PACIFIC JOURNAL OF MATHEMATICS
Vol. 92, No. 2, 1981

PARTITIONS OF GROUPS AND COMPLETE MAPPINGS

RICHARD J. FRIEDLANDER, BASIL GORDON
AND PETER TANNENBAUM

Let G be an abelian group of order n and let k be a divisor of $n-1$. We wish to determine whether there exists a complete mapping of G which fixes the identity element and permutes the remaining elements as a product of disjoint k-cycles. We conjecture that if G has trivial or noncyclic Sylow 2-subgroup then such a mapping exists for every divisor k of $n-1$. Several special cases of the conjecture are proved in this paper. We also prove that a necessary condition for the existence of such a map holds for every k when G is cyclic.

1. Introduction. A complete mapping of a group G is defined to be a bijection $\phi: G \rightarrow G$ such that the mapping $\theta: g \rightarrow g^{-1}\phi(g)$ is also bijective. (Some authors refer to θ, rather than ϕ, as the complete mapping.) If the permutation $\begin{pmatrix} b_1 \, b_2 \cdots b_n \\ c_1 \, c_2 \cdots c_n \end{pmatrix}$ is a complete mapping of G and $g \in G$, then $\begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ c_1g & c_2g & \cdots & c_ng \end{pmatrix}$ is clearly also a complete mapping of G. By suitable choice of g, we can therefore suppose that $b_n = c_n = 1$. Then the complete mapping can be viewed as a permutation $\begin{pmatrix} b_1 \, b_2 \cdots b_{n-1} \\ c_1 \, c_2 \cdots c_{n-1} \end{pmatrix}$ of the nonidentity elements of G. The permutation $\begin{pmatrix} b_1 \, b_2 \cdots b_{n-1} \\ c_1 \, c_2 \cdots c_{n-1} \end{pmatrix}$ is cyclic if and only if it can be written in the form $\begin{pmatrix} a_1 \, a_2 \cdots a_{n-1} \\ a_2 \, a_3 \cdots a_1 \end{pmatrix}$, where $a_1^{-1}a_2, a_2^{-1}a_3, \cdots, a_{n-1}^{-1}a_1$ are all distinct. In this case we say that G is an *R-sequenceable* group with R-sequencing $a_1, a_2, \cdots, a_{n-1}$. Thus a group G is R-sequenceable if and only if it has a complete mapping which fixes the identity element and permutes the remaining elements cyclically. In [2], we determined several infinite classes of R-sequenceable abelian groups (see (1)-(6) below).

In this paper, we generalize the notion of R-sequenceability by asking which groups G of order n have the property that, given any regular partition $k + k + \cdots + k$ (d terms) of $n-1$, there exists a complete mapping of G which fixes the identity element and permutes the remaining elements as a product of d disjoint k-cycles. We call such a mapping a *k-regular complete mapping of G*. That is, given any divisor k of $n-1$, a k-regular complete mapping of G is a permutation $\begin{pmatrix} b_1 \, b_2 \cdots b_{n-1} \\ c_1 \, c_2 \cdots c_{n-1} \end{pmatrix}$ of the nonidentity elements of G whose disjoint cycles each have length k and whose quotients $b_i^{-1}c_i$ also constitute all the nonidentity elements of G. If $k = n - 1$ then the permutation is cyclic and hence is an R-sequencing of G.

There are several contexts in which k-regular complete mappings arise. For example, 6-regular complete mappings of Z_n can be obtained from cyclic Steiner Triple Systems of order $n \equiv 1 \pmod 6$ [9]. Another occurrence of k-regular complete mappings is in connection with a special family of permutation matrices called I-matrices [8]. An additional context in which k-regular complete mappings arise is in the connection between map coloring and R-sequenings of a group [2], [11].

It is well known [6] that if a finite abelian group has a complete mapping, then its Sylow 2-subgroup is either trivial or noncyclic. By a theorem of M. Hall [5], the converse is also true. We conjecture that, given any abelian group G of order n having either trivial or noncyclic Sylow 2-subgroup, there exists a k-regular complete mapping of G for each divisor k of $n - 1$.[1] We have shown this to be true for $n \leqq 15$, as well as for the following general cases:

(1) $k = n - 1$, G is the cyclic group Z_n, where $n > 1$ is odd.

