Pacific Journal of Mathematics

COMPLETE MAPPINGS OF FINITE GROUPS

MARSHALL HALL AND LOWELL J. PAIGE

Vol. 5, No. 4 December 1955

COMPLETE MAPPINGS OF FINITE GROUPS

MARSHALL HALL AND L. J. PAIGE

1. Introduction. A complete mapping of a group G is a biunique mapping $x \longrightarrow \Theta(x)$ of G upon G such that $x \cdot \Theta(x) = \eta(x)$ is a biunique mapping of G upon G. The finite, non-abelian groups of even order are the only groups for which the question of existence or non-existence of complete mappings is unanswered. In a previous paper [4], some progress toward the solution of this problem has been made. We shall show that a necessary condition for a finite group of even order to have a complete mapping is that its Sylow 2-subgroup be non-cyclic, and that this condition is also sufficient for solvable groups. We shall also prove that all symmetric groups $S_n (n > 3)$ and alternating groups A_n possess complete mappings. In the light of these results the following conjecture is advanced:

CONJECTURE. *A finite group G whose Sylow 2-subgroup is non-cyclic possesses a complete mapping.*

It is interesting to compare this conjecture with the results of Bruck [2, p. 105].

2. Complete mappings for the symmetric and alternating groups. The following theorem is a generalization of Theorem 4, [4] and will be necessary for considerations of this and other sections.

THEOREM 1. *Let G be a group, H a subgroup of finite index $(G:H) = k$*[1]. *Let $u_1, u_2, \cdots, u_k$ be a set of elements of G that form both a right and left system of representatives for the coset expansions of G by H. Let S and T be permutations of the integers $1, 2, \cdots, k$ such that*

$$u_i(u_{S(i)}H) = u_{T(i)}H, \qquad i = 1, 2, \cdots, k.$$

[1] The restriction that the index be finite is unnecessary. However, P. Bateman [1] has shown that all infinite groups possess complete mappings and so we have chosen the present restriction for simplicity. In fact, the restriction that G be finite would seem appropriate.

Received December 18, 1953. The work of L. J. Paige was supported in part by the Office of Naval Research.

Pacific J. Math. 5 (1955), 541-549

Then, if there exists a complete mapping for the subgroup H, there exists a complete mapping of G.

COROLLARY 1. *Let G be a factorizable group; that is, $G = A \cdot B$, where A and B are subgroups of G with $A \cap B = 1$. If complete mappings exist for A and B, then there exists a complete mapping for G.*

COROLLARY 2. *If H is a normal subgroup of G, and both H and G/H possess complete mappings then G possesses a complete mapping.*

Proof. By hypothesis,

$$G = u_1H + u_2H + \cdots + u_kH = Hu_1 + Hu_2 + \cdots + Hu_k; \tag{1}$$

and thus the equation

$$u_{S(i)}p = p^* \cdot u_{[S(i),p]}, \qquad (i = 1, 2, \cdots, k),\ p \in H, \tag{2}$$

uniquely defines p^* and $u_{[S(i),p]}$ as functions of p and i. Here, $u_{[S(i),p]} = u_t$ for some $1 \leq t \leq k$. Moreover, p is uniquely defined by p^* and i, for if

$$u_{S(i)}p_1 = p^* u_{[S(i),p_1]},\ u_{S(i)}p_2 = p^* u_{[S(i),p_2]},$$

then we would have

$$u_{[S(i),p_1]}\, p_1^{-1} = u_{[S(i),p_2]}\, p_2^{-1}.$$

Since the u's form a system of representatives this would imply

$$u_{[S(i),p_1]} = u_{[S(i),p_2]}$$

and consequently $p_1 = p_2$.

We have assumed that there exists a complete mapping for H; hence, there is a biunique mapping Θ_1 of H upon H such that the mapping $\eta_1(p) = p \cdot \Theta_1(p)$ is a biunique mapping of H upon H.

Let us define a mapping of G *upon* G in the following manner:

$$\Theta(u_ip^*) = u_{[S(i),p]} \cdot \Theta_1(p), \tag{3}$$

where p, p^*, $u_{[S(i),p]}$ are defined by (2).

