On some finite groups with trivial multiplicator.

In memoriam Tibor Szele.

By B. H. NEUMANN in Manchester.

If a finite group is generated by d elements and defined by e relations between them, then clearly $e \geqq d$. The groups for which $e = d$ are of particular interest because their SCHUR "multiplicator" must be trivial; this is implicit in SCHUR [2, § 3].

One may ask whether a finite group with trivial multiplicator can always be so presented that $e = d$. This is probably a very difficult question, because information on the least possible number of defining relations for a given group is almost completely lacking. We treat here some special types of groups only, all of them metacyclic, and all of them shown by SCHUR himself to have trivial multiplicator.[1])

The simplest example of groups with trivial multiplicator is furnished by the finite cyclic groups, for which $e = d = 1$. As SCHUR [1, X] shows that the p-Sylow subgroup of the multiplicator of a group G is isomorphic to a subgroup of the multiplicator of the p-Sylow subgroup of G, it follows that a group has trivial multiplicator if all its Sylow subgroups are cyclic[2]). These groups, which we shall consider first, include the groups of square-free order[3]).

If all Sylow subgroups of the finite group G are cyclic, then G is metacyclic and can be presented in the form[4])

$$G = \{a, b; a^m = 1, b^n = 1, b^{-1}ab = a^r\}. \qquad (1)$$

[1]) SCHUR calls a group "abgeschlossen" when its multiplicator is trivial; ZASSENHAUS [3, p. 42] uses "abgeschlossen" for a group with trivial centre and only inner automorphisms — more commonly called "vollkommen" or "vollständig". Topological nomenclature, legitimately applied to topological groups, has added to the confusion. We therefore retain the somewhat cumbersome description of such groups as "groups with trivial multiplicator".

[2]) SCHUR [1, XI].

[3]) SCHUR [1] also shows that the order of the multiplicator of G is not divisible by any prime whose square does not divide the order of G. Hence if this order is square-free, the multiplicator is trivial.

[4]) ZASSENHAUS [3, p. 139].

where m, n, r are subject to the restrictions

$$r^n \equiv 1 \pmod{m}, \quad (m, n) = (m, r-1) = 1. \tag{2}$$

We show that G can also be defined, in terms of the same generators, by only two relations[5]), namely

$$a^m = b^n, \; b^{-1} a^s b = a^{s-1}, \tag{3}$$

where s is a solution of

$$(r-1)s \equiv -1 \pmod{m}. \tag{4}$$

This congruence can be solved for s because $r-1$ is by (2) prime to m. We note that the relations (3) are in fact satisfied in G; for (1) implies that

$$b^{-1} a^x b = a^{rx},$$

and thus

$$b^{-1} a^s b = a^{rs} = a^{s-1},$$

as is readily seen upon giving (4) the equivalent form

$$rs \equiv s-1 \pmod{m}.$$

Now let a group be defined by the relations (3), where m, n, r, s are subject to (2) and (4). We deduce from (3) that

$$a^{ms} = b^{-1} a^{ms} b = a^{m(s-1)};$$

hence

$$a^m = 1.$$

Next, if s' denotes the inverse of s modulo m, so that

$$ss' \equiv 1 \pmod{m},$$

we have

$$b^{-1} a b = b^{-1} a^{s's} b = a^{s'(s-1)} = a^{1-s'} = a^r,$$

because, as an immediate consequence of (4),

$$r \equiv 1 - s' \pmod{m}.$$

Thus the relations (1) follow from (3), and G is in fact presented with $e = d = 2$. It may be remarked that we have not used SCHUR's result that these groups have trivial multiplicator; on the contrary the presentation with $e = d$ may be considered as an independent proof of it.

The theorem of SCHUR already quoted, which relates the Sylow subgroups of the multiplicator to those of the group itself, makes it desirable to have some information on the multiplicators of groups of prime power order; and SCHUR [2, § 4] treats three classes of such groups.

The first class consists of the generalized quaternion groups, presented by

$$G = \{a, b; \; a^{2^m} = 1, \; b^2 = a^{2^{m-1}}, \; b^{-1} a b = a^{-1}\},$$

[5]) My original "proof" contained an error, which ROBERTO FRUCHT kindly pointed out to me.

where $m \geqq 2$. Here the first relation follows from the others and can be omitted; for the last two relations imply

$$a^{2^{m-1}} = b^{-1} a^{2^{m-1}} b = a^{-2^{m-1}}$$

Thus the generalized quaternion groups have the presentation

$$G = \{a, b;\ b^2 = a^{2^{m-1}},\ b^{-1} a b = a^{-1}\}, \tag{5}$$

with $e = d = 2$.

