SOLVABILITY OF GROUPS OF ODD ORDER

WALTER FEIT AND JOHN G. THOMPSON

CHAPTER I

1. Introduction

The purpose of this paper is to prove the following result:

THEOREM. *All finite groups of odd order are solvable.*

Some consequences of this theorem and a discussion of the proof may be found in [11].

The paper contains six chapters, the first three being of a general nature. The first section in each of Chapters IV and V summarizes the results proved in that chapter. These results provide the starting point of the succeeding chapter. Other than this, there is no cross reference between Chapters IV, V and VI. The methods used in Chapter IV are purely group theoretical. The work in Chapter V relies heavily on the theory of group characters. Chapter VI consists primarily of a study of generators and relations of a special sort.

2. Notation and Definitions

Most of the following lengthy notation is familiar. Some comes from a less familiar set of notes of P. Hall [20], while some has arisen from the present paper. In general, groups and subsets of groups are denoted by German capitals, while group elements are denoted by ordinary capitals. Other sets of various kinds are denoted by English script capitals. All groups considered in this paper are finite, except when explicitly stated otherwise.

Ordinary lower case letters denote numbers or sometimes elements of sets other than subsets of the group under consideration. Greek letters usually denote complex valued functions on groups. However,

Received November 20, 1962. While working on this paper the first author was at various times supported by the U. S. Army Research Office (Durham) contract number DA-30-115-ORD-976 and National Science Foundation grant G-9504; the second author by the Esso Education Foundation, the Sloan Foundation and the Institute for Defense Analyses. Part of this work was done at the 1960 Summer Conference on Group Theory in Pasadena. The authors wish to thank Professor A. A. Albert of the University of Chicago for making it possible for them to spend the year 1960-61 there. The authors are grateful to Professor E. C. Dade whose careful study of a portion of this paper disclosed several blunders. Special thanks go to Professor L. J. Paige who has expedited the publication of this paper.

σ and τ are reserved for field automorphisms, permutations or other mappings, and ε is used with or without subscripts to denote a root of unity. Bold faced letters are used to denote operators on subsets of groups.

The rational numbers are denoted by $\mathcal{Q}$, while $\mathcal{Q}_n$ denotes the field of nth roots of unity over $\mathcal{Q}$.

Set theoretic union is denoted by $\cup$. If $\mathfrak{A}$ and $\mathfrak{B}$ are sets, $\mathfrak{A} - \mathfrak{B}$ denotes the elements of $\mathfrak{A}$ which are not in $\mathfrak{B}$. $\mathfrak{A} \subset \mathfrak{B}$ means that $\mathfrak{A}$ is a proper subset of $\mathfrak{B}$.

$\langle \cdots \mid \cdots \rangle$	the group generated by $\cdots$ such that $\cdots$. $\langle 1 \rangle$ will be identified with 1.
$\{\cdots \mid \cdots\}$	the set of $\cdots$ such that $\cdots$.
$gp\langle \cdots \mid \cdots \rangle$	the group defined by the generators $\cdots$ with the relations $\cdots$.
$\lvert \mathfrak{X} \rvert$	the number of elements in the set $\mathfrak{X}$.
$\mathfrak{X}^{\#}$	the set of non identity elements in the set $\mathfrak{X}$.
π	a set of primes. If $\pi = \{p\}$, we customarily identify π with p.
π'	the complementary set of primes.
π-number	a non zero integer all of whose prime factors are in π.
n_π	the largest π-number dividing the non zero integer n.
π-group	a group $\mathfrak{X}$ with $\lvert \mathfrak{X} \rvert = \lvert \mathfrak{X} \rvert_\pi$.
π-element	a group element X such that $\langle X \rangle$ is a π-group.
S_π-subgroup of $\mathfrak{X}$	a subgroup $\mathfrak{S}$ of $\mathfrak{X}$ with $\lvert \mathfrak{S} \rvert = \lvert \mathfrak{X} \rvert_\pi$.
S-subgroup of $\mathfrak{X}$	a S_π-subgroup of $\mathfrak{X}$ for suitable π.
Hall subgroup of $\mathfrak{X}$	a S-subgroup of $\mathfrak{X}$.
$\mathfrak{K} \lhd \mathfrak{X}$	$\mathfrak{K}$ is a normal subgroup of $\mathfrak{X}$.
$\mathfrak{K}$ char $\mathfrak{X}$	$\mathfrak{K}$ is a characteristic subgroup of $\mathfrak{X}$.
$f(\mathfrak{X} \bmod \mathfrak{N})$	the inverse image in $\mathfrak{X}$ of $f(\mathfrak{X}/\mathfrak{N})$. Here $\mathfrak{N} \lhd \mathfrak{X}$, and f is a function from groups to subgroups.
$\boldsymbol{O}_\pi(\mathfrak{X})$	the maximal normal π-subgroup of $\mathfrak{X}$.
$\boldsymbol{O}_{\pi_1,\cdots,\pi_n}(\mathfrak{X})$	$\boldsymbol{O}_{\pi_n}(\mathfrak{X} \bmod \boldsymbol{O}_{\pi_1,\cdots,\pi_{n-1}}(\mathfrak{X}))$.
π-closed group	we say that $\mathfrak{X}$ is π-closed if and only if $\mathfrak{X}$ has a normal S_π-subgroup.
$\boldsymbol{F}(\mathfrak{X})$	the Fitting subgroup of $\mathfrak{X}$, the maximal normal nilpotent subgroup of $\mathfrak{X}$.
$\boldsymbol{D}(\mathfrak{X})$	the Frattini subgroup of $\mathfrak{X}$, the intersection of all maximal subgroups of $\mathfrak{X}$.
$\boldsymbol{Z}_n(\mathfrak{X})$	the nth term in the ascending central series of $\mathfrak{X}$, defined inductively by: $\boldsymbol{Z}_0(\mathfrak{X}) = 1$, $\boldsymbol{Z}_1(\mathfrak{X}) =$

