On groups with finite classes of isomorphic subgroups.

By L. FUCHS in Budapest.

To my dear Father on the occasion of his 70th birthday.

§ 1. Introduction.

The set of all subgroups of a given group G can be divided into classes in the following manner: we let two subgroups belong to the same class if and only if they are isomorphic. In a finite group G these classes of isomorphic subgroups possess both of the properties:

(i) there is but a finite number of subgroups in each class,[1])

(ii) there is but a finite number of classes.

It is readily seen that, conversely, any group G with both of the properties (i) and (ii) (in other words, with a finite number of different subgroups) must be finite. As a matter of fact, first of all (i) implies that G is a torsion group, since $\{a\}, \{a^2\}, \ldots$ are different isomorphic subgroups for an element a of infinite order. Further, (ii) implies that the orders of the elements in G constitute a finite set of natural integers; finally, again from (i) we conclude that the set of elements of order n is finite for any fixed n, q. e. d.

On the other hand, it is fairly trivial that there are infinite groups with only one of the properties (i), (ii). Our aim in this note is to characterize all groups with property (i).

Let us remark that certain special cases of this problem have already been discussed. Namely, it has been shown by T. SZELE [7][2]) that a group with only *one* subgroup in each class is isomorphic to some subgroup of the group of all complex roots of unity[3]) (or, in an additive realization: a subgroup of the additive group of all rational numbers modulo 1), and con-

---

[1]) In what follows the term "class" is used for the longer phrase "class of isomorphic subgroups".

[2]) Numbers in brackets refer to the Bibliography given at the end of this paper.

[3]) This group is known to be the direct product of quasicyclic p-groups, exactly one for each prime p.

versely. Further, the present author [4] has characterized all abelian groups in which the classes of isomorphic non-trivial subgroups contain the same finite number $k > 1$ of subgroups: these are finite abelian groups of type (p, p) and (p, p, p) for some prime p. These results are also contained in our discussions.

In order to make the paper easier readable, we have collected in § 2 the terminologies and known facts which are not quite familiar and are needed in what follows.[4]) Then we proceed to consider in § 3 the stated problem only for abelian p-groups; we shall make use of this result in § 4 when we discuss the problem in whole generality. It will turn out that *a group G has property* (i) *if and only if it is a central extension of a group isomorphic to some subgroup of the group of all complex roots of unity by a finite group.* This main result shows the interesting fact that there is no great difference in the group structure if one assumes that each class contains a finite number of subgroups or else but a single subgroup. The final § 5 discusses the problem of [4] without preassuming commutativity; the result is the same as in [4].

§ 2. Preliminaries.

By an FCIS-*group* we shall mean a (multiplicative) group G with finite classes of isomorphic subgroups. It is immediate that in an FCIS-group G there is but a finite number of elements of any given order, in other words, G is an FO-group in the sense of R. BAER [1]. This implies that G is a torsion group, i. e. it contains no element of infinite order.

Since any element (any subgroup) and its conjugates have the same order (are isomorphic), it follows that in G the classes of conjugate elements (subgroups) are finite; hence G is an FC-group.[5]) The number of elements (subgroups) conjugate to a given element a (subgroup A) of G is known to be equal to the index of the normalizer of a (A) in G; consequently, the normalizer of any element (subgroup) has a finite index in G.

By a p-group is meant a group in which the orders of the elements are powers of one and the same prime p. Any G contains a maximal p-subgroup called a Sylow p-group of G. If G is an FCIS-group, then its Sylow p-subgroups have but a finite number of conjugates, and therefore, by the generalized Sylow theorems,[6]) the Sylow p-subgroups of G are conjugate to each other for each prime p. If for some p there is but one Sylow p-subgroup then it is a normal subgroup of G.

---

[4]) For the basic concepts we refer to KUROSH [5], SPEISER [6] or ZASSENHAUS [8].

[5]) An FC-group is defined to be a group with finite classes of conjugate elements. For its fundamental properties we refer e. g. to ERDŐS [3].

[6]) See e. g. KUROSH [5], § 54.