(2) $k = n - 1$, $(n, 6) = 1$ and $n \neq 1$.

(3) $k = n - 1$, G has cyclic Sylow 3-subgroup, where $n > 1$ is odd.

(4) $k = n - 1$, the Sylow 2-subgroup of G is $(Z_2)^m$, where $m > 1$, but $m \neq 3$.

(5) $k = n - 1$, the Sylow 2-subgroup S of G is $Z_2 \times Z_{2^r}$ where either

(i) r is odd, or

(ii) $r \geqq 2$ is even and G/S has a direct cyclic factor of order $\equiv 2$ (mod 3).

(6) $k = n - 1$, $G = Z_2 \times Z_{4r}$, $r \geqq 1$.

(7) k is any divisor of $n - 1$, G is an elementary abelian p-group, $G \neq Z_2$.

(8) k is any divisor of $p - 1$, G is an abelian p-group $p \neq 2$.

(9) $k = 2$ or $(n - 1)/2$, $G = Z_n$, where $n > 1$ is odd.

As mentioned above, cases (1)-(6) give R-sequencings of G and are proved in [2]. Cases (7) and (8) will be proved in § 2 of this paper and case (9) in § 3.

As a necessary condition for solving the cyclic case for *any* divisor k of $n - 1$, we must be able to divide the nonzero residues mod n into $(n - 1)/k$ sets, each of cardinality k, such that the sum

[1] One might also conjecture that there must be a complete mapping corresponding to *any* partition of $n - 1$. However, the cyclic group Z_7 provides a counterexample, as it has no complete mapping that fixes the identity and permutes the remaining elements as a product of a 4-cycle and a 2-cycle.

of the elements in each set is $\equiv 0 \pmod{n}$. (We use additive notation when the group is cyclic.) We will solve this number theory problem in § 4 of this paper.

2. Abelian p-groups.

The following theorem gives an infinite family of groups G of order n for which there exists a k-regular complete mapping for all divisors k of $n-1$.

THEOREM 1. *Suppose G is an elementary abelian p-group of order n, p prime, $G \neq Z_2$. Then for any divisor k of $n-1$, there exists a k-regular complete mapping of G.*

Proof. If $n = p^m$, we can write $G = Z_p \oplus Z_p \oplus \cdots \oplus Z_p$ (m times). G is the additive group of $GF(p^m)$, the finite field of p^m elements. Let α be a generator of the (cyclic) multiplicative group $GF(p^m)^*$ of nonzero elements of $GF(p^m)$. For each divisor k of $n-1$, we define the permutation ϕ by $\phi(x) = \alpha^d x$, where $d = (n-1)/k$. Since α^d has order k in $GF(p^m)^*$ and α^d, $\alpha^d - 1 \neq 0$, the permutation ϕ is a k-regular complete mapping in G. □

THEOREM 2. *Suppose G is an abelian p-group of order $n = p^m$, p prime, $p \neq 2$. Then for any divisor k of $p-1$, there exists a k-regular complete mapping of G.*

Proof. If $G = Z_{p^m}$ then by a result in [3] there exists a unit a in the ring Z_{p^m} such that the mapping $\phi(x) = a \cdot x$ is a k-regular complete mapping of Z_{p^m}.

The result follows by induction and the following observation: If ϕ_1 is a k-regular complete mapping of G_1 and ϕ_2 is a k-regular complete mapping of G_2 then the mapping $(x, y) \to (\phi_1(x), \phi_2(y))$ is clearly a k-regular complete mapping of $G_1 \times G_2$. □

3. Cyclic groups.

In this section we show the existence of k-regular complete mappings of cyclic groups for certain values of k.

THEOREM 3. *If $k = 2$ or $(n-1)/2$, then there exists a k-regular complete mapping of the cyclic group Z_n, where $n > 1$ is odd.*

Proof. The nonzero elements of Z_n are $1, 2, \cdots, n-1$, the nonzero residues mod n. For $k = 2$, we define the permutation ϕ by

$$\phi = (1, n-1)(2, n-2) \cdots \left(\frac{n-1}{2}, \frac{n+1}{2}\right).$$

ϕ is clearly a product of $(n-1)/2$ disjoint 2-cycles. The two differences occuring in the jth factor of ϕ are $j - (n - j) = 2j$ and $(n - j) - j = n - 2j$. As j runs from 1 to $(n - 1)/2$, these differences run through all the nonzero residues mod n, since n is odd. Thus ϕ is a 2-regular complete mapping of Z_n.

