FINITE GROUPS WITH ALL MAXIMAL SUBGROUPS OF PRIME OR PRIME SQUARE INDEX

Thesis by

Joseph Kohler

In Partial Fulfillment of the Requirements
For the Degree of
Doctor of Philosophy

California Institute of Technology
Pasadena, California
1962

ACKNOWLEDGMENTS

I wish to express my appreciation to my advisor Professor Marshall Hall Jr. for his interest, guidance and patience throughout my career as a student.

I am grateful to the California Institute of Technology for assistanceships and to the National Science Foundation for a fellowship.

Special thanks are due to Dr. C. Wright and Dr. S. Golomb for their involvement and encouragement in the writing of this work.

ABSTRACT

In this thesis finite groups whose maximal subgroups are of prime or prime square index are studied. The main problem considered is to find out to what extent this property is inherited by subgroups. The principal results are: this property is inherited by all subgroups if the group considered has odd order. This is not necessarily true if the group has even order. Let n be a positive integer. A group G of even order is constructed which contains a subgroup H, and H contains a maximal subgroup W with $|H:W|$ larger than n.

I. INTRODUCTION

The object of this thesis is to investigate finite groups all of whose maximal subgroups are of prime or prime square index.

A short but ingenious arithmetic argument was given by P. Hall which showed that groups with the above property are solvable.

B. Huppert proved that a finite group all of whose maximal subgroups are of prime index is supersolvable. We recall that a supersolvable group is a group in which all of the chief factors are of prime order. The essence of Huppert's theorem is that if all maximal subgroups of a group G are of prime index, then this property is inherited by all subgroups of G.

Let G be a group all of whose maximal subgroups are of prime or prime square index. We shall prove that all subgroups of G inherit this property, if G has odd order. In case the order of G is even, this need not be true. In fact, given a positive integer n, we shall construct a G of order $2^a p^b$, where p is any odd prime, such that G contains a subgroup and this subgroup in turn contains a maximal subgroup of index greater than n. This is done in section V.

II. NOTATIONS, DEFINITIONS AND RESULTS FROM THE LITERATURE

The following is a list of notations which will be used:

$|G|$ = the order of G; $H \leqslant G$ means H is a subgroup of G, here $H = G$ is permitted; $H < G$ means H is a subgroup of G, but $H \neq G$; $H \trianglelefteq G$ means H is a normal subgroup of G, possibly $H = G$; $H \triangleleft G$ means H is a normal subgroup of G, but $H \neq G$; $Z(G)$ = the center of G; $\phi(G)$ = Frattini subgroup of G; $\Delta(G)$ = the intersection of the non-normal maximal subgroups of G; $r_p(G)$ = the p-rank of the solvable group G; $GL(2, p)$ = the group of all non-singular 2×2 matrices with entries in the field of p elements; $<A, B>$ = the group generated by A and B where A and B are subsets of a group G; J_p = the field with p elements.

A detailed discussion of the Frattini subgroup $\phi(G)$ can be found in Ref. 1. The remaining terms with the exception of p-rank are clear. The definition of p-rank is given below.

The following is a list of definitions which will be used:

Let p be a prime which divides the order of the solvable group G. Suppose that among the chief factors of G, which have order a power of p, the exponent s is the largest one which occurs. Then s is the p-rank of G and is denoted by $r_p(G)$. It is possible that G has several chief factors of order p^s.

A group G is said to have an ordered Sylow tower if it possesses a series

$$G = G_1 \triangleright G_2 \triangleright \dots \triangleright G_s \triangleright G_{s+1} = 1$$

with G_i/G_{i+1} of order $p_i^{s_i}$, where $p_1 < p_2 < \dots < p_s$ and $p_i^{s_i}$ is the highest power of p_i which divides $|G|$.

Let G be a group of all whose maximal subgroups are of prime or prime square index. **We** shall say that G has <u>property M</u>.

The results from the literature not found in the standard texts are:

2. a. Let G be solvable. Let p^{j_p} be the highest power of p which occurs as an index in some maximal chain of subgroups of G. Then $j_p = r_p(G)$ ((3) pg. 411).

2. b. If N is a normal subgroup of G and A a subgroup of G such that $N \leqslant \phi(A)$, then $N \leqslant \phi(G)$ ((4) pg. 162).

2. c. In a group G the subgroup $\Delta(G)$ is nilpotent ((4) pg 167).

III. THE MAIN THEOREMS

Let G be a group with property M. By Theorem 10. 5. 7 of Ref. 1 G is solvable. The proof of this theorem yields more information than just the solvability of G. This we state as

Theorem 3. 1. (P. Hall) Let G be a group with property M. Then there exists a series $G \trianglerighteq K \trianglerighteq 1$ with $|K|$ prime to 6, $|G/K| = 2^a 3^b$ and K has an ordered Sylow tower.

Proof: See the proof of Theorem 10. 5. 7 of Ref. 1.

If 2 does not divide $|G|$ in the above theorem, then G has an ordered Sylowtower. The same is true if 3 does not divide the order of G.

Lemma 3. 1. Let K be a subgroup of GL(2, p) which has odd order and order prime to p, with $p > 3$. Then K is abelian.

Proof: The group GL(2, p) has a normal subgroup G of index 2 consisting of those matrices whose determinant is a square. We observe that $G \geqslant K$ and $G \geqslant Z$, the center of GL(2, p) consisting of all scalar multiples of the identity.

A list of subgroups of G/Z can be found in Ref. 2 on pages 447-450. The subgroups of odd order and order prime to p are cyclic and have order a divisor of $p + 1$ or $p - 1$. Thus KZ/Z is cyclic, and hence KZ is abelian. This implies that K is abelian.

Lemma 3. 2. Let G be a finite subgroup of the multipliative group of a field F. Then G is cyclic.

Proof: Clearly G is abelian. Suppose G is of exponent n. Then every element of G is a root of $x^n - 1 = 0$. But the roots of this equation form a cyclic group. Since G is a subgroup of this group it follows that G is cyclic.

Lemma 3. 3. Let G be an abelian group, and let ρ be an irreducible representation of G over the field F. Then $\rho(G)$ is cyclic.

Proof: Let A be an $F - G$ module which yields the representation ρ. Then A is irreducible. By Schur's Lemma (Theorem 16. 6. 2 on p. 269 of Ref. 1) the ring of operator endomorphisms of A forms a division ring. This division ring is isomorphic to the ring of $n \times n$ matrices whose elements α satisfy

$$\rho(x)\alpha = \alpha\rho(x)$$

for every x in G (Corollary 16. 6. 1 on p. 268 of Ref. 1). But the matrices $\rho(x)$ for x in G are among the choices for α and are therefore in the center of this ring of endomorphisms. The center of a division ring is a field so that $\rho(G)$ is a subgroup of the multiplicative group of a field. Thus, by lemma 3. 2, $\rho(G)$ is cyclic.

Lemma 3. 4. Let G be an irreducible subgroup of $GL(2, p)$, which has odd order and order prime to p, with $p > 3$. Then G is cyclic, and its order is a divisor of $p^2 - 1$.

Proof: By lemma 3.1 G is abelian, and by lemma 3.3 G is cyclic. Suppose $<g> = G$. If the characteristic equation of g were reducible over J_p, then g would be similar to a diagonal matrix. This conflicts with our hypothesis.

Suppose $\psi(x)$ is the characteristic polynomial of g and is irreducible over J_p. Then $\psi(x)$ has degree 2. By Theorem 11 on p. 128 of Ref. 5, it follows that $\psi(x)$ is a divisor of

$$g(x) = x^{p^2} - x .$$

Hence $\psi(x)$ is also a divisor of $x^{p^2-1}-1$. By the Cayley-Hamilton theorem we must have

$$g^{p^2-1} - 1 = 0.$$

Thus

$$g^{p^2-1} = 1,$$

proving the lemma.

