ON FINITE GROUPS WITH 'HIDDEN' PRIMES

L. G. KOVÁCS, JOACHIM NEUBÜSER, B. H. NEUMANN

(Received 11 July 1969)

Communicated by G. E. Wall

1. Introduction

The starting point of this investigation was a question put to us by Martin B. Powell: If the prime number p divides the order of the finite group G, must there be a minimal set of generators of G that contains an element whose order is divisible by p? A set of generators of G is minimal if no set with fewer elements generates G. A minimal set of generators is clearly irredundant, in the sense that no proper subset of it generates G; an irredundant set of generators, however, need not be minimal, as is easily seen from the example of a cyclic group of composite (or infinite) order. Powell's question can be asked for irredundant instead of minimal sets of generators; it turns out that the answer is not the same in these two cases. A different formulation, together with some notation, may make the situation clearer.

Let G be a group; we denote by $\kappa_n(G)$ the set of those elements g of G that are not omissible from some family [1] of n generators of G. Thus $g \in \kappa_n(G)$ if, and only if, there are elements $g_2, \cdots, g_n$ that jointly with g generate G, but by themselves generate a proper subgroup of G. Then

$$\kappa_n(G) \subseteq \kappa_{n+1}(G)$$

for all n. If n is less than the minimal number, say $d = d(G)$, of generators of G, then $\kappa_n(G)$ is empty. We shall call d the 'rank' of G, for brevity, and assume throughout that it is finite; and presently we shall confine attention to finite groups G. Clearly $\kappa_d(G)$ is not empty, but consists of all members of minimal generating sets of G. If G is finite and n large, say $n \geqq |G|$, the order of G, then

$$\kappa_n(G) = G - \phi(G),$$

where $\phi(G)$ denotes the Frattini subgroup; for, by a well-known theorem of Frattini [2], $\phi(G)$ consists of those elements of G that belong to no irredundant generating set of G. We shall show that in fact already

[1] In a family an element may occur repeatedly.

$$\kappa_{d+1}(G) = G - \phi(G). \tag{1}$$

Differently put, this says that *an element belongs to the Frattini subgroup of a group G if, and only if, it can be omitted from every family of $d+1$ generators of G, where d is the rank of G.*

Now it is known that for a finite group G *a prime p divides* $|G/\phi(G)|$ *if p divides* $|G|$; this is an immediate consequence of Huppert [6] III, Satz 3.8. It follows that *if p divides* $|G|$ *then p divides the order of some element outside* $\phi(G)$; and again, by (1), that *if p divides* $|G|$ *then p divides the order of some element of* $\kappa_{d+1}(G)$. This answers Powell's question, not for minimal generating families, but for irredundant generating families: *Every prime that divides the order of a finite group also divides the order of some element of some irredundant set of generators.*

By contrast, not every prime that divides $|G|$ need divide the order of some element of $\kappa_d(G)$. Let us call the prime p a 'hidden prime' of G if it divides $|G|$ but does not divide the order of any element of $\kappa_d(G)$. We answer Powell's original question about minimal sets of generators by showing that groups with hidden primes do indeed exist. The smallest example is a certain splitting extension G of an elementary abelian group A of order 9 by a quaternion group B. If A is generated by u, v and B by a, b, then the action of B on A is given by

$$u^a = v, \qquad v^a = u^2,$$
$$u^b = uv, \qquad v^b = uv^2.$$

The group has order $|G| = 2^3 \cdot 3^2$, and it can be generated by (minimally) two generators, for example by a and bu; and every member of a pair of generators has order 4. Thus 3 is a hidden prime of G. These facts will readily follow from later, more general results.

As the title indicates, the major part of this paper concerns groups with hidden primes. All the examples we know resemble the one above in that they are split extensions of a group A by a group B with the hidden primes dividing $|A|$ but not $|B|$. One of our main aims is a study of the groups that can here occur as the 'top' group B. In particular, we construct to every prime p an infinite sequence of p-groups of this kind: these are then, in a sense, generalizations of the quaternion group.

2. Notation

We summarize the notation we use.

