Pacific Journal of Mathematics

CLOSED FACTORS OF NORMAL Z-SEMIMODULES

DANIEL ALAN MARCUS

Vol. 93, No. 1 March 1981

PACIFIC JOURNAL OF MATHEMATICS
Vol. 93, No. 1, 1981

CLOSED FACTORS OF NORMAL Z-SEMIMODULES

DANIEL A. MARCUS

Let M be a set of positive integers which is closed under multiplication and division whenever possible: if $m, n \in M$ and $m \mid n$, then $n/m \in M$. A *closed factor* of M is a subset $K \subset M$ which is closed under multiplication and for which there is another subset $R \subset M$ such that every member of M is uniquely representable as a product kr with $k \in K$ and $r \in R$. A theory is developed for determining all closed factors of a given M. The theory can be adapted to an analogous problem for convex polyhedral cones.

1. Introduction. The *factorization problem* for a set S with a binary operation $\circ$ can be stated as follows: Determine all pairs of subsets A, B of S such that each member of S is uniquely representable in the form $a \circ b$, $a \in A$, $b \in B$. More generally, if the operation is associative, one can replace the pair (A, B) with a sequence $(A_1, \cdots, A_n)$ of subsets of S.

Several authors have considered this problem for finite abelian groups. A special case, involving only subsets of a certain form, was solved by Hajós in the course of settling a classical conjecture of Minkowski on linear forms. (See [10] for a good exposition of this.) Subsequent work on factorizations of finite abelian group was done by Hajós, Rédei, Sands, and deBruijn. (References appear in [10].) Even for finite cyclic groups, the general factorization problem is unsolved. The corresponding problem for the infinite cyclic group was settled in a negative sense by Swenson in 1974 [12]. Partial results had previously been obtained by deBruijn [1], [3].

In [5], Long characterized all factorizations of the set $\{0, 1, \cdots, n-1\}$ under addition. The corresponding problem for certain subsets of the plane was studied by Stein [11] and Hansen [4].

Complete solutions to the factorization problem have been obtained for certain semigroups. In [2], deBruijn determined all factorizations of the additive semigroup of nonnegative integers. The two-dimensional version of this, in which S is the additive semigroup of nonnegative lattice points in the plane, was solved by Niven [9]. In [6], this author solved the n-dimensional version for all n, including infinite-dimensional cases: i.e., for any free commutative monoid. These results were extended in [7] to include certain submonoids of a free commutative monoid.

The results obtained in [2], [6], [7] and [9] can be summarized by saying that every factorization of one of these semigroups can

be constructed from a descending chain of factors which are closed under the semigroup operation. (See §11.) For the semigroups considered in [2], [6] and [9], it is a simple matter to determine all of the closed factors. (See Proposition 15 in [6].) The latter problem is more difficult, however, for a wider class of semigroups known as *normal Z-semimodules* (defined in §2). While all of the factorizations of these semigroups are not known, it is possible to characterize all of the closed factors. That is the subject of the present work.

In §7 it will be shown how the theory developed here for normal Z-semimodules can be adapted to an analogous problem for convex polyhedral cones.

2. **Normal Z-semimodules.** Let G be free abelian group and let G^+ denote the set of points having nonnegative coordinates with respect to a fixed Z-basis; thus G^+ is a free commutative monoid, or a *free Z-semimodule*. A *normal Z-semimodule* is any semigroup which is isomorphic to an intersection $G^+ \cap H$, where H is a subgroup of G. Some familiar examples of normal Z-semimodules are

(1) The nonnegative points in a sublattice of Z^n;

(2) The nonnegative integer-valued circulations in a digraph (G^+ consists of all nonnegative integer-valued functions on the edges);

(3) The monic polynomials with constant term 1 over a unique factorization domain (G^+ consists of all monic polynomials. This is a multiplicative free Z-semimodule, as is G^+ in all subsequent examples);

(4) The nonzero principal ideals in a Dedekind domain (G^+ consists of all nonzero ideals);

(5) Any set M of positive integers which is closed under multiplication and division whenever possible:

$$m, n \in M, \quad m \mid n \Longrightarrow n/m \in M$$

(G^+ is the set of all positive integers).

