Pacific Journal of Mathematics

SPLITTINGS OF FINITE GROUPS

DEAN ROBERT HICKERSON

Vol. 107, No. 1 January 1983

PACIFIC JOURNAL OF MATHEMATICS
Vol 107, No. 1, 1983

SPLITTINGS OF FINITE GROUPS

DEAN HICKERSON

Let G be a group, written additively, M a set of integers, and S a subset of G. We will say that M and S form a splitting of G if every nonzero element of G has a unique representation as a product ms with $m \in M$ and $s \in S$, while 0 has no such representation. (Here "ms" denotes the sum of m s's if $m \geq 0$ and denotes $-((-m)s)$ if $m < 0$.) Splittings arise in connection with the problem of tiling Euclidean space by translates of certain unions of unit cubes, called "crosses" and "semicrosses".

In this paper, we develop a counting technique which gives information about S if M and G are known. This technique is used to reduce the study of splittings of finite abelian groups to those of nonsingular splittings and of purely singular splittings. (A splitting is nonsingular if every element of M is relatively prime to $|G|$; it is purely singular if, for every prime divisor p of $|G|$, some element of M is divisible by p.) Next, it is shown that every splitting of a noncyclic abelian p-group is nonsingular. A construction is then given which yields many purely singular splittings.

We then discuss a number of results and examples, including some infinite and nonabelian groups, and close with a list of open problems.

TABLE OF CONTENTS

Table of Contents 141
Notation 142
0. Introduction 142
1. General Theory 145
   1.0. A Counting Technique 145
   1.1. Some M-Partitions 149
   1.2. A Decomposition Theorem 151
   1.3. Singular Splittings of Abelian p-Groups 155
   1.4. Some Purely Singular Splittings 159
2. Special Topics 161
   2.0. Purely Singular Splittings with Small $|M|$ 161
   2.1. A Question of Robinson's 165
   2.2. Miscellaneous Results 166
   2.3. Open Problems 170
References 171

Notation.

Symbol	Meaning
$\varnothing$	Empty set
$\lvert S \rvert$	Cardinality of S
$S - T$	Set of elements of S which are not in T
$S \times T$	Direct products of sets S and T
R	Additive group of real numbers
Z	Additive group of integers
C_r	Cyclic group of order r; elements of C_r are denoted by integers $0, \ldots, r-1$
$G \times H$	Direct product of groups G and H
$o(g)$	Order of group element g
mg	For integers $m \geq 0$, sum of m g's. For $m < 0$, $-((-m)g)$
mS	$\{ms\colon s \in S\}$
MS	$\{ms\colon m \in M \,\&\, s \in S\}$ (This notation will be used only when the products ms are all distinct.)
$\gcd(m, n)$	Greatest common divisor of integers m and n
$e_p(m)$	Exponent of p in m; i.e., largest r such that $p^r \mid m$
$p^r \Vert m$	$p^r \mid m$ but $p^{r+1} \nmid m$; i.e., $e_p(m) = r$
$\varphi(m)$	Euler totient function of m
$[x, y)$	Set of real numbers $\geq x$ and $< y$
$q(A, B)$	See Def. 1.0.1
$c(A)$	See Def. 1.0.2
$B \mid A, B < A$	See Def. 1.0.4
$B \mid_M A$	See remarks after Def. 1.0.4
$g \mid h, A(g)$	See Def. 1.1.3
$\dim_p(G)$	See Def. 2.0.0

0. Introduction. Let G be a group, written additively, M a set of integers, and S a subset of G. We will say that M and S form a *splitting* of G if every nonzero element g of G has a unique representation of the form $g = ms$ with $m \in M$ and $s \in S$, while 0 has no such representation. (Here "ms" denotes the sum of m s's if $m \geq 0$, and $-((-m)s)$ if $m < 0$.) We will write "$G - \{0\} = MS$" to indicate that M and S form a splitting of G. M will be referred to as the multiplier set and S as the splitting set. We will also say that M splits G with splitting set S, or simply that M splits G, if the particular set S is not of interest.

For example, let G be the cyclic group of order 16; i.e., the set of integers from 0 to 15 under addition mod 16. Then $M = \{1, 2, 7\}$ and

$S = \{1, 3, 4, 13, 15\}$ form a splitting of G, as shown in the multiplication table below:

$m \backslash s$	1	3	4	13	15
1	1	3	4	13	15
2	2	6	8	10	14
7	7	5	12	11	9

Splittings of finite abelian groups have been studied in [**3**] (where they are called "factorings"), [**7**], [**4**], and [**2**].

Splittings were first considered in [**5**] in connection with the problem of tiling Euclidean space by translates of certain polytopes composed of unit cubes, called k-crosses and k-semicrosses. For positive integers k and n, a k-cross in n-space is formed by attaching to each face of a unit cube an arm of length k. A k-semicross is formed by attaching such an arm to one member of each pair of opposite faces of the original cube. A k-cross is thus a union of $2kn + 1$ unit cubes; a k-semicross is a union of $kn + 1$ unit cubes. Stein has investigated ([**5**], [**6**], [**7**]) the problem of tiling n-space by crosses and semicrosses; i.e., finding a set of translates of a cross (or semicross) whose interiors are pairwise disjoint and whose union is R^n. For example, the 1-cross tiles 2-space; we can center a cross at every integer point (x, y) for which $x \equiv 2y \pmod 5$. Note that the set of centers in this tiling is a subset of Z^2; it is known [**1**, Thm. 2.1] that if a k-cross (or semicross) tiles R^n then it also tiles in such a way that all centers are in Z^n. Further, the set of centers in the above tiling is an additive subgroup of R^2; a tiling whose centers form a subgroup of R^n is called a "lattice tiling". (If the k-cross tiles R^n, it does not necessarily tile in a lattice manner; it is shown in [**6**] that the 4-cross in 10-space tiles but not as a lattice.)

It is possible for a union of integer unit cubes to tile as a lattice in which some coordinates are not integers. For example, the (disconnected) set in R^2 consisting of a square centered at $(0, 0)$ and a square centered at $(2, 0)$ tiles as a lattice, the translating vectors being all points of the form $m(1, 1/2) + n(4, 0)$ with m and n integers. However, there is no lattice tiling by this set in which all coordinates are integers. (Whether this phenomenon can occur for connected sets, such as crosses and semicrosses, is not known.) A lattice tiling in which all coordinates are integers will be called an "integral lattice tiling".

It follows from [**3**, Thm. 1.1] that the k-cross tiles n-space as an integral lattice if and only if $\{\pm 1, \ldots, \pm k\}$ splits some abelian group of order $2kn + 1$. Similarly, the k-semicross tiles n-space as an integral lattice if and only if $\{1, \ldots, k\}$ splits some abelian group of order $kn + 1$. (For this reason, we will be primarily concerned with splittings of finite abelian groups.)

Most of the earlier study of splittings concentrated on the multiplier sets $\{1, \ldots, k\}$ and $\{\pm 1, \ldots, \pm k\}$, which correspond to the semicross and cross, respectively. However, any splitting of a finite abelian group by a multiplier set M generates a tiling by translates of some union of cubes. For instance, as will be shown in §1.4, $M = \{\pm 1, \pm 2, \pm 3, \pm 5, 7\}$ splits $C_2 \times C_2 \times C_7$. From this it follows that translates of the union of 28 unit cubes centered at $(0, 0, 0)$ and at $(m, 0, 0)$, $(0, m, 0)$, and $(0, 0, m)$ for $m \in M$ tile 3-space.

Following [**4**], we make the following definition:

DEFINITION 0.0. A splitting $G - \{0\} = MS$ of a finite group G is called *nonsingular* if every element of M is relatively prime to $|G|$; otherwise the splitting is called *singular*.

Nonsingular splittings are much easier to work with than singular ones. In fact, it is shown in [**4**, Thm. 4] that a set M splits a finite abelian group G nonsingularly if and only if it splits C_p, the cyclic group of order p, for each prime divisor p of $|G|$. (We will show in §2.2 that this is true even if G is nonabelian.)

In §1.0, we develop a counting argument (Thm. 1.0.8) which gives information about S if M and G are known.

Section 1.1 defines some partitions of a group which will be used in applications of the counting argument.

In §1.2, a decomposition theorem (Thms. 1.2.5 and 1.2.6) is given for splittings of finite abelian groups. This result breaks the study of splittings of finite abelian groups into two parts: the study of nonsingular splittings, and that of 'purely singular' splittings (Def. 1.2.4).

In §1.3, we prove a conjecture of Galovich and Stein: if a finite abelian p-group G has a singular splitting, then G is cyclic.

In §1.4, a construction is given (Thm. 1.4.0) which produces some purely singular splittings; it is conjectured that, with some modifications, this construction yields all purely singular splittings of noncyclic abelian groups.

Section 2.0 is concerned with purely singular splittings with small multiplier sets. In particular, we find all finite abelian groups which have a purely singular splitting with $|M| \leq 4$.

In §2.1, we discuss a question due to Raphael Robinson: If M splits a finite abelian group G, must M split $C_{|G|}$? We show that this is not true in general, and give some sufficient conditions on M for the result to hold. In particular, it is shown to hold for the sets $\{1,\ldots,k\}$ and $\{\pm 1,\ldots,\pm k\}$.

Section 2.2 discusses some miscellaneous results and examples.

Finally, some open questions are given in §2.3.

1. General theory.

1.0. A Counting Technique. Let a group G and a multiplier set M be given, and suppose we want to find a set $S \subseteq G$ such that $G - \{0\} = MS$. In general, S is not uniquely determined; for example, if α is an automorphism of G, then $\alpha(S)$ is also a splitting set. S is not even determined up to automorphisms of G; for example, let $G = C_7$, $M = \{1, -1\}$, $S = \{1, 2, 3\}$, and $S' = \{1, 2, 4\}$. Then $G - \{0\} = MS = MS'$, but there is no automorphism α of G such that $S' = \alpha(S)$.

However, a great deal of information about S can be obtained from M and G. Specifically, we will show that for certain subsets A of G, we can determine $|S \cap A|$. First we consider some examples which illustrate the general technique.

Again, let $G = C_7$ and $M = \{1, -1\}$. Partition G into the sets $A = \{1, 6\}$, $B = \{2, 5\}$, $C = \{3, 4\}$, and $D = \{0\}$. Note that if $g \in G$ and $m \in M$, then g and mg lie in the same set. Hence, if S is a splitting set, then, for example, $A = M \cdot (S \cap A)$. Therefore, $|S \cap A| = |A|/|M| = 1$. Similarly, $|S \cap B| = |S \cap C| = 1$ and $|S \cap D| = 0$. (In this example, nothing more can be determined about S; any S which satisfies these cardinality conditions is a splitting set.)