Lemma 3.5. Let G be a cyclic group whose order is a divisor of $p^2 - 1$. Then every irreducible representation of G over J_p has degree one or two.

Proof: Since $|G|$ is prime to p the representations we are concerned with are ordinary. Let $\rho(G)$ be an irreducible representation of G over J_p. Consider the matrix $A = \rho(g)$ where $G = <g>$.

We have

$$A^{p^2-1} = 1,$$

where A has entries in J_p and $\rho(G) = <A>$. The minimum polynomial of A is a divisor of $x^{p^2-1} - 1$ and hence also a divisor of $x^{p^2} - x$. Let $p(x)$ denote an irreducible polynomial over J_p which divides $x^{p^2} - x$. By Theorem 11 on p. 128 of Ref. 5, it follows that $p(x)$ has degree one or two. Thus the characteristic equation of A is a product of irreducible polynomials of degree one or two over J_p, since every irreducible polynomial which divides the characteristic polynomial also divides the minimum polynomial.

We may therefore write

$$|xI - A| = p_1(x) \ldots p_t(x)q_1(x) \ldots q_s(x) ,$$

where the $p_i(x)$ are monic irreducible polynomials of degree two over J_p and the $q_j(x)$ are of degree one over J_p.

Since the representations we are dealing with are ordinary, it follows that A is similar to a diagonal matrix over a suitable finite extension of J_p. We may write

$$A \overset{s}{=} \operatorname{diag}(\epsilon_1, \delta_1, \epsilon_2, \delta_2, \ldots, \epsilon_t, \delta_t, \gamma_1, \ldots, \gamma_s)$$

where ϵ_i, δ_i are the roots of $p_i(x)$ and γ_j is the root of $q_j(x)$. The elements $\gamma_1, \ldots, \gamma_s$ are in J_p but the ϵ_i and δ_i are not in J_p.

The matrix

$$A_i = \begin{pmatrix} 0 & 1 \\ -c_i & -b_i \end{pmatrix},$$

where $p_i(x) = x^2 + b_i x + c_i$ is similar to the matrix

$$\begin{pmatrix} \epsilon_i & 0 \\ 0 & \delta_i \end{pmatrix}$$

because they have the same invariant factors.

This implies A is similar to the matrix $A_1 \oplus \ldots \oplus A_t \oplus [\gamma_1] \oplus \cdots \oplus [\gamma_t]$. We note that ρ can be irreducible over J_p only if $t = 1$ and $s = 0$ or if $t = 0$ and $s = 1$. This proves the lemma.

Lemma 3.6. Let G be an abelian group of exponent dividing $p^2 - 1$ over the field J_p. Then every irreducible representation of G over J_p has degree one or two.

Proof: Let ρ be an irreducible representation of G over J_p. By lemma 3.3 the group $\rho(G)$ is cyclic and by our hypothesis $\rho(G)$ has order dividing $p^2 - 1$. This means $\rho(G)$ is an irreducible representation of a cyclic group whose order divides $p^2 - 1$. By lemma 3.5 we are done.

Theorem 3.2. Let G be a group of odd order which has property $\mathcal{M}$. Then $r_p(G) \leq 2$ for all primes p which divide the order of G.

Proof: Assume the theorem is false. Choose G to satisfy the hypothesis but not the conclusion and to be of minimal order subject to these conditions. Note that if N is any normal subgroup of G larger than the identity, then G/N satisfies the hypothesis and hence the conclusion because of the minimal nature of G.

If G contained two distinct minimal normal subgroups, say N_1

and N_2, then N_1 would be isomorphic to a chief factor of G/N_2 so that G would satisfy our conclusion, contrary to assumption. We may therefore assume that G contains only one minimal normal subgroup which we denote by N.

By Theorem 3.1 G has an ordered Sylow tower. Let P be a Sylow p-subgroup of G where p is the largest prime which divides $|G|$. The group P is normal in G and therefore contains N. Note that $p > 3$ since, if $p = 3$, G is a 3-group and would satisfy our conclusion.

Since $\phi(P)$ is a characteristic subgroup of P and P is normal in G, it follows that $\phi(P)$ is normal in G. Thus either $\phi(P) = 1$, or $\phi(P) \geqslant N$.

Let $1 = P_o \leqslant N_o < P_1 < \ldots < G$ be the upper p-series for G. Then $P_1 = P \times N_o$ since both N_o and P are normal in G. We must have $N_o = 1$, since otherwise G would contain more than one minimal normal subgroup, i.e. $P_1 = P$. By Theorem 18.4.5 (p. 333 of Ref. 1) G/P is faithfully represented by transformation on $P/\phi(P)$, and furthermore G/P has order prime to p.

Consider the case $\phi(P) = 1$. Then P may be regarded as a space on which G/P operates. Also N is a subspace of P.

Assume N is a proper subgroup of P. Then by the theorem of complete reducibility we can find a complement to N, i.e. $P = M \times N$ where M is not the identity and $M \lhd G$. This is a conflict, since M does not contain N.

Assume $P = N$. Then P is a minimal normal subgroup of G.

Since G is solvable it contains a p-complement M. Then $|G:M| = |P|$. Suppose M is not a maximal subgroup of G. Let T be a maximal subgroup of G between M and G. Then T has order divisible by p, and therefore has a non-trivial intersection with P. If $T \cap P$ were equal to P, then T would be all of G so that $1 < T \cap P < P$. Since P is abelian, $T \cap P \triangleleft P$. Also $T \cap P \triangleleft T$ and finally $T \cap P \triangleleft G$ which contradicts the fact that P is a minimal normal subgroup of G. Thus M is a maximal subgroup of G. By property M it follows that $|G:M| = p$ or p^2. Hence $|P| = p$ or p^2. This completes the proof for the case $\phi(P) = 1$.

Consider the case $\phi(P) \geqslant N$. Using the theorem of complete reducibility we may write

$$P/\phi(P) = S_1/\phi(P)x \ldots xS_t/\phi(P)$$

where each $S_i/\phi(P)$ is a space on which G/P operates irreducibly. Nɞte also that each $S_i/\phi(P)$ is a chief factor of $G/\phi(P)$. Since $\phi(P) \geqslant N$ it follows that each of the groups $S_i/\phi(P)$ has order p or p^2.

From lemma 3.4 G/P is isomorphic to a subdirect product of cyclic groups each with order dividing $p^2 - 1$ i.e. G/P is an abelian group with exponent dividing $p^2 - 1$.

Now consider the representation ρ of G on the group N. Since N is a minimal normal subgroup of G, ρ is irreducible over J_p. The group Z(P) is a characteristic subgroup of P not the identity and hence is normal in G. This implies $Z(P) \geqslant N$. Hence the representation of G on N contains P in its kernel. Thus the group $\rho(G)$ is a homomorphic image of G/P, and therefore $\rho(G)$ is an irreducible representation over J_p of an abelian group with exponent dividing $p^2 - 1$. By lemma 3. 6 $\rho(G)$ has degree one or two. This completes the proof of the theorem.

Theorem 3. 3. Let G be a group of odd order which has property M. Then all subgroups of G also have property M.

Proof: This is an immediate consequence of Theorem 3. 2 together with 2. a.

IV. FURTHER THEOREMS ABOUT GROUPS WITH PROPERTY M

Theorem 4.1. Let G be a group with property M. Then $G/\Delta(G)$ is a subdirect product of primitive solvable groups on a prime or prime square number of letters and $\Delta(G)$ is nilpotent.