	$Z(\mathfrak{X})$ = center of $\mathfrak{X}$, $Z_{n+1}(\mathfrak{X}) = Z(\mathfrak{X} \bmod Z_n(\mathfrak{X}))$.
$O^{\pi}(\mathfrak{X})$	the smallest normal subgroup $\mathfrak{Y}$ of $\mathfrak{X}$ such that $\mathfrak{X}/\mathfrak{Y}$ is a π-group.
$[X, Y]$	$X^{-1}Y^{-1}XY = X^{-1}X^{Y}$.
$[X_1, \cdots, X_n]$	$[[X_1, \cdots, X_{n-1}], X_n]$, $n \geqq 3$.
$[\mathfrak{A}, \mathfrak{B}]$	$\langle [A, B] \mid A \in \mathfrak{A}, B \in \mathfrak{B} \rangle$, $\mathfrak{A}$ and $\mathfrak{B}$ being subsets of a group.
$[\mathfrak{A}_1, \cdots, \mathfrak{A}_n]$	$[[\mathfrak{A}_1, \cdots, \mathfrak{A}_{n-1}], \mathfrak{A}_n]$, $n \geqq 3$.
$\mathfrak{X}^{\mathfrak{Y}}$	$\langle X^{Y} \mid X \in \mathfrak{X}, Y \in \mathfrak{Y} \rangle$. If $\mathfrak{X} \subseteq \mathfrak{Y}$, $\mathfrak{X}^{\mathfrak{Y}}$ is called the normal closure of $\mathfrak{X}$ in $\mathfrak{Y}$.
$\mathfrak{X}'$	$[\mathfrak{X}, \mathfrak{X}]$, the commutator subgroup of $\mathfrak{X}$.
$C_n(\mathfrak{X})$	the nth term of the descending central series of $\mathfrak{X}$, defined inductively by: $C_1(\mathfrak{X}) = \mathfrak{X}$, $C_{n+1}(\mathfrak{X}) = [C_n(\mathfrak{X}), \mathfrak{X}]$.
$\Omega_n(\mathfrak{X})$	the subgroup of the p-group $\mathfrak{X}$ generated by the elements of order at most p^n.
$\mho^n(\mathfrak{X})$	the subgroup of the p-group $\mathfrak{X}$ generated by the p^nth powers of elements of $\mathfrak{X}$.
$m(\mathfrak{X})$	the minimal number of generators of $\mathfrak{X}$.
$m_p(\mathfrak{X})$	$m(\mathfrak{P})$, $\mathfrak{P}$ being a S_p-subgroup of $\mathfrak{X}$.
$\mathrm{cl}(\mathfrak{X})$	the class of nilpotency of the nilpotent group $\mathfrak{X}$, that is, the smallest integer n such that $\mathfrak{X} = Z_n(\mathfrak{X})$.
$C_{\mathfrak{B}}(\mathfrak{A})$	the largest subset of $\mathfrak{B}$ commuting elementwise with $\mathfrak{A}$, $\mathfrak{A}$ and $\mathfrak{B}$ being subsets of a group $\mathfrak{X}$. In case there is no danger of confusion, we set $C(\mathfrak{A}) = C_{\mathfrak{X}}(\mathfrak{A})$.
$N_{\mathfrak{B}}(\mathfrak{A})$	the largest subset of $\mathfrak{B}$ which normalizes $\mathfrak{A}$, $\mathfrak{A}$ and $\mathfrak{B}$ being subsets of a group $\mathfrak{X}$. In case there is no danger of confusion, we set $N(\mathfrak{A}) = N_{\mathfrak{X}}(\mathfrak{A})$.
$\ker(\mathfrak{X} \xrightarrow{\alpha} \mathfrak{Y})$	the kernel of the homomorphism α of the group $\mathfrak{X}$ into the group $\mathfrak{Y}$. α will often be suppressed.
$\mathrm{ccl}_{\mathfrak{X}}(\mathfrak{A})$	$\{\mathfrak{A}^{X} \mid X \in \mathfrak{X}\}$, $\mathfrak{A}$ being a subset of $\mathfrak{X}$.
$V(\mathrm{ccl}_{\mathfrak{X}}(\mathfrak{A}); \mathfrak{B})$	$\langle \mathfrak{A}^{X} \mid X \in \mathfrak{X}, \mathfrak{A}^{X} \subseteq \mathfrak{B} \rangle$, the weak closure of $\mathrm{ccl}_{\mathfrak{X}}(\mathfrak{A})$ in $\mathfrak{B}$ with respect to the group $\mathfrak{X}$. Here $\mathfrak{A}$ and $\mathfrak{B}$ are subgroups of $\mathfrak{X}$. If $\mathfrak{A} = V(\mathrm{ccl}_{\mathfrak{X}}(\mathfrak{A}); \mathfrak{B})$, we say that $\mathfrak{A}$ is weakly closed in $\mathfrak{B}$ with respect to $\mathfrak{X}$.
$\pi(\mathfrak{X})$	the set of primes which divide $\lvert \mathfrak{X} \rvert$.
J_n	the n by n matrix with 1 in positions (i, i) and $(j, j+1)$, $1 \leqq i \leqq n$, $1 \leqq j \leqq n-1$, zero elsewhere.