Let $G = C_{16}$ and $M = \{1, -1, 2\}$. Partition G into $A = \{1, 3, 5, 7, 9, 11, 13, 15\}$ and $B = \{0, 2, 4, 6, 8, 10, 12, 14\}$. Note that if $m \in M$, $g \in G$, and $mg \in A$, then $m \in \{-1, 1\}$ and $g \in A$. Hence, if S is a splitting set, $A = \{1, -1\} \cdot (S \cap A)$, whence $|S \cap A| = |A|/2 = 4$. But $15 = |G| - 1 = |M| \cdot |S| = 3|S|$ so $|S| = 5$. Hence $|S \cap B| = |S| - |S \cap A| = 5 - 4 = 1$. That is, S contains 4 odd elements and 1 even element.

By using a finer partition, we can learn more about S. Again let $G = C_{16}$ and $M = \{1, -1, 2\}$. Partition G into $A = \{1, 3, 5, 7, 9, 11, 13, 15\}$, $B = \{2, 6, 10, 14\}$, $C = \{4, 12\}$, $D = \{0, 8\}$. As before, if S is a splitting

set, then $|S \cap A| = 4$. But for $s \in A$, $2s \in B$ so $2(S \cap A) \subseteq B$, and since both $2(S \cap A)$ and B have cardinality 4, $2(S \cap A) = B$. Hence $M \cdot (S \cap A) = A \cup B$ so $S \cap B$ is empty. Next, if $ms \in C$ for $m \in M$, $s \in S$, then either $m \in \{1, -1\}$ and $s \in C$ or $m = 2$ and $s \in B$. The latter is impossible so $C = \{1, -1\} \cdot (S \cap C)$ and $|S \cap C| = 1$. Thus, the 1 even element referred to above is either 4 or 12.

The above examples illustrate what will be done in general: We will partition G into disjoint subsets. If this partition satisfies certain conditions, then we will be able to determine $|S \cap A|$ for each of the subsets A.

DEFINITION 1.0.0. A *partition* of a set X is a set of disjoint nonempty subsets of X whose union is X. If $\mathcal{Q}$ is a partition of X then the equivalence relation associated with $\mathcal{Q}$ is denoted by "$\sim_{\mathcal{Q}}$"; that is, $x \sim_{\mathcal{Q}} y$ if $x \in A$ and $y \in A$ for some $A \in \mathcal{Q}$.

DEFINITION 1.0.1. A partition $\mathcal{Q}$ of a group G is *M-compatible* provided that, for any g and h in G and $m \in M$, if $g \sim_{\mathcal{Q}} h$ then $mg \sim_{\mathcal{Q}} mh$. Equivalently, if $A \in \mathcal{Q}$ and $m \in M$, then $mA \subseteq B$ for some $B \in \mathcal{Q}$.

Given $A, B \in \mathcal{Q}$, we let $q(A, B) = \{m \in M\colon mB \subseteq A\}$.

DEFINITION 1.0.2. For a subset A of a group G, let $c(A)$ be the number of nonzero elements of A; that is, $c(A) = |A|$ if $0 \notin A$ and $c(A) = |A| - 1$ if $0 \in A$.

We now obtain a counting formula related to group splittings.

THEOREM 1.0.3. *Suppose G is a finite group with a splitting $G - \{0\} = MS$, $\mathcal{Q}$ is an M-compatible partition of G, and $A \in \mathcal{Q}$. Then*

$$c(A) = \sum_{B \in \mathcal{Q}} |q(A, B)| \cdot |S \cap B| .$$

Proof. Consider the set of products ms which lie in A. Since $G - \{0\} = MS$, each nonzero element of A has a unique representation of the form ms, so the number of such product is $c(A)$.

Next, partition the set of products ms according to the class $B \in \mathcal{Q}$ which contains s. For $s \in B$, we have $ms \in A$ if and only if $mB \subseteq A$; that is, if and only if $m \in q(A, B)$. Hence the number of products $ms \in A$ with $s \in B$ is $|q(A, B)| \cdot |S \cap B|$. Summing over all $B \in \mathcal{Q}$ gives the result.

Since our goal is to compute $|S \cap A|$ given M and G, we rewrite this result as follows:

$$|S \cap A| = \frac{1}{|q(A, A)|}\left(c(A) - \sum_{\substack{B \in \mathcal{Q} \\ B \neq A}} |q(A, B)| \cdot |S \cap B|\right).$$

This transformation is valid provided that $q(A, A)$ is nonempty, a point which will be discussed later.

As given, it appears that computation of $|S \cap A|$ depends on knowledge of $|S \cap B|$ for all $B \neq A$, while $|S \cap B|$, in turn, depends on $|S \cap A|$. However, if $q(A, B) = \varnothing$ then $|S \cap A|$ does not, in fact, depend on $|S \cap B|$. Hence, to compute all of the numbers $|S \cap A|$, we must be able to list the elements of $\mathcal{Q}$ in such a way that, if $q(A, B) \neq \varnothing$ then B comes before A in the list. That is, the transitive closure of the relation defined by $q(A, B) \neq \varnothing$ must be a partial ordering on $\mathcal{Q}$. Expressing this more constructively, we have:

DEFINITION 1.0.4. Let A and B be elements of an M-compatible partition $\mathcal{Q}$ of a group G. Then B *divides* A (written "$B \mid A$") if there are elements $B = B_0, B_1, \ldots, B_r = A$ of $\mathcal{Q}$ such that, for $0 \leq i < r$, $m_i B_i \subseteq B_{i+1}$ for some $m_i \in M$. Equivalently, B divides A if $nB \subseteq A$ for some n which can be expressed as a (possibly empty) product of elements of M.

We will say that B is a *proper divisor* of A (written "$B < A$") if $B \mid A$ but $B \neq A$.

Divisibility is clearly a reflexive and transitive relation on $\mathcal{Q}$. It need not be a partial ordering. For example, let $G = C_3$, $M = \{2\}$, and $\mathcal{Q} = \{\{0\}, \{1\}, \{2\}\}$. Then $\{1\} \mid \{2\}$ and $\{2\} \mid \{1\}$, but $\{1\} \neq \{2\}$.

Note that divisibility depends on M. That is, if $\mathcal{Q}$ is both M- and N-compatible, it is possible that $B \mid A$ with respect to M but not with respect to N. We will write "$B \mid_M A$" to indicate the dependence on M when necessary. For example, if $G = C_2$, $\mathcal{Q} = \{\{0\}, \{1\}\}$, $M = \{2\}$, and $N = \{1\}$, then $\{1\} \mid_M \{0\}$ but $\{1\} \nmid_N \{0\}$.

DEFINITION 1.0.5. An M-compatible partition $\mathcal{Q}$ of a group G is called an *M-partition* of G if divisibility is a partial ordering on $\mathcal{Q}$.

We can now see that the elements of $\mathcal{Q}$ can be listed as described above only when $\mathcal{Q}$ is an M-partition. Furthermore, if $q(A, B) \neq \varnothing$, then $B \mid A$. Hence, the sum in the formula for $|S \cap A|$ can be restricted to those $B \in \mathcal{Q}$ for which $B < A$.

Returning to the point mentioned earlier about $q(A, A)$ being non-empty, we have the following result:

LEMMA 1.0.6. *Let $\mathcal{A}$ be an M-partition of a group G. Then*:
(0) *If, for each $g \in G$, M contains an element m relatively prime to $o(g)$, then $q(A, A) \neq \varnothing$ for every $A \in \mathcal{A}$.*
(1) *If, for some g, M has no such element, then M does not split G.*

(For abelian groups, this result can be simplified. See Theorem 2.2.2.)
The proof will use the following result, whose proof is omitted.

LEMMA 1.0.7. *If g is a torsion element of a group G, and n is an integer, then*

$$o(ng) = \frac{o(g)}{\gcd(n, o(g))}.$$

Consequently, $o(ng) \mid o(g)$.

Proof of Lemma 1.0.6. To prove (0), let $A \in \mathcal{A}$. Let $g \in A$ and pick $m \in M$ relatively prime to $o(g)$. We will show that $m \in q(A, A)$.

Let B be that element of $\mathcal{A}$ which contains mg. Then $mA \subseteq B$ so $A \mid B$. Also, for some positive integer r, $m^r \equiv 1 \pmod{o(g)}$; in fact we may take $r = \varphi(o(g))$. Hence $m^{r-1}(mg) = m^r g = g \in A$ so $m^{r-1}B \subseteq A$ and $B \mid A$. But, since $\mathcal{A}$ is partially ordered by divisibility, it follows that $A = B$. That is, $mA \subseteq A$ so $m \in q(A, A)$.

To prove (1), suppose $g \in G$ and, for all $m \in M$, $\gcd(m, o(g)) > 1$. Choose $h \in H$ with $o(h)$ maximal subject to the condition that $g = nh$ for some integer n. By Lemma 1.0.7, $o(g) \mid o(h)$, so for $m \in M$, $\gcd(m, o(h)) > 1$; that is, h has the same property as g. In addition, if $h = nk$ for $n \in Z$, $k \in G$ then $o(k) \leq o(h)$.

Suppose M splits G with splitting set S. Then $h = ms$ for some $m \in M$, $s \in S$. From Lemma 1.0.7, $o(h) = o(s)/\gcd(m, o(s)) \leq o(s)$. But $o(s) \leq o(h)$ so we must have $o(s) = o(h)$ and $1 = \gcd(m, o(s)) = \gcd(m, o(h))$, a contradiction. Therefore M does not split G.

Hence, if M splits G, then the formula for $|S \cap A|$ will not involve division by 0. Summarizing the discussion above, we have the following result:

THEOREM 1.0.8. *Let G be a finite group, $G - \{0\} = MS$ a splitting of G, and $\mathcal{A}$ an M-partition of G. Then the values of $|S \cap A|$ for $A \in \mathcal{A}$ can be computed recursively by the formula*

$$|S \cap A| = \frac{1}{|q(A, A)|}\left(c(A) - \sum_{\substack{B \in \mathcal{A} \\ B < A}} |q(A, B)| \cdot |S \cap B|\right),$$

where the sum is over all $B \in \mathcal{A}$ for which $B < A$.

(If we try to apply this result to infinite groups, several things can go wrong. For one thing, the partially ordered set $\mathcal{A}$ may not contain a minimal element, in which case there is no way to start the recursion. Further, the formula above may give one of the indefinite forms $\infty - \infty$ or ∞/∞. In §2.2, we will construct an example in which $|S \cap A|$ is not determined by M and G. In light of this, it is not clear how Theorem 1.0.8 can be generalized to infinite groups.)