A (commutative) p-group Q is called quasicyclic (or of type p^∞) if it has a generating system $a_1, a_2, \ldots$ with the defining relations

$$a_1^p = e, \quad a_{n+1}^p = a_n \qquad (n = 1, 2, \ldots)$$

where e is the group identity. By an important and well-known theorem of R. BAER, a quasicyclic group is a direct factor of any abelian group containing it. For each n, Q contains a unique subgroup of order p^n; this is cyclic and may be generated by a_n. If an abelian p-group contains but a finite number of elements of order p then it is the direct product of a finite number of cyclic and/or quasicyclic p-groups. If $q_1, \ldots, q_t$ are prime powers, then the direct product of the cyclic groups of order $q_1, \ldots, q_t$, respectively, is called an (abelian) group of type $(q_1, \ldots, q_t)$.

$O(a)$ will denote the order of the group element a. The same notation: $O(A)$ will be applied to denote the order of a group A. For a subset S of a group G, $\{S\}$ will denote the subgroup generated by S.

The centralizer of a subset S of G is the set of all x in G with $xa = ax$ for all $a \in S$. The center C of G is the centralizer of G. If $D \subseteq C$ and $G/D \simeq F$, then G will be called a central extension of D by F.

Finally, we mention a theorem due to A. DICMAN [2] and R. BAER [1] implying that in a torsion FC-group (and therefore in an FCIS-group) G any finite set of elements may be imbedded in a finite normal subgroup of G.

§ 3. The case of abelian p-groups.

We begin our discussions with the simplest case when the group dealt with is an abelian p-group; this result will be needed in what follows.

Lemma 1. *An abelian p-group G is an FCIS-group if and only if it is either a finite abelian p-group or the direct product of such a group by a quasicyclic group.*

Assume G is an abelian p-group with finite classes of isomorphic subgroups. G contains but a finite number of elements of order p, so that it is a direct product of a finite number of cyclic and quasicyclic p-groups. What remains to be proved is that there is not more than one quasicyclic component. Suppose A and B are two distinct quasicyclic components with the generators $a_1, a_2, \ldots$ resp. $b_1, b_2, \ldots$ connected by the defining relations

$$a_1^p = e, \; a_{n+1}^p = a_n; \; b_1^p = e, \; b_{n+1}^p = b_n \qquad (n = 1, 2, \ldots).$$

Then the subgroup A_n generated by the elements $a_1, \ldots, a_n, a_{n+1}b_1, a_{n+2}b_2, \ldots$ is again a quasicyclic subgroup of G such that the subgroups $A_1, A_2, \ldots$ are all different, for clearly we have $A \cap A_n = \{a_n\}$. Therefore G has the stated structure, indeed.

Conversely, let G have the structure in question. That G can not contain infinitely many distinct isomorphic subgroups of *finite* order, follows at once from the fact that G is an FO-group. In order to prove the same fact for *infinite* subgroups too, observe that any infinite subgroup F of G must again be the direct product of a finite abelian p-group and a quasicyclic group; further G contains only one quasicyclic group (this is the uniquely determined maximal complete subgroup of G). Since the finite direct components of isomorphic infinite subgroups must again be isomorphic, we infer that there is but a finite number of possibilities for choosing isomorphic distinct infinite subgroups, and this is what we intended to show.

Here we point out to the fact that if we assume that the p-group P contains no two different subgroups isomorphic to each other, then P is necessarily commutative, for, given two elements a and b, we have either $O(a) \mid O(b)$ or $O(b) \mid O(a)$ and hence either $\{a\} \subseteq \{b\}$ or $\{b\} \subseteq \{a\}$. Therefore Lemma 1 implies at once:

Lemma 2. *A p-group P contains no two distinct isomorphic subgroups if and only if it is a cyclic or a quasicyclic p-group.*

The main result of SZELE's paper (mentioned in § 1) follows immediately from Lemma 2. In fact, if G is a group with no two different isomorphic subgroups, then G is a torsion group and for each prime p there is exactly one Sylow p-group of G, whence G is the direct product of p-groups. The application of Lemma 2 to the p-components of G leads us to the conclusion that G is isomorphic to some subgroup of the group of all complex roots of unity. The converse is almost trivial.

