On a problem of L. Fuchs

By JÓZSEF DÉNES in Budapest

Introduction

In his book [2] L. FUCHS raised the following problem: "Delete k elements at random in the Cayley table of a finite group G of order n. Determine the greatest $k=k(n)$ for which

(a) the rest of the table always determines G up to isomorphism;

(b) the table can be reconstructed uniquely from the rest."

The aim of this paper is to solve problem (b) without the restriction that the group is Abelian.

It will be shown that for any given group G of order $n \neq 4$ we have

$$k(n) = 2n-1.$$

Thus $k(n)$ unexpectedly does not depend on the structure of the group, it depends only on the order of the group (Theorem 1). In the case $n=4$ we get $k(n)=3$ (Theorem 2).

I thank for the useful help of Prof. L. FUCHS.

§ 1. Definitions, notations

An abstract group is completely known if each of its elements is represented by a symbol and the product of any two symbols in any given order is exhibited. In finite groups the multiplication rule is given conveniently by a square table (called the Cayley table of the group) in which the products in a row have the same left factor and the products in a column have the same right factor.

Here we shall deal with finite groups, therefore we may assume that the elements of the groups are natural numbers $1, 2, \ldots, n$. Then the Cayley table of a group G is (1) a Latin square, i. e. a quadratic matrix $\|a_{ik}\|$ each of whose rows and columns is a permutation of $1, 2, \ldots, n$; and (2) the quadrangle criterion[1]) holds, i. e., for all indices $i, j, \ldots$, the equalities $a_{ik} = a_{i_1k_1}, a_{il} = a_{i_1l_1}, a_{jk} = a_{j_1k_1}$ imply $a_{jl} = a_{j_1l_1}$.

Conversely, any matrix $\|a_{ik}\|$ with properties (1) and (2) is a Cayley table of a group G; moreover, we may choose an arbitrary row and a column, say the j-th row and the l-th column, and consider them as the products of the elements by the group

[1]) The quadrangle criterion was at first pointed out by FROLOV in [1].

identity from the left and from the right, respectively. Then a_{jl} will be the identity of the arising system G_{jl}, and necessarily $a_{il}a_{jk} = a_{ik}$. Now (1) ensures that G_{jl} is a loop and (2) implies associativity, thus G_{jl} is a group. Clearly, any group with the same Cayley table arises in this way.

All these G_{jl} are isomorphic, for a transition from G_{jl} to G_{rs} means simply that we take three permutations ϱ, σ, τ such that $a \times b = c$ in G_{rs} if and only if $\varrho(a)\sigma(b) = \tau(c)$ in G_{jl}, i. e., the G_{jl} and G_{rs} are isotopic, and hence isomorphic groups.

Note that different multiplication tables of a group can be transformed into one another by row and column interchanges.[2])

If $\|a_{ik}\|$ and $\|b_{ik}\|$ are two Cayles tables, with the same number of rows, then we call the i-th rows corresponding rows, the k-th columns corresponding columns, and a_{ik} and b_{ik} corresponding elements.

Any permutation may be written as product of disjoint cycles. If all these cycles have the same length, the permutation is called regular. If for the permutations σ, τ we have $\sigma(a) \neq \tau(a)$ exactly for k letters a, then we say that they differ in k places.

Deleting k arbitrary elements in the Cayley table of a finite group G of order n, let $k(G)$ denote the greatest number of elements for which the table can be reconstructed uniquely from the rest.

§ 2. Determination of $k(G)$

Lemma 1. *Let π and ϱ denote two distinct regular permutations of degree n and of order l, m ($m \leqq l \leqq n$), respectively. If n is even and π, ϱ are of the form*

$$\pi = (i_1 i_2 \ldots i_n), \quad \varrho = (i_1 i_2 \ldots i_{\frac{n}{2}})(i_{\frac{n}{2}+1} \ldots i_n),$$

then they differ in two places. In all other cases they differ at least in three places.

Proof. Let us suppose that π and ϱ differ in two places. Then there is a transposition τ such that $\pi = \varrho\tau$. Both π and ϱ are products of disjoint cycles. If the letters of τ belong to the same cycle of ϱ, then in the product $\pi\tau$ this cycle splits into two, while in the other case the converse situation holds[3]). As π and ϱ are regular, they must have the indicated form.

Lemma 2. *Two different Cayley tables, A and A', of a group G differ from each other at least in $2n$ places.*

Proof. If all the corresponding rows of the two Cayley tables are different, then every row differs from the corresponding one at least in two places, and the two Cayley tables differ at least in $2n$ places. The same argument applies if the corresponding columns are different.

For the rest of the proof we may assume that the f-th rows and the g-th columns of the two Cayley tables are equal. By the quadrangle criterion $a_{fg} = a'_{fg}$, $a_{fj} = a'_{fj}$. $a_{ig} = a'_{ig}$ imply $a_{ij} = a'_{ij}$ for all indices i, j whence $A = A'$. Thus this case cannot occur.