1.1. Some M-Partitions. In this section, we will discuss some properties of M-partitions, and define some particular M-partitions which will be used later.

THEOREM 1.1.0. *If $\mathcal{A}$ is an M-partition of a finite group G, and $N \subseteq M$, then $\mathcal{A}$ is an N-partition of G.*

Proof. If $g \sim_{\mathcal{A}} h$ and $n \in N$, then $n \in M$ so $ng \sim_{\mathcal{A}} nh$. Thus, $\mathcal{A}$ is N-compatible. Since divisibility is always reflexive and transitive, it remains only to show that if $A \,|_N B$ and $B \,|_N A$, then $A = B$. But every product of elements of N is also a product of elements of M, so $A \,|_N B$ implies that $A \,|_M B$. Similarly, $B \,|_M A$ so $A = B$.

In particular, note that every Z-partition is also an M-partition for every M.

DEFINITION 1.1.1. Let G be a finite group. The *order partition* $\mathcal{O}$ of G is defined by $g \sim_{\mathcal{O}} h$ if $o(g) = o(h)$. The *order* of an equivalence class A in $\mathcal{O}$ is the common order of the elements of A.

THEOREM 1.1.2. *The order partition $\mathcal{O}$ of a finite group G is a Z-partition.*

This follows easily from Lemma 1.0.7.

Note that 0 is in a class by itself in the order partition. In fact, it is not hard to show that the order partition is the coarsest Z-partition for which this is true; that is, every Z-partition which contains $\{0\}$ is a refinement of the order partition.

Another partition which will be used later is defined as follows:

DEFINITION 1.1.3. If g and h are elements of a group G, then g is a *divisor* of h (written "$g \mid h$") if $h = ng$ for some integer n; g and h are *associates* if g is a divisor of h and h is a divisor of g. The *associate partition* of G is the partition of G into classes of associate elements. If $g \in G$ then $A(g)$ is the associate class containing g.

(Implicit in the last two definitions is the easily verified fact that the property of being associates is an equivalence relation on G.)

Note that g and h are associates if and only if they generate the same cyclic subgroup of G. Thus, there is a 1-1 correspondence between associate classes of G and cyclic subgroups of G.

THEOREM 1.1.4. *If G is a finite group then the associate partition of G is a Z-partition of G.*

Proof. Let $\mathcal{Q}$ be the associate partition of G. We first show that $\mathcal{Q}$ is Z-compatible. Suppose $g \sim_{\mathcal{Q}} h$ and $k \in Z$. Then $g \mid h$ so $h = ng$ for some $n \in Z$. Hence $kh = kng = n \cdot kg$, so $kg \mid kh$. Similarly, $kh \mid kg$ so $kg \sim_{\mathcal{Q}} kh$, as required.

We next show that divisibility is a partial order on $\mathcal{Q}$. For suppose $A \mid B$ and $B \mid A$ for $A, B \in \mathcal{O}$. Then $mA \subseteq B$ and $nB \subseteq A$ for some $m, n \in Z$. Let $g \in A$. Then $mg \in B$ so $nmg \in A$. Hence g and nmg are associates; thus $g = knmg$ for some $k \in Z$. Therefore, $mg \mid g$ so g and mg are associates. But $g \in A$ and $mg \in B$ so $A = B$ and divisibility is a partial order on $\mathcal{Q}$. That is, $\mathcal{Q}$ is a Z-partition.

LEMMA 1.1.5. *If g and h are associate elements in a group G, then $o(g) = o(h)$.*

This follows immediately from Lemma 1.0.7.

In light of this result, we can make the following definition.

DEFINITION 1.1.6. Let A be an element of the associate partition of a finite group G. Then $o(A)$ is the common order of the elements of A.

The following lemma is sometimes useful for determining whether two elements of a group are associates.

LEMMA 1.1.7. *Two elements g and h of a finite group G are associates if and only if $g = nh$ for some integer n relatively prime to $|G|$.*

Proof. First suppose $g = nh$ where $\gcd(n, |G|) = 1$. Pick n' so that $nn' \equiv 1 \pmod{|G|}$. Then $n'g = n'nh = h$. Hence $h \mid g$ and $g \mid h$, so g and h are associates.

Now suppose g and h are associates. Then $h \mid g$ so $g = rh$ for some integer r. Further, if $n \in Z$, then $g = nh$ if and only if $n \equiv r \pmod{o(h)}$. Hence we must show that there is an n such that $n \equiv r \pmod{o(h)}$ and $\gcd(n, |G|) = 1$.

Note first that $\gcd(r, o(h)) = 1$ since, by Lemmas 1.1.5 and 1.0.7,

$$o(h) = o(g) = \frac{o(h)}{\gcd(r, o(h))}.$$

Write $|G| = uv$ where u is the largest divisor of $|G|$ all of whose prime factors are divisors of $o(h)$. Note that $\gcd(u, v) = 1$ so, by the Chinese Remainder Theorem, we can pick n such that $n \equiv r \pmod{u}$ and $n \equiv 1 \pmod{v}$. It is easily seen that n satisfies the desired conditions, so the proof is complete.

THEOREM 1.1.8. *The associate partition is the finest Z-partition of a finite group G.*

Proof. Let g and h be associates in G and let $\mathfrak{B}$ be any Z-partition of G. Let A and B be the elements of $\mathfrak{B}$ which contain g and h, respectively. We must show that $A = B$. Since $g \mid h$, $h = ng$ for some $n \in Z$, whence $A \mid B$. Similarly, $B \mid A$ so, since divisibility partially orders $\mathfrak{B}$, $A = B$.

1.2. A Decomposition Theorem. In [**2**: §6, Problem (6)] the following question is asked: If $0 \to A \to G \to B \to 0$ is an exact sequence of finite abelian groups and if M splits A and G, must M split B? An affirmative answer to this follows from Theorem 1.2.1 below. To be precise, Theorem 1.2.1 gives the 'dual' of this; that is, if M splits B and G, then M splits A. However, it is known [**2**: §1] that, for finite abelian groups, there is an exact sequence $0 \to A \to G \to B \to 0$ if and only if there is an exact sequence $0 \to B \to G \to A \to 0$, so the affirmative answer follows.

DEFINITION 1.2.0. Let H be a subgroup of G. A splitting $G - \{0\} = MS$ *induces* a splitting of H if $H - \{0\} = M(S \cap H)$.

THEOREM 1.2.1. *Let H be a normal subgroup of a finite group G. (H and G need not be abelian.) Suppose that M splits both G and G/H. Then every splitting $G - \{0\} = MS$ induces a splitting of H.*

We use the following lemma, the proof of which is straightforward.

LEMMA 1.2.2. *Let H be a normal subgroup of a finite group G and $\mathcal{A}$ an M-partition of G/H. For $A \in \mathcal{A}$, let $A^* = \{g \in G\colon\ g + H \in A\}$. Let $\mathcal{A}^* = \{A^*\colon A \in \mathcal{A}\}$. Then, for $m \in M$ and $A, B \in \mathcal{A}$, we have:*

(0) *$\mathcal{A}^*$ is an M-partition of G;*

(1) *$mA \subseteq B$ if and only if $mA^* \subseteq B^*$;*

(2) *$A \mid B$ if and only if $A^* \mid B^*$;*

(3) $|A^*| = |H| \cdot |A|$.

That is, $\mathcal{A}$ and $\mathcal{A}^*$ have the same structure with respect to scalar multiplication, and each element of $\mathcal{A}^*$ is $|H|$ times as large as the corresponding element of $\mathcal{A}$.

Proof of Theorem 1.2.1. Let $\mathcal{A}$ be an M-partition of G/H in which 0 is in a class by itself; for example, we may take $\mathcal{A}$ to be the order partition. Let $\mathcal{A}^*$ be as defined in the lemma. Let $G - \{0\} = MS$ and $G/H - \{0\} = MT$.

We must show that $H - \{0\} = M(S \cap H)$. Clearly, $M(S \cap H) \subseteq H - \{0\}$. Also, the products ms are all distinct, so $|M(S \cap H)| = |M| \cdot |S \cap H|$. Thus it is sufficient to show that

$$|S \cap H| = \frac{|H| - 1}{|M|}.$$

We will first prove that, for $A \in \mathcal{A}$, $A \neq \{0\}$, we have

$$|S \cap A^*| = |H| \cdot |T \cap A|.$$

Assume this is true for all proper divisors of A. Then, by Theorem 1.0.8, we have

$$|S \cap A^*| = \frac{1}{|q(A^*, A^*)|}\left(c(A^*) - \sum_{\substack{B \in \mathcal{B} \\ B < A^*}} |q(A^*, B)| \cdot |S \cap B|\right).$$

But each $B \in \mathcal{Q}^*$ has the form C^* for some $C \in \mathcal{Q}$. Further, $B \mid A^*$ if and only if $C \mid A$. Hence,

$$|S \cap A^*| = \frac{1}{|q(A^*, A^*)|}\left(c(A^*) - \sum_{\substack{C \in \mathcal{Q} \\ C < A}} |q(A^*, C^*)| \cdot |S \cap C^*|\right).$$

Part (1) of Lemma 1.2.2 implies that $q(A^*, C^*) = q(A, C)$. Part (3) implies, since $0 \notin A$, that $c(A^*) = |A^*| = |H| \cdot |A| = |H|\, c(A)$. Finally, the inductive hypothesis gives $|S \cap C^*| = |H| \cdot |T \cap C|$. Thus,

$$\begin{aligned}|S \cap A^*| &= \frac{1}{|q(A, A)|}\left(|H|\, c(A) - \sum_{\substack{C \in \mathcal{Q} \\ C < A}} |q(A, C)| \cdot |H| \cdot |T \cap C|\right) \\ &= |H| \frac{1}{|q(A, A)|}\left(c(A) - \sum_{\substack{C \in \mathcal{Q} \\ C < A}} |q(A, C)| \cdot |T \cap C|\right) \\ &= |H| \cdot |T \cap A|,\end{aligned}$$

and the formula holds for A.

The above argument fails for $A = \{0\}$ since, in this case, $c(A^*) = c(H) = |H| - 1$ while $c(A) = 0$, so $c(A^*) = |H|\, c(A)$. Instead, we obtain

$$|S \cap A^*| = \frac{|H| - 1}{|q(A, A)|} + |H| \cdot |T \cap A|.$$

But $A = \{0\}$ so $A^* = H$, $q(A, A) = M$, and $|T \cap A| = 0$. Hence,

$$|S \cap H| = \frac{|H| - 1}{|M|},$$

and the proof is complete.