Proof: Decompose the maximal subgroups of G into conjugate classes and represent G by conjugation on these classes of subgroups. This gives a permutation representation π of G where the sets of transitivity are just the sets of conjugate maximal subgroups. Consider the restriction of π to one of these sets. Let M be an element of this set. This restricted representation π^* is equivalent to that arising from the cosets of NM, the normalizer of M in G (p. 242 of Ref. 1).

The group NM is either M or G. If NM is G then the permutation representation π^* is just the identity. If NM = M then π^* is primitive since M is maximal and has degree $|G:M|$ which is a prime or the square of a prime. Since G is solvable the permutation representation π^* is solvable. This proves that G molulo the kernel of π is a subdirect product of primitive solvable groups on a prime or prime square number of letters.

We determine the kernel of π. An element x of G will be in the kernel of π if and only if it normalizes every maximal subgroup of G. A normal maximal subgroup of G has G for its normalizer and a non-normal maximal subgroup is its own normalizer. Hence x will normalize every maximal subgroup of G if and only if it is contained in the intersection $\Delta(G)$ of the non-normal maximal subgroups of G. This completes the proof of the theorem except for the nilpotency of $\Delta(G)$, which follows at once from 2.c.

A number of theorems dealing with primitive solvable permutation groups will be proved. These theorems are well known but will be convenient to have in the form given below.

In what follows Ω will denote a set of objects permuted by a group G. We shall also assume that the identity of G is the only element of G which fixes every element in Ω. The elements of Ω will be denoted by small Greek letters.

By the orbit under G of the element α in Ω we mean the set

$$\alpha^G = \{\alpha^g \mid g \in G\}$$

We denote the subgroup of G fixing α by G_α.

We shall use S_Ω to denote the group of all permutations on Ω.

Lemma 4.1. Let G be primitive on Ω and $N \trianglelefteq G$. Then N is transitive on Ω.

Proof: Let α^N, β^N, ... be the orbits of N. We first show that an element g of G permutes these orbits among themselves. Select α^N an orbit. Then

$$\begin{aligned}(\alpha^N)^g &= \alpha^{gg^{-1}Ng} \\ &= (\alpha^g)^N \\ &= \beta^N\end{aligned}$$

is an orbit of N. This shows that these orbits form sets of imprimitivity for G and hence there can be only one of them. Thus N is transitive on Ω.

Lemma 4. 2. Let A be transitive on Ω, C the centralizer of A in S_Ω and N the normalizer of A in S_Ω. Then an element of C which fixes an object in Ω must be the identity. Hence for α in Ω the group N_α is faithfully represented by the automorphisms it induces on A.

Proof: Let $\alpha \in \Omega$ such that $c \in C$ fixes α. Now $c = c^a$ for all a in A. We also have c^a fixing α^a for every a in A. Since A is transitive c fixes Ω.

Theorem 4. 2. Let G be primitive on Ω where Ω has $n > 1$ objects. If G is solvable then

i) there is exactly one minimal normal subgroup A of G.

ii) A is elementary abelian, transitive and regular.

iii) $n = p^k = |A|$ where p is a prime.

iv) $G/A \cong G_\alpha \cong$ to some group of automorphisms of A.

v) $G \leq N$ the normalizer of A in S_Ω.

vi) $G = G_\alpha A$ and $G_\alpha \cap A = 1$.

Proof: Let A be a minimal normal subgroup of G. Since G is solvable A is elementary abelian. A is transitive by lemma 4. 1 Select $\alpha \in \Omega$. Since A is contained in its centralizer C in S_Ω it follows that $A_\alpha \leq C_\alpha$. But lemma 4. 2 implies $C_\alpha = 1$ and hence $A_\alpha = 1$. This proves that A is regular. Hence $|A|$ equals the number of elements in Ω. But A is elementary abelian and thus of prime power order, say p^k.

Now

$$|G_\alpha A| = \frac{|G_\alpha||A|}{|A \cap G_\alpha|} = \frac{|G_\alpha||A|}{|A_\alpha|} = |G_\alpha||A| = |G_\alpha|n.$$

The degree of a transitive permutation group is equal to the index of the largest subgroup which fixes a letter. Thus $n = |G:G_\alpha|$ so that

$$|G_\alpha|n = |G_\alpha||G:G_\alpha| = |G|.$$

Hence $G_\alpha A = G$ and since $A_\alpha = 1$ it follows that $G_\alpha \cap A = 1$.

Now $G_\alpha/G_\alpha \cap A \cong G_\alpha A/A = G/A$ and since A is regular $G_\alpha \cap A = 1$. Hence $G/A \cong G_\alpha \leq N_\alpha$ where N is the normalizer of A in S_Ω. By lemma 4. 2 N_α is isomorphic to some group of automorphisms of A.

Assume there exists B a minimal normal subgroup of G different from A. Then $A \cap B = 1$. Consider (A, B). It is contained in both A and B so that $(A, B) = 1$. Thus A and B centralize each other. The group $D = \langle A, B\rangle$ also centralizes A and D is transitive on Ω since it contains A. Let α be an element of Ω and consider D_α. By lemma 4. 2 $D_\alpha = 1$ and hence $|D| = n$. But $|A| = n$ and hence $D = A$, a conflict, since $D \geq B$. This proves that A is the only minimal normal subgroup of G.

Let G be a primitive solvable group on 9 letters. Let A be the unique minimal normal subgroup of G which we know exists by part i) of Theorem 4. 2. By part ii) of Theorem 4. 2 we may, after suitably labeling the objects permuted, assume that A is generated by a and b where

$$a = (037)(142)(568)$$

$$b = (051)(364)(782) .$$

Let N be the normalizer of A in the symmetric group on $\Omega = \{0,1,\ldots,8\}$. Note that N is the normalizer of the regular representation of A and hence the holomorph of A. Thus by Theorem 6. 3. 2 of Ref. 1 the subgroup fixing 0 is isomorphic to the group of all automorphisms of A. This group is just the group of all non-singular 2 x 2 matrices with entries in GF(3) and hence of order 48. Thus $|N| = 432$.

By part v) of Theorem 4. 2 G is a subgroup of N. Note that N is itself a solvable group and that A is a chief factor of N. The remaining chief factors of N are also chief factors of N/A which is isomorphic with the group of all non-singular matrices over GF(3). This latter group modulo its center is of order 24 and is isomorphic to the symmetric group on 4 letters. Hence the chief factors of N are $2, 3, 2^2, 2, 3^2$.

Let G be a primitive solvable group on 4 letters. Then G is a subgroup of the symmetric group S on 4 letters which is itself solvable. The chief factors of S are $2, 3, 2^2$.

A primitive group G on 3 letters is a subgroup of the symmetric group on 3 letters and a primitive group on 2 letters is just cyclic of order 2.

Lemma 4.3. Let G be a primitive solvable group on a prime or prime square number of letters. Then for all primes p which divide $|G|$ we have $r_p(G) \leqslant 2$.

Proof: Let A denote the unique minimal normal subgroup of G. If $|A| = p$, a prime, then G/A is cyclic with order dividing $p-1$. Hence $r_q(G) = 1$ for all primes q which divide $|G|$.

Assume $|A| = p^2$ with $p > 3$. Then G/A is isomorphic to a solvable group of 2×2 matrices over $GF(p)$. Let T be any solvable group of 2×2 matrices with entries in $GF(p)$ where $p > 3$. Form the group $TZ = R$ where Z consists of all non-zero scalar multiples of the identity. The group R is solvable and the chief factors of T are among those of R. The group R has a normal series

$$R > R_1 > Z > 1$$

where R_1 consists of those elements R with determinant one. The group R_1/Z is a solvable subgroup of the group H defined on page 436 of Ref. 2. All of the possible subgroups of H are given in articles 325 and 326 of Ref. 2. The solvable groups S among these are:

1) S has a normal subgroup of order p which is its own centralizer.