$|S|$ = cardinal of the set S;
$|G|$ = order of the group G;
$|g|$ = order of the element g;
$|G : S|$ = index of the subgroup S in G;

https://doi.org/10.1017/S1446788700009757 Published online by Cambridge University Press

$S \subseteq T$ means S is a subset of T;
$S \leqq G$ means S is a subgroup of G;
$gp(g_1, g_2, \cdots, g_n)$, $gp(S)$, $gp(S, T)$ = (sub-)group generated by $g_1, g_2, \cdots, g_n$, by S, by S and T;
$d = d(G)$ = rank or minimal number of generators of G;
$g^h = h^{-1}gh$; $g^{1+h+\cdots+k} = gg^h \cdots g^k$;
$[g, h] = g^{-1+h} = g^{-1}h^{-1}gh$;
$\zeta(G)$ = centre of G;
$\delta(G)$ = derived group of G;
$\phi(G)$ = Frattini subgroup of G;
$\psi(G) = G - \kappa_d(G)$ = set of elements contained in no minimal generating set of G.

3. Some general results

We begin by proving the result summarized in formula (1). We have to show that if the element $h \in G$ can be omitted from every set of $d+1$ generators of G, then h can be omitted from every set of generators of G.

Let then $h \in G - \kappa_{d+1}(G)$, and let $g_1, g_2, \cdots, g_d$ form a (necessarily minimal) set of generators of G. Then

$$\begin{aligned} G &= gp(g_1, g_2, \cdots, g_d) = gp(h, g_1, g_2, \cdots, g_d) \\ &= gp(h, g_1h, g_2, \cdots, g_d) = gp(g_1h, g_2, \cdots, g_d). \end{aligned}$$

By repeated application, preceded and followed by a rearrangement of the generators, we see that also

$$gp(g_1h_1, g_2h_2, \cdots, g_dh_d) = G,$$

where $h_1, h_2, \cdots, h_d \in G - \kappa_{d+1}(G)$; and then further

$$gp(g_1k_1, g_2k_2, \cdots, g_dk_d) = G,$$

where $k_1, k_2, \cdots, k_d \in gp(G - \kappa_{d+1}(G)) = K$, say. We note that K is clearly a characteristic subgroup of G.

Now let $k \in K$ be arbitrary, and assume that

$$gp(k, f_1, f_2, \cdots) = G,$$

with finitely or infinitely many f_j. Let $g_1, g_2, \cdots, g_d$ be a (fixed, minimal) set of generators of G. Then we can express each g_i as a word in k and the f_j:

$$g_i = u_i(k, f_1, f_2, \cdots),$$

and thus, as K is normal in G, also in the form

$$g_i = v_i(f_1, f_2, \cdots)k_i^{-1},$$

https://doi.org/10.1017/S1446788700009757 Published online by Cambridge University Press

where $k_i \in K$. But then, as $g_1k_1, g_2k_2, \cdots, g_dk_d$ also, by what we have just seen, generate G, we have

$$gp(f_1, f_2, \cdots) = G.$$

Thus k is omissible from every generating family of G, that is to say, $k \in \phi(G)$. It follows that

$$K \leqq \phi(G).$$

But evidently

$$\phi(G) \subseteq G - \kappa_{d+1}(G) \subseteq K,$$

and (1) follows.

An epimorphism $\theta : G \to H$ will be called *rank preserving* if the rank of H equals that of G, that is if

$$d(G\theta) = d(G).$$

The following fact is almost obvious.

LEMMA 3.1. *If θ is a rank preserving epimorphism, then*

$$\psi(G\theta) \leqq \psi(G)\theta.$$

PROOF. We establish the equivalent inclusion

$$\kappa_d(G)\theta \leqq \kappa_d(G\theta).$$

If $g \in \kappa_d(G)$, then there are elements $g_2, \cdots, g_d \in G$ such that

$$gp(g, g_2, \cdots, g_d) = G,$$

and thus

$$gp(g\theta, g_2\theta, \cdots, g_d\theta) = G\theta.$$

As the rank of $G\theta$ is d,

$$gp(g_2\theta, \cdots, g_d\theta) \neq G\theta,$$

whence $g\theta \in \kappa_d(G\theta)$, as required.

The example of the dihedral group of order 12,

$$G = gp(a, b; a^6 = b^2 = (ab)^2 = 1),$$

and the epimorphism θ of G onto the four-group, with $a^3 \in \psi(G)$ but $a^3\theta \notin \psi(G\theta)$, shows that the inclusion can be proper. The example of the direct product G of a cyclic group C of order 6 by a cyclic group of order 2, together with any epimorphism θ of G onto C shows that the assumption that θ is rank preserving cannot be omitted, because if c is a generator of C, then $c^3 \in \psi(G\theta)$ but $c^3 \notin \psi(G)\theta$.

By contrast the Frattini subgroup has the property that

$$\phi(G)\theta \leqq \phi(G\theta),$$

where the homomorphism θ need not even be rank preserving (see for example Gaschütz [3], Satz 3).