As a special case of Theorem 1, we have the following result:

THEOREM 1.2.3. *Let H and K be finite groups, which need not be abelian. If M splits both $H \times K$ and K, then M splits H.*

For, let $G = H \times K$ in Theorem 1, and note that $G/H \cong K$.

We will now use this result to prove a decomposition theorem for splittings of finite abelian groups.

DEFINITION 1.2.4. A splitting $G - \{0\} = MS$ of a finite group G is *purely singular* if, for every prime divisor p of $|G|$, at least one element of M is divisible by p.

THEOREM 1.2.5. *Let $G - \{0\} = MS$ be a splitting of a finite abelian group G. Then there exist subgroups H and K of G such that*:

(0) $G = H \times K$;

(1) *the given splitting induces a nonsingular splitting of H*;

(2) *the given splitting induces a purely singular splitting of K.*

Further, H and K are uniquely determined by these conditions.

Proof. Let P be the set of prime divisors of elements of M. Let $H = \{g \in G$: no prime divisor of $o(g)$ is in $P\}$ and $K = \{g \in G$: every prime divisor of $o(g)$ is in $P\}$. It follows from the factorization of G as a direct product of its Sylow subgroups that $G = H \times K$.

Let $k \in K$ and consider the representation of k in the form ms. Lemma 1.0.7 shows that $o(k) = o(s)/\gcd(m, o(s))$ so $o(s) \mid mo(k)$. Hence, if p is a prime divisor of $o(s)$, then either $p \mid m$ or $p \mid o(k)$. In either case, $p \in P$. Therefore, $s \in K$. It follows that the given splitting induces a splitting of K. That this splitting is purely singular follows from the definition of K.

Now apply Theorem 1, noting that H is normal in G and that $G/H \cong K$. It follows that the given splitting induces a splitting of H, which must be nonsingular because of the definition of H.

The uniqueness of H and K follows easily by considering the possible prime factors of $|H|$ and $|K|$.

The converse of this theorem is also true, that is, if H and K are finite abelian groups such that M splits H nonsingularly and M splits K purely singularly, then M splits $H \times K$. In fact, the following more general result follows from [**4**: Thm. 1]:

THEOREM 1.2.6. *Let H be a subgroup of the finite abelian group G. Suppose M splits both H and G/H and that the splitting of H is nonsingular. Then M splits G.*

(For nonabelian groups, this result does not hold. See §2.2.)

Taken together, these theorems reduce the study of splittings of finite abelian groups to the study of nonsingular and of purely singular splittings. (At least, if we are only interested in questions of the form "Does M split G?" this is true. However, there is no obvious way to find *all* splittings of $H \times K$ given those of H and K.)

Nonsingular splittings of abelian groups have been investigated in [**4**]. In particular, the following theorem [**4**: Thm. 4] reduces their study to the case of cyclic groups of prime order.

THEOREM 1.2.7. *Let G be a finite abelian group and M a set of integers relatively prime to $|G|$. Then M splits G if and only if M splits C_p for each prime divisor p of $|G|$.*

The next two sections are concerned with purely singular splittings of abelian groups. In §1.3, it will be shown that an abelian p-group with a purely singular splitting must be cyclic. (Note that "singular" and "purely singular" are equivalent for p-groups.) Section 1.4 presents some purely singular splittings of noncyclic groups.

1.3. Singular Splittings of Abelian p-Groups. In [**2**: §6, Problem (4)], Galovich and Stein conjectured that every splitting of a non-cyclic abelian p-group is nonsingular, and proved this for groups of the form $C_{p^n}^k$ where p is prime and $k \geq 2$. In this section, we will prove their conjecture in general.

THEOREM 1.3.0. *If G is a finite abelian p-group with a singular splitting, then G is cyclic.*

Before proving this, we give a simplification of Theorem 1.0.8 for p-groups.

LEMMA 1.3.1. *Let $\mathcal{Q}$ be a Z-partition of a finite (possibly nonabelian) p-group G. If $A \in \mathcal{Q}$, $0 \notin A$, and $B \mid A$, then there is an integer $r \geq 0$ such that, for $m \in Z$, $mB \subseteq A$ if and only if $p^r \| m$.*

Proof. Let $m \in Z$ and write $m = p^r n$ with $p \nmid n$. Let $g \in B$. By Lemma 1.1.7, mg and $p^r g$ are associates. Hence $mB \subseteq A$ if and only if $p^r g \in A$. It therefore suffices to show that if $p^r g \in A$ and $p^s g \in A$ then $r = s$. If $r < s$ then $p^r g \in A$ and $p^{s-r} \cdot p^r g \in A$ so $p^{s-r} A \subseteq A$. But for sufficiently large k, $p^k A = \{0\}$, contradicting $A \neq \{0\}$. Hence $r \geq s$. Similarly $s \geq r$ so $r = s$.

THEOREM 1.3.2. *Let $G - \{0\} = MS$ be a splitting of a finite (possibly nonabelian) p-group G, and let $\mathcal{Q}$ be a Z-partition of G in which 0 is in a class by itself. For $r \geq 0$, let μ_r be the number of elements m of M for which $p^r \| m$.*

(0) *If $A \in \mathcal{Q}$ and $A \neq \{0\}$, then*

$$|S \cap A| = \frac{1}{\mu_0}\left(|A| - \sum_{\substack{r \geq 1 \\ p^r B \subseteq A}} \mu_r |S \cap B|\right).$$

(1) *If $A \in \mathcal{Q}$, $\mu_r \neq 0$, and $p^r A = \{0\}$, then $|S \cap A| = 0$.*

Proof. Let $A \in \mathcal{Q}$. By Theorem 1.0.8,

$$|S \cap A| = \frac{1}{|q(A, A)|}\left(c(A) - \sum_{\substack{B \in \mathcal{Q} \\ B < A}} |q(A, B)| \cdot |S \cap B|\right).$$

If $A \neq \{0\}$ then $c(A) = |A|$. Also, since $1A \subseteq A$, Lemma 1.3.1 implies that $mA \subseteq A$ if and only if $p \nmid m$; hence $|q(A, A)| = \mu_0$. Similarly, if $B < A$, then $p^r B \subseteq A$ for a unique $r \geq 1$, and $|q(A, B)| = \mu_r$. Part (0) follows immediately.

To prove part (1), suppose $A \in \mathcal{Q}$, $\mu_r \neq 0$, $p^r A = \{0\}$, and $s \in S \cap A$. Let $p^r \| m$ for $m \in M$. Then $m = p^r k$ for some k, so $ms = p^r ks = k \cdot p^r s = k \cdot 0 = 0$. But this contradicts $G - \{0\} = MS$, so $|S \cap A| = 0$.

We will also need the following result:

LEMMA 1.3.3. *Let $G = C_{p^{e_0}} \times \cdots \times C_{p^{e_k}}$, where $k \geq 0$ and $1 \leq e_0 \leq \cdots \leq e_k$. If $g \in G$ then the number of solutions h of $ph = g$ is either* 0 *or* p^{k+1}.

Proof. Suppose h_0 satisfies $ph_0 = g$. Then, for any h, $ph = g$ if and only if $p(h - h_0) = 0$. Letting $h - h_0 = (a_0, \ldots, a_k)$, we have $p(h - h_0) = 0$ if and only if $p^{e_i - 1} \mid a_i$ for $0 \leq i \leq k$. Since there are p possible values for each a_i, the result follows.

We are now ready to prove Theorem 1.3.0. Let $G = C_{p^{e_0}} \times \cdots \times C_{p^{e_k}}$, where $k \geq 0$ and $1 \leq e_0 \leq \cdots \leq e_k$, and suppose $G - \{0\} = MS$ is a singular splitting.

Let $\mathcal{Q}$ be the associate partition of G and consider the associate class $A(g_0)$, where $g_0 = (p^{e_0 - 1}, 0, \ldots, 0)$. Since the splitting $G - \{0\} = MS$ is singular, $\mu_r \neq 0$ for some $r \geq 1$. But $p^r g_0 = 0$ so $p^r A(g_0) = \{0\}$. By part (1) of Theorem 1.3.2, $|S \cap A(g_0)| = 0$. By part (0) of the same theorem,

$$|S \cap A(g_0)| = \frac{1}{\mu_0}\left(|A(g_0)| - \sum_{\substack{r \geq 1 \\ p^r B \subseteq A(g_0)}} \mu_r |S \cap B|\right).$$

Since $|A(g_0)| = p - 1$, this gives

$$p - 1 = \sum_{\substack{r \geq 1 \\ p^r B \subseteq A(g_0)}} \mu_r |S \cap B|.$$

We will show that, for $1 \leq r < e_0$, there are exactly p^{rk} classes B for which $p^r B \subseteq A(g_0)$, while, for $r \geq e_0$, there are none. Also, the value of

$|S \cap B|$ depends only on r. It will follow that the above sum is divisible by p^k. Hence $k = 0$ and G is cyclic.

First suppose $p^r B \subseteq A(g_0)$. If $r \geq e_0$ then, for $g \in B$, the zeroth component of $p^r g$ is 0, contradicting the fact that $p^r g$ is an associate of g_0. Hence $r < e_0$.

Next observe that if $p^r B \subseteq A(g_0)$ then $o(B) = p^{r+1}$ and $|B| = p^r(p-1)$.

Now suppose $0 \leq r \leq e_0 - 2$ and $p^r B \subseteq A(g_0)$. We will show that there are exactly p^k classes C such that $pC = B$. We first count the elements $h \in G$ such that $ph = g$, where g is a given element of B. Let $g = (a_0, a_1, \ldots, a_k)$. Since $p^r g$ is an associate of $g_0 = (p^{e_0-1}, 0, \ldots, 0)$, we have $p^{e_0-1-r} \mid a_0$ and $p^{e_i-r} \mid a_i$ for $1 \leq i \leq k$. Since $r \leq e_0 - 2$, $e_0 - 1 - r \geq 1$ and, for $1 \leq i \leq k$, $e_i - r \geq e_0 - r \geq 1$. Hence $p \mid a_i$ for all i so, by Lemma 1.3.3, the number of h's is p^{k+1}.

Since $|B| = p^r(p-1)$, the number of $h \in G$ for which $ph \in B$ is $p^r(p-1)p^{k+1}$. But each such h lies in exactly one class C for which $pC \subseteq B$. Therefore the number of classes C is $p^r(p-1)p^{k+1}/|C| = p^r(p-1)p^{k+1}/p^{r+1}(p-1) = p^k$, as claimed.