2) S is cyclic.

3) S is dihedral of order $2d$ where S contains a normal cyclic

subgroup of order d.

4) S is isomorphic to the alternating group on 4 letters.

5) S is isomorphic to the symmetric group on 4 letters.

In 1) S has a normal series $S > P > 1$ where $|P| = p$ and S/P is isomorphic to a group of automorphisms of P. Hence S/P is cyclic with order dividing $p-1$. Hence $r_q(S) = 1$ for all primes q which divide $|S|$. For S cyclic we also have $r_q(S) = 1$ for all primes q which divide $|S|$. In 3) S has a normal series $S > D > 1$ where S/D has order 2 and D is cyclic. The group D has a series of characteristic subgroups each of prime index in the one above it. Hence $r_q(S) = 1$ for all primes which divide $|S|$. In 4) and 5) we have $r_q(S) = 1$ for $q \neq 2$ and $r_q(S) = 2$ for $q = 2$. Thus $r_q(R_1/Z) \leq 2$ in all cases. The groups R/R_1 and Z are cyclic so that $r_q(R) \leq 2$ for all primes q which divide $|R|$. The same also holds for T.

For $p = 3$ we have a primitive group on 9 letters i.e. a subgroup of N the group of order 432. The chief factors of N are $2, 3, 2^2, 2, 3^2$ so that any primitive solvable group on 9 letters has chief factors which are divisors of 2, 3, 4 and 9. Thus $r_q(G) \leq 2$ for all primes which divide $|G|$.

For $p = 2$ we have a primitive group on 4 letters. Such a group is a subgroup of the symmetric group on 4 letters and therefore has chief factors which are divisors of 2, 3 and 2^2. This proves the lemma in all cases.

Lemma 4. 4. A subdirect product G of any finite number of primitive solvable groups on a prime or prime square number of letters has $r_p(G) \leq 2$ for all primes which divide $|G|$.

Proof: First we show this for direct products and observe that subdirect products, whenever the number of factors is finite, are subgroups of the direct product. The chief factors of a direct product are just those of the individual groups used to form the direct product. By lemma 4. 3 we are done.

Theorem 4. 3. Let $G/\Delta(G)$ be a subdirect product of groups each of which is isomorphic to a primitive solvable group on a prime or prime square number of letters. Then G has property M.

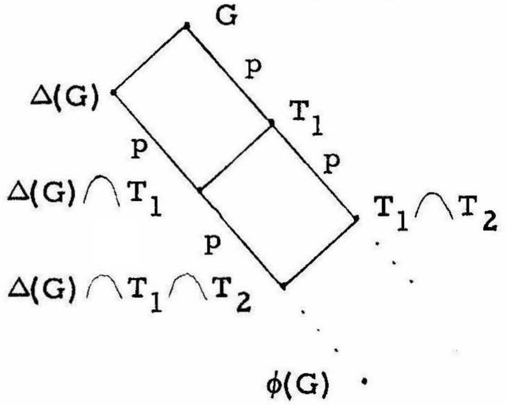
Proof: By lemma 4. 4 $r_p(G/\Delta(G)) \leq 2$ for all primes which divide its order. Now consider $r_p(\Delta(G)/\phi(G))$ for any prime p which divides the order of $\Delta(G)/\phi(G)$.

We may write

$$\phi(G) = \left(\bigcap_{\substack{T \underset{\max}{<} G \\ T \lhd G}} T \right) \cap \Delta(G)$$

$$= \bigcap_{\substack{T \underset{\max}{<} G \\ T \lhd G}} [T \cap \Delta(G)]$$

A maximal subgroup which is also normal must be of prime index. By repeated use of the second isomorphism theorem we obtain a series of subgroups from $\Delta(G)$ to $\phi(G)$ each of prime index in the one above it and normal in the entire group G.



All indices marked with a p in the diagram are primes and therefore $r_p(\Delta(G)/\phi(G)\ ) = 1$ for all primes p which divide $|\Delta(G)/\phi(G)|$. By 2. a all maximal indices between G and $\phi(G)$ are either prime or the square of a prime. Hence $G/\phi(G)$ has property M.

There is a 1 - 1 correspondence between the maximal subgroups of G and those of $G/\phi(G)$. Therefore the maximal indices of G are the same as those of $G/\phi(G)$. This shows that G has property M.

It now follows that whenever $G/\phi(G)$ is a subdirect product of primitive solvable groups on a prime or prime square number of letters or if $G/\phi(G)$ is any homomorphic image of such a group then G has property M.

Lemma 4. 5. Let G be a group with an ordered Sylow tower. Then every subgroup of G has an ordered Sylow tower.

Proof: By hypothesis G has a series

$$G = G_1 \triangleright G_2 \triangleright \dots \triangleright G_s \triangleright G_{s+1} = 1$$

with G_i/G_{i+1} of order $p_i^{s_i}$, where $p_1 < p_2 < \dots < p_2$. G_2 is a characteristic subgroup of G since it is a normal p_1-complement of G. Similarly, G_3 is a characteristic subgroup of G_2. A characteristic subgroup of a characteristic subgroup is characteristic in the entire group. Thus, G_3 is a characteristic subgroup of G. Continuing this procedure shows that each G_i is a characteristic subgroup of G.

Consider the series

$$H = H_1 \geqslant H_2 \geqslant \dots \geqslant H_s \geqslant H_{s+1} = 1$$

where $H_i = H \cap G_i$. Since $G_i \triangleleft G$ it follows that $H_i \triangleleft H$. The order of H_i is divisible only by primes in the set $\{p_i, p_{i+1}, \dots, p_s\}$ and $|H:H_i|$ is divisible only by primes in the set $\{p_1, p_2, \dots, p_{i-1}\}$. This means H has an ordered Sylow tower.

Theorem 4. 4. Let G be a group whose order is not divisible by 6. If every maximal subgroup of G has property M then G is solvable.

Proof: Use induction on $|G|$. The hypothesis is satisfied by all factor groups of G. Let M be any maximal subgroup of G. By Theorem 3. 1 M has an ordered Sylow tower. Let p be the smallest prime which divides $|G|$ and let P be a Sylow p-subgroup of G. Let N be the normalizer in G of P.

Every proper subgroup of G is contained in a maximal subgroup.

By lemma 4. 5 every proper subgroup of G has an ordered Sylow tower.

Assume G is p-normal. If $N = G$ then $Z(P)$ is a solvable normal subgroup of G and we are done by induction. If N is a proper subgroup of G then it has an ordered Sylow tower. Since p is the smallest prime which divides $|N|$ it follows that N contains a normal p-complement. By Theorem 14. 4. 6 of Ref. 1 G contains a normal subgroup with a p-factor group. Since the normal subgroup is proper it has an ordered Sylow tower. Thus, G is an extension of a solvable group by a p-group and hence is itself solvable.

Assume G is not p-normal. By lemma 19. 3. 2 of Ref. 1 G satisfies the hypothesis of a theorem of Burnside. By Theorem 4. 2. 5 of Ref. 1 G contains a p-subgroup $H = h_1 h_2 \cdots h_r$, where each $h_i \triangleleft H$. The groups $h_1, h_2, \ldots, h_r$ form a complete set of conjugates in N(H), the normalizer of H in G. The number r is prime to p. If H is normal in G then we are done by induction. If H is not normal in G then N(H) is a proper subgroup of G and has, therefore, an ordered Sylow tower. Thus, N(H) has a normal p-complement K. This implies $(K, H) = 1$ so that $N(H) = K \times H$. Hence N(H) cannot induce an automorphism of order prime to p on H. But $h_1, h_2, \ldots, h_r$ form a complete set of conjugates of h_1 in N(H). This means that N(H) must induce an automorphism of order prime to p on H. This contradiction proves that $H \triangleleft G$.