It is clear that normal Z-semimodules are the kernels of homomorphisms from free Z-semimodules to abelian groups, and that every such kernel is a normal Z-semimodule. In [8] it is shown that every normal Z-semimodule is uniquely representable as the kernel of a homomorphism $G^+ \to A$ (where G^+ is a free Z-semimodule and A is an abelian group) having the property that for each basis element b of G^+, the members of G^+ not involving b (i.e., generated by basis elements other than b) map onto A. This property is called *strong surjectivity*. We note that the basis elements of a free Z-semimodule are uniquely determined as the minimal nontrivial elements in the natural partial ordering.

The result described above will be used in the present work to solve the following combinatorial problem:

Let M be a normal Z-semimodule with multiplicative notation. A *direct decomposition*, or *factorization*, of M is a decomposition of M as a direct product of subsets. Thus if A and B are subsets of M such that each $m \in M$ is uniquely representable in the form $ab (a \in A, b \in B)$, then $M = A \times B$ is a direct decomposition of M. Call A and B *factors* of M in this case. A *closed factor* of M is a factor of M which is closed under multiplication. The problem is to determine, in some sense, all closed factors of a given M.

3. Notation and terminology. From now on, the symbol N denotes a free Z-semimodule with multiplicative notation, and we employ the notation and terminology of the positive integers: The basis elements of N are called *primes* and are denoted by the letters $p, q, r, \cdots$. Divisibility in N (indicated by a vertical bar) is defined in the obvious way, as are GCD's and relative primeness. The rank of N (the number of primes) is an arbitrary cardinal.

The symbol M denotes a *normal subsemimodule* of N: i.e., a subset which is closed under multiplication and division whenever possible, as in Example 5. Equivalently, M is the kernel of a homomorphism from N to an abelian group. We will also say that M is *normally embedded* in N in this case. Thus M represents a typical normal Z-semimodule.

For a subset $X \subset N$, let $[X]$ denote the set of all products of elements of X, including the empty product 1. We write $[x, y, \cdots]$ for $[\{x, y, \cdots\}]$. Thus $[X]$ is the monoid generated by X.

Let $\langle X \rangle$ denote the group generated by X, so that $\langle N \rangle$ is the free abelian group generated by the primes of N. A subsemimodule $S \subset N$ is normally embedded in N iff $\langle S \rangle \cap N = S$.

Call an element $x \in X$ *minimal in* X if it has no divisors in X other than itself and 1. Equivalently, x is minimal in the division ordering on $X - \{1\}$. Denote by $X^{\min}$ the set of all minimal elements in X.

It is easy to see that for M normally embedded in N, $N = [M^{\min}]$.

For subsets $X, Y \subset N$, define

$$X/Y = \{x \in X : y \nmid x \quad \forall y \in Y, y \neq 1\} .$$

Clearly $X/Y = X/Y^{\min}$.

Finally, for subsets $X, Y \subset N$, define

$$XY = \{xy : x \in X, y \in Y\} .$$

4. Examples of closed factors.

EXAMPLE 1. For any M, let $\{m_i, i \in I\}$ be a family of pairwise relatively prime members of M, indexed by some set I. Then

$$[m_i: i \in I]$$

is a closed factor of M, the complementary factor being

$$\{m \in M: m_i \nmid m \quad \forall i \in I\} .$$

This should be regarded as a trivial sort of closed factor.

EXAMPLE 2. $N = [p, q]$ (where p and q are understood to be the primes of N) and M is the kernel of the mapping

$$N \longrightarrow \boldsymbol{Z}/4\boldsymbol{Z}$$

determined by

$$p \longmapsto 1 , \quad q \longmapsto 3 .$$

Then $M = [p^4, q^4, pq]$, and $[p^4, q^4, p^2q^2]$ is a closed factor of M. The complementary factor is $\{1, pq\}$.