If G is a group of prime power order then $\psi(G) = \phi(G)$, as every element outside the Frattini subgroup can be embedded in a basis modulo the Frattini subgroup, and this is necessarily a generating family of G with $d(G)$ elements. In general, however, $\psi(G)$ need not even be a subgroup, as is seen by considering the cyclic group of order 6. Here ψ is the set union of all kernels of rank preserving epimorphisms of the group. This set union must always be contained in $\psi(G)$:

LEMMA 3.2. *If N is the kernel of a rank preserving epimorphism θ of G, then*

$$N \subseteq \psi(G).$$

The proof is easy and omitted.

One might then guess that $\psi(G)$ is always the set union of all kernels of rank preserving epimorphisms of G. This is indeed the case if G is supersoluble, but not in general. We shall not prove these facts; but we gratefully acknowledge that Professor Gaschütz has found for us the following example of a group G in which $\psi(G)$ is not the set union of any normal subgroups:

$$G = gp(a_1, a_2, a_3, a_4, b, c;\ a_i^2 = (a_i a_j)^2 = b^2 = c^3 = (bc)^2 = 1,$$
$$a_1^b = a_2,\ a_3^b = a_4,\ a_1^c = a_2,\ a_2^c = a_1 a_2,\ a_3^c = a_4,\ a_4^c = a_3 a_4).$$

This group can be described as the central factor group of the (non-standard) wreath product of a four-group by the symmetric group of degree 3. It is soluble of length 3, has order 96, and is generated by 2 elements, for example by ba_1 and ca_3; no pair of generators includes b, whence $b \in \psi(G)$; but the normal closure of b is the whole of G.

We also require a converse of Lemma 3.2.

LEMMA 3.3. *If N is a finite normal subgroup of G such that $d(G/N) < d(G)$, then N is not contained in $\psi(G)$; equivalently, if N is a finite normal subgroup of G contained in $\psi(G)$, then the natural epimorphism with kernel N is rank preserving.*

PROOF. Assume $d(G/N) < d(G) = d$. Let $h_1, \cdots, h_{d-1}$ be so chosen that $h_1 N, \cdots, h_{d-1} N$ generate G/N. By a theorem of Gaschütz [4] there exist elements $n_1, \cdots, n_{d-1}, n_d$ of N such that $h_1 n_1, \cdots, h_{d-1} n_{d-1}, n_d$ generate G. Thus $n_d \in \kappa_d(G)$, and the lemma follows.

4. The construction of examples

We know of only one method of making groups G with 'hidden' primes, namely to construct G as an extension of a group A by a group B, with $d(B) = d(G)$: this ensures that $A \subseteq \psi(G)$, by Lemma 3.2. If all elements of G whose orders are divisible by the prime p are made to lie in A, then p is hidden in G.

The example described in the introduction is of this kind, with A elementary abelian and B nilpotent. We shall study such extensions of elementary abelian by

nilpotent groups in greater detail in the next sections. In this section we present examples to show that neither A nor B need be soluble.

To show that A can be chosen insoluble, we construct G as the twisted wreath product [7] of an alternating group A_p of prime degree $p \geqq 5$ by a quaternion group B; the central involution in B is to do the 'twisting' by inducing the automorphism τ of A_p which is induced by transformation by the transposition of two permuted symbols. A transversal of the centre of B then does the wreathing, and A is the fourth direct power of A_p. If B is generated by a, b and if $u \in A$ has a full cycle of order p as its component in one of the four direct factors of A and the identity permutation in the other three, then G can be generated by a and bu: we omit the verification. Thus $d(G) = 2$. Now if g is a member of a pair of generators of G, then g is modulo A one of the generators, of order 4, of B. Thus its square is of the form

$$g^2 = a^2 f$$

where $f \in A$. Hence

$$g^4 = f\tau^* f,$$

where τ^* is the automorphism of A obtained by applying τ to all four direct factors A_p simultaneously. The components of $f\tau^* f$ in each direct factor are then of the forms $v\tau v$, possibly different permutations v in the four copies of A_p. Now $v\tau v$ cannot have order p, because in the splitting extension of A_p by τ, namely the symmetric group S_p, the element $v\tau v$ is the square of the odd permutation tv, where t is the transposition which induces τ; and a full cycle in A_p (or S_p for that matter) cannot be the square of an odd permutation. Thus the order of $v\tau v$, and also the order of g, is not divisible by p, and p is a hidden prime in G.