This theorem is not true if we allow 6 to divide $|G|$. The linear fractional groups $LF(2, p)$ are simple for $p > 3$. From the discussion given in chapter XX of Ref. 2 it follows that the maximal subgroups of

LF(2, p) all have property M, if p is not congruent to ± 1 modulo 5. This raises the following question. Are there any other simple groups whose maximal subgroups have property M ?

V. CONSTRUCTION OF EXAMPLES

5.1. In this section examples of groups of order $2^a p^b$, with $p \geqslant 3$, will be constructed which have property M but also contain subgroups which do not have this property. In fact given any positive integer m such a group will be constructed which has a subgroup containing a maximal subgroup of index at least m.

In order to construct the examples it will be necessary to use facts about Kronecker products and commutators. These results are given in 5.2. They are followed in 5.3 by a brief discussion of the construction procedure. This is followed by 5.4 which gives the details of the construction. The final step, 5.5, will be to show that the groups constructed have the properties mentioned in the first paragraph.

5.2. Let A and B be groups. Suppose ρ is an absolutely irreducible representation of A of degree m and τ is an absolutely irreducible representation of B of degree n both over the same field F. Form the direct product $A \times B$ of A and B and consider the representation

$$(a, b) \rightarrow \rho(a) \otimes \tau(b) .$$

This also yields a representation of the group ring of $A \times B$ over F. Since ρ is absolutely irreducible there exists an element x_{ik} in R_A, the group ring of A, such that $\rho(x_{ik}) = e_{ik}$, the matrix with a 1 in position (i, k) and zeros elsewhere. For the same reason there exists a $y_{j\ell}$ in R_B such that $\tau(y_{j\ell}) = e_{j\ell}$. Here the indices i, k run independently from 1 through m and the indices j, ℓ run independently from 1 through n.

Forming the m^2n^2 Kronecker products

$$\rho(x_{ik}) \otimes \tau(y_{j\ell})$$

we obtain the m^2n^2 one spot matrices which span the full mn x mn matrix ring over the field **F**. Hence the representation

$$(a, b) \rightarrow \rho(a) \otimes \tau(b)$$

is an absolutely irreducible representation of **A** x **B**.

Lemma 5.1. Let G be a group and let G_{t+1} be the $(t+1)^{st}$ term in the descending central series of G. Then

$$(xy, a_2, \ldots, a_t) \equiv (x, a_2, \ldots, a_t)(y, a_2, \ldots, a_t)$$

modulo G_{t+1}.

Proof: We use induction on t. For $t = 2$ we have the relation

$$(xy, a_2) = (x, a_2)(x, a_2, y)(y, a_2)$$

(see relation 10.2.1.2 on p. 150 of Ref. 1). Reading this relation modulo G_3 gives the desired result since (x, a_2, y) is in G_3.

The induction hypothesis asserts

$$(xy, a_2, \ldots, a_{t-1}) \equiv (x, a_2, \ldots, a_{t-1})(y, a_2, \ldots, a_{t-1})$$

mod G_t. Then

$$(xy, a_2, \ldots, a_t) = ((xy, a_2, \ldots, a_{t-1}), a_t)$$

The right side is then equal to

$$((x, a_2, \ldots, a_{t-1})(y, a_2, \ldots, a_{t-1})\alpha, a_t)$$

where α is an element of G_t.

Using the rules on page 150 of Ref. 1 we expand (abc, d) as follows

$$\begin{aligned}(abc, d) &= (ab, d)(ab, d, c)(c, d)\\ &= (a, d)(a, d, b)(b, d)(ab, d, c)(c, d)\end{aligned}$$

Set

$$a = (x, a_2, \ldots, a_{t-1})$$

$$b = (y, a_2, \ldots, a_{t-1})$$

$$c = \alpha$$

$$d = a_t$$

and read the result mod G_{t+1}. Note that the elements (a, b, d), (ab, d, c) and (c, d) are in G_{t+1}. Therefore (a, d) and (b, d) are the only terms not reducing to the identity mod G_{t+1}. Thi s gives the desired result.

Our next step will be an extension of the preceding lemma. Consider

$$(a, \ldots, xy, \ldots, a_t)$$

where $a_i = xy$. We may write this as

$$((a_1, \ldots, xy), a_{i+1}, \ldots, a_t)$$

Note that

$$((a_1, \ldots, a_{i-1}), xy) = ((a_1, \ldots, a_{i-1}), y)((a_1, \ldots, a_{i-1}), x)(((a_1, \ldots, a_{i-1}), x), y)$$

Set

$$(a_1, \ldots, a_{i-1}, y) = x_2$$

$$(a_1, \ldots, a_{i-1}, x) = x_1$$

$$(a_1, \ldots, a_{i-1}, x, y) = x_3$$

Using lemma 5.1 we may write

$$(x_2 x_1 x_3, a_{i+1}, \ldots, a_t)$$

$$\equiv (x_2, a_{i+1}, \ldots, a_t)(x_1, a_{i+1}, \ldots, a_t)(x_3, a_{i+1}, \ldots, a_t)$$

mod G_{t+1}. Corollary 10.2.1 on page 151 of Ref. 1 together with the fact that $(x_3, a_{i+1}, \ldots, a_t)$ is in G_{t+1} yields

$$(a_1, \ldots, xy, \ldots, a_t) \equiv (a_1, \ldots, x, \ldots, a_t)(a_1, \ldots, y, \ldots, a_t)$$

mod G_{t+1}. We state this result as Lemma 5.2.

Lemma 5.2. Let G be a group and let G_{t+1} be the $(t+1)^{st}$ term in the descending central series for G. Then

$$(a_1, \ldots, xy, \ldots, a_t) \equiv (a_1, \ldots, x, \ldots, a_t)(a_1, \ldots, y, \ldots, a_t)$$

mod G_{t+1}.

5. 3. Before proceeding with the actual construction a brief discussion of what is being done will be given.

We begin with $K = A_1 * \ldots * A_t$, the free product of elementary abelian groups each of order p^2. Let $A_i = \langle a_i, b_i \rangle$.

The automorphism group of K has a subgroup $H = H_1 \times H_2 \times \ldots \times H_t$, where H_i induces the identity automorphism on A_j for $j \neq i$ and a dihedral group of order 8 on A_i.

Let G denote the semi-direct product of K by H. The details of the construction and the properties of the semi-direct product are given in section 6. 5 of Ref. 1. One of these properties is that $K \triangleleft G$.

Since $K \triangleleft G$ and K_{t+1} is characteristic in K it follows that $K_{t+1} \triangleleft G$. We consider the finite group G/K_{t+1}.

A commutator $(\alpha_1, \alpha_2, \ldots, \alpha_t)$ is said to be of type A if each α_i is either a_i or b_i for $i = 1, 2, \ldots, t$. Thus there are 2^t commutators of type A. We make no assumptions regarding any commutators not of type A. The subgroup of K/K_{t+1} we are interested in is the group W generated by all elements of the form

$$(\alpha_1, \alpha_2, \ldots, \alpha_t)K_{t+1}$$

where $(\alpha_1, \alpha_2, \ldots, \alpha_t)$ is of type A. From our choice of H and the properties of commutators it will follow that this subgroup W is normal in G/K_{t+1}. Moreover it is elementary abelian and can therefore be regarded as a vector space on which G/K_{t+1} operates.

We shall prove that the structure of this group W as a vector space is isomorphic to the Kronecker product of t two dimensional vector spaces and that the representation which arises is just the Kronecker product of the representations $\rho_1(H_1)$, $\rho_2(H_2), \ldots, \rho_t(H_t)$ which are induced by H_i on A_i. Each of the representations ρ_i will be faithful representations of H_i and absolutely irreducible.