In order to show that Θ is biunique, assume that

$$\Theta(u_i p_1^*) = \Theta(u_j p_2^*).$$

Then,

$$u_{[S(i),\,p_1]} \cdot \Theta_1(p_1) = u_{[S(j),\,p_2]} \cdot \Theta_1(p_2);$$

and this can happen only when $u_{[S(i),\,p_1]} = u_{[S(j),\,p_2]}$ implying $\Theta_1(p_1) = \Theta_1(p_2)$ or $p_1 = p_2$. Now,

$$u_{[S(i),\,p_1]} = u_{[S(j),\,p_1]},$$

and it would follow from (2) that $i = j$. If G is finite we may conclude immediately that Θ is a biunique mapping of G *upon* G. If G is infinite, we note from (2) that if p is kept fixed, then as i ranges over $1, 2, \cdots, k$; $u_{[S(i),\,p]}$ ranges over all coset representatives. Thus for any element $u_t \cdot p'$, we first find p from $p' = \Theta_1(p)$; and then holding p fixed we vary i to find the p^* such that $u_{S(i)} \cdot p = p^* \cdot u_t$. For this i and p^* we have

$$\Theta(u_i p^*) = u_t \cdot \Theta_1(p) = u_t \cdot p',$$

and every element of G is an image of some element of G under the mapping Θ.

Let us now show that Θ is a complete mapping for G. Consider

$$\eta(u_i p^*) = u_i p^* \cdot \Theta(u_i p^*) = u_i p^* u_{[S(i),\,p]} \cdot \Theta_1(p) = u_i u_{S(i)} \cdot p\ \Theta_1(p).$$

First, if $\eta(u_i p_1^*) = \eta(u_j p_2^*)$, we have

$$u_i u_{S(i)} p_1\ \Theta_1(p_1) = u_j u_{S(j)} \cdot p_2\ \Theta_1(p_2), \quad \text{or} \quad u_{T(i)} H = u_{T(j)} H, \tag{4}$$

and this is impossible unless $i = j$. Consequently from (4),

$$p_1\ \Theta_1(p_1) = p_2\ \Theta_1(p_2)$$

and Θ_1 being a complete mapping implies $p_1 = p_2$. Again the finite case is completed and if G is infinite we note that there is but one i such that $u_i u_{S(i)} H = u_{T(i)} H$ and the subsequent solution for p^* is straightforward.

Corollary 1 follows from the observation that the elements of A form a system of coset representatives satisfying the hypothesis of the theorem.

Corollary 2 is proved by noting that if

$$\Theta(u_iH) = u_{S(i)}H$$

in G/H, then

$$u_i(u_{S(i)}H) = \eta(u_iH) = u_{T(i)}H.$$

We will use Theorem 1, to show that an earlier conjecture [4, p. 115] concerning complete mappings for the symmetric groups $S_n (n > 3)$ was wrong.

THEOREM 2. *There exist complete mappings for the symmetric group S_n if if $n > 3$.*

COROLLARY. (See conjecture [4, p. 115]). *There exist Latin squares orthogonal to the symmetric group S_n for all $n > 3$.*

Proof. The proof will be by induction and we note first that S_3 has no complete mapping [3, p. 420]. Thus we must exhibit a complete mapping for S_4. We may express $S_4 = A \cdot B$, where

$$A \equiv \{1, (123), (132)\},$$

$$B \equiv \{1, (12), (34), (12)(34), (1324), (1423), (14)(23), (13)(24)\},$$

are subgroups of S_4 with $A \wedge B = 1$. Moreover, there exist complete mappings for A and B given by:

$$\Theta(1) = 1, \Theta(123) = (123), \Theta(132) = (132)$$

for A; and

$$\Theta(1) = 1, \Theta(12) = (34), \Theta(34) = (1324), \Theta(12)(34) = (13)(24)$$

$$\Theta(1324) = (14)(23), \Theta(1423) = (12)(34),$$

$$\Theta(14)(23) = (12), \Theta(13)(24) = (14)(23),$$

for B. The fact that S_4 has a complete mapping now follows from the corollary of Theorem 1.