$SL(2, p)$	the group of 2 by 2 matrices of determinant one with coefficients in $GF(p)$, the field of p elements.
special p-group	an elementary abelian p-group, or a non abelian p-group whose center, commutator subgroup and Frattini subgroup coincide and are elementary.
extra special p-group	a non abelian special p-group whose center is of order p.
self centralizing subgroup of $\mathfrak{X}$	a subgroup $\mathfrak{A}$ of $\mathfrak{X}$ such that $\mathfrak{A} = C(\mathfrak{A})$. Notice that self centralizing subgroups are abelian.
self normalizing subgroup of $\mathfrak{X}$	a subgroup $\mathfrak{A}$ of $\mathfrak{X}$ such that $\mathfrak{A} = N(\mathfrak{A})$.
$\mathscr{SCN}(\mathfrak{X})$	the set of self centralizing normal subgroups of $\mathfrak{X}$.
$\mathscr{SCN}_m(\mathfrak{X})$	$\{\mathfrak{A} \mid \mathfrak{A} \in \mathscr{SCN}(\mathfrak{X}), m(\mathfrak{A}) \geqq m\}$.
$\text{И}_{\mathfrak{X}}(\mathfrak{A})$	the set of subgroups of $\mathfrak{X}$ which $\mathfrak{A}$ normalizes and which intersect $\mathfrak{A}$ in the identity only. In case there is no danger of confusion, we set $\text{И}_{\mathfrak{X}}(\mathfrak{A}) = \text{И}(\mathfrak{A})$. If $\text{И}(\mathfrak{A})$ contains only the identity subgroup, we say that $\text{И}(\mathfrak{A})$ is trivial.
$\text{И}_{\mathfrak{X}}(\mathfrak{A}; \pi)$	the π-subgroups in $\text{И}(\mathfrak{A})$.
section	if $\mathfrak{H}$ and $\mathfrak{K}$ are subgroups of the group $\mathfrak{X}$, and $\mathfrak{H} \lhd \mathfrak{K}$, then $\mathfrak{K}/\mathfrak{H}$ is called a section.
factor	if $\mathfrak{H}$ and $\mathfrak{K}$ are normal subgroups of $\mathfrak{X}$ and $\mathfrak{H} \subseteq \mathfrak{K}$, then $\mathfrak{K}/\mathfrak{H}$ is called a factor of $\mathfrak{X}$.
chief factor	if $\mathfrak{K}/\mathfrak{H}$ is a factor of $\mathfrak{X}$ and a minimal normal subgroup of $\mathfrak{X}/\mathfrak{H}$, it is called a chief factor of $\mathfrak{X}$.

If $\mathfrak{H}/\mathfrak{K}$ and $\mathfrak{L}/\mathfrak{M}$ are sections of $\mathfrak{X}$, and if each coset of $\mathfrak{K}$ in $\mathfrak{H}$ has a non empty intersection with precisely one coset of $\mathfrak{M}$ in $\mathfrak{L}$ and each coset of $\mathfrak{M}$ in $\mathfrak{L}$ has a non empty intersection with precisely one coset of $\mathfrak{K}$ in $\mathfrak{H}$, then $\mathfrak{H}/\mathfrak{K}$ and $\mathfrak{L}/\mathfrak{M}$ are *incident sections.*

If $\mathfrak{H}/\mathfrak{K}$ is a section of $\mathfrak{X}$ and $\mathfrak{L}$ is a subgroup of $\mathfrak{X}$ which contains at least one element from each coset of $\mathfrak{K}$ in $\mathfrak{H}$, we say that $\mathfrak{L}$ *covers* $\mathfrak{H}/\mathfrak{K}$. We say that $\mathfrak{L}$ *dominates* the subgroup $\mathfrak{K}$ provided $\mathfrak{L}$ covers the section $N_{\mathfrak{X}}(\mathfrak{K})/C_{\mathfrak{X}}(\mathfrak{K})$. The idea to consider such objects stems from [17].

If $\mathfrak{F} = \mathfrak{H}/\mathfrak{K}$ is a factor of $\mathfrak{X}$, we let $C_{\mathfrak{X}}(\mathfrak{F})$ denote the kernel of the homomorphism of $\mathfrak{X}$ into Aut $\mathfrak{F}$ induced by conjugation. Similarly, we say that X in $\mathfrak{X}$ centralizes $\mathfrak{F}$ (or acts trivially on $\mathfrak{F}$) provided $X \in C(\mathfrak{F})$.

We say that $\mathfrak{X}$ has a *Sylow series* if $\mathfrak{X}$ possesses a unique $S_{p_1,\ldots,p_i}$-subgroup for each $i = 1, \cdots, n$, where $\pi(\mathfrak{X}) = \{p_1, \cdots, p_n\}$. The ordered

n-tuple $(p_1, \cdots, p_n)$ is called the *complexion* of the series [18].

A set of pairwise permutable Sylow subgroups of $\mathfrak{X}$, one for each prime dividing $|\mathfrak{X}|$, is called a *Sylow system* for $\mathfrak{X}$. This definition differs only superficially from that given in [16].

P. Hall [18] introduced and studied the following propositions:

E_π $\mathfrak{X}$ contains at least one S_π-subgroup.

C_π $\mathfrak{X}$ satisfies E_π, and any two S_π-subgroups of $\mathfrak{X}$ are conjugate in $\mathfrak{X}$.

D_π $\mathfrak{X}$ satisfies C_π, and any π-subgroup of $\mathfrak{X}$ is contained in a S_π-subgroup of $\mathfrak{X}$.

E_π^* $\mathfrak{X}$ contains a nilpotent S_π-subgroup.

In [19], P. Hall studied the *stability group* $\mathfrak{A}$ of the chain $\mathscr{C}$: $\mathfrak{X} = \mathfrak{X}_0 \supseteqq \mathfrak{X}_1 \supseteqq \cdots \supseteqq \mathfrak{X}_n = 1$, that is, the group of all automorphisms α of $\mathfrak{X}$ such that $(\mathfrak{X}_i X)^\alpha = \mathfrak{X}_i X$ for all X in $\mathfrak{X}_{i-1}$ and each $i = 1, \cdots, n$. If $\mathfrak{B}$ and $\mathfrak{X}$ are subgroups of a larger group, and if $\mathfrak{B}$ normalizes $\mathfrak{X}$, we say that $\mathfrak{B}$ *stabilizes* $\mathscr{C}$ provided $\mathfrak{B}/C_{\mathfrak{B}}(\mathfrak{X})$ is a subgroup of the stability group of $\mathscr{C}$.

By a *character* of $\mathfrak{X}$ we always mean a complex character of $\mathfrak{X}$ unless this is precluded by the context. A *linear character* is a character of degree one. An *integral linear combination* of characters is a linear combination of characters whose coefficients are rational integers. Such an integral linear combination is called a *generalized character*. If $\mathscr{S}$ is a collection of generalized characters of a group, let $\mathscr{I}(\mathscr{S})(\mathscr{C}(\mathscr{S}))$ be respectively the set of all integral (complex) linear combinations of elements in $\mathscr{S}$. Let $\mathscr{I}_0(\mathscr{S})$, $\mathscr{C}_0(\mathscr{S})$ be the subsets of $\mathscr{I}(\mathscr{S})$, $\mathscr{C}(\mathscr{S})$ respectively consisting of all elements α with $\alpha(1) = 0$.