In order to do this we must identify this group with the Kronecker product of two dimensional spaces. The linear transformations induced on the commutators

$$(a_1, a_2, \ldots, a_t)K_{t+1}$$

by the elements of G/K_{t+1} will have the right properties. The problem will be to prove the independence of these commutators in order to insure that we do indeed have the Kronecker product space and not some quotient space of it.

The proof of the independence will be divided into two stages. The first stage will be to show that a dependence relation among the commutators of type A mod K_{t+1} leads to another relation in the free product of cyclic groups of order p modulo the $(t+1)^{st}$ term in its descending central series. We shall then show, by constructing an example, that such a relation cannot hold. This conflict will prove the independence of the commutators of type A mod K_{t+1}.

5.4. Let p be an odd prime. Let D be the subgroup of GL(2, p) which is generated by

$$x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Then D has defining relations

$$x^2 = 1, \quad y^4 = 1 \text{ and } x^{-1}yx = y^{-1}$$

and $|D| = 8$.

This group is absolutely irreducible. If D were reducible over some extension E, of J_p, then it would be completely reducible because $|D|$ and p are relatively prime. This would mean that D would be similar to a group of diagonal matrices and thus abelian. But D is not abelian. Hence D is absolutely irreducible.

Let $K = A_1 * \ldots * A_t$ be the free product of the groups $A_1, \ldots, A_t$ where each A_i is elementary abelian and of order p^2.

Any automorphism σ_i of A_i can be extended to an automorphism of K by having σ_i induce the identity automorphism on A_j for $j \neq i$.

Suppose $A_i = < a_i, b_i >$. Now define

$$a_i^{x_i} = a_i \qquad a_i^{y_i} = b_i^{-1}$$

$$b_i^{x_i} = b_i^{-1} \qquad b_i^{y_i} = a_i$$

for $i = 1, 2, \ldots, t$. Then $< x_i, y_i > = H_i$ is a group of automorphisms of A_i which is isomorphic to D. We extend H_i to a group of automorphisms of K by assuming that each element of H_i induces the identity on A_j for $j \neq i$.

The group $< H_1, H_2, \ldots, H_t > = H$ is also a group of automorphisms of K and in fact this group is the direct product i.e. $H = H_1 \times H_2 \times \ldots \times H_t$.

Now let K and H be the K and H of Theorem 6. 5. 1 on page 88 of Ref. 1. Form G the semi-direct product of K by H.

By Theorem 6. 5. 3 on page 89 of Ref. 1 K is a normal subgroup of G and H is a subgroup of G. Also $K \cap H = 1$ and $G = HK$.

Let K_{t+1} be the $(t+1)^{st}$ term of the descending central series of K. This group is a characteristic subgroup of K and since K is normal in G it follows that K_{t+1} is normal in G.

A commutator of the form $(\alpha_1, \ldots, \alpha_t)$ where $\alpha_i = a_i$ or $\alpha_i = b_i$ is said to be of type A. Consider the subgroup of K generated by all commutators of type A and K_{t+1}. By Corollary 10. 2. 1 on page 151 of Ref. 1 the commutators of type A commute with one another mod K_{t+1}.

Our next assertion is that any one of the commutators $(\alpha_1, \ldots, \alpha_t)$ of type A has order p mod K_{t+1} or else is congruent to the identity mod K_{t+1}. Note that

$$1 \equiv (\alpha_1^p, \alpha_2, \ldots, \alpha_t) \text{ mod } K_{t+1}$$

because $\alpha_1^p = a_1^p$ or $\alpha_1^p = b_1^p$ both of which are the identity of K. But

$$(\alpha_1^p, \alpha_2, \ldots, \alpha_t) \equiv (\alpha_1, \alpha_2, \ldots, \alpha_t)^p \text{ mod } K_{t+1}$$

by lemma 5. 2 which proves the assertion.

The group G/K_{t+1} has a normal Sylow p-subgroup, namely K/K_{t+1}. A Sylow 2-subgroup of G/K_{t+1} is HK_{t+1}/K_{t+1} which is isomorphic to H. We shall use H to denote this subgroup of G/K_{t+1}. Any element of G/K_{t+1} has a representation in the form kh where k is in K/K_{t+1} and h is in H. Consider $[(a_1, \ldots, a_t)K_t]^{kh}$. This equals,

$$(a_1, \ldots, a_t)^{kh}K_{t+1} = (a_1, \ldots, a_t)^{h}K_{t+1}$$

by Corrolary 10. 2. 1 on page 151 of Ref. 1. Now h can be written $h = h_1h_2 \ldots h_t$ where h_i is in H_i for $i = 1, 2, \ldots, t$. Since h_i and h_j commute for $i \neq j$ and h_i centralizes A_j for $i \neq j$ it follows that

$$(a_1, \ldots, a_t)^{h}K_{t+1} = (a_1^{h_1}, \ldots, a_t^{h_t})K_{t+1}$$

But $a_i^{h_i}$ is either a_i^{ϵ} or b_i^{δ} where $\epsilon = \pm 1$ and $\delta = \pm 1$. From lemma 5. 2 it follows that a commutator of type A mod K_{t+1} under an element of G/K_{t+1} is replaced by another commutator of type A or the inverse of such a commutator. This proves that the group generated by the elements

$$(a_1, \ldots, a_t)K_{t+1}$$

where $(a_1, \ldots, a_t)$ ranges over all commutators of type A is a normal, elementary abelian p-subgroup of G/K_{t+1}. Hence W can be regarded as a vector space on which G/K_{t+1} operates.

Assume the 2^t elements $(a_1, \ldots, a_t)K_{t+1}$ where $(a_1, a_2, \ldots, a_t)$ is of type A are independent i. e. $|W| = p^{2^t}$.

If $h = h_1h_2 \ldots h_t$ is an element of H and $(a_1, a_2, \ldots, a_t)$ is of type A then

$$(a_1, a_2, \ldots, a_t)^h \equiv (a_1^{h_1}, a_2^{h_2}, \ldots, a_t^{h_t})$$

$$\equiv (a_1^{r_1} b_1^{s_1}, a_2^{r_2} b_2^{s_2}, \ldots, a_t^{r_t} b_t^{s_t})$$

$$\equiv \Pi(\beta_1, \beta_2, \ldots, \beta_t)^{\epsilon(\beta_1, \beta_2, \ldots, \beta_t)} \bmod K_{t+1}.$$

Here the product extends over all commutators of type A. From lemma 5.2 $\epsilon(\beta_1, \beta_2, \ldots, \beta_t)$ is the product of the exponents which occur on $\beta_1, \beta_2, \ldots, \beta_t$. For example, if $(\beta_1, \beta_2, \ldots, \beta_t) = (a_1, b_2, a_3, \ldots, a_t)$ then $\epsilon(a_1, b_2, a_3, \ldots, a_t) = r_1 s_2 r_3 \ldots r_t$.

Let $V_i = \{u_i, v_i\}$ $i = 1, 2, \ldots, t$ be t two dimensional vector spaces over J_p and suppose the representation of H_i on V_i is the group of matrices D relative to the basis $\{u_i, v_i\}$. Suppose also that the representation of H_i on V_j for $j \neq i$ is the identity.

Form the Kronecker product $V_1 \otimes V_2 \otimes \ldots \otimes V_t$ of the vector spaces V_i $i = 1, 2, \ldots, t$. A basis for this space is given by the vectors

$$\overline{a}_1 \otimes \overline{a}_2 \otimes \ldots \otimes \overline{a}_t$$

where $\overline{a}_i$ is either u_i or v_i.