Lemma 3. *If G and G' are different groups of the same order n ($n \neq 4$), then their arbitrary Cayley tables, A and A' differ from each other at least in $2n$ places.*

---

[2]) Similar transformations of Latin squares are described in SCHÖNHARDT [4].

[3]) The same statement is in SERRET [5], p. 230.

P r o o f. We may suppose that at least one pair of corresponding rows of A and A' is equal. Otherwise we could use the same inference as that in the proof of Lemma 2 to obtain the desired conclusion.

Every finite group may be represented as a group of regular permutations (see e. g. JORDAN [3]). Such representations[4]) of G and G' are

$$x_i \to \begin{pmatrix} x \\ xx_i \end{pmatrix} \qquad (x_i \in G)$$

and

$$x_i' \to \begin{pmatrix} x \\ x x_i' \end{pmatrix} \qquad (x_i' \in G'),$$

where we may suppose that x varies over the elements of the equal row.

Let P, P' denote the regular permutation groups corresponding to G, G'. They are different, thus their intersection

$$H = P \cap P'$$

(a subgroup of the symmetric group of degree n) is of order $s \leqq \frac{n}{2}$. Clearly $n-s$ rows of the Cayley tables of G and G' are different, $n-s \geqq \frac{n}{2}$.

At first we consider the case when $s \leqq \frac{n}{3}$ and the set $(P \cup P') \setminus H$ does not contain both permutations of the form

$$\pi = (i_1 i_2 \dots i_n), \quad \varrho = (i_1 i_2 \dots i_{\frac{n}{2}})(i_{\frac{n}{2}+1} \dots i_n).$$

Then we have $3(n-s) \geqq 2n$.

By Lemma 1, the Cayley tables of G and G' are different at least in $3(n-s)$ places, so at least in $2n$ places.

If $s = \frac{n}{2}$ and the set $(P \cup P') \setminus H$ does not contain π and ϱ, then we show that the unequal corresponding rows differ from each other at least in four places. We verify that ψ and σ ($\psi \in P \setminus H$, $\sigma \in P' \setminus H$) differ from each other at least in four places. If they differed from each other only in three places, then there would be a cycle φ of order 3 such that $\sigma\varphi = \psi$. Taking into consideration the regularity of ψ and σ and the fact that p is a product at least two transpositions, the difference between the numbers of cycles of ψ and σ is 2, or 0. Then ψ and σ must have the form 1), or 2):

1) $\psi = (i_1 i_2 \dots i_n), \quad \sigma = (i_1 \dots i_{\frac{n}{3}})(i_{\frac{n}{3}+1} \dots i_{\frac{2n}{3}})(i_{\frac{2n}{3}+1} \dots i_n),$

2) $\psi = (i_1 \dots i_j\, i_{j+1} \dots i_{j+k}\, i_{j+k+1} \dots i_m)(\dots)(\dots)\dots,$
$\sigma = (i_1 \dots i_j\, i_{j+k+1} \dots i_m\, i_{j+1} \dots i_{j+k})(\dots)(\dots)\dots.$

As H is a subgroup of index 2 in P and P', the powers of ψ and σ of even exponents are in H. Now we restrict ourselves to the case $n > 6$. In the first alternative

[4]) Latin squares may be represented by permutations. If the Latin square is a Cayley table, then it may be represented by regular permutations. Further details may be found in SCHÖNHARDT [4].

$\psi^{n-2}\sigma^2 \in H$ and $\psi^{n-2}\sigma^2\,(i_{\frac{n}{2}}) = i_n$. Since is regular, $\psi^{n-2}\sigma^2$ must be equal to the identical permutation. But because of $\psi^{n-2}\sigma^2\,(i_{\frac{n}{2}+2}) = i_2$ this is impossible. In the second case we may suppose that ψ and σ do not consist of a single cycle, for otherwise $\{\psi\} = P$ and $\{\sigma\} = P'$ are cyclic groups and our statement is trivial. We may assume $j \geqq 3$. As $\sigma^2 \in H$, $\psi^{m-2}\sigma^2$ is regular and $\psi^{m-2}\sigma^2(i_3) = i_3$, so it is the identical permutation. But because of $\psi^{m-2}\sigma^2(i_2) \neq i_2$, this is impossible.

Finally if $s \leqq \frac{n}{2}$ and $\pi, \varrho \in (P \cup P') \setminus H$ then $P = \{\pi\}$, $P' = \{\sigma, \varrho\}$ where σ is an arbitrary element of P' not in $\{\varrho\} = R$. Clearly $P \cap R = \varepsilon$ (the identical permutation) as every cycle of a power $\pi^k (\neq \varepsilon)$ contains letters both larger and smaller than $\frac{n}{2}$; and this is impossible for the elements of R. So $H \cap R = \varepsilon$. Therefore the products $\alpha\beta$ $(\alpha \in H, \beta \in R)$ are different. As the index of R is 2, the order of H is at most 2. Therefore we may have only two equal rows in arbitrary Cayley tables of G and G'.