Let us now assume that S_n has a complete mapping with $n > 3$. Then,

$$S_{n+1} = S_n + (1, n+1)S_n + (2, n+1)S_n + \cdots + (n, n+1)S_n,$$

$$= S_n + S_n(1, n+1) + S_n(2, n+1) + \cdots + S_n(n, n+1).$$

Clearly, two cosets $(j, n+1)S_n$ and $(k, n+1)S_n$ $(j \neq k)$ being equal would imply $(j, k, n+1) \in S_n$ and this is impossible.

Now note that

$$(j, n+1)(j+1, n+1)S_n = (j, j+1, n+1)S_n = (j+1, n+1)S_n$$

if $1 \leq j \leq n-1$. Also, $(n, n+1)(1, n+1)S_n = (1, n+1)S_n$.

We now see that the coset representatives of S_{n+1} by S_n satisfy the conditions of Theorem 1 under the obvious mapping $S(1) = 1$, $S(i) = i+1$ for $2 \leq i \leq n$ and $S(n+1) = 2$. Hence, S_{n+1} has a complete mapping and our induction is complete.

The corollary follows from Theorem 7 of [4].

It should be pointed out that the coset representatives used for S_{n+1} in the argument above do not form a group and hence Theorem 1 is sufficiently stronger than the corollary to be of decided interest.

THEOREM 3. *There exists a complete mapping for the alternating group A_n, for all n.*

Proof. A_1, A_2, and A_3 (the cyclic group of order 3) possess complete mappings. Hence assume that there exists a complete mapping for A_n. Then,

$$A_{n+1} = A_n + (1, n, n+1)A_n + (1, n+1, n)A_n + (2, n+1)(1, n)A_n$$

$$+ (3, n+1)(1, n)A_n + \cdots + (n-1, n+1)(1, n)A_n$$

and the coset representatives are valid for either a right or left coset decomposition for A_{n+1} by A_n.

It is a simple, straightforward verification that the permutation S, given by

$$S(1) = 1, S(2) = 2, S(3) = 3, S(i) = i+1 \ (4 \leq i \leq n), S(n+1) = 4$$

satisfies the conditions of our Theorem 1. Here we meet a slight difficulty if $n = 3$, but it is known [3, p. 422] that there exists a complete mapping for A_4 and we may take $n = 4$ as the basis for our induction.

3. Groups of order 2^n. Although it has been indicated in the literature [4] that the results of this section are known, it seems desirable (and necessary for completeness) to include the proofs of these results.

LEMMA 1. *Let G be a non-abelian group of order 2^n and possess a cyclic*

subgroup of order 2^{n-1}. *Then a complete mapping exists for* G.

Proof. It is known [5, p. 120] that G is one of the following groups:

(I) Generalized Quaternion Group $(n \geq 3)$, $A^{2^{n-1}} = 1$, $B^2 = A^{2^{n-2}}$, $BAB^{-1} = A^{-1}$.

(II) Dihedral Group $(n \geq 3)$, $A^{2^{n-1}} = 1$, $B^2 = 1$, $BAB^{-1} = A^{-1}$.

(III) $(n \geq 4)$, $A^{2^{n-1}} = 1$, $B^2 = 1$, $BAB^{-1} = A^{1+2^{n-2}}$.

(IV) $(n \geq 4)$, $A^{2^{n-1}} = 1$, $B^2 = 1$, $BAB^{-1} = A^{-1+2^{n-2}}$.

In each case, the elements of the group are of the form

$$A^{\alpha}B^{\beta}(\alpha = 0, 1, \cdots, 2^{n-1} = 1; \quad \beta = 0, 1).$$

Let us define a mapping Θ as follows: (let $m = 2^{n-2}$),

$$\Theta(A^k) = A^k;\ k = 0, 1, \cdots, m-1;$$

$$\Theta(A^k) = A^{k-m} \cdot B;\ k = m, m+1, \cdots, 2m-1;$$

$$\Theta(A^k \cdot B) = A^{-(k+1)};\ k = 0, 1, \cdots, m-1;$$

$$\Theta(A^k \cdot B) = A^{m-(k+1)}B;\ k = m, m+1, \cdots, 2m-1.$$

Clearly, Θ is biunique and we will show that it is a complete mapping for groups I and II. Thus,