For $h = h_1 h_2 \ldots h_t$ an element of H we have

$$(\overline{a}_1 \otimes \overline{a}_2 \otimes \ldots \otimes \overline{a}_t)^h = \overline{a}_1^{h_1} \otimes \overline{a}_2^{h_2} \otimes \ldots \otimes \overline{a}_t^{h_t}.$$

Expanding this gives

$$(r_1 u_1)(s_1 v_1) \otimes (r_2 u_2)(s_2 v_2) \otimes \ldots \otimes (r_t u_t)(s_t v_t)$$

$$= \sum \delta(\overline{\beta}_1, \overline{\beta}_2, \ldots, \overline{\beta}_t)\overline{\beta}_1 \otimes \overline{\beta}_2 \otimes \ldots \otimes \overline{\beta}_t$$

where $\delta(\overline{\beta}_1, \overline{\beta}_2, \ldots, \overline{\beta}_t)$ is the product of the coefficients of $\overline{\beta}_1, \overline{\beta}_2, \ldots, \overline{\beta}_t$.

Hence, assuming the independence of the elements $(a_1, \ldots, a_t)K_{t+1}$ where $(a_1, \ldots, a_t)$ is of type A, the representations which arise on **W** and V are equivalent. But the one arising on V is the Kronecker product of groups each isomorphic with D and thus absolutely irreducible. Hence the representation induced on **W** by G/K_{t+1} is absolutely irreducible. Thus **W** is a chief factor of G/K_{t+1}.

We now prove the independence of the elements $(a_1, \ldots, a_t)K_{t+1}$ where $(a_1, \ldots, a_t)$ is of type A.

Consider the group K. Among its elements are those which become the identity if we set each $b_i = 1$ for $i = 1, 2, \ldots, t$. The set of all such elements forms a normal subgroup X of K.

Let $\overline{K} = \langle a_1 \rangle * \langle a_2 \rangle * \ldots * \langle a_t \rangle$ be the free product of the groups $\langle a_1 \rangle, \ldots, \langle a_t \rangle$. Then $\overline{K} \triangleleft K$ and $\overline{K} \cap X = 1$. Every coset of X in K contains an element which belongs to $\overline{K}$. Consider the coset kX where k is any element of K. Set all of the b's which occur in k equal to the identity. Suppose the resulting element is k_1. Then $kX = k_1 k_1^{-1} kX$ and $k_1^{-1}k$ is in X. Thus $kX = k_1 X$ and k_1 is in $\overline{K}$. By Theorem 6.5.3 on page 89 of Ref. 1 K is the semi-direct product of X by $\overline{K}$. Thus the correspondence

$$\overline{k}X \longleftrightarrow \overline{k}$$

is an isomorphism between K/X and $\overline{K}$.

Suppose there is a dependency relation among the commutators of type A i.e.

$$\Pi(a_1, \ldots, a_t)^{\epsilon(a_1, \ldots, a_t)} \equiv 1 \bmod K_{t+1}$$

where the product extends over the commutators of type A and at least one $\epsilon(a_1, \ldots, a_t)$ is not congruent to zero mod p.

The terms in this product may be ordered in any way we wish since they commute mod K_{t+1}. They will be ordered as follows. Let $(\gamma_1, \ldots, \gamma_t)$ and $(\beta_1, \ldots, \beta_t)$ be two commutators of type A. Then $(\gamma_1, \ldots, \gamma_t)$ shall precede $(\beta_1, \ldots, \beta_t)$ if $\gamma_1 = \beta_1, \ldots, \gamma_{i-1} = \beta_{i-1}$ but $\gamma_i = a_i$ while $\beta_i = b_i$.

Suppose this ordering to have been carried out and that

$$(\delta_1, \ldots, \delta_t)^{\epsilon(\delta_1, \ldots, \delta_t)}$$

is the first element in the product with an exponent not congruent to zero mod p. If this term is not $(a_1, \ldots, a_t)$ relabel a's and b's and make it this element. This may alter the order of the other terms. However, this will be of no consequence. We shall take the groups X and $\overline{K}$ after this relabeling has been done.

Then

$$(1) \qquad (a_1, \ldots, a_t)^{\epsilon(a_1, \ldots, a_t)} \Pi(a_1, \ldots, a_t)^{\epsilon(a_1, \ldots, a_t)} \equiv 1 \bmod K_{t+1}$$

where the product extends over all the commutators of type A with the exception of $(a_1, \ldots, a_t)$. Each of the terms in the product

$$\Pi(a_1, \ldots, a_t)^{\epsilon(a_1, \ldots, a_t)}$$

has a b_i in some position. Also $\epsilon(a_1, \ldots, a_t)$ is not congruent to zero mod p.

Relation 1 becomes

$$(a_1, \ldots, a_t)^{\epsilon(a_1, \ldots, a_t)} \equiv 1 \bmod X\, K_{t+1}$$

Since $\epsilon(a_1, \ldots, a_t)$ is not congruent to zero mod p we also have the relation

$$(a_1, \ldots, a_t) \equiv 1 \bmod X\, K_{t+1} .$$

Thus for some x in X

$$(a_1, \ldots, a_t) = x \, \Pi \text{ commutators of wt}(t + 1).$$

If this relation is read mod X then the left side can be the identity only if $(a_1, \ldots, a_t)$ is the identity of K because $\overline{K} \cap X = 1$. Also reading mod X replaces a commutator of wt(t + 1) by another commutator of wt(t + 1). Thus the element

$$(a_1, \ldots, a_t)X$$

of K/X is a product of commutators of wt(t + 1). This implies $(a_1, \ldots, a_t)$ is a product of commutators of wt(t + 1) in $\overline{K}$ because of the isomorphism between K/X and $\overline{K}$. From this we conclude that whenever we have a free product $\overline{K} = \langle a_1 \rangle * \ldots * \langle a_t \rangle$ of cyclic groups of order p it is also true that

$$(a_1, \ldots, a_t) \equiv 1 \bmod \overline{K}_{t+1} .$$

By Theorem 12.1.1 on page 312 of Ref. 1 any group T which is generated by t elements of order p, say $T = \langle c_1, \ldots, c_t \rangle$ with

$c_i^p = 1$, is a homomorphic image of $\overline{K} = \langle a_1 \rangle * \ldots * \langle a_t \rangle$ under the correspondence

$$a_i \to c_i \,.$$

If T_{t+1} is the identity then the kernel of this homomorphism contains $\overline{K}_{t+1}$. Hence the mapping

$$a_i\overline{K}_{t+1} \to c_i$$

is also a homomorphism from K/K_{t+1} onto T.

Suppose it is possible to construct a group $T = \langle c_1, \ldots, c_t \rangle$ with $c_i^p = 1$ for $i = 1, 2, \ldots, t$ and $T_{t+1} = 1$. Suppose further that $(c_1, \ldots, c_t)$ is not the identity. This will be in conflict with the relation

$$(a_1, \ldots, a_t) \equiv 1 \bmod \overline{K}_{t+1} ,$$

because this relation implies $(c_1, \ldots, c_t) = 1$.

In this event the assumption which led to the relation

$$(a_1, \ldots, a_t) \equiv 1 \bmod \overline{K}_{t+1}$$

cannot hold.

We now proceed to the construction of the group T. It will be a group of matrices with $(t+1)$ rows and $(t+1)$ columns under matrix multiplication. The entries of these matrices will be from J_p.