§ 4. The main result.

Let now G be an arbitrary FCIS-group and consider the center C of G. C is the direct product of its p-components C_p where C_p — as a commutative p-group of the FCIS-property — is a group described by Lemma 1. First of all we intend to show

Lemma 3.[7]) *The factorgroup G/C of an FO-group G with respect to its center C contains but a finite number of cosets whose order is a power of a fixed prime p.*

In fact, let a be an element of a possibly least order in a coset $[a]$ of G/C of order p^r. Then $O(a) = p^s$ with $s \geqq r$, for if we had $O(a) = p^s n$ with $n > 1$ and $(n, p) = 1$, then by solving the equation $nu + p^s v = 1$ for rational

[7]) The statement of this lemma is due to BAER [1]. The proof given here, although different from BAER's proof, owes something to [1].

integers u, v, we should get

$$a = a^{uu} a^{p^s v} = a'a'' \quad \text{with} \quad a'' \in C,\ O(a') = p^s < O(a),$$

in contradiction to the choice of a in $[a]$. — Let p^t be the maximum of the orders of the elements in the finite direct factor of C_p. If C_p itself is finite then obviously $O(a) \leqq p^{r+t}$ and if C_p is infinite then $a^{p^{r+t}}$ is either e or $\neq e$ and in this latter case it belongs to the quasicyclic direct factor of C_p whence $a^{p^{r+t}} = c^{p^{r+t}}$, $(ac^{-1})^{p^{r+t}} = e$ for some $c \in C_p$, which contradicts the choice of a in the coset $[a] = [ac^{-1}]$. Thus we may conclude that in G/C the set of cosets of order $\leqq p^r$ is finite. But there must exist an integer m for which G/C does not contain cosets of order $\geqq p^m$, for in the contrary case from what has been shown it follows the existence of a sequence of elements $a_1, a_2, \ldots$ not in C such that their orders are powers of p and $a_1^p \in C, a_{n+1}^p \equiv a_n \pmod{C}$ for $n = 1, 2, \ldots$ The normalizer N of some element not commuting with $a_1 (\notin C)$ contains C and is of finite index in G, hence there exist elements a_i and a_j $(i < j)$ such that $a_i \equiv a_j \pmod{N}$. Therefore $a_j^{p^{j-i}} \equiv a_j \pmod{N}$ and, the order of a_j being a power of p, we arrive at $a_j \in N$, so that $a_1 \in N$, a contradiction. And this completes the proof of our Lemma 3.

What we have now verified implies that the set $\mathfrak{S}_p$ consisting of all elements in G whose order is some power of a fixed p is contained in a finite number of cosets modulo C. Hence the centralizer Z_p of $\mathfrak{S}_p$ is the meet of the normalizers of a finite number of elements of $\mathfrak{S}_p$, and since the meet of a finite number of subgroups of finite index is again of finite index, we obtain the finiteness of the index of Z_p in G. This leads us to the conclusion that Z_p *contains almost all* (i. e. all except for a finite number of) *the Sylow q-subgroups of* G. This is a fortiori true if Z_p is the centralizer of some subset of $\mathfrak{S}_p$.

Next let us consider the p-subgroups of G and assume that there is an infinite set of different primes $p_1, p_2, \ldots$ for which G contains at least two distinct isomorphic p-groups, say, A_{p_i} and B_{p_i}. Denote by $Z^*_{p_i}$ the centralizer of the union $A_{p_i} \cup B_{p_i}$. Now we omit the primes $p_i (\neq p_1)$ for which A_{p_i} and B_{p_i} do not belong to $Z^*_{p_1}$ — in view of the preceding paragraph these are finite in number, — and then repeat this process instead of p_1 for the next remaining prime of the sequence $p_2, p_3, \ldots$, and so on. Considering that if A_{p_j} and B_{p_j} belong to $Z^*_{p_i}$ then A_{p_i} and B_{p_i} belong to $Z^*_{p_j}$, the result of the latter process is an infinite subsequence $q_1, q_2, \ldots$ of $p_1, p_2, \ldots$ having the property that for all $i \neq j$ the groups A_{q_i} and B_{q_i} lie in the centralizer of $A_{q_j} \cup B_{q_j}$. Consequently, the groups A_{q_i}, B_{q_i} are permutable with A_{q_j} and B_{qj} for different primes q_i and q_j, and therefore selecting for each q_i one of A_{q_i} and B_{q_i}, we obtain a direct product in G. All of these direct products are different but isomorphic, so that we get a contradiction to the FCIS-property of G; this shows that *for almost all primes p, the group G does not contain distinct isomorphic p-subgroups.* In particular, for almost all primes p