For $k = (n - 1)/2$, we define the permutation ϕ to be the product of two k-cycles $\phi_1 = (a_1, a_2, \cdots, a_k)$ and $\phi_2 = (-a_1, -a_2, \cdots, -a_k)$, where the a_i are determined as follows:

$$a_i = \begin{cases} (-1)^{i-1}(2i - 1) ; & 1 \leqq i \leqq \dfrac{n+3}{4} \\ (-1)^{i}(2i - 1) ; & \dfrac{n+7}{4} \leqq i \leqq \dfrac{n-1}{2} \end{cases} \quad \text{if} \quad n \equiv 1 \pmod 4$$

and

$$a_i = \begin{cases} (-1)^{i-1}(2i - 1) ; & 1 \leqq i \leqq \dfrac{n+1}{4} \\ (-1)^{i}(2i - 1) ; & \dfrac{n+5}{4} \leqq i \leqq \dfrac{n-1}{2} \end{cases} \quad \text{if} \quad n \equiv 3 \pmod 4 .$$

In either case, since $-a_i = n - a_i$, it is easily checked that the elements $\pm a_i$, $1 \leqq i \leqq k$, run through all the nonzero residue mod n. If $n \equiv 1 \pmod 4$, the differences $a_{i+1} - a_i$ in ϕ_1 are $(-1)^i(4i)$ (when $1 \leqq i \leqq (n - 1)/4$), $(-1)^{i+1}(4i)$ (when $(n + 7)/4 \leqq i \leqq (n - 3)/2$), ± 2 and 3. A straightforward check shows that, since n is odd, these differences are all distinct and, along with their negatives, run through all the nonzero residues mod n. The verification for $n \equiv 3 \pmod 4$ is entirely similar. Thus, in either case, $\phi = \phi_1\phi_2$ is an $(n - 1)/2$-regular complete mapping of Z_n. □

For the case $k = 6$, a 6-regular complete mapping of Z_n for $n \equiv 1 \pmod 6$ can be constructed from a *CIP*-neofield N_v of order $v \equiv 2 \pmod 6$ [1] or from an *HP I*-matrix of order $m \equiv 0 \pmod 6$ [8]. This result can be extended to show the existence of a 6-regular complete mapping of any abelian group of order $\equiv 1 \pmod 6$ [14].

4. A related number theoretic problem. Let $\phi: G \to G$ be a complete mapping of G, normalized (as in the introduction) so that ϕ fixes the identity element of G. Then as already noted, ϕ can be regarded as a permutation $\begin{pmatrix} b_1 \, b_2 \cdots b_n \\ c_1 \, c_2 \cdots c_n \end{pmatrix}$ of the elements of G with the property that $a_i = b_i^{-1}c_i$ $(i = 1, \cdots, n - 1)$ also constitute all the nonidentity elements of G. We now decompose this permutation into a product of disjoint cycles, and suppose that $(b_1 b_2 \cdots b_r)$ is a typical one of these cycles. Thus $c_i = b_{i+1}$ for $i < r$, while $c_r = b_1$. Hence

$a_1 a_2 \cdots a_r = (b_1^{-1} c_1)(b_2^{-1} c_2) \cdots (b_r^{-1} c_r) = (b_1^{-1} b_2)(b_2^{-1} b_3) \cdots (b_r^{-1} b_1) = 1$. We have thus proved the following:

THEOREM 4. *Suppose that ϕ is a complete mapping of G whose associated permutation is the product of disjoint cycles of lengths $r_1, r_2, \cdots, r_v$. Then the elements of G can be partitioned into disjoint subsets S_i of cardinality r_i $(1 \leqq i \leqq v)$ such that the product of the elements in each subset S_i (taken in a suitable order) is* 1.