EXAMPLE 3. $N = [p, q, r, s]$ and M is the kernel of the mapping $N \to \boldsymbol{Z} \oplus (\boldsymbol{Z}/2\boldsymbol{Z})$ determined by

$$\begin{aligned} p &\longmapsto (1, 0) \\ q &\longmapsto (-1, 0) \\ r &\longmapsto (1, 1) \\ s &\longmapsto (-1, 1) . \end{aligned}$$

Then $M = [pq, rs, p^2s^2, q^2r^2]$, and $[pqrs, p^2s^2, q^2r^2]$ is a closed factor of M. The complementary factor is $[pq] \cup [rs]$.

EXAMPLE 4. $N = [p, q, r, s]$, and M is the kernel of the mapping $N \to \boldsymbol{Z}$ determined by

$$\begin{aligned} p &\longmapsto 3 \\ q &\longmapsto -3 \\ r &\longmapsto 2 \\ s &\longmapsto -2 . \end{aligned}$$

Then $M = [pq, rs, p^2s^3, q^2r^3]$, and $[p^2s^3, q^2r^3]$ is a closed factor of M. The complementary factor is

$$\{p^aq^ar^bs^b: a, b \in \boldsymbol{Z};\ a, b \geqq 0; \quad \text{and} \quad a < 2 \quad \text{or} \quad b < 3\} .$$

We note some common features in all of these examples. First, in each case the complementary factor consists of everything in M

which is not divisible by any of the generators of the closed factor. We will see that the complementary factor always has this form. More interestingly, in each case the closed factor has the form

$$M \cap [n_i : i \in I]$$

where the n_i are pairwise relatively prime members of N. In Example 1 the n_i are just the m_i. In Examples 2-4 the closed factors are, respectively,

$$M \cap [p^2, q^2]$$
$$M \cap [ps, qr]$$
$$M \cap [p^2, q^2, r^3, s^3] .$$

We will prove (Theorem 2) that all closed factors have this form. However such intersections are not always factors, as the following shows:

EXAMPLE 5. $N = [p, q]$, and N is the kernel of the mapping $N \to Z/4Z$ defined by $p, q \mapsto 1$. Thus $M = [p^4, p^3q, p^2q^2, pq^3, q^4]$. The intersection $M \cap [p^2, q^2] = [p^4, p^2q^2, q^4]$ is not a factor of M since if it were, the complementary factor would contain pq^3 and p^3q; but then the equation $(p^4)(pq^3) = (p^2q^2)(p^3q)$ would contradict unique representation.

5. **Theory of normal Z-semimodules.** Let M and N be as in §2. Clearly M is the kernel of the natural mapping

$$\varphi : N \longrightarrow \langle N \rangle / \langle M \rangle .$$

We define congruence mod M in terms of this mapping. For $n_1, n_2 \in N$, we have

$$n_1 \equiv n_2 (\text{mod } M) \quad \text{iff} \quad \varphi(n_1) = \varphi(n_2) .$$

This is just congruence mod the group $\langle M \rangle$, so that

$$n_1 \equiv n_2 (\text{mod } M) \text{ iff } n_1 m_1 = n_2 m_2 \text{ for some } m_1, m_2 \in M .$$

We note that $n \in M$ iff $n \equiv 1 (\text{mod } M)$, since $N \cap \langle M \rangle = M$.

Let $f : N \to G$ be any mapping (i.e., semigroup homomorphism) from N to an abelian group G, and suppose that M is the kernel. It is easy to show that the following conditions are equivalent:

(1) The image of f is a subgroup of G;

(2) Every member of N divides some member of M.

