Communicated 14 April 1954 by T. NAGELL

Some groups of order $p^r q^s$ with Abelian subgroups of order p^r contained in the central

By ERIK GÖTLIND

The group of order $p^r q^s$ where p and q are different prime numbers may be generated by $A_i B_j$ where A_i runs through all elements of a subgroup of order p^r and B_j all elements of a subgroup of order q^s. There are $p^r q^s$ $A_i B_j$ and they are all different. Hence they exhaust the group $G_{p^r q^s}$. (Here and in the following "G_n" denotes a group of order n.) This means that if under certain conditions every A_i must be permutable with every B_j and if a pair of groups, G_{p^r}, G_{q^s}, fulfils these conditions, there is one and only one group of order $p^r q^s$ with just these groups as subgroups, because the relations between A_i and B_j are completely determined in this case. If under these conditions one of the groups in the pair, say G_{p^r}, is Abelian, G_{p^r} is contained in the central of the group $G_{p^r q^s}$.

It has been shown that if $p > q^s$ and $p \not\equiv 1 \pmod q$ and G_{p^r} is a cyclic subgroup of $G_{p^r q^s}$, then G_{p^r} must be contained in the central of $G_{p^r q^s}$. This also means that there can only be as many abstract groups of a given order $p^r q^s$ with these conditions fulfilled as there are different groups of order q^s.[1] In the following the case where G_{p^r} is an Abelian group generated by two elements will be considered and the theorem to be deduced is:

Theorem: *If G_{p^r} is an Abelian subgroup of $G_{p^r q^s}$ generated by two elements of different order and $p > q^s$ and $p \not\equiv 1 \pmod q$, or if G_{p^r} is an Abelian subgroup of $G_{p^r q^s}$ generated by two elements of the same order and $p > q^s$ and $p^2 \not\equiv 1 \pmod q$, then G_{p^r} must be contained in the central of $G_{p^r q^s}$.*

The proof requires some lemmas.

Lemma 1. When $p > q^s$, there is only one subgroup of order p^r of the group $G_{p^r q^s}$.

Suppose G_{p^r} and G'_{p^r} were two different subgroups of $G_{p^r q^s}$. Then G'_{p^r} would contain at least some element, say A', not contained in G_{p^r} and of order p^v, where $v \neq 0$. $(A')^n A_i$ would then produce p^{r+1} different elements, when n takes the values $1, 2, \ldots, p$, and A_i runs through all elements of G_{p^r}. They are all different, because if $(A')^m A_i = (A')^n A_j$ we would have $(A')^{m-n} = A_j A_i^{-1}$ and A' would be an element of G_{p^r} if $m \neq n$, contrary to the assumptions, because in this case $m - n \not\equiv 0 \pmod p$.

[1] E. GÖTLIND: Några satser om grupper av ordningen $p^r q^s$. (Some lemmas about groups of order $p^r q^s$.) *Norsk Matematisk Tidsskrift*, 1948, p. 11, together with a correction note to this paper: Not till uppsatsen "Några satser om grupper av ordningen $p^r q^s$", the same journal, 1949, p. 59.

When $m = n$ we get $A_i = A_j$ as the only possibility. Hence there are p^{r+1} different elements of the type $(A')^n A_i$ all belonging to the group $G_{p^r q^s}$. But when $p > q^s$, p^{r+1} is greater than $p^r q^s$ and in this case p^{r+1} different elements of $G_{p^r q^s}$ is an impossibility. This means that when $p > q^s$ there cannot exist more than one subgroup of order p^r, and this group must be self-conjugated.

Lemma 2. When $p > q^s$ and $p \not\equiv 1 \pmod q$, an element $B\ (\neq E)$ in a subgroup G_{q^s} of the group $G_{p^r q^s}$ cannot be non-permutable with one and only one of the base elements of an Abelian subgroup G_{p^r} of $G_{p^r q^s}$.

Let $A_1, A_2, \ldots, A_n$ be the base elements of G_{p^r}, and let A_1 be an element not permutable with the given B. A_i is of order p^{r_i}. Transformation of A_i with B gives:

$$B A_1 B^{-1} = A_1^t A_2^{w_2} \ldots A_n^{w_n} \tag{1}$$

$$B A_i B^{-1} = A_i \qquad (i = 2, 3, \ldots, n) \tag{2}$$

where $t = 1$ and $w_i = 0$ for all i do not both hold. (We know that a relation of type (1) must hold when $p > q^s$ because in this case G_{p^r} is self-conjugated, as was shown above.) Iterated transformation of A_1 using (1) and (2) gives

$$B^m A_1 B^{-m} = A_1^{t^m} A_2^{w_2 + w_2 t + \cdots + w_2 t^{m-1}} \ldots A_n^{w_n + w_n t + \cdots + w_n t^{m-1}}. \tag{3}$$