$$A^k \cdot \Theta(A^k) = A^k \cdot A^k = A^{2k};\ k = 0, 1, \cdots, m-1.$$

$$A^k \cdot \Theta(A^k) = A^k \cdot A^{k-m}B = A^{2k-m}B;\ k = m, m+1, \cdots, 2m-1.$$

$$A^kB \cdot \Theta(A^kB) = A^kB\,A^{-(k+1)} = A^{2k+1}B;\ k = 0, 1, \cdots, m-1.$$

$$A^kB \cdot \Theta(A^kB) = A^kBA^{m-(k+1)}B = A^{2k+1-m}B^2;\ k = m, m+1, \cdots, 2m-1.$$

We see that we have a complete mapping if $B^2 = 1$ or $B^2 = A^{2^{n-2}}$.

A slight calculation in the evaluation of $A^k \cdot B\,\Theta(A^kB)$, will show that this mapping is also a complete mapping for the group IV. It is necessary to use the fact that $n \geq 4$.

In order to obtain a complete mapping for group III, we define:

$$\Theta(A^k) = A^{k-1}; \qquad \text{for } k = 1, 2, \cdots, m.$$

$$\Theta(A^k) = A^{(k-1)+m}B; \qquad \text{for } k = m+1, m+2, \cdots, 2m.$$

$$\Theta(A^k \cdot B) = A^{k+m}; \qquad \text{for } k = 0, 1, \cdots, m-1.$$

$$\Theta(A^k \cdot B) = A^k \cdot B; \qquad \text{for } k = m, m+1, \cdots, 2m-1.$$

The verification that this mapping is a complete mapping for group III is straightforward and will be omitted.

This completes the proof of the lemma.

THEOREM 4. *Every non-cyclic 2-group G has a complete mapping.*

Proof. This theorem is known to be true for abelian groups [4]. We may use induction to prove the theorem if G has a normal subgroup K such that K and G/K are both non-cyclic Corollary 2, Theorem 1).

In view of Lemma 1, we assume that G is a non-abelian group of order 2^n and does not possess a cyclic subgroup of order 2^{n-1}; this implies $n \geq 4$. If G contains only one element of order 2, G would have to be the generalized quaternion group [5, p. 118] contrary to our assumption. Hence G contains an element of order 2 in its center and another element of order 2. These elements together generate a four group V.

If V is contained in two distinct maximal subgroups M_1 and M_2, then $M_1 \cap M_2 = K \supset V$ is a normal subgroup of G such that both G/K and K are non-cyclic. In this case the theorem would follow by induction.

We now suppose that V is contained in a unique maximal subgroup M_1. G, being non-cyclic, contains another maximal subgroup M_2 and if $M_1 \cap M_2$ is non-cyclic our induction again applies. Taking $M_1 \cap M_2$ to be cyclic, we see that M_1 is a group of order 2^{n-1} containing a cyclic subgroup of order 2^{n-2} and also the four group V. Thus M_1 is of the type II, III or IV of Lemma 1 or possibly an abelian group with $A^{2^{n-2}} = 1$, $B^2 = 1$, $BAB^{-1} = A$. In all cases, $M_1 \cap M_2 = \{A\}$. Now let C be any element of M_2 not in $\{A\}$. Then by the normality of $\{A\}$, $C^2 = A^r$, where r is even since otherwise C would be of order 2^{n-1} and G has no cyclic subgroup of order 2^{n-1}. Also $C^{-1}AC = A^u$ with u odd.

Now consider the group $H = \{A^2, B\}$, which is non-cyclic since $n \geq 4$. Here,

$$M_1 = H + HA = H + AH, \text{ and}$$

$$G = M_1 + M_1 C = M_1 + CM_1 .$$

Thus,

$$G = H + HA + HC + HAC = H + AH + CH + CAH,$$

where $CAH = ACH$ since

$$A^{-1} C^{-1} AC = A^{u-1} \in H .$$

We see that the elements 1, A, C, AC are two-sided coset representatives for H in G.