If α and β are complex valued class functions on $\mathfrak{X}$, then the inner product and weight are denoted by

$$(\alpha, \beta)_{\mathfrak{X}} = \frac{1}{|\mathfrak{X}|} \sum_{X \in \mathfrak{X}} \alpha(X)\overline{\beta(X)}\,,$$

$$\|\alpha\|_{\mathfrak{X}}^2 = (\alpha, \alpha)_{\mathfrak{X}}\,.$$

The subscript $\mathfrak{X}$ is dropped in cases where it is clear from the context which group is involved.

The principal character of $\mathfrak{X}$ is denoted by $1_{\mathfrak{X}}$; the character of the regular representation of $\mathfrak{X}$ is denoted by $\rho_{\mathfrak{X}}$. If α is a complex valued class function of a subgroup $\mathfrak{H}$ of $\mathfrak{X}$, then α^* denotes the class function of $\mathfrak{X}$ induced by α.

The *kernel of a character* is the kernel of the representation with the given character.

A generalized character is *n-rational* if the field of its values is linearly disjoint from $\mathscr{Q}_n$.

A subset $\mathfrak{A}$ of the group $\mathfrak{X}$ is said to be a *trivial intersection set in* $\mathfrak{X}$, or a *T.I. set in* $\mathfrak{X}$ if and only if for every X in $\mathfrak{X}$, either

$$X^{-1}\mathfrak{A}X \cap \mathfrak{A} \subseteq \{1\}$$

or

$$X^{-1}\mathfrak{A}X = \mathfrak{A} .$$

If $\mathfrak{H}$ is a normal subgroup of the group $\mathfrak{X}$ and θ is a character of $\mathfrak{H}$, $\mathfrak{I}(\theta)$ denotes the *inertial group* of θ, that is

$$\mathfrak{I}(\theta) = \{X \mid X \in \mathfrak{X}, \theta(X^{-1}HX) = \theta(H) \quad \text{for all} \quad H \in \mathfrak{H}\} .$$

Clearly, $\mathfrak{H} \subseteq \mathfrak{I}(\theta)$ for all characters θ of $\mathfrak{H}$.

A group $\mathfrak{X}$ is a *Frobenius group* with *Frobenius kernel* $\mathfrak{H}$ if and only if $\mathfrak{H}$ is a proper normal subgroup of $\mathfrak{X}$ which contains the centralizer of every element in $\mathfrak{H}^\#$. It is well known (see 3.16) that the Frobenius kernel $\mathfrak{H}$ of $\mathfrak{X}$ is also characterized by the conditions

1. $\mathfrak{H} \lhd \mathfrak{X}, 1 \subset \mathfrak{H} \subset \mathfrak{X}$.
2. $\mathfrak{I}(\theta) = \mathfrak{H}$ for every non principal irreducible character θ of $\mathfrak{H}$.

We say that $\mathfrak{X}$ is of *Frobenius type* if and only if the following conditions are satisfied:

(i) If $\mathfrak{H}$ is the maximal normal nilpotent S-subgroup of $\mathfrak{X}$, then $1 \subset \mathfrak{H} \subset \mathfrak{X}$.

(ii) If $\mathfrak{E}$ is a complement for $\mathfrak{H}$ in $\mathfrak{X}$, then $\mathfrak{E}$ contains a normal abelian subgroup $\mathfrak{A}$ such that $\mathfrak{I}(\theta) \cap \mathfrak{E} \subseteq \mathfrak{A}$ for every non principal irreducible character θ of $\mathfrak{H}$.

(iii) $\mathfrak{E}$ contains a subgroup $\mathfrak{E}_0$ of the same exponent as $\mathfrak{E}$ such that $\mathfrak{E}_0\mathfrak{H}$ is a Frobenius group with Frobenius kernel $\mathfrak{H}$.

In case $\mathfrak{X}$ is of Frobenius type, the maximal normal nilpotent S-subgroup of $\mathfrak{X}$ will be called the *Frobenius kernel* of $\mathfrak{X}$.

A group $\mathfrak{S}$ is a *three step group* if and only if

(i) $\mathfrak{S} = \mathfrak{S}'\mathfrak{Q}^*$, where $\mathfrak{Q}^*$ is a cyclic S-subgroup of $\mathfrak{S}$, $\mathfrak{Q}^* \neq 1$, and $\mathfrak{S}' \cap \mathfrak{Q}^* = 1$.

(ii) $\mathfrak{S}$ contains a non cyclic normal S-subgroup $\mathfrak{H}$ such that $\mathfrak{S}'' \subseteq \mathfrak{H}C(\mathfrak{H}) \subseteq \mathfrak{S}'$, $\mathfrak{H}C(\mathfrak{H})$ is nilpotent and $\mathfrak{H}$ is the maximal normal nilpotent S-subgroup of $\mathfrak{S}$.

(iii) $\mathfrak{H}$ contains a cyclic subgroup $\mathfrak{H}^* \neq 1$ such that for Q in $\mathfrak{Q}^{*\#}$, $C_{\mathfrak{S}'}(Q) = \mathfrak{H}^*$.

3. Quoted Results

For convenience we single out various published results which are of use.

3.1. ([19] *Lemma* 1, *Three subgroups lemma*). *If* $\mathfrak{H}, \mathfrak{K}, \mathfrak{L}$ *are subgroups of the group* $\mathfrak{X}$ *and*

$$[\mathfrak{H}, \mathfrak{K}, \mathfrak{L}] = [\mathfrak{K}, \mathfrak{L}, \mathfrak{H}] = 1, \quad \textit{then } [\mathfrak{L}, \mathfrak{H}, \mathfrak{K}] = 1 .$$

3.2. [20] $F(\mathfrak{X}) = \cap C_{\mathfrak{X}}(\mathfrak{D})$, *the intersection being taken over all chief factors* $\mathfrak{D}$ *of the group* $\mathfrak{X}$.