Let I denote the identity matrix and let E_{ij} be the matrix with a 1 in position (i, j) and zeros elsewhere. The group $T = \langle c_1, \ldots, c_t \rangle$ where

$$\begin{aligned} c_1 &= I + E_{21} \\ c_2 &= I + E_{32} \\ &\;\vdots \\ c_t &= I + E_{t+1,\, t} \end{aligned}$$

The inverse of c_i is $I - E_{i+1,\, i}$. Consider the commutator

$$\begin{aligned} (c_1, c_2) &= (I - E_{21})(I - E_{32})(I + E_{21})(I + E_{32}) \\ &= I - E_{31}, \end{aligned}$$

and then

$$\begin{aligned} (c_1, c_2, c_3) &= (I + E_{31})(I - E_{43})(I - E_{31})(I + E_{43}) \\ &= I + E_{41} \end{aligned}$$

Continuing we have

$$(c_1, c_2, \ldots, c_t) = I + \epsilon E_{t+1,\, 1}$$

where $\epsilon = \pm 1$ depending on whether t is even or odd. In either case $(c_1, c_2, \ldots, c_t) \neq 1$.

Now T is a subgroup of P consisting of all matrices of the form

$$\begin{pmatrix} 1 & & & & & \\ & 1 & & 0 & & \\ & & \cdot & & & \\ & & & \cdot & & \\ & * & & & \cdot & \\ & & & & & 1 \end{pmatrix}$$

where the starred portion can be filled in arbitrarily and the zero means all entries above the main diagonal are zero.

Every element of P can be uniquely expressed in the form $I+A$ where A is a strictly triangular matrix. Let $I + A$ and $I + B$ be two elements of P. The inverse of $I + A$ has the form $I - A + A^2 - \dots$. This series terminates since A is a nilpotent matrix. The same applies to the element $I + B$.

If C and D are any two strictly triangular matrices then their product has zeros on the main and second from main diagonals i. e. CD has the form

$$\begin{pmatrix} 0 & & & & & \\ 0 & 0 & & & 0 & \\ & 0 & \cdot & & & \\ & & \cdot & \cdot & & \\ & & & \cdot & \cdot & \\ & * & & & \cdot & 0 \\ & & & & 0 & 0 \end{pmatrix}$$

Consider the commutator of $I + A$ and $I + B$ i. e.

$$(I - A + A^2 - \dots)(I - B + B^2 - \dots)(I + A)(I - B).$$

Our remarks about the product CD show that this commutator has the form $I + E$ where E has zeros on the main and second from main diagonals. Thus the group (P, P) consists of elements of the form

$$\begin{pmatrix} 1 & & & & & \\ 0 & 1 & & & & \\ & 0 & \cdot & 0 & & \\ & & \cdot & \cdot & & \\ & * & & \cdot & 1 & \\ & & & & 0 & 1 \end{pmatrix}$$

We shall assume the group P_i, the i^{th} term of the descending central series of P, consists of elements of the form $I + E$ where E is a triangular matrix with zeros on the main, second from main and so on up to and including the i^{th} from main diagonals. Let $I + A$ be any element of P and let $I + E$ be any element of P_i. We verify by direct calculation that a strictly triangular matrix multiplied on the left or right by a matrix, which is strictly triangular and has zeros on the i^{th} from main as well as on all preceding diagonals, yields a matrix which is again strictly triangular and has zeros on the $(i+1)^{st}$ from main as well as on all preceding diagonals. Using this to compute the commutator $(I + E, I + A)$ we see that $(P_i, P) = P_{i+1}$ consists of elements of the form

$$\begin{array}{c} \\ \\ \\ \\ \\ i+1 \\ \\ \\ \\ \\ \\ \end{array}\left(\begin{array}{ccccccccccc}
1 &&&&&&&&&& \\
0 & 1 &&&&&&&&& \\
\cdot & 0 & \cdot &&&& 0 &&&& \\
\cdot & \cdot & \cdot & \cdot &&&&&&& \\
\cdot & \cdot && \cdot & \cdot &&&&&& \\
0 & \cdot &&& \cdot & \cdot &&&&& \\
& 0 &&&& \cdot & \cdot &&&& \\
&& \cdot &&&& \cdot & \cdot &&& \\
& * & \cdot &&&&& \cdot & \cdot && \\
&&& \cdot &&&&& \cdot & 1 & \\
&&&&& 0 & \cdot & \cdot & \cdot & 0 & 1
\end{array}\right)$$

From this it follows that $P_{t+1} = 1$. Since $T \leqslant P$ it follows that $T_{t+1} = 1$.

Hence $T = \langle c_1, c_2, \ldots, c_t \rangle$ with $c_i^p = 1$ for $i = 1, 2, \ldots, t$ and $(c_1, c_2, \ldots c_t) \neq 1$. Also $T_{t+1} = 1$. Therefore the relation

$$(a_1, \ldots, a_t) \equiv 1 \bmod \overline{K}_{t+1}$$

is not valid. Hence our assumption about a dependency relation among the commutators of type A mod K_{t+1} is invalid.

5.5. We now show that G/K_{t+1} has property M and that it contains subgroups which do not possess property M.

Using the collection formula of P. Hall we may write the elements of K/K_{t+1} in the form

$$a_1^{\alpha_1} \dots a_t^{\alpha_t} b_1^{\beta_1} \dots b_t^{\beta_t} \Pi c_i K_{t+1}$$

where c_i ranges over some set of commutators of weight at least two. Reading this modulo the derived group R of K/K_{t+1} we obtain an elementary abelian group generated by the cosets

$$a_1R, \dots a_tR, \ b_1R, \dots b_tR .$$

This group is elementary abelian so that $R \geqslant \phi(K/K_{t+1})$. But the Frattini subgroup contains the derived group and therefore $R = \phi(K/K_{t+1})$. The representation of G/K_{t+1} on R is a sum of t representations of degree 2. This proves that the p-rank of $G/K_{t+1}/\phi(K/K_{t+1})$ is 2.

We shall apply 2.b with $A = K/K_{t+1}$ and $N = \phi(K/K_{t+1})$. Note that N is normal in G/K_{t+1} since it is a characteristic subgroup of A which is normal in G/K_{t+1}. Now 2.b says that $\phi(K/K_{t+1}) \leqslant \phi(G/K_{t+1})$. Hence the p-rank of $G/K_{t+1}/\phi(G/K_{t+1})$ is at most 2.

The maximal indices of $G/K_{t+1}/\phi(G/K_{t+1})$ are the same as the maximal indices of G/K_{t+1}. But by 2.a the maximal indices of $G/K_{t+1}/\phi(G/K_{t+1})$ which are powers of p are p or p^2. Hence a maximal subgroup of G/K_{t+1} which has index a power of p is of index p or p^2.

The only other prime which divides the order of G/K_{t+1} is 2. Since the Sylow p-subgroup of G/K_{t+1} is normal we have $r_2(G/K_{t+1})=1$.

By 2. a any maximal subgroup of G/K_{t+1} which has index a power of 2 has index 2.

Since G/K_{t+1} is solvable all maximal subgroups have prime power index and therefore we have accounted for all possible maximal indices. They are 2, p or p^2 so that G/K_{t+1} has property M.

Consider the subgroup HW of G/K_{t+1}. Then $\mathbf{W}$ will be operated on absolutely irreducibly by H and therefore H is a maximal subgroup of HW. But $|HW : H| = |\mathbf{W}| = p^{2^t}$.

REFERENCES

1. Hall, M. : The theory of groups. New York: MacMillan, 1959.

2. Burnside, W. : Theory of groups of finite order, 2nd ed. New York: Dover, 1955.

3. Huppert, B. : Normalteiler and maximale Untergruppen endlicher Gruppen. Math. Zeitschrift, vol. 60, pp. 409-434, 1954.

4. Gaschutz, W. : Uber die ϕ-Untergruppe endlicher Gruppen Math. Zeitschrift, vol. 58, pp. 160-170, 1953.

5. Albert, A. A. : Fundamental concepts of higher algebra. University of Chicago Press, 1956.