In this construction the quaternion group can be replaced by an insoluble group, namely as follows.

Let B denote the generalized direct product of 19 copies of the binary icosahedral group, amalgamating all their centres: thus B is an extension of a cyclic group C of order 2 by the direct product of 19 icosahedral groups. The significance of the number 19 is that a product of that many, but not more, icosahedral or binary icosahedral groups can be generated by two elements (Hall [5], Gaschütz [4], Satz 3; see also Neumann and Neumann [8]). If B is generated by two elements a, b, say, then they generate the direct product of the 19 icosahedral groups modulo C in the only way in which two elements can generate this direct product, namely so that their projections on the 19 direct factors are mutually inequivalent (in the sense of Hall [5]). Then it can be verified, either by using one of Hall's enumeration procedures (especially 3.2 of [5]) or by running one's eye down the list 10.1 in [8], that there are just 3 projections of a (and, of course, also 3 different projections of b) of order 2. In the binary icosahedral groups, before the centres are amalgamated, these 3 elements then have order 4, and because there are an odd number of them, the order of a (and of b) remains a multiple of 4 also after

the amalgamation of the centres. It follows that a has order 60, and a^{30} is the generating element of the centre C. To sum up:

LEMMA 4.1. *Every member of a pair of generating elements of B, the generalized direct product of* 19 *binary icosahedral groups with all centres amalgamated to form a cyclic centre C of order* 2, *that is every element of $\kappa_2(B)$, has a non-trivial power in C.*

This is the same situation as in the quaternion group, and we use it in the same way. Thus we construct G as the twisted wreath product of an alternating group A_p of prime degree $p \geqq 7$ by our present group B, with the central involution, that is the generator of C, doing the 'twisting' in the same way as described above. One has to verify again that $d(G) = 2$, and we again omit the verification. Then it follows as before that p is a hidden prime in G; the reason why here one chooses $p \geqq 7$ is that 2, 3, and 5 necessarily divide the order of an element of $\kappa_2(B)$, so that these small primes cannot be hidden in this type of group.

Instead of using the alternating group A_p in this construction, one can take a cyclic group of order p, and make the central involution simply invert all elements of the (now abelian) group A: thus one mixes two procedures, the one just sketched and the other described in the introduction, and the resulting group will be an extension of an abelian group by an insoluble group and hiding an arbitrary prime $p \geqq 7$.

The order of G constructed in this way is

$$|G| = (\tfrac{1}{2}p!)^{\frac{1}{2}|B|} \cdot |B|$$

or

$$|G| = p^{\frac{1}{2}|B|} \cdot |B|$$

in the cases of insoluble or soluble A, respectively, where

$$|B| = 2.60^{19}.$$

The smallest value of p, namely 7, gives groups whose orders are, very roughly, $10^{20.10^{33}}$ and $10^{5.10^{33}}$. We know of no way of making smaller examples with insoluble A and B, but the smallest example with abelian A and insoluble B has order 14,520 only. We now describe it, not because it has any intrinsic interest, but for later reference.

We take B as the binary icosahedral group and A as the elementary abelian group of order 11^2; and we make B act on A without non-trivial fixed points. Specifically, if A is generated by u, v with defining relations

$$u^{11} = v^{11} = [u, v] = 1$$

and B by a, b with defining relations

$$a^5 = b^3 = (ab)^2,$$

we define the action of B on A by

https://doi.org/10.1017/S1446788700009757 Published online by Cambridge University Press

$$u^a = u^2, \qquad v^a = v^6,$$
$$u^b = u^7v^6, \qquad v^b = u^2v^5;$$

and G is, as before, the splitting extension of A by B. It is not difficult to see that G is generated by two elements, for example by a and bu. Now if $g \in G$ is written in the form

$$g = yx \quad \text{with} \quad y \in B,\ x \in A$$

and if $y \neq 1$, then the order of g equals the order of y; this follows from a very simple remark:

LEMMA 4.2. *Let y be an element of finite order $n > 1$ in a group, let x be another element of the group, and denote by X the subgroup generated by x and its conjugates under powers of y. If X is abelian and y acts without fixed points on $X-\{1\}$, then the order of yx is n.*

PROOF. Put $(yx)^n = z$. Then $z \in X$, as $y^n = 1$. Also, trivially, $z^{yx} = z$. Hence

$$z^y = z^{x^{-1}} = z,$$

as X is abelian; and $z = 1$, as y has no other fixed point in X. This proves the lemma. Its assumptions could be weakened, but in their present form they are easily verified where we require the lemma.