We now specialize to the case where $G = Z_n$, the cyclic group of order n, and we go over to additive notation. We further suppose that ϕ is a k-regular permutation of $Z_n^* = Z_n \backslash \{0\}$ for some $k > 1$, i.e., that $\phi(0) = 0$, while the remaining $n - 1$ elements of Z_n fall into $(n - 1)/k$ cycles, each of length k. In this case, Theorem 4 asserts that if such a complete mapping ϕ exists, then the nonzero elements Z_n^* can be partitioned into $(n - 1)/k$ sets of cardinality k, where the sum of the elements in each set is $\equiv 0 \pmod{n}$. The purpose of this section is to show that this necessary condition for the existence of ϕ is always fulfilled as long as $k | n - 1$ and n is odd. (Of course the condition that n be odd is needed, for only then is the sum of *all* the elements of Z_n congruent to $0 \pmod{n}$.) We state this formally as a theorem, although the proof will not be achieved until the end of the section.

THEOREM 5. *Suppose n is odd and $k | n - 1$, where $k > 1$. Then the nonzero residues* $\pmod{n}$ *can be partitioned into $(n - 1)/k$ sets of cardinality k, so that the sum of the elements of each set is* $\equiv 0$ $\pmod{n}$.

We remark that if $k | l | (n - 1)$, and that if Theorem 5 has been proved for sets of cardinality k, then it also holds for sets of cardinality l. Indeed the required sets of cardinality l can be obtained by simply grouping together the sets of cardinality k (in groups of l/k). This reduces the proof of Theorem 5 to the case where k is a prime. For $k = 2$ the theorem is trivial, since the required sets are then just $\{1, n-1\}, \{2, n-2\}, \cdots, \{(n-1)/2, (n+1)/2\}$. For odd values of k we have not been able to take effective advantage of the reduction to primes. Instead we will proceed by mathematical induction through the odd values of k. The kernel of the proof is a discussion of the case $k = 3$.

When $k = 3$, the conditions $k | n - 1$ and n odd of Theorem 5 are together equivalent to $n \equiv 1 \pmod{6}$. In this case Theorem 5 reduces to

THEOREM 6. *If $n \equiv 1 \pmod 6$, then the nonzero residues $(\operatorname{mod} n)$ can be partitioned into $(n-1)/3$ triples such that the elements of each triple have sum $\equiv 0 \pmod n$.*

This theorem was proved by Skolem [12], [13] for $n \equiv 1$ or $7 \pmod{24}$, and by Hanani [7] for $n \equiv 13$ or $19 \pmod{24}$. For the purpose of extending to arbitrary odd k, it is necessary to strengthen Hanani's result by proving a conjecture of Skolem [13, p. 274]. We will therefore have to make a fairly elaborate detour. This investigation was originally carried out by one of us (B.G.) in collaboration with W. H. Mills [4]. Related constructions were later carried out by O'Keefe in [10] and Doner in [1]. Since [4] is not in general circulation, we will reproduce the details of the construction here.

Given a set $A = \{a_1, a_2, \cdots, a_m\}$ of m integers and a set $B = \{b_1, b_2, \cdots, b_{2m}\}$ of $2m$ integers, we will say that B *covers* A if B can be partitioned into m disjoint pairs $(b_{i_1}, b_{j_1}), \cdots, (b_{i_m}, b_{j_m})$ with $b_{j_\lambda} - b_{i_\lambda} = a_\lambda$ $(1 \leqq \lambda \leqq m)$. We will prove the following conjecture of Skolem:

THEOREM 7. *$A_m = \{1, 2, 3, \cdots, m\}$ is covered by $B_m = \{1, 2, 3, \cdots, 2m-1, 2m+\varepsilon\}$, where $\varepsilon = 0$ if $m \equiv 0$ or $1 \pmod 4$, and $\varepsilon = 1$ if $m \equiv 2$ or $3 \pmod 4$.*

Clearly if B covers A, and $\gamma \neq 0$, then any set of the form $\gamma B + \delta = \{\gamma b_1 + \delta, \cdots, \gamma b_{2m} + \delta\}$ covers γA and $-\gamma A$.

LEMMA 1. *If $u \geqq 1$, the set $F_u = \{1, 3, 5, \cdots, 2u-1\}$ is covered by $G_u = \{1, 2, 3, \cdots, 2u\}$.*

Proof. An appropriate division of G_u into pairs is given by $(i, 2u+1-i)$, $1 \leqq i \leqq u$.