An easy induction, which we omit, shows that, for $0 \leq r \leq r + s < e_0$ and $p^r B \subseteq A(g_0)$, there are exactly p^{sk} classes C such that $p^s C \subseteq B$. In particular, letting $r = 0$ shows that, for $0 \leq s < e_0$, there are exactly p^{sk} classes C for which $p^s C \subseteq A(g_0)$.

Finally we show that, if $B \mid A(g_0)$, then $|S \cap B|$ depends only on the value of r for which $p^r B \subseteq A(g_0)$. This is vacuously true for $r \geq e_0$, so let $0 \leq r < e_0$ and assume that, for any $t > r$ and $p^t C \subseteq A(g_0)$, $|S \cap C| = \alpha_t$. Let $p^r B \subseteq A(g_0)$. By Theorem 1.3.2,

$$|S \cap B| = \frac{1}{\mu_0}\left(|B| - \sum_{\substack{s \geq 1 \\ p^s C \subseteq B}} \mu_s |S \cap C|\right).$$

But if $p^s C \subseteq B$ then $p^{r+s} C \subseteq A(g_0)$ so $|S \cap C| = \alpha_{r+s}$. Also, the number of such classes C is p^{sk}. Finally $|B| = p^r(p-1)$, so

$$|S \cap B| = \frac{1}{\mu_0}\left(p^r(p-1) - \sum_{s \geq 1} p^{sk} \alpha_{r+s}\right),$$

which depends only on r. Calling the expression on the right α_r, and performing a reverse induction on r gives the desired result for all $r \geq 0$.

In particular, letting $r = 0$ gives

$$0 = |S \cap A(g_0)| = \frac{1}{\mu_0}\left(p - 1 - \sum_{s \geq 1} p^{sk} \alpha_s\right),$$

so

$$p - 1 = \sum_{s \geq 1} p^{sk} \alpha_s = p^k \sum_{s \geq 1} p^{(s-1)k} \alpha_s .$$

Hence $p^k \mid p - 1$ which implies that $k = 0$. That is, G is cyclic.

As an example of the above, consider the group $G = C_4 \times C_{16}$. Figure 1.3.4 shows the associate partition of G. (Each circle represents a class in the partition. The symbols inside denote the elements of the class. For example, "38" denotes the ordered pair $(3, 8)$. For the second component of such a pair, $A = 10, \ldots, F = 15$. A line downward from A to B indicates that $A = 2 \cdot B$.) In this example, we have $p = 2$, $k = 1$, $e_0 = 2$, $e_1 = 4$, and $g_0 = (2, 0)$. The divisors of $A(g_0)$ are indicated by the dashed box in Figure 1.3.4. Note that while the overall structure of the associate partition is rather complicated, the divisors of $A(g_0)$ have the simple structure described in the proof.

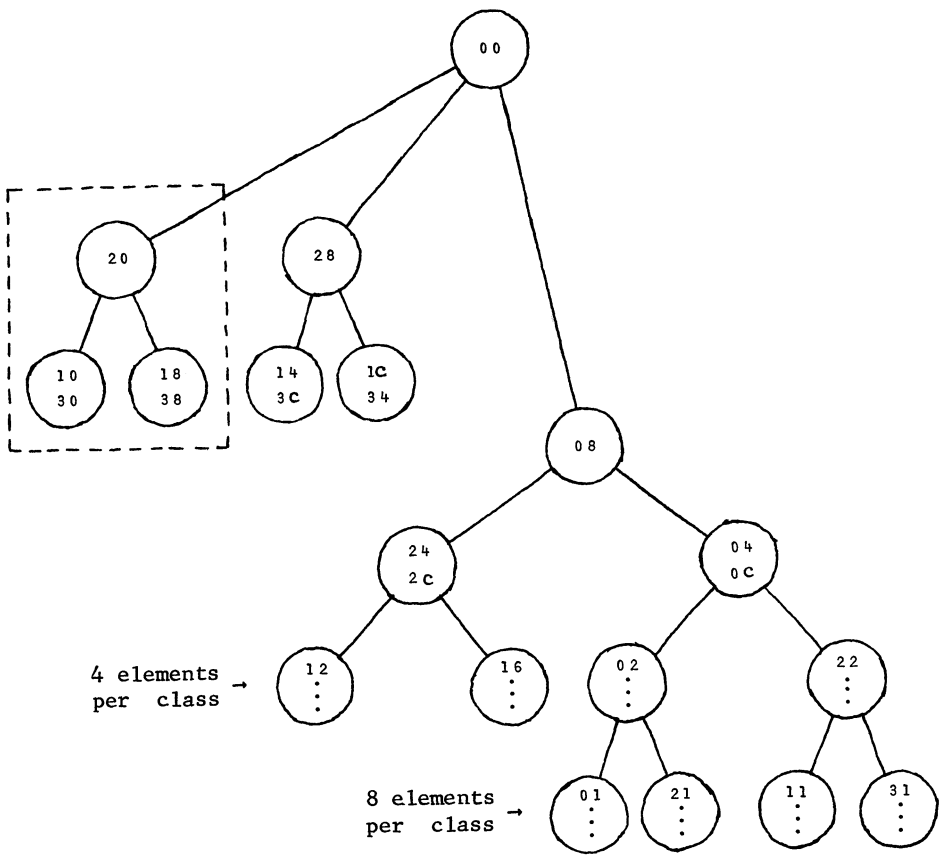

FIGURE 1.3.4

1.4. Some Purely Singular Splittings. In this section, we present a method for constructing purely singular splittings.

THEOREM 1.4.0. *Let G be a finite group with a splitting $G - \{0\} = MS$. Let r be relatively prime to $|G|$ and suppose that the cyclic group of order r has a splitting $C_r - \{0\} = M'S'$, with $|S'| = |S|$, in which every element of S' has order r. Then there is a purely singular splitting $(G \times C_r) - \{0\} = \overline{M}\overline{S}$ for which $|\overline{S}| = |S|$.*

Proof. Let θ be a 1-1 mapping from S onto S'. Let $\overline{S} = \{(s, \theta(s)): s \in S\}$.

For integers m and n, let $f(m, n)$ be an integer congruent to m mod $|G|$ and congruent to n mod r. (By the Chinese remainder theorem, $f(m, n)$ exists and is unique mod $|G|r$.) Let

$$M_1 = \{f(m, n): m \in M \text{ and } 0 \leq n < r\}$$

and

$$M_g = \{f(0, m'): m' \in M'\}.$$

We will show that

$$M_1\overline{S} = (G - \{0\}) \times C_r$$

and

$$M_g\overline{S} = \{0\} \times (C_r - \{0\}).$$

Then letting $\overline{M} = M_1 \cup M_g$, it will follow that $(G \times C_r) - \{0\} = \overline{M}\overline{S}$, so $\overline{M}$ and $\overline{S}$ form a splitting of $G \times C_r$. Further, if p is a prime divisor of $|G \times C_r|$, then either $p \,\|\, |G|$ or $p \mid r$. In the first case, all elements of M_g are divisible by p; in the second case all elements of M_r which have the form $f(m, 0)$ are. Hence the splitting is purely singular.

To prove that the two equations above hold, it suffices to show that, in each case, the set on the left is contained in that on the right, that the products $\overline{m}\overline{s}$ which occur in the set on the left are distinct, and that the cardinalities are the same on both sides.

First, consider an arbitrary product $\overline{m}\overline{s}$ with $\overline{m} \in \overline{M}$ and $\overline{s} \in \overline{S}$. We have $\overline{m} = f(m, n)$ for some m and n, while $\overline{s} = (s, \theta(s))$ for some $s \in S$. Then

$$\overline{m}\overline{s} = (f(m, n)s, f(m, n)\theta(s)) = (ms, n\theta(s)),$$

where the second equation follows from the definition of $f(m, n)$.

For $\overline{m} \in M_1$, we have $m \in M$ and $0 < n < r$. Since $G - \{0\} = MS$, $ms \neq 0$. Since $\theta(s)$ has order r, $n\theta(s) \neq 0$. Hence $M_1\bar{S} \subseteq (G - \{0\}) \times (C_r - \{0\})$. If $\overline{m}_0\bar{s}_0 = \overline{m}_1\bar{s}_1$ then, letting $\overline{m}_i = f(m_i, n_i)$ and $\bar{s}_i = (s_i, \theta(s_i))$ for $i = 0, 1$, we have $m_0s_0 = m_1s_1$ and $n_0\theta(s_0) = n_1\theta(s_1)$. Hence $m_0 = m_1$ and $s_0 = s_1$, so $(n_0 - n_1)\theta(s_0) = 0$. Since $\theta(s_0)$ has order r, $r \mid n_0 - n_1$ so $n_0 = n_1$. Thus $\overline{m}_0 = \overline{m}_1$ and $\bar{s}_0 = \bar{s}_1$; i.e., the products $\overline{m}\bar{s}$ are all distinct. Finally,

$$\begin{aligned} |M_1\bar{S}| &= |M_1| \cdot |\bar{S}| = |M|(r-1) \cdot |S| = (|G| - 1)(r-1) \\ &= |(G - \{0\}) \times (C_r - \{0\})|, \end{aligned}$$

so the first equation has been proved.

The proof of the other equation is similar.

For example, let $G = C_2 \times C_2$, $M = \{1\}$, $S = \{01, 10, 11\}$, $r = 7$, $M' = \{1, -1\}$, and $S' = \{1, 2, 3\}$. Let θ map the elements of S to those of S' in the order listed, so that $\bar{S} = \{011, 102, 113\}$. Let $f(m, n)$ be the smallest nonnegative integer that is $\equiv m \pmod 4$ and $\equiv n \pmod 7$, so that $\overline{M} = \{1, 9, 17, 25, 5, 13, 21\} \cup \{8, 20\}$. Then $(C_2 \times C_2 \times C_7) - \{0\} = \overline{MS}$ is a purely singular splitting.

All of the purely singular splittings of noncyclic groups which I know of are obtained by essentially the construction given in Theorem 1.4.0. I say "essentially" because the construction can be modified in several ways. For example, in defining f, it is not necessary to assume $f(m, n) \equiv m \pmod{|G|}$; it is sufficient to let $f(m, n) \equiv m \pmod g$, where g is the least common multiple of the orders of elements of G. (Thus, in the above example, we could let $\overline{M} = \{\pm 1, \pm 3, \pm 5, 7\} \cup \{\pm 2\}$, for example.) Further modifications of $\overline{M}$ are possible. However, $\bar{S}$ seems to be much more constrained, (except for the choice of the mapping θ). This suggests the following partial converse to Theorem 1.4.0.