To conclude the discussion of the example, we remark that a member of a pair of generators of G must be of the form $g = yx$ with $y \in B-\{1\}$ and $x \in A$, and by the lemma its order is then that of y, that is 3, 4, 5, 6, or 10; and G 'hides' 11.

5. Extensions of abelian groups

We now restrict attention to the case that A is abelian, as in the example of § 1 and the last example of § 4; and we shall in fact assume, without significant loss of generality, that A is an elementary abelian p-group, where p is the prime to be 'hidden'. We look for conditions on B that allow us to 'hide' p in a splitting extension G of A by B.

THEOREM 5.1. *Let the finite group G be a splitting extension of an elementary abelian p-group A by a group B; put $d = d(G)$. Then the following three conditions are jointly necessary and sufficient for p to be 'hidden' in G:*

(5.11) *$d(B) = d$,*

(5.12) *p does not divide the order of any element b of $\kappa_d(B)$;*

(5.13) *no element of $\kappa_d(B)$ commutes with any element $\neq 1$ of A; or, differently put: elements of B outside $\psi(B)$ transform A without (non-trivial) fixed points.*

PROOF. First assume p to be hidden in G. Then $A \subseteq \psi(G)$, and (5.11) follows from Lemma 3.3. Let $b \in \kappa_d(B)$; there are then $b_2, \cdots, b_d$ such that $b, b_2, \cdots, b_d$

https://doi.org/10.1017/S1446788700009757 Published online by Cambridge University Press

generate B. By the theorem of Gaschütz [4] already quoted, there are elements $a_1, a_2, \cdots, a_d$ in A such that $g_1 = ba_1$, $g_2 = b_2 a_2, \cdots, g_d = b_d a_d$ generate G; as they generate minimally, their orders are not divisible by p, and it follows that the order of b is not divisible by p, confirming (5.12). Finally, if $a \in A$ commutes with b, then a also commutes with g_1, and as the orders of g_1 and a are co-prime, g_1 is a power of $g_1 a$, and $g_1 a, g_2, \cdots, g_d$ also generate G. Hence p does not divide the order of $g_1 a$; but this is the product of the orders of g_1 and of a, and the latter is p if it is not 1: thus $a = 1$, and (5.13) follows.

Conversely, assume (5.11–5.13), and let $g \in G$ be an element outside $\psi(G)$: we have to show that p does not divide the order of g. We write $g = ba$ with $b \in B$, $a \in A$. There are elements $g_2 = b_2 a_2, \cdots, g_d = b_d a_d$ such that $g, g_2, \cdots, g_d$ generate G. Then $b, b_2, \cdots, b_d$ generate B, and by (5.11) minimally. Thus $b \in \kappa_d(B)$. Denote the order of b by n, and consider

$$g^n = (ba)^n = a^{b^{n-1}+b^{n-2}+\cdots+1} = a^*,$$

say. Now a^* commutes with b, because

$$(a^*)^b = a^{1+b^{n-1}+\cdots+b} = a^{b^{n-1}+\cdots+b+1} = a^*,$$

as A is abelian. By (5.13) then $a^* = 1$, and g has the same order as b. By (5.12) this is not divisible by p, and the theorem follows.

Theorem 5.1 answers our question as to what finite groups B can be used to hide a *given* prime p. We now ask more generally for an intrinsic condition on B which ensures that B can be used to 'hide' *some* prime. Let us call such a group B 'secretive': thus B is secretive if there exists a prime p and a splitting extension G of an elementary abelian p-group by B such that p is 'hidden' in G. We derive from Theorem 5.1 an intrinsic condition for a group to be secretive.

THEOREM 5.2. *Let B be a finite group of rank $d = d(B) \geqq 2$. If B has a representation over the field of complex numbers such that no element outside $\psi(B)$ has an eigenvalue* 1, *then B is secretive.*

PROOF. Let p be a prime that does not divide the order of B. We derive from the given representation of B a representation modulo p by the standard procedure: first we find an associated representation over a Galois field of characteristic p, as described in Curtis and Reiner [1, § 82], and then consider this as a representation over $GF(p)$, of suitably enhanced degree. Now the eigenvalues of an element $b \in \kappa_d(B)$, of order n, say, were certain n-th roots of unity other than 1; and as p does not divide n, they are still different from 1 in the representation modulo p.