LEMMA 2. *If $u \neq 1$ or 3, then F_u is covered by $H_u = \{0, 3, 4, 5, \cdots, 2u+1\}$.*

Proof. We use induction from u to $u+2$. We have $F_2 = \{1, 3\}$ and $H_2 = \{0, 3, 4, 5\}$. The pairs $(4, 5)$ and $(0, 3)$ give a covering of F_2 by H_2. For the other initial value of the induction, namely $u = 5$, we have $F_5 = \{1, 3, 5, 7, 9\}$ and $H_5 = \{0, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. The desired covering of F_5 by H_5 is provided by pairs $(7, 8)$, $(3, 6)$, $(5, 10)$, $(4, 11)$ and $(0, 9)$.

Now assume the lemma true for u, and consider $F_{u+2} = \{1, 3, 5, \cdots, 2u+3\}$ and $H_{u+2} = \{0, 3, 4, 5, \cdots, 2u+5\}$. We form the pairs $(0, 2u+3)$ and $(3, 2u+4)$. These give the differences $2u+3$

and $2u + 1$. The remaining elements of F_{u+2} constitute the set F_u, while the remaining elements of H_{u+2} form the set $\{4, 5, 6, \cdots, 2u + 2, 2u + 5\} = -1 \cdot H_u + (2u + 5)$. By induction (and the above remarks) this set covers F_u, completing the induction.

LEMMA 3. *If $u \neq 1, 2, 4$, then F_u is covered by $J_u = \{0, 2, 3, \cdots, 2u - 2, 2u - 1, 2u + 1\}$.*

Proof. We form the pair $(2, 2u + 1)$, which has difference $2u - 1$. The remaining elements of F_u constitute the set F_{u-1}, while the remaining elements of J_u constitute the set H_{u-1} of Lemma 2. Therefore, Lemma 3 follows from Lemma 2.

LEMMA 4. *If $u \neq 2$ or 4, then F_u is covered by $K_u = \{0, 1, 4, 5, 6, \cdots, 2u + 1\}$.*

Proof. We again use induction from u to $u + 2$. We have $F_1 = \{1\}$ and $K_1 = \{0, 1\}$ so clearly K_1 covers F_1. For the other initial value $u = 6$, we have $F_6 = \{1, 3, 5, 7, 9, 11\}$ and $K_6 = \{0, 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$. A covering of F_6 by K_6 is given by the pairs $(6, 7)$, $(9, 12)$, $(5, 10)$, $(1, 8)$, $(4, 13)$ and $(0, 11)$.

Now assume the lemma proved for some integer u, and consider $F_{u+2} = \{1, 3, 5, \cdots, 2u + 3\}$ and $K_{u+2} = \{0, 1, 4, 5, 6, \cdots, 2u + 5\}$. We form the pairs $(0, 2u + 3)$ and $(1, 2u + 2)$ with differences $2u + 3$ and $2u + 1$ respectively. The remaining elements of F_{u+2} constitute F_u, while the remaining elements of K_{u+2} form the set $\{4, 5, 6, \cdots, 2u + 1, 2u + 4, 2u + 5\} = -1 \cdot K_u + (2u + 5)$. By induction, $-1 \cdot K_u + (2u + 5)$ covers F_u, and the proof is complete.

LEMMA 5. *If $u > 1$, then F_u is covered by $L_u = \{0, 1, 2, 4, 5, 6, \cdots, 2u - 1, 2u + 1\}$.*

Proof. We form the pair $(2, 2u + 1)$, which has a difference of $2u - 1$. The remaining elements of F_u form the set F_{u-1}, while the remaining elements of L_u form the set K_{u-1} of Lemma 4. For $u \neq 3$ or 5, Lemma 5 now follows from Lemma 4. Finally, consider $u = 3$ and 5. We have $L_3 = \{0, 1, 2, 4, 5, 7\}$ and $L_5 = \{0, 1, 2, 4, 5, 6, 7, 9\}$. The required coverings of F_3 and F_5 are given respectively by $(1, 2)$, $(4, 7)$, $(0, 5)$ and $(7, 8)$, $(2, 5)$, $(1, 6)$, $(4, 11)$, $(0, 9)$.