CONJECTURE 1.4.1. Suppose the finite noncyclic abelian group $\overline{G}$ has a purely singular splitting $\overline{G} - \{0\} = \overline{MS}$. Then there exist a group G and an integer r such that:

(0) $\overline{G} \cong G \times C_r$,

(1) $|G|$ is relatively prime to r,

(2) if π is the projection from $\overline{G}$ to G, then π restricted to $\bar{S}$ is 1-1 and, for some set $M \subseteq Z$, $G - \{0\} = M\pi(S)$ is a nonsingular splitting,

(3) if π' is the projection from $\overline{G}$ to C_r, then π' restricted to S is 1-1, every element of $\pi'(S)$ has order n, and, for some $M' \subseteq Z$, $C_r - \{0\} = M'\pi'(S)$.

(This might also be true for nonabelian groups, but I have not looked at enough examples to justify stating this as a conjecture.)

We will now determine under what conditions the splitting of C_r used in Theorem 1.4.0 exists.

THEOREM 1.4.2. *Let r and k be positive integers. Then C_r has a splitting $C_r - \{0\} = MS$, with $|S| = k$, in which every element of S has order r, if and only if every prime divisor of r is* $\equiv 1 \pmod{k}$.

Proof. Suppose C_r has such a splitting. Let $\mathcal{O}$ be the order partition of C_r, and let $R \in \mathcal{O}$ be the equivalence class of order r. Note that $|S \cap R| = k$ while $|S \cap A| = 0$ for $A \in \mathcal{O}$, $A \neq R$. Let p be a prime divisor of r and consider the equivalence class P of order p. By Theorem 1.0.8,

$$0 = |S \cap P| = \frac{1}{|q(P,P)|}\left(c(P) - \sum_{\substack{B \in \mathcal{O} \\ B < P}} |q(P,B)| \cdot |S \cap B|\right)$$

$$= \frac{1}{|q(P,P)|}(p - 1 - |q(P,R)| \cdot k).$$

Hence $p - 1 = |q(P,R)| \cdot k$, so $p \equiv 1 \pmod{k}$, which proves the "only if" part.

Now suppose all prime divisors of r are $\equiv 1 \pmod{k}$. For each such prime p, let g_p be an integer whose multiplicative order mod p is k. Let g be an integer whose multiplicative order mod r is k and which is $\equiv g_p \pmod{p}$ for each prime divisor p of r. (The existence of g_p and g follows from standard results on congruences.) Note that for every divisor $d \neq 1$ of r, g has multiplicative order k mod d.

Let $S = \{1, g, \ldots, g^{k-1}\}$, considered as a subset of C_r. From the preceding paragraph it follows that, for any integer m which is not divisible by r, the set mS has cardinality k. Further, two such sets are either disjoint or equal. Letting M contain exactly one element from each set in the induced partition of $C_r - \{0\}$ completes the proof.

2. Special topics.

2.0. Purely Singular Splittings with Small $|M|$. In this section we will characterize purely singular splittings of abelian groups for which $|M| \leq 4$. We first show that if p is a prime divisor of $|G|$, then the number of elements of M which are divisible by p cannot be very large.

DEFINITION 2.0.0. Let G be a finite abelian group and p a prime. Then the *p-dimension* of G (written "$\dim_p(G)$"), is the number of p-groups which occur in the factorization of G as a product of cyclic groups of prime power order.

For example, for $G = C_2 \times C_2 \times C_4 \times C_3$, $\dim_2(G) = 3$, $\dim_3(G) = 1$, and $\dim_p(G) = 0$ for $p > 3$.

THEOREM 2.0.1. *Let G be a finite abelian group with a splitting $G - \{0\} = MS$. Let p be a prime divisor of $|G|$ and δ_p be the number of elements of M which are divisible by p. Then*

$$p^{\dim_p(G)}\delta_p < |M| .$$

Proof. Let $A = pG$ and $B = G - pG$. It is easily seen that $\{A, B\}$ is a Z-partition of G in which $B < A$. Further, $q(B, B)$ consists of those elements of M which are not divisible by p, so $|q(B, B)| = |M| - \delta_p$. By Theorem 1.0.8, we obtain

$$|S \cap B| = \frac{1}{|q(B, B)|}c(B) = \frac{|B|}{|M| - \delta_p} = \frac{|G| - |pG|}{|M| - \delta_p}.$$

A simple counting argument using the coordinate representation of elements of G shows that

$$|pG| = |G|p^{-\dim_p(G)}.$$

Hence,

$$\begin{aligned} |G| > |G| - 1 &= |M| \cdot |S| \geq |M| \cdot |S \cap B| \\ &= |M| \cdot |G| \cdot \frac{1 - p^{-\dim_p(G)}}{|M| - \delta_p}. \end{aligned}$$

Simplifying this inequality gives the desired result.

COROLLARY 2.0.2. *Let $G - \{0\} = MS$ be a purely singular splitting of a finite abelian group G, and p a prime divisor of $|G|$. Then*

$$p^{\dim_p(G)} < |M| .$$

Proof. This follows from Theorem 2.0.1 since $\delta_p \geq 1$.

THEOREM 2.0.3. *If $G - \{0\} = MS$ is a purely singular splitting of a nontrivial finite abelian group, then $|M| \geq 3$.*

Proof. Since G is nontrivial, $\dim_p(G) \geq 1$ for some p. By Corollary 2.0.2,

$$|M| > p^{\dim_p(G)} \geq 2.$$

THEOREM 2.0.4. *If $G - \{0\} = MS$ is a purely singular splitting with $|M| = 3$, then $G = C_{2^{2r}}$ for some $r \geq 0$. Moreover, each such group has such a splitting.*

Proof. If $p \mid\mid G|$, then $p^{\dim_p(G)} < 3$ so $p = 2$ and $\dim_p(G) = 1$; that is, $G = C_{2^s}$ for some s. But $3 \mid\mid G| - 1$ so s is even.

Further, $C_{2^{2r}}$ has the splitting $C_{2^{2r}} - \{0\} = MS$ with $M = \{1, -1, 2\}$ and $S = \{n\colon 0 < n < 2^{2r} \text{ and } 2 \mid e_2(n)\}$.

THEOREM 2.0.5. *If $G - \{0\} = MS$ is a purely singular splitting with $|M| = 4$, then G is either trivial or equal to C_9.*

Proof. From $p^{\dim_p(G)} < 4$ it follows that $\dim_p(G) = 1$ and either $p = 2$ or $p = 3$. But $4 \mid\mid G| - 1$ so $p \neq 2$. Hence $G = C_{3^s}$. As before, s must be even; say $s = 2r$. We must show that $r \leq 1$.

Suppose $r \geq 2$. By applying Theorem 1.3.2 to the order partition of $G = C_{3^{2r}}$ (or, equivalently, by considering the polynomials $M(x)$ and $S(x)$ defined in [**2**: Lemma 3.2]), it is not hard to show that the multiple of 3 in M is not divisible by 9, and that the given splitting of G induces a splitting of the cyclic subgroup of order 81. Hence, it suffices to show that C_{81} has no splitting in which M consists of three elements not divisible by 3 and one element divisible by 3 but not by 9.

If C_{81} had such a splitting, then it can be shown in a straightforward manner that the splitting set S must consist of eighteen elements which are not divisible by 3 and two elements which are divisible by 9 but not by 27. Thus, we can write

$$S = S_0 \cup 9S_2,$$

where

$$|S_0| = 18, |S_2| = 2,$$

and the elements of S_0 and S_2 are not divisible by 3. Similarly,

$$M = M_0 \cup 3M_1,$$

where

$$|M_0| = 3, \qquad |M_1| = 1,$$

and the elements of M_0 and M_1 are not divisible by 3.

For M and S to form a splitting of C_{81}, it must also be true that

M_0S_0 is a reduced residue system (r.r.s.) mod 81,
M_1S_0 is a r.r.s. mod 27,
M_0S_2 is a r.r.s. mod 9,
M_1S_2 is a r.r.s. mod 3.

Since $|M_1| = 1$, it follows that S_0 and S_2 are reduced residue systems mod 27 and mod 3, respectively.

Without loss of generality, we may assume that $1 \in M_0$. (Otherwise we can multiply all elements of M by a suitable integer and reduce mod 81.) So let $M_0 = \{1, \alpha, \beta\}$.

Suppose $c \in S_0$. Then αc (taken mod 81) is not in S_0 since, if it were, the products $\alpha \cdot c$ and $1 \cdot \alpha c$ would be equal, and M_0S_0 could not be a r.r.s. mod 81. Similarly, $\beta c \notin S_0$. Consider the element $\alpha\beta c$. For this to be in M_0S_0, we must have either αc, βc, or $\alpha\beta c$ in S_0. The first two possibilities have been excluded, so $\alpha\beta c \in S_0$.

It follows that $(\alpha\beta)^r c \in S_0$ for all r. But S_0 is a r.r.s. mod 27 so $28c$ and $55c$ cannot be in S_0. Hence $(\alpha\beta)^r \not\equiv 28,55 \pmod{81}$ for all r. If d, the multiplicative order of $\alpha\beta$ mod 81, is divisible by 3, then $((\alpha\beta)^{d/3})^3 \equiv 1 \pmod{81}$ from which it follows easily that $(\alpha\beta)^{d/3} \equiv 28$ or $55 \pmod{81}$. Hence $3 \nmid d$. But $d \mid \varphi(81) = 54$ so $d = 1$ or 2 and $\alpha\beta \equiv \pm 1 \pmod{81}$.

Next consider the element $\alpha^2 c$. For this to be in M_0S_0, either $\alpha^2 c$, αc, or $\alpha^2\beta^{-1}c$ must be in S_0 (where "β^{-1}" denotes the inverse of β mod 81). If $\alpha^2 c \in S_0$ then $\beta \cdot \alpha^2 c = \alpha \cdot \alpha\beta c$ gives two representations of $\alpha^2\beta c$ as an element of M_0S_0, so $\alpha^2 c \notin S_0$. Since we have already seen that $\alpha c \notin S_0$, we must have $\alpha^2\beta^{-1}c \in S_0$. As before, it follows that $\alpha^2\beta^{-1} \equiv \pm 1 \pmod{81}$, so $\alpha^2 \equiv \pm\beta \pmod{81}$.

Combining these results, we get $\alpha^3 \equiv \alpha\alpha^2 \equiv \pm\alpha\beta \equiv \pm 1 \pmod{81}$ so $\alpha \equiv \pm 1 \pmod{27}$ and $\beta \equiv \pm 1 \pmod{27}$. Hence, some two elements of $M_0 = \{1, \alpha, \beta\}$ are congruent mod 27 and so are congruent mod 9. But this contradicts the fact that M_0S_2 is a r.r.s. mod 9. Therefore, C_{81} has no purely singular splitting with $|M| = 4$, and the proof is complete.