there is but one Sylow p-group with no two different isomorphic subgroups; this unique Sylow p-subgroup is a normal subgroup of G and is, by Lemma 2, a cyclic or a quasicyclic p-group. Let us denote by D the direct product of these Sylow p-groups.

We consider the primes which occur as orders of elements in G but not in D. The set of these primes is finite: $p_1, \ldots, p_k$. The cross-cut of the centralizers $Z_{p_1}, \ldots, Z_{p_k}$ of the sets $\mathfrak{S}_{p_1}, \ldots, \mathfrak{S}_{p_k}$, respectively, contains the Sylow p-groups of G for almost all primes p, hence contains almost all p-components of D. Furthermore it is clear that D lies in the centralizer of any of its elements. Consequently, the factorgroup G/C contains p-subgroups only for a finite number of primes p, and in view of Lemma 3 it results that G/C is finite. C contains but a finite number of p-components C_p which are proper direct products of cyclic groups and possibly a quasicyclic group; thus if we omit from C a finite number of cyclic p-groups in the obvious manner, we get a subgroup C^* of C which is isomorphic to a group consisting of some complex roots of unity and C^* is still of finite index in G. This establishes the necessity part of the following theorem.

Theorem 1. *G is an FCIS-group if and only if it is a central extension of a group isomorphic to some subgroup of the multiplicative group of all complex roots of unity, by a finite group.*

In order to prove even the sufficiency of the condition contained in this theorem, first of all we show that a group G which is a central extension of a group C^* isomorphic to some group of complex roots of unity by a finite group, may be represented as a direct product:

$$G = F \times H$$

where $F \subseteq C^*$, H contains elements of order p but for a finite number of primes p, and the orders of the elements in F are relatively prime to those in H. Take a representative system modulo C^*: $g_1, \ldots, g_k$, and then form the subgroup $G^* = \{g_1, \ldots, g_k\}$. G^* is a finite group, for evidently G is now an FC-group, and therefore the p-components of C^* for all the primes p which occur as orders of elements in G^*, generate together with G^* a group H. The remaining p-components of C^* generate a group F. Obviously, $F \cap H = e$; F and H are normal subgroups of G. On account of the fact that the orders of the elements in F and H are by construction relatively prime, we must have $G = F \times H$ satisfying the requirements; q. e. d.

Now, if T is some subgroup of G, then $T = (F \cap T) \times (H \cap T)$ holds, since G is a torsion group, and F, H do not contain elements of the same order. C^* and hence F does not contain distinct isomorphic subgroups, and thus $T_1 \cong T_2$ implies not only $F \cap T_1 \cong F \cap T_2$ but also $F \cap T_1 = F \cap T_2$. Therefore it will suffice to verify that in H there are no infinitely many distinct isomorphic subgroups T.