LEMMA 6. *If $u \geqq 4$, then F_u is covered by $M_u = \{0, 4, 5, 6, \cdots, 2u + 1, 2u + 3\}$.*

Proof. We form the three pairs $(0, 2u - 1)$, $(4, 2u + 1)$, $(8, 2u + 3)$

with differences $2u-1$, $2u-3$, $2u-5$ respectively. The remaining elements of F_u form the set F_{u-3}. If $u=4$, the remaining elements of M_4 form the set $\{5, 6\}$, which covers F_1. If $u>4$, the remaining elements of M_4 form the set $\{5, 6, 7, 9, \cdots, 2u-2, 2u\} = L_{u-3}+5$. In this case the result follows from Lemma 5, and the proof is complete.

We are now ready to prove Theorem 7. There are six special cases which do not fit into the general pattern. We deal with them separately in the following lemma.

LEMMA 7. *If $m=2, 3, 6, 7, 10$ or 11, there is a covering of $A_m = \{1, 2, \cdots, m\}$ by $B_m = \{1, 2, \cdots, 2m-1, 2m+1\}$.*

Proof. Write $m = 2h+\delta$, where $\delta = 0$ or 1 and $h = 1, 3$ or 5. We begin by forming the pairs $(1, 2)$ and $(2+i, h+2+2i)$, $1 \leqq i \leqq m-h$. These pairs have differences $1, h+1, h+2, \cdots, m$. If $h=1$ these pairs constitute the desired covering. If $h=3$ we are left with the problem of covering $\{2, 3\}$ by $\{6+2\delta, 8+2\delta, 10+2\delta, 13+2\delta\}$, which can clearly be done. If $h=5$, we must cover $\{2, 3, 4, 5\}$ by $\{8+2\delta, 10+2\delta, 12+2\delta, 14+2\delta, 16+2\delta, 18+2\delta, 19+2\delta, 21+2\delta\}$. The required covering is $(8+2\delta, 10+2\delta)$, $(18+2\delta, 21+2\delta)$, $(12+2\delta, 16+2\delta)$, $(14+2\delta, 19+2\delta)$.

Proof of Theorem 7. Let $m = 2h+\delta$, where $\delta = 0$ or 1. By Lemma 5, we can assume that $m \neq 2, 3, 6, 7, 10$ or 11. We now use induction on m. Note first that $\varepsilon = 0$ if h is even, and $\varepsilon = 1$ if h is odd. We begin by forming the pairs $(i, h+2i)$, where $1 \leqq i \leqq m-h = h+\delta$. Then we are left with the problem of covering $\{1, 2, \cdots, h\}$ by the union of the sets $\{h+2\delta+2i-1 \mid 1 \leqq i \leqq h\}$, $\{3h+2\delta+j \mid 1 \leqq j \leqq h-1\}$ and $\{2m+\varepsilon\}$. Now the set $\{1, 2, \cdots, u\}$ can be covered by $\{1, 2, \cdots, 2u-1, 2u+\varepsilon'\}$, where $u = [h/2]$ and $\varepsilon' = 0$ if $u \equiv 0$ or $1 \pmod 4$, $\varepsilon' = 1$ if $u \equiv 2$ or $3 \pmod 4$. If $u = 0$ this is trivial, if $u = 2, 3, 6, 7, 10$ or 11 it follows from Lemma 7, while for all other u it follows from the induction hypothesis. We now distinguish four cases:

Case 1. $h \equiv 0$ or $2 \pmod 8$. Here $\varepsilon = \varepsilon' = 0$. Then as just noted, we can cover $\{2, 4, 6, \cdots, h\}$ by $\{h+2\delta+2i-1 \mid 1 \leqq i \leqq h\}$. By Lemma 1, we can cover $\{1, 3, 5, \cdots, h-1\}$ by $\{3h+2\delta+j \mid 1 \leqq j \leqq h\}$.

Case 2. $h \equiv 1$ or $3 \pmod 8$. Here $\varepsilon = 1$, $\varepsilon' = 0$. By assumption we can cover $\{2, 4, 6, \cdots, k-1\}$ by $\{h+2\delta+2i-1 \mid 1 \leqq i \leqq h-1\}$. By Lemma 3 we can cover $\{1, 3, 5, \cdots, h\}$ by $\{3h+2\delta-1\} \cup \{3h+$

$2\delta + j \mid 1 \leqq j \leqq h - 1\} \cup \{2m + 1\}$ unless $h = 1$, 3 or 7. Here $h \neq 7$, while $h = 1$, 3 correspond to $m = 2, 3, 6, 7$.

