COMPLETE MAPPINGS OF FINITE GROUPS

L. J. PAIGE

1. Introduction. A *complete mapping* of a group, loop, or quasigroup G is a biunique mapping $x \longrightarrow \theta(x)$ of G upon G such that $x \times \theta(x) \equiv \eta(x)$ is a biunique mapping of G upon G. This concept was introduced by H.B.Mann [3]; other applications have been indicated by R.H.Bruck [2], and Paige [6]. However, the determination of all groups which possess a complete mapping is still an open question. For abelian groups and groups of infinite order the problem has been answered in [1] and [5].

The first part of the present paper considers the question of complete mappings for finite non-abelian groups; the latter part is devoted to an application of complete mappings in the construction of orthogonal Latin squares.

2. Complete mappings. We shall consider finite groups G written multiplicatively, the identity element being $g_1 = 1$. A group G will be called an *admissible group* if there exists a complete mapping for G; otherwise G is said to be non-admissible.

It should be noted that all groups of odd order are admissible by letting $\theta(x) = x$.

THEOREM 1. *A necessary condition that G be an admissible group is that there exist an ordering of the elements of G such that $g_1 \times g_2 \times \cdots \times g_n = 1$.*

COROLLARY. *If G is an admissible group, the product of the elements of G in any order is an element of the commutator subgroup of G.*

Proof. Assume that $x \longrightarrow \theta(x)$ is a complete mapping for G. Without loss of generality we can take $\theta(1) = \eta(1) = 1$. Now consider $g_2 \times \theta(g_2)$; here $g_2^{-1} \neq \theta(g_2)$, so that $\theta(g_2)^{-1}$ occurs among the remaining elements of G. Then let $\theta(g_2)^{-1} = g_3$ and form the product $g_2 \times \theta(g_2) \times g_3 \times \theta(g_3)$. We continue in this manner and ultimately reach a product

$$g_2 \times \theta(g_2) \times g_3 \times \theta(g_3) \times \cdots \times g_s \times \theta(g_s) = 1, \tag{1}$$

Received October 16, 1950.

Pacific J. Math. 1 (1951), 111-116.

where $\theta(g_{i-1}) = g_i^{-1} (i = 3, \cdots, s)$ and $\theta(g_s) = g_2^{-1}$.

If $s < n$, we repeat the process beginning with $g_{s+1} \times \theta(g_{s+1})$ and finally we arrive at a series of cycles similar to (1) whose product is the identity. Thus, $\eta(g_1) \times \eta(g_2) \times \cdots \times \eta(g_n) = 1$, completing the proof and yielding the corollary as a consequence.

We note that in the cycle represented by (1), the elements

$$g_2 \times \theta(g_2) \times \cdots \times g_i \times \theta(g_i) = \eta(g_2) \times \cdots \times \eta(g_i) \qquad (i \leq s),$$

are all distinct; for the equality of two such products would imply $\theta(g_i) = \theta(g_j)$ or $i = j$. Hence, we have the following result.

THEOREM 2. *A necessary condition that G be admissible is that there exist an ordering of the elements of G into subsets, such that in each subset, the elements*

$$g_{i_2},\ g_{i_2} \times g_{i_3},\ \cdots,\ g_{i_2} \times g_{i_3} \times \cdots \times g_{i_s} = 1 \tag{2}$$

are all distinct.

In the most favorable case where G possesses a single subset of $n - 1$ nonidentity elements which satisfy condition (2), we may prove that G is an admissible group. To do this, let g_2 be the element that is not represented in the set of elements (2). Construct the mapping $\theta(x)$ as follows: $\theta(1) = 1$, $\theta(g_2)$ is the solution of the equation $g_2 \times x = g_{i_2}$, and successively let $g_{i+1} = \theta(g_i)^{-1}$, and let $\theta(g_{i+1})$ be the solution of the equation $g_{i+1} \times x = g_{i_{i+1}}$. All the $\theta(x)$'s are are distinct and different from 1; for if $\theta(g_k) = \theta(g_s)$, $k \neq s$, we would have

$$g_2 \times \theta(g_k) = g_{i_2} \times \cdots \times g_{i_k} = g_{i_2} \times \cdots \times g_{i_s} = g_2 \times \theta(g_s),$$

the inner equality being contrary to hypothesis for $k \neq s$. Moreover if $\theta(g_k) = 1$, we would have $g_2 = g_{i_2} \times \cdots \times g_{i_k}$, contrary to the selection of g_2. Thus, we have proved the following theorem.