Let us suppose that among the elements of $P \setminus H$ and $P' \setminus H$ there are pairs, other than π and ϱ and their inverses whose letters differ from each other in two places. If π^k, ϱ' $(\pi^k \neq \pi, \varrho' \neq \varrho)$ is such a pair, then ϱ' would not be an element of $\{\varrho\}$, $\varrho' \notin \{\varrho\}$, $\varrho'\varrho$ would not be regular.

As the elements of the sets $P \setminus H$ and $P \setminus H$ differ at least in three places from each other, except for π and ϱ, arbitrary Cayley tables of G and G' differ at least in $3(n-4)+2\cdot 2$ places from each other. This number is $\geqq 2n$ when $n > 7$.

It remains to consider the cases when $n \leqq 7$. If n is a prime number, then all groups of order n are cyclic groups and so our statement is trivial.

The only case that remained is $n = 6$. In view of Lemma 2, we may without loss of generality suppose that G and G' are not isomorphic, and so the groups in question are the cyclic and the dihedral groups of order six. Now

$$P = \{(123456)\}, \qquad P' = \{(123)(456), (16)(25)(34)\}.$$

H cannot contain the only permutation $(14)(25)(36)$ of order 2 because $\varrho(14)(25)(36) = (123)(456)(14)(25)(36) = (153426)$ and $(153426) \notin P'$. Thus $s = 1$ and therefore arbitrary Cayley tables of G and G' differ from each other in $3(n-3) + 2\cdot 2 = 3n - 5 = 13 > 2\cdot 6$ places. This finishes the proof of Lemma 3.

Theorem 1. *For a group G of order n we have*

$$k(G) = 2n - 1 \qquad (n \neq 4).$$

Proof. Let us delete $2n-1$ arbitrary elements in a Cayley table A of the group G of order $n (n \neq 4)$. Suppose that there is a Cayley table A' $(A \neq A')$ of G having the property that the rest of A may be completed to A'. Then clearly, A and A' differ in $2n-1$ places, which is impossible because of Lemmas 2 and 3.

We have to prove now that we can delete $2n$ elements of a Cayley table A of a group G of order n, such that the rest of the table may be completed to a Cayley table A' different from A. If we exchange arbitrary symbols, a and b, throughout in A, then we obtain a new Cayley table differing from A exactly in $2n$ places. So the proof of our statement is completed.

Corollary. *Two different Cayley tables of arbitrary groups of order n $(n \neq 4)$ are different from each other at least in $2n$ places.*

Theorem 2. *An arbitrary Cayley table of the cyclic group of order* 4 *differs at least in four places from an arbitrary Cayley table of Klein's group.*

Proof. The two Cayley tables given below are different in four places.

a	b	c	d
b	c	d	a
c	d	a	b
d	a	b	c

(cyclic group of order 4)

a	b	c	d
b	a	d	c
c	d	a	b
d	c	b	a

(KLEIN's group)

In order to complete our proof we have to show that all distinct Latin squares are different from each other in at least four places.

This follows from the fact that if two corresponding rows (columns) are unequal, then they differ at least in two places. Thus if there is a pair of unequal corresponding rows, then there are at least two pairs of unequal columns, and therefore at least four different places.

§ 3. Remarks

The following statements are immediate consequences of our results above:

1) The result remains the same if we restrict the class of groups to any one of the following classes of finite groups: (i) solvable groups; (ii) nilpotent groups; (iii) abelian groups; (iv) cyclic groups.

2) If we suppose that the Cayley tables have to be normal, then[5] $k(G) = 2n-1$ for all n (inclusively the case $n=4$).

It seems to be natural to raise the following problem:

What is the number of multiplication tables of distinct groups of order n that differ from each other at most in m places?

References

[1] M. FROLOV, Recherches sur les permutations carrées, *Journal de Math. Spec.*, (3) **4** (1890), 111.
[2] L. FUCHS, *Abelian groups* (Budapest, 1958).
[3] C. JORDAN, *Traité des Substitutions* (Paris, 1870).
[4] E. SCHÖNHARDT, Über lateinische Quadrate und Unionen, *J. reine angew. Math.*, **163** (1930), 183–229.
[5] J. H. SERRET, *Handbuch der höheren Algebra*, 2. Auflage (Leipzig, 1879).
[6] A. SPEISER, *Theorie der Gruppen von endlicher Ordnung* (Basel, 1956).
[7] H. J. ZASSENHAUS, *The Theory of Groups* (New York, 1958).

(Received June 13, 1961)

[5]) A Cayley table is called normal if its main diagonal contains only unit elements. For some properties of normal Cayley tables see ZASSENHAUS [7], p. 29.