Hypothesis implies that H contains but a finite number of quasicyclic p-groups: $A_{p_1}, \ldots, A_{p_s} (\subseteq C^*)$ where $p_1, \ldots, p_s$ are different primes. The direct product $A = A_{p_1} \times \ldots \times A_{p_s}$ is of finite index in H, thus a representative system modulo A generates a finite subgroup B of H such that $\{A, B\} = H$. Let $O(B) = n$ and A_1 the subgroup generated by those elements of A which are of order $\leqq n$. Then $B_1 = \{B, A_1\}$ is again a finite subgroup of H; let r be the number of all subgroups of B_1. Now, if T is any subgroup of H, then consider the powers $p_i^{k_i}$ which occur as orders of elements in T. If k_i is not bounded for some p_i, then for this prime A_{p_i} exists and is surely contained in T. For the primes p_i of bounded exponents k_i, we take the least upper bound m_i and then consider a cyclic subgroup $A_{p_i}^{(m_i)}$ of order $p_i^{m_i}$ in T. For the sake of uniformity we may set $A_{p_i} = A_{p_i}^{(m_i)}$ if $m_i = \infty$. Then

$$T' = \{A_{p_1}^{(m_1)}, \ldots, A_{p_s}^{(m_s)}\}$$

is a subgroup in T such that T may be written in the form

$$T = \{T', B'\} \qquad \text{for some } B' \subseteq B_1.$$

Now if T and S are isomorphic subgroups of H, then the corresponding groups T' and S' are generated by isomorphic $A_{p_i}^{(m_i)}$. Since at most n different groups $A_{p_i}^{(m_i)}$ may exist for fixed p_i and m_i, we obtain that H contains at most $n^s r$ different subgroups isomorphic to T. This completes the proof of Theorem 1.

The last part of our proof implies the interesting

Corollary. *In an FCIS-group the number of subgroups in the classes of isomorphic subgroups is bounded.*[8])

§ 5. The case if the classes contain the same number of subgroups.

If G is an FCIS-group then the classes containing G and $\{e\}$ respectively, are exhausted by these trivial subgroups of G. Leaving these trivial cases out of consideration, it may happen that all other classes (i. e. the classes of the non-trivial isomorphic subgroups) consist of the same number $k > 1$ of subgroups. The problem of determining all groups with this special property has been discussed in [4] for abelian groups only; now we solve this problem without preassuming commutativity.[9])

Suppose that in G the classes of non-trivial isomorphic subgroups contain the same number $k > 1$ of subgroups. Then G is a torsion group and there is a prime p for which G contains elements of order p. The set of these elements is finite, and G being an FC-group, this finite set generates a finite subgroup F of G. It is quite evident that G contains no sub-

[8]) Therefore Theorem 1 describes at the same time the structure of all groups in which the classes contain a bounded number of subgroups.

[9]) In the proof we need almost nothing from the discussions above.

group isomorphic to but different from F. Hence by $k>1$ we obtain $F=G$, i. e. *G is a finite group.*

If G is not a p-group, then let us consider the Sylow p-groups of G. Their number is equal to k and is $\equiv 1 \pmod p$ for each prime p dividing the order n of G. But k is the index of the normalizer of any Sylow p-group and therefore k divides n what is incompatible with the last congruence. This inference shows that *G is a p-group.* — Let the order of G be denoted by $n=p^s$; we may assume $s>1$, for the trivial case $s=1$ (in which G has only trivial subgroups) may be excluded.

By a known theorem,[10]) in the p-group G the number of subgroups of a given order p^r is $\equiv 1 \pmod p$ where $r<s$. If $r=1$, we get $k\equiv 1 \pmod p$. Applying this result to $r=2$, and taking into account that there are exactly two types of groups of order p^2: the abelian groups of type (p^2) and (p,p), respectively, we conclude that, by the FCIS-property of G, in G only one type can exist. G as a finite p-group has a non-trivial center C which must contain a subgroup of order p. This group, together with any other group of order p (such a subgroup necessarily exists in G, because of $k>1$), generates an abelian group of type (p,p). Therefore G contains no cyclic group of order $\geqq p^2$, i. e. *all of its elements $\neq e$ are of order p.*

If $n=p^2$, we obtain the group of type (p,p).