3.3. [20] *If* $\mathfrak{X}$ *is solvable, then* $C(F(\mathfrak{X})) = Z(F(\mathfrak{X}))$.

3.4. *Let* p *be an odd prime and* $\mathfrak{X}$ *a* p*-group. If every normal abelian subgroup of* $\mathfrak{X}$ *is cyclic, then* $\mathfrak{X}$ *is cyclic. If every normal abelian subgroup of* $\mathfrak{X}$ *is generated by two elements, then* $\mathfrak{X}$ *is isomorphic to one of the following groups*:

(i) *a central product of a cyclic group and the non abelian group of order* p^3 *and exponent* p.

(ii) *a metacyclic group.*

(iii) $gp\langle A, B \mid [B, A] = C, [C, A] = B^{rp^{n-1}}, C^p = [B, C] = A^p = B^{p^n} = 1, n > 1, (r, p) = 1\rangle$.

(iv) *a* 3*-group.*

A proof of this result, together with a complete determination of the relevant 3-groups, can be found in the interesting papers [1] and [2].

3.5. [20] *If* $\mathfrak{X}$ *is a non abelian* p*-group,* p *is odd, and if every characteristic abelian subgroup of* $\mathfrak{X}$ *is cyclic, then* $\mathfrak{X}$ *is a central product of a cyclic group and an extra special group of exponent* p.

3.6. ([22] *Hilfssatz* 1.5). *If* σ *is a* p'*-automorphism of the* p*-group* $\mathfrak{X}$, p *is odd, and* σ *acts trivially on* $\Omega_1(\mathfrak{X})$, *then* $\sigma = 1$.

3.7. [20] *If* $\mathfrak{A}$ *and* $\mathfrak{B}$ *are subgroups of a larger group, then* $[\mathfrak{A}, \mathfrak{B}] \lhd \langle\mathfrak{A}, \mathfrak{B}\rangle$.

3.8. *If the* S_p*-subgroup* $\mathfrak{P}$ *of the group* $\mathfrak{X}$ *is metacyclic, and if* p *is odd, then* $\mathfrak{P} \cap O^p(\mathfrak{X})$ *is abelian.*

This result is a consequence of ([23] Satz 1.5) and the well known fact that subgroups of metacyclic groups are metacyclic.

3.9. [28] *If* $\mathfrak{A}$ *is a normal abelian subgroup of the nilpotent group* $\mathfrak{X}$ *and* $\mathfrak{A}$ *is not a proper subgroup of any normal abelian subgroup of* $\mathfrak{X}$, *then* $\mathfrak{A}$ *is self centralizing.*

3.10. *If* $\mathfrak{P}$ *is a* S_p*-subgroup of the group* $\mathfrak{X}$, *and* $\mathfrak{A} \in \mathscr{SCN}(\mathfrak{P})$, *then* $C(\mathfrak{A}) = \mathfrak{A} \times \mathfrak{D}$ *where* $\mathfrak{D}$ *is a* p'*-group.* The proof of Lemma 5.7 in [27] is valid for all finite groups, and yields the preceding statement.

3.11. *Let* $\mathfrak{A}$ *and* $\mathfrak{B}$ *be subgroups of a group* $\mathfrak{X}$, *where* $\mathfrak{A}$ *is a* p*-group and* $\mathfrak{B}$ *is a* p'*-group normalized by* $\mathfrak{A}$. *Suppose* $\mathfrak{A}_1$ *is a subgroup of* $\mathfrak{A}$ *which does not centralize* $\mathfrak{B}$. *If* $\mathfrak{B}_1$ *is a subgroup of* $\mathfrak{B}$ *of least order subject to being normalized by* $\mathfrak{A}$ *and not centralized by* $\mathfrak{A}_1$, *then* $\mathfrak{B}_1$ *is a special* q*-group for some prime* q, $\mathfrak{A}_1$ *acts trivially on* $D(\mathfrak{B}_1)$ *and* $\mathfrak{A}$ *acts irreducibly on* $\mathfrak{B}_1/D(\mathfrak{B}_1)$. This statement is a paraphrase of Theorem C of Hall and Higman [21].

3.12. ([3] *Lemma* 1). *Let* A *be a nonsingular matrix and let* σ *be a permutation of the elements of* A. *Suppose that* $\sigma(A)$ *can be derived from* A *by permuting the columns of* A *and* $\sigma(A)$ *can also be derived from* A *by permuting the rows of* A. *Then the number of rows left fixed by* σ *is equal to the number of columns left fixed by* σ.

The next two results follow from applying 3.12 to the character table of a group $\mathfrak{X}$.

3.13 (*Burnside*). *A group of odd order has no non principal real valued irreducible characters.*

3.14. *If* σ *is an automorphism of the group* $\mathfrak{X}$ *then the number of irreducible characters fixed by* σ *is equal to the number of conjugate classes fixed by* σ.

3.15. ([8] *Lemma* 2.1). *Let* $\mathfrak{P}$ *be a* p*-group for some prime* p *and let* θ *be an irreducible character of* $\mathfrak{P}$ *with* $\theta(1) > 1$. *Then* $\Sigma\theta_i(1)^2 \equiv 0 \pmod{\theta(1)^2}$, *where the summation ranges over all irreducible characters* θ_i *of* $\mathfrak{P}$ *with* $\theta_i(1) < \theta(1)$.

Let $\mathfrak{L}$ *be a Frobenius group with Frobenius kernel* $\mathfrak{H}$. *Then*

3.16. (i). ([7], [26]). $\mathfrak{H}$ *is a nilpotent* S*-subgroup of* $\mathfrak{L}$ *and* $\mathfrak{L}$ $\mathfrak{H}\mathfrak{E}$ *for some subgroup* $\mathfrak{E}$ *of* $\mathfrak{L}$ *with* $\mathfrak{H} \cap \mathfrak{E} = 1$.