However, B is an element in G_{q^s} and hence of order q^u where $u \neq 0$ $(B \neq E)$. Substituting q^u for m in (3) we get

$$B^{q^u} A_1 B^{-q^u} = E A_1 E = A_1 = A_1^{t^{q^u}} A_2^{w_2 + w_2 t + \cdots + w_2 t^{q^u - 1}} \ldots A_n^{w_n + w_n t + \cdots + w_n t^{q^u - 1}}.$$

Hence

$$t^{q^u} \equiv 1 \pmod{p^{r_1}} \tag{4}$$

and

$$w_i + w_i t + \cdots + w_i t^{q^u - 1} \equiv 0 \pmod{p^{r_i}}. \tag{5}$$

From the number theory we know that

$$t^{\varphi(p^{r_1})} \equiv 1 \pmod{p^{r_1}} \tag{6}$$

and (4) together with (6) gives

$$\varphi(p^{r_1}) \equiv 0 \pmod q \tag{7}$$

when $t \not\equiv 1 \pmod{p^{r_1}}$. But p and q are different prime numbers. Hence (7) implies

$$p - 1 \equiv 0 \pmod q.$$

When $p - 1 \not\equiv 0 \pmod q$ the only possibility is that $t \equiv 1 \pmod{p^{r_1}}$ which gives $t = 1$ and in that case (5) is reduced to

$$q^u w_i \equiv 0 \pmod{p^{r_i}} \qquad (i = 2, 3, \ldots, n)$$

and since $(p, q) = 1$

$$w_i \equiv 0 \pmod{p^{r_i}}$$

which gives $w_i = 0$. This means that when $p - 1 \not\equiv 0 \pmod{q}$ (1) takes the form $B A_1 B^{-1} = A_1$ and Lemma 2 is proved.

Lemma 3. When $p > q^s$ and $p \not\equiv 1 \pmod{q}$, an element B ($\neq E$) in a subgroup $G_q s$ of the group $G_p r_q s$ cannot be non-permutable with both of two base elements generating an Abelian subgroup $G_p r$ and being of different order.

Let A_1 of order p^t and A_2 of order p^u be two base elements together generating $G_p r$, and let $p^t > p^u$. It is assumed in the following that $p > q^s$.

Suppose we have

$$B A_1 B^{-1} = A_1^m A_2^n \tag{8}$$

$$B A_2 B^{-1} = A_1^v A_2^w \tag{9}$$

where $m = 1$ and $n = 0$ do not both hold and $v = 0$ and $w = 1$ do not both hold. (The transformation of A_1 and A_2 with B gives elements contained in $G_p r$ when $p > q^s$ according to Lemma 1.)

The proof of Lemma 3 will proceed in three steps (3a, 3b, 3c).

3 a. If there were an element A_i in $G_p r$ with which B were permutable, it could not be of the highest order (in $G_p r$) if $p \not\equiv 1 \pmod{q}$.

A_i belongs to $G_p r$ and hence must be of the form

$$A_i = A_1^h A_2^k$$

because A_1 and A_2 generated $G_p r$. If A_i should be of the highest order (which is p^t) in $G_p r$, it must hold that

$$h \not\equiv 0 \pmod{p} \tag{10}$$

because otherwise A_i could not be of higher order than p^{t-1}. But when (10) is fulfilled A_i and A_2 form a base for $G_p r$. Then we would have a base consisting of one element permutable with B, A_i, and one not permutable with B, A_2. However, this is impossible according to Lemma 2 when $p \not\equiv 1 \pmod{q}$. Hence A_i cannot be of the highest order when $p \not\equiv 1 \pmod{q}$.

3 b. If there were an element B of order q^m ($m \neq 0$) fulfilling (8) and (9), every element of the highest order (p^t) in $G_p r$ would be contained in a cycle (produced through iterated transformations with B) of q^i ($1 \leq i \leq m$) different elements all of the highest order, provided that $p \not\equiv 1 \pmod{q}$.