Define

$$\Theta(1) = 1, \quad \Theta(A) = C, \quad \Theta(C) = AC, \quad \Theta(AC) = A,$$

and compute:

$1 \cdot \Theta(1)H = 1 \cdot H$;

$A \cdot \Theta(A)H = ACH$;

$C \cdot \Theta(C)H = CACH = C^2 \cdot C^{-1} AC = A^r \cdot A^u H = AH$ since r is even, u odd;

$AC \cdot \Theta(AC)H = ACAH = C \cdot C^{-1} ACH = CA^u H = CAH = ACH$.

Hence, with these representatives the hypotheses of Theorem 1 are satisfied and G has a complete mapping.

4. Solvable Groups. The existence of complete mappings for solvable groups is answered in the following theorems.

THEOREM 5. *A finite group G whose Sylow 2-subgroup is cyclic does not have a complete mapping.*

Proof. Let a Sylow 2-subgroup S^2 of G be cyclic of order 2^m. Then the automorphisms of S^2 are a group of order 2^{m-1}. Hence in G, S^2 is in the center of its normalizer. By a theorem of Burnside [5, p. 139], G has a normal subgroup K (of odd order) with S^2 as its coset representatives. Since $G/K = S^2$ is cyclic, the derived group G' is contained in K; and clearly,

$$\prod_{g \in G} g \equiv \left(\prod_{s \in S^2} s \right)^{(K:1)} \pmod{K}.$$

S^2 is cyclic of order 2^m and hence $\prod_{s \in S^2} s = p$, where p is the unique element of order 2 of S^2. Thus,

$$\prod_{g \in G} g \equiv p^{(K:1)} \equiv p \pmod{K};$$

and since $G' \subset K$, the Corollary of Theorem 1 [4, p. 111] is violated and G does not have a complete mapping.

THEOREM 6. *A finite solvable group G whose Sylow 2-subgroup is non-cyclic has a complete mapping.*

Proof. By a theorem of Philip Hall, a solvable group has a p-complement for every prime p dividing its order. Thus, if S^2 is a Sylow 2-subgroup of G and H is a 2 complement, $G = H \cdot S^2$ and $H \cap S^2 = 1$. S^2 has a complete mapping by Theorem 4 and H, being of odd order, has a complete mapping. By Corollary 1 of Theorem 1, G has a complete mapping.

As further evidence in support of our conjecture we have the following special theorem.

THEOREM 7. *Let G be a finite group whose Sylow 2-subgroup is not cyclic. If G has $(G:S^2)$ Sylow 2-subgroups and the intersection of any two Sylow 2-subgroups is the identity, G possesses a complete mapping.*

Proof. By a well known theorem of Frobenius, G is a factorable group; that is, $G = N \cdot S^2$, where N is the normal subgroup consisting of all elements of odd order. We now apply Corollary 1 of Theorem 1.

REFERENCES

1. P. Bateman, *Complete mappings of infinite groups*, Amer. Math. Monthly **57** (1950), 621-622.

2. R.H. Bruck, *Finite Nets, I. Numerical Invariants*, Can. J. Math. **3** (1951), 94-107.

3. H.B. Mann, *The construction of orthogonal latin squares*, Ann. Math. Statistics **13** (1942), 418-423.

4. L.J. Paige, *Complete mappings of finite groups*, Pacific J. Math. **1**(1951), 111-116.

5. H. Zassenhaus, *The theory of groups*, Chelsea Publishing Co., New York, New York, 1949.

OHIO STATE UNIVERSITY
THE INSTITUTE FOR ADVANCED STUDY AND
UNIVERSITY OF CALIFORNIA, LOS ANGELES

PACIFIC JOURNAL OF MATHEMATICS

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any of the editors. Manuscripts intended for the outgoing editors should be sent to their successors. All other communications to the editors should be addressed to the managing editor, Alfred Horn, at the University of California Los Angeles 24, California.

50 reprints of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is $12.00; single issues, $3.50; back numbers (Volumes 1, 2, 3) are available at $2.50 per copy. Special price to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues, $1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to the publishers, University of California Press, Berkeley 4, California.

Printed at Ann Arbor, Michigan. Entered as second class matter at the Post Office, Berkeley, California.

*During the absence of E.G. Straus.

UNIVERSITY OF CALIFORNIA PRESS · BERKELEY AND LOS ANGELES

Pacific Journal of Mathematics
Vol. 5, No. 4 December, 1955