Thus we have B acting, with the elements outside $\psi(B)$ fixed-point-free, on a vector space over $GF(p)$, that is an elementary abelian p-group. We may choose this abelian group minimal, that is to say so that B acts irreducibly on it; and we then denote it by A and form the splitting extension G of A by B. It is clear that conditions (5.12) and (5.13) are satisfied (even without the assumed minimality

of A). To be able to apply Theorem 5.1 we have to establish also (5.11); this will be done in several steps.

(5.21) Let $b \in \kappa_d(B)$ and $a \in A$. If $b^a \in B$ then $a = 1$; for then $[b, a] \in B$; but also $[b, a] \in A$, as A is normal: hence $[b, a] = 1$, and by (5.13), already established, $a = 1$.

(5.22) Let B' be a complement, other than B, of A in G. Then

$$B \cap B' = \psi(B) \cap \psi(B').$$

For by the Zassenhaus conjugacy theorem (see e.g. Scott [9], Theorem 9.3.9 and the remark following its proof), B and B' are conjugate in G, and the element transforming B into B' can be chosen in A, say $B^a = B'$. Clearly then also $\psi(B)^a = \psi(B')$. Thus if $b' \in B \cap B'$, then $b' = b^a$ for some $b \in B$; and if $b' \notin \psi(B')$, then $b \notin \psi(B)$, and (5.21) implies that $a = 1$. This is impossible, as B and B' were assumed distinct. It follows that $B \cap B' \subseteq \psi(B')$, and by symmetry $B \cap B' \subseteq \psi(B) \cap \psi(B')$. The reverse inclusion is obvious, and the result follows.

(5.23) Let $b_1, b_2, \cdots, b_d$ generate B, and choose $a \in A - \{1\}$. Denote by H the group generated by $b_1 a, b_2, \cdots, b_d$; then H is mapped onto B by the retraction of G onto B. If H intersects A trivially, then H is isomorphic to B and a complement, distinct from B, of A in G; but $d \geqq 2$ by assumption, and thus there is an element, namely b_2, in $B \cap H$ but not in $\psi(B)$. This is contrary to (5.22), and it follows that H intersects A non-trivially. As A is minimal normal and H covers G/A, we deduce that $H = G$. Thus G has been shown to have rank $d(G) \leqq d = d(B)$. But $d(B) \leqq d(G)$ is obvious, and (5.11) is established. Application of Theorem 5.1 now completes the proof of Theorem 5.2.

COROLLARY 5.3. *Let B be a subdirect product of groups $B_1, B_2, \cdots, B_r$ that satisfy the conditions of Theorem* 5.2, *and thus are secretive. If*

$$d(B) = d(B_1) = d(B_2) = \cdots = d(B_r),$$

then B also satisfies the conditions of Theorem 5.2, *and thus is also secretive.*

The condition on the ranks ensures that if $b \in \kappa_d(B)$ then the projection of B onto B_i maps b on an element $b_i \in \kappa_d(B_i)$. If B is made to act on the direct sum of spaces, one for each B_i, as B_i acts on its space, that is so that $b_i \in \kappa_d(B_i)$ acts without non-trivial fixed points, then every $b \in \kappa_d(B)$ acts also without fixed points, and the corollary follows. The corollary provides a method of making secretive groups that act reducibly; this is, in fact, the only way in which such groups can be made, but we omit the proof of this assertion.

It is then reasonable to restrict attention to groups B that have irreducible, faithful representations of the kind assumed in Theorem 5.2. Such a group must have cyclic centre; for the fixed-point space of the centre is invariant under the whole group, hence trivial because of irreducibility and faithfulness; but an

abelian group with fixed-point free representation is cyclic. There is also a partial converse to this:

COROLLARY 5.4. *Let B be a finite group of rank $d = d(B) \geqq 2$. If the centre $\zeta(B)$ is cyclic and if every element of $\kappa_d(B)$ has a non-trivial power in $\zeta(B)$, then B is secretive.*

PROOF. The cyclic centre $\zeta(B)$ has a representation without non-trivial fixed points. The induced representation of B (see e.g. Curtis and Reiner [1], Chapter VIII) then evidently satisfies the conditions of Theorem 5.2.

The binary icosahedral group, which is secretive (as shown in § 4) but does not satisfy the last condition of Corollary 5.4, shows that its conditions are sufficient only, not necessary. The corollary will be applied especially to p-groups.

There are some improvements of Theorem 5.2 that we shall not need to use and do not prove. If B is secretive and no primes are hidden in B, then B has a representation as assumed in Theorem 5.2; and the only restrictions on the primes that can then be hidden 'under' B are the obvious ones: they must not divide the order of B. If B is a secretive p-group, so that $\psi(B) = \phi(B)$, then in a representation as assumed in Theorem 5.2 the elements outside $\phi(B)$ have their p-th powers still acting without fixed points; and the elements of order p all lie in $\phi(B)$.