Case 3. $h \equiv 4$ or 6 (mod 8). Here $\varepsilon = 0$, $\varepsilon' = 1$. By assumption we can cover $\{2, 4, 6, \cdots, h\}$ by $\{h + 2\delta + 2i - 1 \mid 1 \leqq i \leqq h - 1) \cup \{3h + 2\delta + 1\}$. By Lemma 2 we can cover $\{1, 3, 5, \cdots, h - 1\}$ by $\{3h + 2\delta - 1\} \cup \{3h + 2\delta + j \mid 2 \leqq j \leqq h\}$ unless $h = 2$ or 6. Here $h \neq 2$. For $h = 6$ a suitable covering of $\{1, 2, 3, 4, 5, 6\}$ is given by $(23 + 2\delta, 24 + 2\delta)$, $(9 + 2\delta, 11 + 2\delta)$, $(19 + 2\delta, 22 + 2\delta)$, $(17 + 2\delta, 21 + 2\delta)$, $(15 + 2\delta, 20 + 2\delta)$, $(7 + 2\delta, 13 + 2\delta)$.

Case 4. $h \equiv 5$ or 7 (mod 8). Here $\varepsilon = \varepsilon' = 1$. By assumption we can cover $\{2, 4, 6, \cdots, h - 1\}$ by $\{h + 2\delta + 2i - 1 \mid 1 \leqq i \leqq h - 2\} \cup \{3h + 2\delta - 1\}$. By Lemma 6 we can cover $\{1, 3, 5, \cdots, h\}$ by $\{3h + 2\delta - 3\} \cup \{3h + 2\delta + j \mid 1 \leqq j \leqq h - 1\} \cup \{2m + 1\}$ if $h \geqq 7$. There remains $h = 5$, which corresponds to $m = 10$ and 11. This completes the proof of Theorem 7.

Proof of Theorem 6. Let $n = 6m + 1$. It is trivial to check that the nonzero residues (mod n) are the disjoint union of the four sets A_m, $B_m + m$, $-A_m$, $-(B_m + m)$. By Theorem 7 $B_m + m$ covers A_m. This means that $(B_m + m) \cup A_m$ is a union of triples (a, b, c) where $a \in A_m$, $b, c \in B_m + m$, and $a = b - c$. The triples $(a, -b, c)$ and $(-a, b, -c)$ then exhaust all the nonzero residues (mod n), and each one has sum zero.

We turn now to the case $k \geqq 4$ of Theorem 5. It is convenient to prove it in the following somewhat sharper form.

THEOREM 8. *Suppose n is odd and $k \mid n - 1$, where $k \geqq 4$. Then the nonzero integers in the interval $[-(n - 1)/2, (n - 1)/2]$ can be partitioned into $(n - 1)/k$ disjoint sets of cardinality k, so that the sum of the elements in each set is* 0.

Proof. Again we note that this is trivial when k is even, for then we need merely split the interval $[1, (n - 1)/2]$ into $(n - 1)/k$ sets of cardinality $k/2$, and then adjoin to each of these sets the negatives of its elements. Suppose next that $k = 5$. The conditions that n is odd and $k \mid n - 1$ then yield $n = 10m + 1$. We begin by forming the $2m$ triples $(a, -b, c)$ and $(-a, b, -c)$ constructed in Theorem 6. If $m \equiv 0$ or 1 (mod 4), the elements of these triples constitute all the nonzero integers in the interval $[-3m, 3m]$, and each triple has sum zero. The remaining nonzero integers in the interval $[-(n - 1)/2, (n - 1)/2] = [-5m, 5m]$ are symmetric about 0, and there are $2(5m - 3m) = 4m$ of them. They can therefore be partitioned into $2m$ pairs of the form $(-j, j)$. To each of the above $2m$ triples we adjoin one of these pairs. This has the effect of decomposing the nonzero integers of $[-5m, 5m]$ into $2m$ sets of cardinality 5, where the sum of the integers in each set is zero.