3.16. (ii). ([4] *p.* 334). *If* p, q *are primes then every subgroup of* $\mathfrak{E}$ *of order* pq *is cyclic. If* $p \neq 2$ *then a* S_p*-subgroup of* $\mathfrak{E}$ *is cyclic.*

3.16. (iii). ([7] *Lemma* 2.1 *or* [10] *Lemma* 2.1). *A non principal irreducible character of* $\mathfrak{H}$ *induces an irreducible character of* $\mathfrak{L}$. *Furthermore every irreducible character of* $\mathfrak{L}$ *which does not have* $\mathfrak{H}$ *in its kernel is induced by a character of* $\mathfrak{H}$. *Thus in particular any complex representation of* $\mathfrak{L}$, *which does not have* $\mathfrak{H}$ *in its kernel,* *contains the regular representation of* $\mathfrak{E}$ *as a constituent when restricted to* $\mathfrak{E}$.

We will often use the fact that the last sentence of 3.16 (iii) is valid if "complex representation of $\mathfrak{L}$" is replaced by "representation of $\mathfrak{L}$ over a field of characteristic prime to $|\mathfrak{L}|$".

4. Elementary Results

LEMMA 4.1. *Let* $\mathfrak{X}$ *be a group with center* $\mathfrak{Z}$ *and let* λ *be an irreducible character of* $\mathfrak{X}$. *Then* $\lambda(1)^2 \leqq |\mathfrak{X} : \mathfrak{Z}|$.

Proof. For $Z \in \mathfrak{Z}$, $|\lambda(Z)| = \lambda(1)$. Therefore

$$|\mathfrak{X}| \geqq \Sigma_{\mathfrak{Z}} |\lambda(Z)|^2 = |\mathfrak{Z}|\lambda(1)^2$$

LEMMA 4.2. *Let* α *be a generalized character of the group* $\mathfrak{X}$. *Suppose that* R, X *are commuting elements of* $\mathfrak{X}$ *and the order of* R *is a power of a prime* r. *Let* $\mathscr{F}$ *be an algebraic number field which contains the* $|\mathfrak{X}|$th *roots of unity and let* $\mathfrak{r}$ *be a prime ideal in the ring of integers of* $\mathscr{F}$ *which divides* r. *Then*

$$\alpha(RX) \equiv \alpha(X) \pmod{\mathfrak{r}} .$$

Proof. It is clearly sufficient to prove the result for a generalized character, and thus for every irreducible character, of the abelian group $\langle R, X\rangle$. If α is an irreducible character of $\langle R, X\rangle$ then $\alpha(RX) = \alpha(R)\alpha(X)$ and $\alpha(R) \equiv 1 \pmod{\mathfrak{r}}$. This implies the required congruence.

LEMMA 4.3. *Let* $\mathfrak{H}$ *be a normal subgroup of the group* $\mathfrak{X}$ *and let* λ *be an irreducible character of* $\mathfrak{X}$ *which does not contain* $\mathfrak{H}$ *in its kernel. If* $X \in \mathfrak{X}$ *and* $C(X) \cap \mathfrak{H} = \langle 1\rangle$, *then* $\lambda(X) = 0$.

Proof. Let $\mu_1, \mu_2, \cdots$ be all the irreducible characters of $\mathfrak{X}/\mathfrak{H} = \bar{\mathfrak{X}}$. Let $\lambda_1, \lambda_2, \cdots$ be all the remaining irreducible characters of $\mathfrak{X}$. If $C(X) \cap \mathfrak{H} = \langle 1\rangle$, then $C(X)$ is mapped isomorphically into $C(\bar{X})$ where $\bar{X}$ is the image of X in $\bar{\mathfrak{X}}$. Consequently

$$\Sigma_i |\mu_i(X)|^2 = |C(\bar{X})| \geqq |C(X)| = \Sigma_i |\mu_i(X)|^2 + \Sigma_i |\lambda_i(X)|^2 .$$

This yields the required result.

Lemma 4.3 is of fundamental importance in this paper.

LEMMA 4.4. *Let* $\mathfrak{H}$ *be a normal subgroup of the group* $\mathfrak{X}$. *Assume that if* θ *is any nonprincipal irreducible character of* $\mathfrak{H}$ *then* θ^* *is* *a sum of irreducible characters of $\mathfrak{X}$, all of which have the same degree and occur with the same multiplicity in θ^*. For any integer d let ξ_d be the sum of all the irreducible characters of $\mathfrak{X}$ of degree d which do not have $\mathfrak{H}$ in their kernel. Then $\xi_d = a\gamma^*$, where a is a rational number and γ is a generalized character of $\mathfrak{H}$.*

Proof. Let $\theta_1^*, \theta_2^*, \cdots$ be all the distinct characters of $\mathfrak{X}$ which are induced by non principal irreducible characters of $\mathfrak{H}$ and which are sums of irreducible characters of $\mathfrak{X}$ of degree d. Suppose that $\theta_i^* = a_i\Sigma_j\lambda_{ij}$, where λ_{ij} is an irreducible character of $\mathfrak{X}$ for all values of j. It is easily seen that $\theta_1^*, \theta_2^*, \cdots$ form a set of pairwise orthogonal characters. Hence $\xi_d = \Sigma_i(1/a_i)\theta_i^*$. This proves the lemma.

If $\mathfrak{H}$ is a normal subgroup of the group $\mathfrak{X}$, $X \in \mathfrak{X}$, and φ is a character of $\mathfrak{H}$, then φ^X is defined by $\varphi^X(H) = \varphi(X^{-1}HX)$, $H \in \mathfrak{H}$.