THEOREM 3. *A sufficient condition that G be an admissible group is that there exist an ordering of the nonidentity elements of G, such that the elements*

$$g_2 \times \cdots \times g_i \qquad \text{for} \quad (i = 2, \cdots, n)$$

are all distinct and $g_2 \times \cdots \times g_n = 1$.

For abelian groups, Theorem 1 is also a sufficient condition that G be admissible and we conjecture that this is likewise the case for non-abelian groups.

However, the best we have been able to prove are theorems of the following type.

THEOREM 4. *Let H be a normal subgroup of G. If G/H admits a complete mapping θ_1, H a complete mapping θ_2, then G is an admissible group.*

Proof. Let $G/H \cong K$, the elements of K being $e, p, q, \cdots$. Let u_p be an element of G that maps upon $p \in K$. Every element of G has the form $u_p \times h$ or $h \times u_p$, where $p \in K$, $h \in H$. The equality of $u_p \times h$ and $u_q \times h'$ implies $p = q$ and $h = h'$.

Define $\theta(u_p \times h) = \theta_2(h)\, u_{\theta_1(p)}$. Obviously this mapping is biunique of G upon G. Consider

$$(3) \qquad u_p \times h \times \theta_2(h) u_{\theta_1(p)} = u_q h' \theta_2(h') u_{\theta_1(q)} \; .$$

This implies

$$u_p \times u_{\theta_1(p)} \times H = u_q \times u_{\theta_1(q)} \times H \qquad \text{or} \quad u_{p \times \theta_1(p)} \times H = u_{q \times \theta_1(q)} \times H \, ,$$

whence $p \times \theta_1(p) = q \times \theta_1(q)$ or $p = q$, since θ_1 is a complete mapping for K. It then follows from (3) that $h = h'$ and θ is a complete mapping for G.

THEOREM 5. *If G is a group containing a subgroup H of odd order such that G/H is a nonadmissible abelian group, then G is nonadmissible.*

Proof. If G/H is a nonadmissible abelian group, G/H possesses a single element of order 2 [6; p.49]. Let this coset be $g_2 \times H$. Considering the product of the elements of G modulo H, we have $\prod_{i=1}^{n} g_i \equiv g_2 \bmod H$. Since g_2 is not in H, the product of the elements of G in any order is not in H. However, H contains the commutator subgroup of G and it follows from Corollary 1 of Theorem 1 that G is not admissible.

The two preceding theorems may be used to establish the admissibility or nonadmissibility of many groups. Often it is necessary to develop other techniques, as for example in groups of order 2^n. Here we are able to argue modulo the commutator subgroup and establish by mathematical induction the admissibility of those groups whose commutator subgroups are not cyclic. The remaining cases have been analyzed by Bruck and found to be admissible except in the obvious case where G is cyclic of order 2^n.

3. Orthogonal Latin squares. Recalling the definition of a Latin square [3, p.418], we see that the multiplication table of a quasigroup, loop, or group G is a Latin square. Indeed, any Latin square of order m may be used to define a quasigroup of order m. Mann [3, 4] has shown how Latin squares, orthogonal to a group G, may be constructed by means of complete mappings. (A Latin square L is said to be orthogonal to a group G if L is orthogonal to the multiplication table of G.) We may extend these results in the following manner.

For convenience we shall assume henceforth that the elements of a group or quasigroup G are $1, 2, \cdots, n$.

THEOREM 6. *Let G be a quasigroup. Let $\theta_1, \theta_2, \cdots, \theta_n$ be n complete mappings of G with the following property*:

$$(4) \qquad \theta_i(g) \neq \theta_j(g), \qquad \text{for } i \neq j, \qquad \text{all } g \in G.$$

Construct a Latin square S by placing j in the kth row and $\theta_j(k)$th column. Then S is orthogonal to G.

Moreover, all Latin squares S, orthogonal to G, may be represented in this manner.