When these conditions hold, the kernel of the induced group homomorphism $\langle N \rangle \to G$ is just $\langle M \rangle$; it follows that image of f is naturally isomorphic to $\langle N \rangle / \langle M \rangle$. In particular, any surjective mapping $N \to G$ having kernel M is equivalent to φ.

We can always arrange for a given M to be the kernel of a surjective mapping from some free Z-semimodule by removing the primes of N which fail to divide anything in M. It is possible, however, to attain stronger conditions:

In accordance with the definition in §1, φ is strongly surjective if and only if for each prime p, the restriction

$$\{n \in N: p \nmid n\} \longrightarrow \langle N\rangle/\langle M\rangle$$

is surjective.

THEOREM 0. *Every normal Z-semimodule can be represented as the kernel M of a strongly surjective mapping from a free Z-semimodule N to an abelian group G. This representation is unique up to isomorphism.*

This is Theorem 1 in [8] for the special case $R = Z$. The mapping referred to can be assumed to be the natural mapping from N to $\langle N\rangle/\langle M\rangle$, as noted earlier for any surjective mapping.

Thus we can assume that the embedding $M \subset N$ is such that φ is strongly surjective. This embedding, which is uniquely determined up to isomorphism, is called the *canonical embedding* of M. The factor group $\langle N\rangle/\langle M\rangle$ is an invariant of M, called the *cogroup* of M.

In [8] it is also shown (Lemma 1) that φ is strongly surjective if and only if each $n \in N$ is a GCD from M:

$$\forall n \in N,\ n = \mathrm{GCD}(m_1, \cdots, m_t) \quad \text{for some} \quad m_1, \cdots, m_t \in M\,.$$

Finally we note that as an immediate consequence of Theorem 0 we can assume that the following condition holds:

$$(*) \qquad \begin{array}{l} \forall n \in N \text{ and } \forall \text{ prime } p,\ \exists x \in N \\ \text{such that } x \equiv n (\mathrm{mod}\, M) \text{ and } p \nmid x\,. \end{array}$$

6. **Theory of closed factors.** We assume from now on that the containment $M \subset N$ is the canonical embedding of a normal Z-semimodule M in a free Z-semimodule N.

Let K be a closed factor of M with complementary factor R, and let $\pi = \pi_K$ denote the obvious projection of M on K.

PROPOSITION 1. $\pi(km) = k\pi(m) \forall k \in K,\ m \in M$.

Proof. $m = \pi(m)r,\ r \in R$, so $km = k\pi(m)r$.

PROPOSITION 2. *If $k \in K$, $m \in M$ and $k \mid m$, then $k \mid \pi(m)$.*

Proof. $\pi(m) = \pi(km/k) = k\pi(m/k)$.

Next we show that K is itself a normal Z-semimodule. In fact K is normally embedded in N:

PROPOSITION 3. $\langle K \rangle \cap N = K$.

Proof. Let $h, k \in K$ and suppose $h/k = n \in N$. Necessarily $n \in M$ since $h/k \in \langle M \rangle \cap N = M$. Then

$$h = \pi(h) = \pi(kn) = k\pi(n)$$

implying that $\pi(n) = n$. Thus $n \in K$.

PROPOSITION 4. $R = M/K$.

Proof. It is clear that $R \supset M/K$. Conversely, suppose $r \in R$, $k \in K$, and $k \mid r$. Then $k \mid \pi(r)$ by Proposition 2. But $\pi(r) = 1$, so $k = 1$.

Thus we have $M = K \times (M/K)$ whenever K is a closed factor of M.

Next we let F denote the set of GCD's from K:

$$F = \{\mathrm{GCD}(k_1, \cdots, k_t) : k_1, \cdots, k_t \in K\} .$$

We will show that F is freely generated by a set of pairwise relatively prime members of N and that $K = M \cap F$.

THEOREM 1. *Let* $f \in F$, $n \in N/M$, *and suppose* $f \equiv n \pmod{M}$. *Then* $f \equiv n \pmod{K}$.