LEMMA 4.5. *Let $\mathfrak{H}$ be a normal subgroup of the group $\mathfrak{X}$ and let θ be an irreducible character of $\mathfrak{H}$. Suppose $\mathfrak{X}$ contains a normal subgroup $\mathfrak{X}_0$ such that $\mathfrak{I}(\theta) \subseteq \mathfrak{X}_0$ and such that $\mathfrak{X}_0/\mathfrak{H}$ is abelian. Then θ^* is a sum of irreducible characters of $\mathfrak{X}$ which have the same degree and occur with the same multiplicity in θ^*. This common degree is a multiple of $|\mathfrak{X}:\mathfrak{I}(\theta)|$. If furthermore $\mathfrak{H}$ is a S-subgroup of $\mathfrak{X}_0$, then θ^* is a sum of $|\mathfrak{I}(\theta):\mathfrak{H}|$ distinct irreducible characters of degree $|\mathfrak{X}:\mathfrak{I}(\theta)|\theta(1)$.*

Proof. Let θ_1 be the character of $\mathfrak{I}(\theta) = \mathfrak{I}$ induced by θ. Let λ be an irreducible constituent of θ_1 and let $\mu_1, \mu_2, \cdots, \mu_m$ be all the irreducible characters of $\mathfrak{I}/\mathfrak{H}$. Choose the notation so that $\lambda\mu_i = \lambda$ if and only if $1 \leqq i \leqq n$. Since $\theta_{1|\mathfrak{H}} = |\mathfrak{I}:\mathfrak{H}|\theta$, we get that $\lambda_{|\mathfrak{H}} = a\theta$ for some integer a. Thus,

$$\sum_{j=1}^{m} \lambda\mu_j = a\theta_1 . \tag{4.1}$$

Hence, every irreducible constituent of $a\theta_1$ is of the form $\lambda\mu_j$, so all irreducible constituents of θ_1 have the same degree. The characters $\mu_1, \mu_2, \cdots$ form a group $\mathfrak{M}$ which permutes the irreducible constituents of $a\theta_1$ transitively by multiplication. Hence for every value of j there are exactly n values of i such that $\lambda\mu_j\mu_i = \lambda\mu_j$. If now $\lambda_1, \lambda_2, \cdots,$ are the distinct irreducible characters which are constituents of $a\theta_1$, then (4.1) implies that $a\theta_1 = n\Sigma\lambda_i$.

Suppose $\mathfrak{A}$ is a complement to $\mathfrak{H}$ in $\mathfrak{I}$, $\mathfrak{H}$ being a S-subgroup of $\mathfrak{I}$. We must show that θ_1 is a sum of $|\mathfrak{A}|$ distinct irreducible characters of $\mathfrak{I}$. For any subgroups $\mathfrak{K}_1, \mathfrak{K}$ of $\mathfrak{I}$ with $\mathfrak{H} \subseteq \mathfrak{K}_1 \subseteq \mathfrak{K}$, and any character φ of $\mathfrak{K}_1$, let $\varphi^{\mathfrak{K}}$ denote the character of $\mathfrak{K}$ induced by φ.

Suppose $\mathfrak{K}$ has the property that $\theta^{\mathfrak{K}}$ is a sum of $|\mathfrak{K}:\mathfrak{H}|$ distinct irreducible characters of $\mathfrak{K}$, where $\mathfrak{H} \subseteq \mathfrak{K} \subseteq \mathfrak{I}$. Let $\mathfrak{M}_{\mathfrak{K}}$ be the multiplicative group of linear characters of $\mathfrak{K}$ which have $\mathfrak{H}$ in their kernel, and let $\lambda_{\mathfrak{K}}$ be an irreducible constituent of $\theta^{\mathfrak{K}}$. Then $\lambda_{\mathfrak{K}}(1) = \theta(1)$ is prime to $|\mathfrak{A} \cap \mathfrak{K}|$, and it follows from Lemma 4.2 that $\lambda_{\mathfrak{K}}$ does not vanish on any element of $\mathfrak{A} \cap \mathfrak{K}$ of prime power order. This in turn implies that

$$\theta^{\mathfrak{K}} = \sum_{\mu \in \mathfrak{M}_{\mathfrak{K}}} \lambda_{\mathfrak{K}}\mu \, .$$

If $\mathfrak{K} = \mathfrak{I}$, we are done. Otherwise, let $\mathfrak{L}$ contain $\mathfrak{K}$ as a subgroup of prime index. It suffices to show that $\lambda_{\mathfrak{K}}^{\mathfrak{L}}$ is reducible, or equivalently, that $\lambda_{\mathfrak{K}}^{L} = \lambda_{\mathfrak{K}}$ for every L in $\mathfrak{L}$. This is immediate, since $(\theta^{\mathfrak{K}})^{L} = \theta^{\mathfrak{K}}$, so that $\lambda_{\mathfrak{K}}^{L} = \lambda_{\mathfrak{K}}\mu$ for some μ in $\mathfrak{M}_{\mathfrak{K}}$. Since $\mathfrak{A}$ is abelian, it follows that $\mu = 1$, as required.

To complete the proof of the lemma (now that the necessary properties of $\mathfrak{I}$ have been established), it suffices to show that if

$$\theta_1 = b\Sigma_i\lambda_i \, ,$$

where the λ_i are distinct irreducible characters of $\mathfrak{I}$, then each $\lambda_i^{\mathfrak{X}_0}$ is irreducible, and $\lambda_i^{\mathfrak{X}_0} \neq \lambda_j^{\mathfrak{X}_0}$ for $\lambda_i \neq \lambda_j$. For if this is proved, the normality of $\mathfrak{X}_0$ in $\mathfrak{X}$ implies the lemma. The definition of $\mathfrak{I}$ implies that $\lambda_{i|\mathfrak{I}}^{\mathfrak{X}_0}$ is a sum of $|\mathfrak{X}_0 : \mathfrak{I}|$ distinct irreducible characters of $\mathfrak{I}$. Furthermore, λ_i is the only irreducible constituent of $\lambda_{i|\mathfrak{I}}^{\mathfrak{X}_0}$ whose restriction to $\mathfrak{H}$ is not orthogonal to θ. Thus, if $\lambda_i^{\mathfrak{X}_0} = \lambda_j^{\mathfrak{X}_0}$, then $\lambda_i = \lambda_j$. Since $\lambda_i^{\mathfrak{X}_0}$ vanishes outside $\mathfrak{I}$, a simple computation yields that $\|\lambda_i^{\mathfrak{X}_0}\|^2 = 1$. Therefore $\lambda_i^{\mathfrak{X}_0}$ is irreducible. The proof is complete.