Proof. Obviously the square S is a Latin square and it is orthogonal to G since the number pairs $[k \times \theta_j(k), j]$ assume n^2 distinct values.

Conversely, let S be any Latin square orthogonal to G. Let j occupy the row and column positions $(1, i_{j,1}), \cdots, (n, i_{j,n})$ in S, where $(i_{j,1}, \cdots, i_{j,n})$ is, of necessity, some permutation of $(1, 2, \cdots, n)$. Let $\theta_j(k)$ be defined by $\theta_j(k) = i_{j,k}$. The assumption that $k \times \theta_j(k) = h \times \theta_j(h) = m$ for $k \neq h$ leads to a contradiction, in that the number pair (m, j) would occur twice in the orthogonal Latin squares G and S. Since $i_{r,k} \neq i_{s,k}$ for $r \neq s$, property (4) is satisfied, and this completes the proof.

Although anticipated in part by Theorem 2 of [3], we may improve upon the previous result for a group G.

THEOREM 7. *A necessary and sufficient condition that there exist a Latin square orthogonal to a group G is that there exist a complete mapping $\theta(x)$ for G.*

Proof. The necessity follows trivially from Theorem 6. The sufficiency is evident from the fact that, given one complete mapping $\theta(x)$ of G, we may define n complete mappings of G satisfying (4) by letting $\theta(x) \times i = \theta_i(x)$, $i = 1, 2, \cdots, n$.

A more convenient method of obtaining a Latin square orthogonal to a group G is to apply the following theorem.

THEOREM 8. *Let G be a group, $\theta(x)$ a complete mapping for G. Construct a*

Latin square S as follows: In the ith row and kth column place $i \times k \times \theta(k)$. Then S is a Latin square orthogonal to G.

Proof. Trivially, S is a Latin square. In the orthogonal squares the number pairs are $[i \times k, i \times k \times \theta(k)]$; and every pair (r, s), $(r, s = 1, 2, \cdots, n)$, exists since the equations $i \times k = r$, $i \times k \times \theta(k) = s$ have a unique solution. Thus the Latin square S is orthogonal to G.

Theorem 8 is a variation of the method employed by Mann [4, p.253] and is simpler to compute.

The problem of finding more than two mutually orthogonal Latin squares has its basis in investigations of finite plane geometries [4] and nets [2]. Theorem 6 yields easily formulated but involved results in this connection. The representation of Theorem 8 yields more interesting results. Consider the case of two Latin squares S_1 and S_2 represented in the manner of Theorem 8 and orthogonal to a group G. Then S_1 will be orthogonal to S_2 if and only if the number pairs

$$[i \times k \times \theta_1(k),\ i \times k \times \theta_2(k)] \qquad (i, k = 1, 2, \cdots, n)$$

take on every value (r, s), $(r, s = 1, 2, \cdots, n)$. Hence, we can conclude immediately that a necessary and sufficient condition for S_1 to be orthogonal to S_2 is that the equation

$$r \times \theta_1(k)^{-1} = s \times \theta_2(k)^{-1} \tag{5}$$

have a unique solution k for all pairs (r, s). The generalization to any number of mutually orthogonal Latin squares of this type should be apparent.

We note from (5) that if $\theta_2(x) = \theta_1(x) \times x$ is a complete mapping, our condition is trivially satisfied. In the case that G is abelian of order $2^n (n > 1)$ and every element of order 2, $\theta_2(x) = \theta_1(x) \times x$ is a complete mapping. Thus for this group it is always possible to find at least two Latin squares mutually orthogonal to G. This brings us to an interesting question that we have been unable to answer: For a given group G, what is the maximum number of mutually orthogonal Latin squares orthogonal to G?

In conclusion, we would like to conjecture that there exist no Latin squares orthogonal to a symmetric group.

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*, Canadian Journal of Mathematics (To be published).

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

4. ———, *On orthogonal Latin squares*, Bull. Amer. Math. Soc., 50 (1944), 249-257.

5. L. J. Paige, *A note on finite abelian groups*, Bull. Amer. Math. Soc., 53 (1947), 590-593.

6. ———, *Neofields*, Duke Math. J., 16 (1949), 39-60.

University of California, Los Angeles