6. A class of secretive p-groups

Among the secretive groups are the groups, studied and almost completely determined by Zassenhaus [10], which have a representation in which every element $\neq 1$, whether in ψ or not, acts without fixed points. The examples we have presented in § 1 and § 4 are of this kind, or derived from such groups. We now use Corollary 5.4 to show that there are other secretive groups.

The groups we construct will be p-groups where p is an arbitrary prime; and they depend on three further parameters q, r, s subject to

$$0 \leqq r < s \leqq q+r. \tag{6.1}$$

We use the following abbreviations:

$$p^q = Q, \quad p^r = R, \quad p^s = S,$$

and note that the restraints (6.1) imply that

$$p|Q,\ pR|S,\ S|QR. \tag{6.2}$$

We begin by defining an abelian group:

$$\begin{aligned} &H = gp(h_1, h_2, \cdots, h_{pR}, z;\ [h_i, h_j] = 1 \text{ for } 1 \leqq i < j \leqq pR; \\ &h_1^Q = h_2^Q = \cdots = h_{pR}^Q = z,\ z^p = 1; \quad h_1 h_{R+1} h_{2R+1} \cdots h_{(p-1)R+1} = 1, \\ &h_2 h_{R+2} h_{2R+2} \cdots h_{(p-1)R+2} = 1, \cdots \quad h_R h_{2R} h_{3R} \cdots h_{pR} = 1). \end{aligned} \tag{6.3}$$

https://doi.org/10.1017/S1446788700009757 Published online by Cambridge University Press

The generator z can, of course, be eliminated; and so can the R generators $h_{(p-1)R+1}, h_{(p-1)R+2}, \cdots, h_{pR}$, using the last R relations. The elements

$$(6.4) \qquad h_1, k_2 = h_1^{-1}h_2, k_3 = h_2^{-1}h_3, \cdots, k_{(p-1)R} = h_{(p-1)R-1}^{-1}h_{(p-1)R}$$

are then easily seen to form a basis of H. The first of them has order pQ, the others have order Q, and the order of H is

$$|H| = pQ^{(p-1)R}.$$

The symmetry of (6.3) in the generators $h_1, h_2, \cdots, h_{pR}$ shows that H has an automorphism β, say, which permutes these generators cyclically and thus has order pR. The action of β on the basis (6.4) is more complicated (especially the action on the last basis element), but nevertheless it is not difficult, though somewhat laborious, to verify that the only elements of H fixed by β are the powers of z. We omit the computations.

We now form a group B by adjoining to H an element b that induces β on H, and that further satisfies $b^S = z$. This is legitimate, as (6.2) ensures that the order pR of β divides S. The order of b is then pS, and B is presented in the form

$$(6.5) \qquad B = gp(H, b; h_1^b = h_2,\ h_2^b = h_3, \cdots, h_{pR}^b = h_1,\ b^S = z).$$

The order of B is

$$|B| = pQ^{(p-1)R}S.$$

A presentation of B in terms of two generators $a = h_1$ and b is given by

$$(6.6) \qquad \begin{aligned} B = gp(a, b; a^Q = a^S, [a, a^{b^i}] = 1 \quad &\text{for} \quad 1 \leqq i \leqq S, \\ a^{1+b^R+b^{2R}+\cdots+b^{(p-1)R}} &= 1). \end{aligned}$$

Some of the commutativity relations in (6.6) are redundant. We omit the verification of the equivalence of (6.6) and (6.5).

It is now easy to see that *the centre* $\zeta(B)$ *is cyclic*; for if we write an element of B in the form hb^m where $h \in H$, and ask for this to be in the centre, we have at once that h must be in the centre, and thus, by what has been said about the elements fixed by β, it is a power of z; and this in turn is a power of b. Thus $\zeta(B)$ is a subgroup of the cyclic group generated by b. In fact the least positive power of b that induces the identity automorphism on H is b^{pR}, so $\zeta(B)$ is generated by b^{pR}.