For the quaternion group itself, that is for $m = 2$, we get

$$b^2 = a^2,\ b^{-1} a b = o^{-1},$$

which can be put into the equivalent but more symmetrical form

$$a^2 = b^2 = (a b)^2.$$

We mention without proof another pair of relations that define the quaternion group, namely

$$a^{-1} b a = b^{-1},\ b^{-1} a b = a^{-1}.$$

The second class that SCHUR considers consists also of groups whose orders are powers of 2, namely the groups presented by

$$G = \{a, b;\ a^{2^m} = 1,\ b^2 = 1,\ b^{-1} a b = a^{-1+2^{m-1}}\},$$

where $m \geqq 3$. We show that these groups can also be given by the defining relations

$$a^{2^m} = b^2,\ b^{-1} a^{2^{m-2}-1} b = a^{2^{m-2}+1} \tag{6}$$

First we note that the relations (6) are satisfied in G; for

$$b^{-1} a^{2^{m-2}-1} b = a^{(2^{m-2}-1)(2^{m-1}-1)} = a^{2^{2m-3}-2^{m-1}\cdot 2^{m-2}+1} = a^{2^{m-2}+1},$$

because (using $m \geqq 3$)

$$2^{2m-3} \equiv 0,\ -2^{m-1} - 2^{m-2} \equiv 2^{m-2} \pmod{2^m}.$$

Conversely, assuming (6) and putting briefly

$$2^{m-2} - 1 = s,\ 2^{m-2} + 1 = t,$$

we have

$$a^{s^2} = b^{-2} a^{s^2} b^2 = a^{t^2},$$

that is

$$a^{t^2 - s^2} = 1.$$

Now

$$t^2 - s^2 = 2^{2m-4} + 2^{m-1} + 1 - 2^{2m-4} + 2^{m-1} - 1 = 2^m.$$

Hence

$$a^{2^m} = 1.$$

Finally we put

$$s' \equiv s^3 \equiv 2^{2m-4} - 2^{m-2} - 1 \pmod{2^m}.$$

Then

$$ss' \equiv 1 \pmod{2^m},$$
$$ts' \equiv 2^{m-1} - 1 \pmod{2^m},$$

and

$$b^{-1}ab = b^{-1}a^{ss'}b = a^{ts'} = a^{2^{m-1}}$$

Thus the original defining relations of G follow from (6), and G is presented with $e = d = 2$.

The last class of groups to be considered includes p-groups for all primes p. The groups are presented in the form

$$G = \{a, b;\ a^{p^m} = 1,\ b^{p^n} = 1,\ b^{-1}ab = a^{1+p^{m-n}}\},$$

where $m > n > 0$ if p is an odd prime, and $m - 1 > n > 0$ if $p = 2$. The groups have order p^{m+n}. We show that they can be defined by the pair of relations

$$a^{p^m} = b^{p^n},\ b^{-1}ab = a^{1+p^{m-n}} \tag{7}$$

These relations are evidently satisfied in G, and it only remains to show that they imply the given relations. First we have that

$$a^{p^m} = b^{-1}a^{p^m}b = a^{p^m(1+p^{m-n})},$$

hence

$$a^{p^{2m-n}} = 1;$$

it follows that the order of a is a power of p. Next, putting briefly

$$p^n = P,\ p^{m-n} = Q,$$

we have

$$a = b^{-P}ab^P = a^{(1+Q)^P},$$

whence the order of a divides $(1 + Q)^P - 1$. We show that

$$(1 + Q)^P - 1 \equiv p^m \pmod{p^{m+1}};$$

it then follows that no higher power of p than p^m divides $(1 + Q)^P - 1$, and thus the order of a divides p^m. It suffices to show that if

$$x \equiv p^u \pmod{p^{u+1}},$$

then

$$(1 + x)^p - 1 \equiv p^{u+1} \pmod{p^{u+2}}. \tag{8}$$

provided $u \geqq 1$ for odd p, or $u \geqq 2$ for $p = 2$; for starting with $x = Q$, we have

$$Q = p^{m-n} \equiv p^{m-n} \pmod{p^{m-n+1}},$$

and applying the above step inductively n times, we obtain

$$(1 + Q)^{p^n} - 1 \equiv p^{m-n+n} = p^m \pmod{p^{m+1}}$$

as asserted. The inductive step itself is obvious when it is observed that in the expansion

$$(1+x)^p-1=\binom{p}{1}x+\binom{p}{2}x^2+\cdots+\binom{p}{p}x^p$$

the first term on the right-hand side is

$$px\equiv p^{u+1}\ (\mathrm{mod}\ p^{u+2}),$$

whereas the further terms are all divisible by p^{2u+1} at least, except for the last one, which is divisible by p^{pu}; now $2u+1\geqq u+2$ when $u\geqq 1$, and $pu\geqq u+2$ when either $p>2$, $u\geqq 1$, or $p=2$, $u\geqq 2$. Thus all terms except the first one are divisible by p^{u+2}, and (8) follows. Therefore (7) entails

$$a^{p^m}=1,$$

and G is seen to be defined by (7). These groups then are also presented with $e=d=2$.

It is clear that these examples do not exhaust the finite groups that can be presented with $e=d=2$; but a systematic study, even only of the metacyclic groups with this property, is beyond the scope of the present note.

Bibliography.

[1] I. Schur, Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, *J. Reine Angew. Math.* **127** (1904), 20—50.

[2] I. Schur, Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen. *J. Reine Angew. Math.* **132** (1907), 85—137.

[3] H. Zassenhaus, Lehrbuch der Gruppentheorie, Erster Band, *Leipzig—Berlin*, 1937.

(Received September 1, 1955.)