Proof. Write $f = \mathrm{GCD}(k_1, \cdots, k_t)$, $k_i \in K$. For each i we have $nk_i/f \in \langle M \rangle \cap N = M$, so for each i

$$k_1\pi(nk_i/f) = k_i\pi(nk_1/f)$$

by Proposition 1. Thus

$$k_1 \mid f\pi(nk_1/f) .$$

Writing $nk_1/f = kr$ with $k \in K$, $r \in R$, we have $k_1 \mid fk$. It follows that $r \mid n$. But $r \in M$ and $n \in N/M$, so $r = 1$. Thus $nk_1 = fk$, implying $n \equiv f \pmod{K}$.

COROLLARY 1. $K = M \cap F$.

Proof. Trivally $K \subset M \cap F$. Conversely if $f \in M \cap F$ then $f \equiv$

$1 (\mathrm{mod}\, M)$, hence $f \equiv 1 (\mathrm{mod}\, K)$, hence $f \in K$ by Proposition 3.

COROLLARY 2. *If $f \in F$ and $f \mid k \in K$, then $k/f \in F$.*

Proof. By (*) of §5, there exist elements $n_i \in N$ such that

$$n_i \equiv f (\mathrm{mod}\, M) \quad \text{and} \quad \mathrm{GCD}(n_i) = 1 .$$

Moreover the n_i can be assumed to be in N/M since any nontrivial divisors in M can be factored out without affecting the congruence and GCD conditions. Then by Theorem 1 we have $n_i \equiv f (\mathrm{mod}\, K)$ for all i, hence $n_i k/f \in \langle K \rangle \cap N = K$. Finally

$$k/f = \mathrm{GCD}(n_i k/f) \in F .$$

(We should note that there may be infinitely many elements $n_i k/f$; nevertheless their GCD is equal to the GCD of a finite subfamily of them, hence the GCD is in F.)

THEOREM 2. *$F = [n_i : n \in I]$, where $\{n_i : n \in I\}$ is a family of pairwise relatively prime members of N.*

Proof. It is sufficient to show that F is closed under

(1) multiplication;
(2) taking GCD's; and
(3) division whenever possible.

(1) and (3) show that F is a normal $\boldsymbol{Z}$-semimodule, normally embedded in N, and hence $F = [F^{\min}]$; moreover the members of $F^{\min}$ are pairwise relatively prime by (2).

Let $e, f \in F$ and write

$$e = \mathrm{GCD}(h_1, \cdots, h_s)$$
$$f = \mathrm{GCD}(k_1, \cdots, k_t)$$

with all $h_i, k_i \in K$. Then

$$ef = \mathrm{GCD}(\text{all } h_i k_j)$$

and

$$\mathrm{GCD}(e, f) = \mathrm{GCD}(h_1, \cdots, h_s, k_1, \cdots, k_t) .$$

Clearly F is closed under taking the GCD of any number of elements.

It remains to show that if $e/f \in N$, then $e/f \in F$. For each i, we have $f \mid h_i$, hence $h_i/f \in F$ by Corollary 2 to Theorem 1. Finally, then,

$$e/f = \mathrm{GCD}(h_1/f, \cdots, h_s/f) \in F$$

by (2).

Combining results, we have

COROLLARY 1. *$K = M \cap F$ where F is freely generated by a set of pairwise relatively prime members of N, and the containment $K \subset F$ is the canonical embedding of the normal Z-semimodule K in a free Z-semimodule.*

The fact that $K \subset F$ is the canonical embedding follows from the fact that everything in F is a GCD from K (see §5). We should note here that the divisibility relation in the free Z-semimodule F is the same as that induced from N since F is normally embedded in N.