Next we need to show that the elements of $\kappa_2(B)$, that is – as B is a p-group – the elements outside $\phi(B)$, have a non-trivial power in $\zeta(B)$. To this end we write an element of B in the form $x = ka^mb^n$ where k is an element of the subgroup generated by $k_2, k_3, \cdots, k_{(p-1)R}$; as these k_i are conjugates of $[a, a^b]$ and thus in the derived group $\delta(B)$, they are in $\phi(B)$, and in order that x be outside $\phi(B)$, m or n or both must be prime to p.

https://doi.org/10.1017/S1446788700009757 Published online by Cambridge University Press

We assume first that n is not divisible by any higher power of p than R. Then there is a power of x of the form

$$x' = k'a^{m'}b^R.$$

Now

$$x'^p = (k'a^{m'})^{1+b^R+b^{2R}+\cdots+b^{(p-1)R}}b^{pR} = b^{pR};$$

for the last relation of (6.6) together with the fact that $k'a^{m'}$ is a product of conjugates of a, all of which commute, implies that

$$(k'a^{m'})^{1+b^R+b^{2R}+\cdots+b^{(p-1)R}} = 1.$$

As $1 \neq b^{pR} \in \zeta(B)$, we see that x has a non-trivial power in $\zeta(B)$.

If, on the other hand, n is divisible by a higher power of p than R, that is to say, if b^n is a power of b^{pR}, then b^n is in the centre; and p does not divide m. Now

$$x^Q = k^Q a^{mQ} b^{nQ} = z^m,$$

as $k^Q = 1$, $a^Q = z$, and $b^{pRQ} = 1$; this last equation follows from (6.2) and the fact that b has order pS. Thus we see that *every element of* $\kappa_2(B)$ *has a non-trivial power in* $\zeta(B)$; and this combines with the fact, already shown, that $\zeta(B)$ is cyclic, and with Corollary 5.4, to show:

THEOREM 6.7. *The groups B defined by* (6.6), *with Q, R, S powers of the prime p and subject to the restraints* (6.2), *are secretive.*

Denote B by $B(p; q, r, s)$ to indicate its dependence on these parameters. It is not difficult to see, by considering the orders of B, $\delta(B)$, and $\zeta(B)$, that the values of p, q, r, s are uniquely determined by B: thus $B(p; q, r, s)$ is isomorphic to $B(p'; q', r', s')$ only if $p = p', q = q', r = r', s = s'$. The groups $B(2; q, 0, 1)$ are generalized quaternion groups of order 2^{q+2}. The groups $B(2; 2, 0, 2)$ and $B(2; 1, 1, 2)$ are the smallest groups of our kind which are not generalised quaternion groups; both of them have order 32. All groups $B(p; 1, 0, 1)$ are groups of maximal class of order p^{p+1} which are not isomorphic to the Sylow p-subgroups of the symmetric groups of degree p^2. All groups $B(p; q, r, s)$ are metabelian and of rank 2. All these facts are either immediate consequences of our construction and discussion, or easy to verify: we omit the verification.

We owe to Dr. I. D. Macdonald the knowledge of a secretive 2-group of rank 3; we do not, however, know of any secretive p-groups of rank 3 or higher for primes $p > 2$, nor of secretive 2-groups of higher rank than 3.

References

[1] Charles W. Curtis, Irving Reiner, *Representation theory of finite groups and associative algebras* (Interscience, New York, London, Sydney, 1962).

[2] G. Frattini, 'Intorno alla generazione dei gruppi di operazioni', *Atti R. Accad. dei Lincei, Rendiconti* (IV) 1 (1885), 281–285.

[3] Wolfgang Gaschütz, 'Über die Φ-Untergruppe endlicher Gruppen', *Math. Zeitschr.* 58 (1953), 160–170.
[4] Wolfgang Gaschütz, 'Zu einem von B. H. und H. Neumann gestellten Problem', *Math. Nachr.* 14 (1956), 249–252.
[5] P. Hall, 'The Eulerian functions of a group', *Quart. J. Math.* (*Oxford*) 7 (1936), 134–151.
[6] B. Huppert, *Endliche Gruppen* I (Springer-Verlag, Berlin, Heidelberg, New York, 1967).
[7] B. H. Neumann, 'Twisted wreath products of groups', *Arch. Math.* 14 (1963), 1–6.
[8] Bernhard H. Neumann und Hanna Neumann, 'Zwei Klassen charakteristischer Untergruppen und ihre Faktorgruppen', *Math. Nachr.* 4 (1951), 106–125.
[9] W. R. Scott, *Group theory* (Prentice-Hall, Englewood Cliffs, 1964).
[10] Hans Zassenhaus, 'Über endliche Fastkörper', *Abh. math. Sem. Hansisch. Univ.* 11 (1936), 187–220.

Australian National University, Canberra
Rheinisch-Westfälische Technische Hochschule, Aachen
Australian National University, Canberra