eng-hao, "On the commutators in two classes of finite simple groups", Shuxue Jinzhan 8(1965), 202-208. (Chinese).

49. Ts'eng K'en Cheng and Liu Chiung Sheng, "On the commutators of the simple Mathieu groups", J. Chinese Univ. Sci. Techn. 1(1965), No.1, 43-48. (Chinese).

50. J. H. Walter, "The characterization of finite groups with abelian Sylow 2-subgroups", Annals. of Maths (2) 89(1969), 405-514.

51. H. N. Ward, "On Ree's series of simple groups", Trans. American Math. Soc. 121(1966), 62-89.

52. D. Wright, "The Irreducible Characters of the Simple Group of M. Suzuki of Order 448, 345, 497, 600", J. of Algebra 29(1974), 303-323.

53. Xu Ch'eng Hao, "Commutators in the Symplectic Groups", Shuxue Jinzhan 7(1964), 443-448. (Chinese).