(*Note*: The fact that $\alpha\beta c$ and $\alpha^2\beta^{-1}c$ are in S_0 if c is in S_0 is a disguised version of the fact that every tiling of Z^2 by the 1-semicross which has $(0, 0)$ as a center also has $(1, 1)$ and $(2, -1)$ as centers. This sort of argument does not apply to $|M_0| = 4$, for example, since Z^3 can be tiled in more than one way by 1-semicrosses.)

For $|M| = 5$, it can be shown by similar techniques that if $G - \{0\} = MS$ is a purely singular splitting of a finite abelian group, then $G = C_{2^r} \times C_{2^s} \times C_{3^t}$ where $t \equiv r + s \pmod 4$. However, I do not know which of these groups actually have such splittings.

2.1. A Question of Robinson's. Raphael Robinson has raised the following question [**2**: §6, Problem (8)]: If M splits a finite abelian group G, must M also split $C_{|G|}$? We will show that this is not true in general, although it is true for certain sets M. In particular, it is true if M is either of the sets $\{1, \ldots, n\}$ or $\{\pm 1, \ldots, \pm n\}$.

In §1.4, we showed that the group $G = C_2 \times C_2 \times C_7$ has the splitting $G - \{0\} = MS$ where $M = \{\pm 1, \pm 2, \pm 3, \pm 5, 7\}$ and $S = \{011, 102, 113\}$. We now show that M does not split C_{28}.

Let $\mathcal{O}$ be the order partition of C_{28}. For $d \mid 28$, let O_d be the class in $\mathcal{O}$ of order d. If $C_{28} - \{0\} = MS$, then Theorem 1.0.8 gives $|S \cap O_{28}| = 2$ and $|S \cap O_{14}| = 2/3$. Hence M does not split C_{28}.

Suppose M is a set of integers, G is a finite abelian group which is not cyclic, and M splits G purely singularly. Since G is not cyclic, $\dim_p(G) \geq 2$ for some prime p. By Theorem 2.0.1,

$$\delta_p < |M|/p^2,$$

where δ_p is the number of elements of M which are divisible by p. Furthermore, $\delta_p \geq 1$ since the splitting is purely singular, so $p^2 < |M|$. We thus have the following result:

THEOREM 2.1.0. *Let M be a set of nonzero integers such that, for all primes p, the number of elements of M which are divisible by p is either* 0 *or* $\geq |M|/p^2$. *Then, if M splits the finite abelian group G purely singularly, G must be cyclic.*

We next show that a set M which satisfies the conclusion of this theorem always splits $C_{|G|}$ if it splits G.

THEOREM 2.1.2. *Let M be a set of nonzero integers. Suppose that M does not split any finite abelian noncyclic groups purely singularly. Then, if M splits the finite abelian group G, it also splits $C_{|G|}$.*

Proof. By Theorem 1.2.5, we can write $G = H \times K$, where M splits H nonsingularly and M splits K purely singularly. By assumption, K must be cyclic. Also, by Theorem 1.2.7, M splits C_p for every prime divisor p of

$|H|$. By the same theorem, M must then split $C_{|H|}$. Further, this splitting is nonsingular. By Theorem 1.2.6, we can combine this splitting with the splitting of K to obtain a splitting of $C_{|H|} \times K$. But $|H|$ is relatively prime to $|K|$ and K is cyclic, so $C_{|H|} \times K$ is isomorphic to $C_{|G|}$. This completes the proof.

It is easy to verify that the sets $\{1,\ldots,n\}$ and $\{\pm 1,\ldots,\pm n\}$ satisfy the hypotheses of Theorem 2.1.0, so we have the following result:

COROLLARY 2.1.3. *If M is either of the sets $\{1,\ldots,n\}$ or $\{\pm 1,\ldots,\pm n\}$ and M splits the finite abelian group G, then M splits $C_{|G|}$.*

2.2. Miscellaneous Results. In this section, we discuss a number of results and examples, most of which concern generalizations of previous results to infinite or nonabelian groups.

(0) According to Theorem 1.2.6, if H is a subgroup of a finite abelian group G, M splits H nonsingularly, and M splits G/H, then M splits G. We will now show that this is not always true in the nonabelian case.

Let $G = \{(i, j)\colon 0 \le i < 7 \,\&\, 0 \le j < 4\}$. Define addition on G by $(i,j) + (k,l) = (i + k(-1)^j, j + l)$ where addition is taken mod 7 in the first component and mod 4 in the second. It is easy to verify that G is a group; in fact it is a semidirect product of $H = \{(i,0)\colon 0 \le i < 7\}$ and $K = \{(0,j)\colon 0 \le j < 4\}$. Let $M = \{1,2,3\}$. Then M splits H nonsingularly and M splits $K \cong G/H$. Suppose $G - \{0\} = MS$. The associate partition of G is shown in Figure 2.2.0. (The notation here is similar to that of Figure 1.3.4; solid lines denote multiplication by 2, dashed lines denote multiplication by 7.) Let $A = \{(0,2)\}$. By Theorem 1.0.8, $|S \cap B| = 1$ for each of the 7 proper divisors B of A. Hence $|S \cap A| = -3$, which is impossible. Therefore, M does not split G.

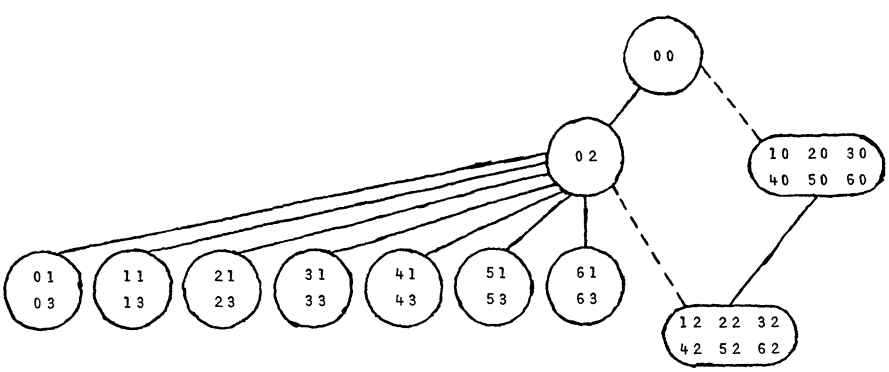

FIGURE 2.2.0

Although Theorem 1.2.6 does not extend to nonabelian groups, the following special case is true.

THEOREM 2.2.1. *Let H and K be finite groups. If M splits H nonsingularly and M splits K, then M splits $H \times K$.*

Proof. Let $H - \{0\} = MS$ and $K - \{0\} = MT$. Let

$$U = (S \times \{0\}) \cup (H \times T).$$

Since $(H - \{0\}) \times \{0\} = M(S \times \{0\})$, it suffices to show that $H \times (K - \{0\}) = M(H \times T)$.

Let $m \in M$ and $(h, t) \in H \times T$. Then $m(h, t) = (mh, mt)$. Since $K - \{0\} = MT$, $mt \neq 0$. Hence $M(H \times T) \subseteq H \times (K - \{0\})$. Also, if $m(h, t) = m'(h', t')$. then $mt = m't'$ so $m = m'$ and $t = t'$. Also, $mh = m'h' = mh'$ so $m(h - h') = 0$. But the splitting of H is nonsingular so $\gcd(m, |H|) = 1$ and $h = h'$. Thus, all the products in $M(H \times T)$ are distinct, so

$$|M(H \times T)| = |M| \cdot |H| \cdot |T| = |H|(|K| - 1) = |H \times (K - \{0\})|,$$

completing the proof.

(1) We next present a simplification of Lemma 1.0.6 for finite abelian groups.

THEOREM 2.2.2. *Let $\mathcal{Q}$ be an M-partition of a finite group G. Then:*

(0) *If M contains an element m which is relatively prime to $|G|$, then $q(A, A) \neq \varnothing$ for every $A \in \mathcal{Q}$. (This is true even if G is nonabelian.)*

(1) *If G is abelian, and M does not contain such an element, then M does not split G.*

Proof. To prove part (0), note that m is relatively prime to $o(g)$ for all $g \in G$, so the conclusion follows from part (0) of Lemma 1.0.6.

For part (1), suppose G is abelian and M splits G. By part (1) of Lemma 1.0.6, for each $g \in G$, M contains an element relatively prime to $o(g)$. It therefore suffices to show that G contains an element whose order is divisible by every prime divisor of $|G|$. But this follows easily from the representation of G as a direct product of its Sylow subgroups.

I do not know whether part (1) of this result holds for nonabelian groups. The above proof does not work, since a nonabelian group G need not contain an element whose order is divisible by every prime divisor of $|G|$. (For instance, the symmetric group on 3 letters has no such element.)

(2) In [**2**: §6, Problem (9)], the following question is asked: If $\{1,\ldots,k\}$ splits an abelian group G with $|G| = 2kn + 1$, must $\{\pm 1,\ldots,\pm k\}$ also split G? This is clearly not true for all G, since $\{1,2\}$ splits C_9 but $\{\pm 1, \pm 2\}$ does not. In fact, it is not true even if G is required to be a cyclic group of prime order.

To see this, let $k = 2$. It is not hard to verify that, for prime p, $\{1,2\}$ splits C_p if and only if the multiplicative order d of 2 mod p is even, while $\{\pm 1, \pm 2\}$ splits C_p if and only if d is divisible by 4. Hence if $d \equiv 2 \pmod 4$, then $\{1,2\}$ will split C_p but $\{\pm 1, \pm 2\}$ will not. The smallest prime for which this occurs is $p = 281$, for which $d = 70$.

(3) Let G have two splittings with the same multiplier set M, say $G - \{0\} = MS = MS'$. Let $\mathcal{A}$ be an M-partition of G. It follows from Theorem 1.0.8 that, for finite G, $|S \cap A| = |S' \cap A|$ for any $A \in \mathcal{A}$. We now show that this is not always true for infinite G.