LEMMA 4.6. *Let p be an odd prime and let $\mathfrak{P}$ be a normal S_p-subgroup of the group $\mathfrak{P}\mathfrak{H}\mathfrak{E}$. Assume that $\mathfrak{H}\mathfrak{E}$ is a Frobenius group with Frobenius kernel $\mathfrak{H}$, $\mathfrak{H}\mathfrak{E}$ is a p'-group and $\mathfrak{H} \cap \mathfrak{E} = 1$.*

(i) *If $C_{\mathfrak{P}}(\mathfrak{E}) = 1$, then $\mathfrak{H} \subseteq C(\mathfrak{P})$.*

(ii) *If $C_{\mathfrak{P}}(E)$ is cyclic for all elements $E \in \mathfrak{E}^{\#}$, then $|\mathfrak{E}|$ is a prime or $\mathfrak{H} \subseteq C(\mathfrak{P})$.*

(iii) *If $1 \neq C_{\mathfrak{P}}(\mathfrak{H}) \subseteq C_{\mathfrak{P}}(\mathfrak{E})$, then either $\mathfrak{P}$ is cyclic or $C_{\mathfrak{P}}(\mathfrak{E})$ is not cyclic.*

Proof. $\mathfrak{H}\mathfrak{E}$ is represented on $\mathfrak{P}/D(\mathfrak{P})$. Suppose that $\mathfrak{H} \not\subseteq C(\mathfrak{P})$. By 3.16 (iii) $\mathfrak{E}$ has a fixed point on $\mathfrak{P}/D(\mathfrak{P})$, and thus on $\mathfrak{P}$. This proves (i). If $|\mathfrak{E}|$ is not a prime, let $1 \subset \mathfrak{E}_0 \subset \mathfrak{E}$. Then 3.16 (iii) implies that $\mathfrak{E}_0$ has a non-cyclic fixed point set on $\mathfrak{P}/D(\mathfrak{P})$, and thus on $\mathfrak{P}$. This proves (ii).

As for (iii), let k be the largest integer such that $\mathfrak{H}$ has a non trivial fixed point on $Z_k(\mathfrak{P})/Z_{k-1}(\mathfrak{P})$. It follows that $\mathfrak{H}$ has a non trivial fixed point on $Z_k(\mathfrak{P})/D(Z_k(\mathfrak{P}))$. If $Z_k(\mathfrak{P})$ is not cyclic then since $\mathfrak{H}\mathfrak{E}$ is completely reducible on $Z_k(\mathfrak{P})/D(Z_k(\mathfrak{P}))$ (i) implies (iii) by 3.16 (iii). Suppose that $Z_k(\mathfrak{P})$ is cyclic. If $k \geqq 2$, then by [10] Lemma 1.4, $\mathfrak{P}$ is cyclic. Since $Z_2(\mathfrak{P})$ is of class 1 or 2, $\Omega_1(Z_2(\mathfrak{P}))$ is of exponent p. As $Z_2(\mathfrak{P})$ is not cyclic neither is $\Omega_1(Z_2(\mathfrak{P}))$. Thus it may be assumed that $\mathfrak{P} = \Omega_1(Z_2(\mathfrak{P}))$ is non cyclic of exponent p and class at most 2. If $\mathfrak{P}$ is abelian then (iii) follows from (i). If $\mathfrak{P}$ is of class 2 then by (i) $\mathfrak{E}$ has a fixed point on $\mathfrak{P}/\mathfrak{P}'$ and on $\mathfrak{P}'$. As $\mathfrak{P}$ has exponent p this implies that $C_{\mathfrak{P}}(\mathfrak{E})$ is not cyclic as required.

5. Numerical Results

In this section we state some elementary number theoretical results and some inequalities. The inequalities can all be proved by the methods of elementary calculus and their proof is left to the reader.

LEMMA 5.1. *If p, q are primes and*

$$p \equiv 1 \pmod q\,, \qquad q^3 \equiv 1 \pmod p$$

then $p = 1 + q + q^2$.

Proof. Let $p = 1 + nq$. Since $p > q$, $q \not\equiv 1 \pmod p$. Hence

$$1 + q + q^2 = mp\,.$$

Reading $(\bmod q)$ yields $m = 1 + rq$. Therefore

$$1 + q + q^2 = 1 + (r + n)q + rnq^2\,.$$

If $r \neq 0$ then the right hand side of the previous equation is strictly larger than the left hand side. Thus $r = 0$ as required.

The first statement of the following lemma is proved in [5]. The second can be proved in a similar manner.

LEMMA 5.2. *Let p, q be odd primes and let $n \geqq 1$.*

(i) *If q^m divides $(p^n - 1)(p^{n-1} - 1) \cdots (p - 1)$ then $q^m < p^n$.*

(ii) *If q^m divides $(p^{2n} - 1)(p^{2(n-1)} - 1) \cdots (p^2 - 1)$ then $q^m < p^{2n-1}$.*

If $x \geqq 5$, then

$$3^{x-2} > x^2\,, \tag{5.1}$$

$$5^{x-1} > 80x\,, \tag{5.2}$$

$$3^x x > 20(2x^2 + 1)\,. \tag{5.3}$$

If $x \geqq 7$, then

$$3^{x-2} > 2x^2\,, \tag{5.4}$$

$$3^x - 3 > 28x^2 , \tag{5.5}$$

$$7^x > 4x^2 \cdot 3^x + 1 . \tag{5.6}$$

$$5^x > 4x^2 3^x + 1 \quad \text{for } x \geqq 13 . \tag{5.7}$$

$$(x^y - 1) - (x - 1)y - \frac{(x-1)^3}{4} > 0 \quad \text{for } x, y \geqq 3 . \tag{5.8}$$

$$x^y - 1 > 4y^2 \quad \text{for } x \geqq 3,\ y \geqq 5, \text{ or } x \geqq 5, y \geqq 3 . \tag{5.9}$$

$$x^{y-2} > y^2 \quad \text{for } x \geqq 3,\ y \geqq 5 \text{ or } x \geqq 10,\ y \geqq 3 . \tag{5.10}$$

$$\frac{y^x - 1}{y - 1} > \frac{x^y - 1}{x - 1} \quad \text{for } x > y \geqq 3 . \tag{5.11}$$

$$y^2 \frac{(y^{x-1} - 1)}{y - 1} > x^2 \frac{(x^{y-1} - 1)}{x - 1} \quad \text{for } x > y \geqq 3 . \tag{5.12}$$