COROLLARY 2. *If $K = K_1 \times K_2$, where K_1 and K_2 are closed under multiplication, then the members of K_1 are relatively prime to the members of K_2.*

Proof. This follows from Corollary 1 and uniqueness of the canonical embedding. If we let $K_1 \subset F_1$ and $K_2 \subset F_2$ denote the canonical embeddings of K_1 and K_2 in free Z-semimodules, then the induced mapping of K into the direct product $F_1 \times F_2$ must be the canonical embedding of K. The resulting isomorphism $F \to F_1 \times F_2$ shows that any member of K_1 and any member of K_2 have no common factor in F, hence no common factor in N.

Clearly this result generalizes to a decomposition of K into any number of closed factors, even infinitely many. In particular we obtain the following when all of the factors are cyclic:

COROLLARY 3. *If K is free, then the members of $K^{\min}$ are pairwise relatively prime.*

In other words, the only free closed factors of M are the trivial ones in Example 1 of §4. This result could also have been obtained directly from Corollary 1: Necessarily $K = F$ by uniqueness of the canonical embedding.

We have established a one-to-one correspondence between the closed factors K of M and certain families of pairwise relatively prime members of N. As we have seen (Example 5 of §4), not all families of this type correspond to closed factors. The next result provides a characterization of those which do:

THEOREM 3. *Let $\{n_i : i \in I\}$ be a family of pairwise relatively prime members of N, and set $F = [n_i : i \in I]$, $K = M \cap F$. Then the*

following conditions are equivalent:

(1) MF *is normally embedded in* N;

(2) $\pi_F(M) \subset M$ (*note that* F *is a factor of* N);

(3) $M/F = M/K$;

(4) K *is a factor of* M *and* F *is the set of* GCD's *from* K.

Proof. (1) $\Rightarrow$ (2). For $m \in M$, write $m = fr$ with $f \in F$ and $r \in N/F$. Then $r \in MF$ by (1). Then $r \in M$, implying $f \in M$.

(2) $\Rightarrow$ (3). $M/F \subset M/K$ trivially. Conversely, if $m \in M/K$, then $\pi_F(m) = 1$. Then $m \in M \cap (N/F) = M/F$.

(3) $\Rightarrow$ (2). First notice that $M = K(M/K)$. For $m \in M$, write $m = kr$ with $k \in K$, $r \in M/K$. (We are not assuming that this representation is unique.) Then $r \in M/F \subset N/F$, so $\pi_F(m) = k \in M$.

((2) and (3)) $\Rightarrow$ (4). By (3), we have

$$M = K(M/K) = K(M/F) = K \times (M/F) ,$$

with the last part justified by the fact that $K \subset F$ and $M/F \subset N/F$. Thus K is a factor of M. Moreover it is clear that F contains all GCD's from K since F is closed under taking GCD's. Finally, let $f \in F$; we know that everything in N is a GCD from M (§5), hence we can write

$$f = \mathrm{GCD}(m_1, \cdots, m_t),\ m_i \in M .$$

For each i we have $f \mid m_i$, hence $f \mid \pi_F(m_i)$ by Proposition 2. Thus

$$f = \mathrm{GCD}(\pi_F(m_1), \cdots, \pi_F(m_t)) .$$

The $\pi_F(m_i)$ are in M by condition (2), hence they are in K.

(4) $\Rightarrow$ (1). We must show that if

$$m_1 f_1 = m_2 f_2 x \quad \text{with} \quad m_1, m_2 \in M;\ f_1, f_2 \in F,\ x \in N$$

then $x \in MF$. Write

$$x = mn \quad \text{with} \quad m \in M,\ n \in N/M .$$

We claim that $n \in F$. Clearly f_2 divides some $k \in K$; from

$$m_1 f_1 k/f_2 = m_2 kmn$$

we obtain $n \equiv f (\mathrm{mod}\, M)$, where $f = f_1 k/f_2$. Note that $f \in \langle F \rangle \cap N = F$. Then $n \equiv f (\mathrm{mod}\, K)$ by Theorem 1, hence $n \in \langle F \rangle \cap N = F$.

The proof is now complete.