Let G be the set of dyadic rationals mod 1; i.e., G is the set of rationals in $[0, 1)$ whose denominators are powers of 2, under addition mod 1. Let $M = \{1,2\}$ and let $\mathcal{A}$ be the partition of G in which each element of G is in a class by itself. It is easily verified that $\mathcal{A}$ is an M-partition. Let

$$\begin{aligned} S &= G \cap \bigcup_{n \geq 1} \left[\frac{1}{2^{2n}}, \frac{1}{2^{2n-1}}\right) \\ &= G \cap \left(\left[\frac{1}{4}, \frac{1}{2}\right) \cup \left[\frac{1}{16}, \frac{1}{8}\right) \cup \left[\frac{1}{64}, \frac{1}{32}\right) \cup \cdots\right) \end{aligned}$$

and

$$S' = -S = G \cap \left(\left(\frac{1}{2}, \frac{3}{4}\right] \cup \left(\frac{7}{8}, \frac{15}{16}\right] \cup \cdots\right).$$

Then $G - \{0\} = MS = MS'$. However, $1/4$ is in S but not in S', so $|S \cap \{1/4\}| = 1 \neq 0 = |S' \cap \{1/4\}|$.

(4) As mentioned before (Theorem 1.2.7), a set M splits a finite abelian group G nonsingularly if and only if it splits C_p for each prime divisor p of $|G|$. We now show that is is also true for nonabelian groups.

THEOREM 2.2.3. *Let G be a finite group and M a set of nonzero integers. Then M splits G nonsingularly if and only if M splits C_p for each prime divisor p of $|G|$.*

Proof. We may assume that every element of M is relatively prime to $|G|$. For, if $p \,||\, G|$ and $p \mid m$, then M cannot split G nonsingularly, nor can M split C_p.

Let $\mathcal{A}$ be the associate partition of G. By the preceding paragraph, if $m \in M$ and $A \in \mathcal{A}$, then $mA = A$. Hence, M splits G if and only if, for each $A \in \mathcal{A}$, there is a set $T \subseteq A$ such that $A = MT$. In particular, if g is an element of order p, the associate class containing g has the form $C_p - \{0\}$, whence M splits C_p. This proves the "only if" part.

Suppose M splits C_p for each prime divisor p of $|G|$. Given $A \in \mathcal{A}$, let H be the subgroup of G generated by A. Since H is cyclic, Theorem 1.2.7 implies that M splits H nonsingularly; say $H - \{0\} = MS$. Letting $T = S \cap A$, it is easy to see that $A = MT$. Hence M splits G, and the proof is complete.

(5) In [**3**], Hamaker showed that $M = \{1, 3, 27\}$ does not split any finite abelian group. In fact it does not split any finite group. For, if M splits G, then $|G| \equiv 1 \pmod 3$, so the splitting is nonsingular. By Theorem 2.2.3, it suffices to show that M does not split C_p for any prime p, which Hamaker did.

We now show that M does split an infinite abelian group. Let G be the set of rationals in $[0, 1)$ whose denominators are powers of 3, under addition mod 1. We claim that M splits G. We will construct the splitting set S by the following infinite recursive process: Start with $S_0 = \varnothing$. Given S_n, define $T_n = S_n \cup 3S_n \cup 27S_n$. Let t be a nonzero element of $G - T_n$ whose denominator is as small as possible, and let

$$S_{n+1} = S_n \cup \left\{ \frac{t}{27}, \frac{1}{9} + \frac{t}{81} \right\}.$$

Finally, let $S = \bigcup_{n \geq 0} S_n$ and $T = S \cup 3S \cup 27S$.

We first prove by induction that, for $n \geq 0$, S_n, $3S_n$, and $27S_n$ are pairwise disjoint and that

$$3T_n \subseteq T_n \subseteq G - \{0\}.$$

This is clearly true for $n = 0$, so assume it is true for some $n \geq 0$. Let $U = \{t/27, 1/9 + t/81\}$, so that $S_{n+1} = S_n \cup U$ and $T_{n+1} = T_n \cup MU$. It is easy to verify that the six elements of MU are distinct. Further, for each $g \in MU$, we have $3^r g = t$ for some t. (See Fig. 2.2.4, in which a line from g down to h means that $g = 3h$.) Hence, if $g \in T_n$, then, since $3T_n \subseteq T_n$, we would have $t \in T_n$, contradicting the choice of t. Hence MU and T_n are disjoint. It follows that S_n, $3S_n$, and $27S_n$ are pairwise disjoint. Also, $3MU \subseteq MU \cup \{3t\}$. But $3t \in T_n$ by the minimality of t. Hence $3T_{n+1} \subseteq T_{n+1}$. Clearly, $0 \notin MU$ so $T_{n+1} \subseteq G - \{0\}$, completing the induction.

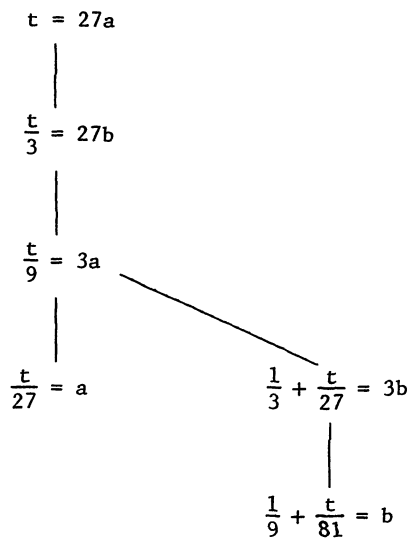

FIGURE 2.2.4

Since S_n, $3S_n$, and $27S_n$ are pairwise disjoint for all n, it follows that S, $3S$, and $27S$ are pairwise disjoint. Further, $T = G - \{0\}$. For, if t is a nonzero element of $G - T$ with minimal denominator, then t would have been the chosen element of $G - T_n$ for some n. But then $t = 27a$ where $a = t/27 \in S_{n+1} \subseteq S$, so $t \in 27S$, a contradiction. It follows that $G - \{0\} = MS$; i.e., M splits G.

2.3. Open Problems. We close with a list of open problems, some of which have already been mentioned.

(0) Does Theorem 1.3.0 generalize to nonabelian groups? That is, if a finite p-group G has a singular splitting, must G be cyclic?

(1) Does there exist a splitting $G - \{0\} = MS$ of a finite group G in which no element of M is relative prime to $|G|$? (By Theorem 2.2.2, such a group must be nonabelian.)

(2) Prove Conjecture 1.4.1. Is the conjecture true for nonabelian groups?

(3) If M splits some finite group G, must it split infinitely many finite groups? Must it split C_p for some prime p?

(4) Which sets M split infinitely many finite groups in a purely singular manner? (As shown in Section 2.0, $\{1, -1, 2\}$ has this property, but no set of cardinality 4 does.)

(5) Is there a set M which does not split any nontrivial group?

(6) Find necessary and sufficient conditions that M split some nontrivial group. This problem is also of interest for certain restricted classes of groups, such as abelian groups, finite groups, finite abelian groups, or cyclic groups.

(7) Is there a set M which splits some nonabelian group but does not split any nontrivial abelian group?

(8) Generalize Theorem 1.0.8 to infinite groups.

(9) Find necessary and sufficient conditions on M so that, if M splits the finite abelian group G, then M splits $C_{|G|}$. (See §2.1.)

References

1. H. Everett and D. Hickerson, *Packing and covering by translates of certain nonconvex bodies*, Proc. Amer. Math. Soc., **75** (1979), 87–91.

2. S. Galovich and S. Stein, *Splittings of Abelian groups by integers*, Aequationes Mathematicae, **22** (1981), 249–267.

3. W. Hamaker, *Factoring groups and tiling space*, Aequationes Mathematicae, **9** (1973), 145–149.

4. W. Hamaker and S. Stein, *Splitting groups by integers*, Proc. Amer. Math. Soc., **46** (1974), 322–324.

5. S. Stein, *Factoring by subsets*, Pacific J. Math., **22** (1967), 523–541.

6. _____, *A symmetric star body that tiles but not as a lattice*, Proc. Amer. Math. Soc., **36** (1972), 543–548.

7. _____, *Algebraic tiling*, Amer. Math. Monthly, **81** (1974), 445–462.

Received June 12, 1980 and in revised form May 15, 1981.

University of California
Davis, CA 95616

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

DONALD BABBITT (Managing Editor)
University of California
Los Angeles, CA 90024

HUGO ROSSI
University of Utah
Salt Lake City, UT 84112

C. C. MOORE and ARTHUR OGUS
University of California
Berkeley, CA 94720

J. DUGUNDJI
Department of Mathematics
University of Southern California
Los Angeles, CA 90089-1113

R. FINN and H. SAMELSON
Stanford University
Stanford, CA 94305

ASSOCIATE EDITORS

R. ARENS
E. F. BECKENBACH (1906–1982)
B. H. NEUMANN
F. WOLF
K. YOSHIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF ARIZONA
UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA, RENO
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON
UNIVERSITY OF SOUTHERN CALIFORNIA
STANFORD UNIVERSITY
UNIVERSITY OF HAWAII
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON

Pacific Journal of Mathematics
Vol. 107, No. 1 January, 1983

John Kelly Beem and Phillip E. Parker, Klein-Gordon solvability and the geometry of geodesics 1
David Borwein and Amnon Jakimovski, Transformations of certain sequences of random variables by generalized Hausdorff matrices 15
Willy Brandal and Erol Barbut, Localizations of torsion theories 27
John David Brillhart, Paul Erdős and Richard Patrick Morton, On sums of Rudin-Shapiro coefficients. II 39
Martin Lloyd Brown, A note on tamely ramified extensions of rings 71
Chang P'ao Ch'ên, A generalization of the Gleason-Kahane-Żelazko theorem 81
I. P. de Guzman, Annihilator alternative algebras 89
Ralph Jay De Laubenfels, Extensions of d/dx that generate uniformly bounded semigroups 95
Patrick Ronald Halpin, Some Poincaré series related to identities of 2×2 matrices 107
Fumio Hiai, Masanori Ohya and Makoto Tsukada, Sufficiency and relative entropy in $*$-algebras with applications in quantum systems 117
Dean Robert Hickerson, Splittings of finite groups 141
Jon Lee Johnson, Integral closure and generalized transforms in graded domains 173
Maria Grazia Marinari, Francesco Odetti and Mario Raimondo, Affine curves over an algebraically nonclosed field 179
Douglas Shelby Meadows, Explicit PL self-knottings and the structure of PL homotopy complex projective spaces 189
Charles Kimbrough Megibben, III, Crawley's problem on the unique ω-elongation of p-groups is undecidable 205
Mary Elizabeth Schaps, Versal determinantal deformations 213
Stephen Scheinberg, Gauthier's localization theorem on meromorphic uniform approximation 223
Peter Frederick Stiller, On the uniformization of certain curves 229
Ernest Lester Stitzinger, Engel's theorem for a class of algebras 245
Emery Thomas, On the zeta function for function fields over F_p 251