If $n=p^3$, then the number of subgroups of order p is equal to

$$k=\frac{p^3-1}{p-1}=p^2+p+1.$$

If any two of them generate an abelian subgroup of type (p,p), then the number of subgroups of order p^2 is

$$\binom{p^2+p+1}{2} : \binom{p+1}{2} = p^2+p+1$$

($p+1$ is the number of different subgroups of order p in the group of type (p,p)). This is equal to k, and therefore in G any two subgroups of order p must generate a subgroup of order p^2. This fails to happen in the non-commutative p-group of order p^3 ($p\geqq 3$) all of whose elements are of order p. Indeed, such a group is generated by two elements a, b connected by the defining relations $a^p=b^p=(a^{-1}b^{-1}ab)^p=e$, $b^{-1}aba^{-1}=a^{-1}b^{-1}ab$, $ba^{-1}b^{-1}a=$ $=a^{-1}b^{-1}ab$. It follows that G is an abelian group of type (p,p,p). On the other hand, such a group has the properties required.

Finally, we show that $n\geqq p^4$ is impossible. To this end we consider the subgroups of order p^3 in G; such groups surely exist in G.

If G contains no non-commutative subgroup of order p^3, then all of its subgroups of order p^3 are abelian of type (p,p,p). k — determined as the

[10]) See e. g. SPEISER [6] or ZASSENHAUS [8].

number of subgroups of order p — is equal to $\frac{p^s-1}{p-1}$. Let N denote a subgroup of the center C of G with $O(N)=p$. N is contained in $\frac{p^s-p}{p^2-p}$ subgroups of type (p,p). Taking into account that the total number of subgroups of order p^2 must be equal to $k=\frac{p^s-1}{p-1}$, we obtain that

$$\frac{p^s-1}{p-1}-\frac{p^s-p}{p^2-p}=p^{s-1}$$

is the number of subgroups of type (p,p) not containing N. Together with N each of these subgroups generates an abelian group of type (p,p,p); their number equals

$$p^{s-1}:\frac{(p^3-p)(p^3-p^2)}{(p^2-1)(p^2-p)}=p^{s-3}.$$

Thus the number of subgroups of type (p,p,p) containing N is divisible by p. But this number must be equal to the number of all subgroups of type (p,p) in the factorgroup G/N and this number leaves the remainder 1 when divided by p.

On the other hand, if G contains a non-commutative group of order p^3,[11]) then it can not contain abelian subgroups of type (p,p,p). The center C of G is now of order p, for if C contained a group of type (p,p) then this group and any subgroup not contained in it which is of order p, would generate a group of type (p,p,p) in G. A similar argument leads us to the result that any subgroup of type (p,p) must contain C. Consequently, the number of subgroups of type (p,p) is $\frac{p^s-p}{p^2-p}=\frac{p^{s-1}-1}{p-1}$, and this is surely different from the number $\frac{p^s-1}{p-1}$ of subgroups of order p in G.

The last two paragraphs complete the proof of the impossibility of $n\geqq p^4$. Hence we arrive at the following result.

Theorem 2.[12]) *In a group G the classes of non-trivial isomorphic subgroups contain the same number $k>1$ of subgroups if and only if G is a finite abelian group of type (p,p) or (p,p,p).*

---

[11]) This second alternative is only in case $p\geqq 3$ possible.

[12]) The case when the set of classes of non-trivial isomorphic subgroups is void is tacitly excluded.

Bibliography.

[1] R. Baer, Finiteness properties of groups. *Duke Math. J.* **15** (1948), 1021—1032.
[2] А. П. Дицман, О *p*-группах. Докл. Акад. Наук СССР. **15** (1937), 71—76.
[3] J. Erdős, The theory of groups with finite classes of conjugate elements. *Acta Math. Acad. Sci. Hung.* **5** (1954), 45—58.
[4] Л. Фукс, Об абелевых группах, в которых классы изоморфных собственных подгрупп содержат одинаковое число подгрупп, Чехословацкий Мат. Ж. **2** (77) (1952), 387—390.
[5] А. Г. Курош, Теория групп (Москва, 1953).
[6] A. Speiser, *Die Theorie der Gruppen von endlicher Ordnung* (Berlin, 1927).
[7] T. Szele, On groups with atomic layers. *Acta Math. Acad. Sci. Hung.* **3** (1952), 127—129.
[8] H. Zassenhaus, *Lehrbuch der Gruppentheorie* (Leipzig—Berlin, 1937).

(Received May 26, 1954.)