The most important part of Theorem 3 is the equivalence of conditions (1) and (4). We know that every closed factor K of M

occurs in a condition (4) situation, hence such factors correspond to sets $\{n_i: i \in I\}$ for which MF is normally embedded in N. These MF's are among the normal Z-semimodules M', $M \subset M' \subset N$, such that M' is normally embedded in N, and if we let G denote the cogroup of M ($G = \langle N \rangle / \langle M \rangle$), then the semimodules M' are in one-to-one correspondence with the subgroups of G. Specifically, if for each subgroup $H \subset G$ we let M_H denote the kernel of the natural mapping

$$\varphi_H: N \longrightarrow G/H ,$$

then the correspondence $H \leftrightarrow M_H$ is one-to-one and each M'(as above) is of the form M_H. In this correspondence $H = \langle M' \rangle / \langle M \rangle$.

Summarizing what we have said, there are one-to-one correspondences

$$\{\text{closed factors } K \text{ of } M\} \longleftrightarrow \{\text{certain } F\text{'s}\}$$
$$\{\text{normal } MF\text{'s}\} \longleftrightarrow \{\text{certain subgroups } H \subset G\}$$

where F is used generically to represent a free semimodule of the form $[n_i: i \in I]$ where the n_i are pairwise relatively prime members of N. The F's occurring in the first correspondence are the ones for which MF is normal.

This raises two questions:

(1) To what extent is F determined by a normal MF?

and

(2) Which subgroups $H \subset G$ occur in the correspondence?

Answers are provided by

THEOREM 4. *Let H be a subgroup of G. Then $M_H = MF$ for some $F = [n_i: i \in I]$ with pairwise relatively prime $n_i \neq 1$, if and only if the members of $M_H^{\min} - M$ are pairwise relatively prime. In that case the members of $M_H^{\min} - M$ are among the n_i, and all other n_i are in M.*

Proof. If $M_H = MF$ with F as above, then $M_H^{\min} \subset M^{\min} \cup F^{\min}$, hence

$$M_H^{\min} - M \subset F^{\min} = \{n_i: i \in I\} .$$

Moreover if $n_i \in F^{\min} - M$, then from

$$M_H = [M_H^{\min}] = [M_H^{\min} - M]M$$

we conclude that n_i is divisible by some $n \in M_H^{\min} - M$; we know $n = n_j$ for some $j \in I$, hence $n_j | n_i$. It follows that $n_j = n_i$. Thus

$$F^{\min} - M \subset M_H^{\min} - M$$

implying that M contains all n_i which are not in $M_H^{\min} - M$.

Finally, suppose the members of $M_H^{\min} - M$ are pairwise relatively prime. Then $M_H = MF$, where $F = [M_H^{\min} - M]$, and the proof is complete.

It should be noted that when a subgroup H of G corresponds to a normal MF and hence to a closed factor K of M, then H is the cogroup of K. We prove this by showing that K is the kernel of a strongly surjective mapping of N onto H. The surjective mapping $N \to G$ restricts to a surjective mapping $M_H \to H$; since $M_H = MF$ and M is the kernel, the restriction $F \to H$ is surjective. Moreover everything in F is a GCD from the kernel K. It follows by Lemma 1 of [8] that $F \to H$ is strongly surjective.

Now we look back at the examples of §4 in the light of these results.

In Example 1, $F = K$; $MF = M$; and $H = \{0\}$.

In Example 2, $F = [p^2, q^2]$; $MF = [p^2, q^2, pq]$; and $H = \{0, 2\}$.

In Example 3, $F = [ps, qr]$; $MF = [pq, rs, ps, qr]$; and $H = \boldsymbol{Z}/2\boldsymbol{Z}$.

In Example 4, $F = [p^2, q^2, r^3, s^3]$; $MF = [pq, rs, p^2, q^2, r^3, s^3]$; and $H = 6\boldsymbol{Z}$.

In each case $MF = M_H$ and H is the cogroup of K.