The transformation of an element of the highest order with B will give a new element contained in $G_p r$ (according to Lemma 1 because it is assumed that $p > q^s$) and of the same order as the transformed element. Let A_{10} be an element of the highest order (p^t), and let A_{1i} be defined thus:

$$B^i A_{10} B^{-i} = A_{1i}. \tag{11}$$

But B is of order q^m. Hence

$$B^{q^m} A_{10} B^{-q^m} = E A_{10} E = A_{10} = A_{1q^m}.$$

This means that there can be at most q^m different elements in the cycle of elements of the highest order constructed through repeated transformation with B and starting from a given element of the highest order in $G_p r$. However, two elements, say A_{1i} and A_{1j} (where $i \neq j$), of such a cycle cannot be equal if $i - j \not\equiv 0 \pmod q$ and $p \not\equiv 1 \pmod q$ because, if they were, we would have

$$B^i A_{10} B^{-i} = B^j A_{10} B^{-j}$$

according to (11) and hence

$$B^{i-j} A_{10} = A_{10} B^{i-j} \tag{12}$$

But (12) is impossible when $p \not\equiv 1 \pmod q$ because then 3a holds, and A_{10} which is of the highest order cannot be permutable with B^v where $v \not\equiv 0 \pmod q$ since this implies that A_{10} is permutable with B. (When $v \not\equiv 0 \pmod q$ there is a k such that $v k \equiv 1 \pmod{q^m}$ and k iterated transformations of A_{10} with B^v will give $B^{vk} A_{10} = A_{10} B^{-vk}$ and hence $B A_{10} = A_{10} B$.) Hence $i - j \equiv 0 \pmod q$ if two elements A_{1i} and A_{1j} in the cycle are alike and the number of different elements in the cycle is $\equiv 0 \pmod q$.

3 c. When two cycles contain some element in common they contain all elements in common.

If there were an element A_{2j} belonging to a cycle C_2 contained in the cycle C_1 constructed on A_{10}, then for some i:

$$B^i A_{10} B^{-i} = A_{2j}. \tag{13}$$

But then $B^v A_{2j} B^{-v}$ will also belong to C_1 for all v ($B^v A_{2j} B^{-v} = B^{v+i} A_{10} B^{-v-i}$ according to (13)), and since the cycle C_2 may be constructed on A_{2j} (as on every other element belonging to the cycle C_2) we get that $C_1 = C_2$.

3a, 3b and 3c then give that when $p > q^s$ and $p \not\equiv 1 \pmod q$ every element of the highest order in $G_p r$ belongs to one and only one cycle of the type described. Hence the number N of elements of the highest order in $G_p r$ must be a multiple of q, because in every cycle the number of different elements is a multiple of q (according to 3b). The number of highest-order elements in $G_p r$ is

$$N = p^u \varphi(p^t) = p^{u+t-1}(p-1)$$

(which means A_2^i for all i combined with the A_1^j where $(j, p^t) = 1$).

Hence

$$p^{u+t-1}(p-1) \equiv 0 \pmod q.$$

But since $(p, q) = 1$ we get

$$p - 1 \equiv 0 \pmod q$$

which contradicts the assumption that $p \not\equiv 1 \pmod q$. This means that no B ($\neq E$) can be non-permutable with both A_1 and A_2 when $p > q^s$ and $p \not\equiv 1 \pmod q$. Thus Lemma 3 is proved.

Lemma 4. When $p > q^s$ and $p^2 \not\equiv 1 \pmod q$, an element $B\ (\neq E)$ in a subgroup G_{q^s} of the group $G_{p^r q^s}$ cannot be non-permutable with both of two base elements generating an Abelian subgroup G_{p^r} and being of the same order.

4 a. Like 3a with the difference that when $p^t = p^u$, $A_i\ (= A_1^h A_2^k)$ is of the highest order provided that h or k or both are incongruent 0 modulo p.

4 b. Like 3b.

4 c. In this case the value of N is

$$N = p^t \varphi(p^t) + (p^t - \varphi(p^t))\varphi(p^t) = p^{2(t-1)}(p^2 - 1).$$

Hence because N must be a multiple of q

$$p^{2(t-1)}(p^2 - 1) \equiv 0 \pmod q$$

and since $(p, q) = 1$ we get

$$p^2 - 1 \equiv 0 \pmod q.$$

Hence we get that in this case no $B\ (\neq E)$ can be non-permutable with both A_1 and A_2 when $p > q^s$ and $p^2 \not\equiv 1 \pmod q$. ($p^2 \not\equiv 1 \pmod q$ implies that $p \not\equiv 1 \pmod q$, which is a condition needed for the proof.)

Lemmas 2, 3 and 4 immediately give the theorem.

A consequence of the theorem, together with the result mentioned in the beginning, is that when $p > q^s$ and $p^2 \not\equiv 1 \pmod q$ there are only as many abstract groups of order $p^2 q^s$ as twice the number of abstract groups of order q^s, because in this case there are only two groups of order p^r, the Abelian groups (2) and (1,1) and each of them determines one and only one group of order $p^2 q^s$ together with a given group of order q^s. For instance, when $p > q^4$ and $p^2 \not\equiv 1 \pmod q$, there are 30 groups of order $p^2 q^4$.

Uppsala Universitet.

Tryckt den 6 oktober 1954

Uppsala 1954. Almqvist & Wiksells Boktryckeri AB