If $m \equiv 2$ or 3 (mod 4), the elements of the triples $(a, -b, c)$ and $(-a, b, -c)$ of Theorem 5 constitute the integers $1, 2, \cdots, 3m - 1$, $3m + 1$ and their negatives. The remaining nonzero integers in the interval $[-5m, 5m]$ are therefore $3m$ and $\{v \mid 3m + 2 \leqq v \leqq 5m\}$, together with their negatives. Since this set is symmetric about 0, we can again split it into $2m$ pairs of the form $(-j, j)$ and adjoin one pair to each triple, giving the desired partition of $[-5m, 5m]$ into sets of cardinality 5.

Exactly the same construction will clearly now carry us from k to $k + 2$ for any $k \geqq 5$. It is no longer necessary to distinguish between the various residues of m (mod 4), since for $k \geqq 5$, the elements of our k-sets constitute all the nonzero integers in $[-(n - 1)/2, (n - 1)/2]$.

We note that the hypothesis in this section that ϕ is a k-regular permutation can easily be dispensed with, using a very slight modification of the above technique. The only essential requirement is that 0 must be the only fixed point of ϕ. For simplicity we confined ourselves to the regular case, which seems to be the most interesting in applications. In a later paper the results of this section will be extended to arbitrary groups of odd order.

Note added in proof. A direct, constructive proof of Skolem's conjecture (Theorem 7), appears also in R. O. Davies, "On Langford's problem (II), Math. Gaz., 43 (1959), pp. 253-255. We are grateful to D. G. Rogers (private communication) for pointing out this result as informing us of the following 3-regular complete mapping of Z_{25}: $\phi = (1, 8, 5)(2, 10, 11)(3, 6, 24)(4, 14, 16)(7, 19, 17)(9, 15, 20)(12, 23, 18)(13, 22, 21)$. The above partition was obtained by D. G. Rogers and F. W. Roush by means of a computer search.

REFERENCES

1. J. R. Doner, *CIP neofields and combinatorial designs*, Ph.D. dissertation, University of Michigan, 1972.
2. R. J. Friedlander, B. Gordon and M. D. Miller, *On a group sequencing problem of Ringel*, Proc. 9th S.E. Conference on Combinatorics, Graph Theory and Computing, 307-321.
3. R. J. Friedlander, Robert W. Jamison and Peter Tannenbaum, *Regular complete mappings of Z_n*, to appear.
4. B. Gordon and W. H. Mills, *A theorem on triples of integers*, unpublished manuscript.
5. M. Hall, *A combinatorial problem on abelian groups*, Proc. Amer. Math. Soc., **3** (1952), 584-587.

6. M. Hall and L. J. Paige, *Complete mappings of finite groups*, Pacific J. Math., **5** (1955), 541–549.

7. H. Hanani, *A note on Steiner triple systems*, Math. Scand., **8** (1960), 154–156.

8. D. Hsu, *I-matrices and triple systems, I. HP I-matrices and Steiner triple systems*, to appear.

9. E. C. Johnsen and T. F. Storer, *Combinatorial structures in loops, IV; Steiner triple systems in neofields*, Math. Z., **138** (1974), 1–14.

10. E. S. O'Keefe, *Verification of a conjecture of T. Skolem*, Math. Scand., **9** (1961), 80–82.

11. G. Ringel, *Map Color Theorem*, Springer-Verlag, New York, 1974.

12. T. Skolem, *On certain distributions of integers in pairs with given differences*, Math. Scand., **5** (1957), 57–68.

13. ———, *Some remarks on the triple systems of Steiner*, Math. Scand., **6** (1958), 273–280.

14. P. Tannenbaum, *Abelian Steiner triple systems*, Canad. J. Math., **28** (1976), 1251–1268.

Received September 12, 1979 and in revised form April 8, 1980. The first author was supported in part by University of Missouri-St. Louis Faculty Summer Research Fellowship.

THE UNIVERSITY OF MISSOURI
ST LOUIS, MO 63121
THE UNIVERSITY OF CALIFORNIA
LOS ANGELES, CA 90024
AND
THE UNIVERSITY OF ARIZONA
TUCSON, AZ 85721