As a further illustration of the theory we determine all closed factors of M in Example 3. The subgroups of $G = \boldsymbol{Z} \oplus (\boldsymbol{Z}/2\boldsymbol{Z})$ are

$$n\boldsymbol{Z},\ n \geqq 0\ ;$$
$$n\boldsymbol{Z} \oplus (\boldsymbol{Z}/2\boldsymbol{Z})\ ,\quad n \geqq 0\ ;$$

and the cyclic groups

$$\langle (n, 1) \rangle\ ,\quad n \geqq 1\ .$$

When $H = \{0\}$, $M_H = M$. F can be taken to be $[m]$ for any $m \in M$, or $[m_1, m_2]$ for any relatively prime elements $m_1, m_2 \in M$. The closed factor K is just F.

When $H = \boldsymbol{Z}$, $M_H = [p, q, r^2, s^2, rs]$. M contains rs, so $F = [p, q, r^2, s^2]$ intersects M in the closed factor

$$K = [pq, r^2s^2, p^2s^2, q^2r^2]\ .$$

When $H = 2\boldsymbol{Z}$, $M_H = [p^2, q^2, r^2, s^2, pq, rs]$. M contains pq and rs, so $F = [p^2, q^2, r^2, s^2]$ intersects M in the closed factor

$$K = [p^2q^2, r^2s^2, p^2s^2, q^2r^2]\ .$$

When $H = n\boldsymbol{Z}$, $n \geqq 3$, $M_H^{\min}$ contains p^n and $p^{n-2}r^2$, neither of which are in M. The members of $M_H^{\min} - M$ are not pairwise relatively prime, so H is not the cogroup of any closed factor of M.

We have already seen that $H = Z/2Z$ is the cogroup of the closed factor in Example 3.

When $H = Z \oplus (Z/2Z)$, $M_H = N$; then $F = N$ and $K = M$.

When $H = nZ \oplus (Z/2Z)$, $n \geqq 2$, $M_H^{\min} - M$ contains p^n and $p^{n-1}r$, so no closed factor results from H.

When $H = \langle (1, 1) \rangle$, $M_H = [r, s, p^2, q^2, pq]$. M contains pq, so $F = [r, s, p^2, q^2]$ intersects M in the closed factor

$$K = [p^2q^2, rs, p^2s^2, q^2r^2] .$$

Finally, when $H = \langle (n, 1) \rangle$, $n \geqq 2$, $M_H^{\min} - M$ contains p^{2n} and $p^{n-1}r$. No closed factor results from H.

7. **Splitting subcones of a convex cone.** All of the theory developed in §6 for Z-semimodules can be adapted to finite-dimensional normal R-semimodules, which are convex cones in real vector spaces. By a *convex cone* we mean what is usually referred to as a "pointed convex polyhedral cone", the nonnegative span of a finite set of vectors such that the span contains no nonzero linear subspace. Such a cone can be represented isomorphically as the set of nonnegative points in a subspace of R^n, where n is the number of facets of M. We refer to this representation, which is unique up to isomorphism, as the *canonical embedding* of M in the positive orthant $(R^+)^n$.

A *splitting subcone* of a convex cone M is a convex subcone which is a direct summand of M, the complementary summand being a subset (not necessarily a subcone) of M. Theorems 1–4, adapted to convex cones, provide a theory by which the splitting subcones of a given M can be determined by considering subspaces of the *cospace* of M, the latter being defined as the factor space $R^n/\langle M \rangle$, where M is canonically embedded in $(R^+)^n$ and $\langle M \rangle$ is the subspace generated by M.

The results for convex cones can be stated in the same multiplicative number-theoretic language used in the paper if one agrees to represent the additive group R^n with multiplicative notation, so that the standard basis vectors are represented as "primes" $p, q, r \cdots$ and scalar multipliers become exponents. The natural partial ordering on R^n becomes "divides", with GCD's and relative primeness interpreted accordingly. The only real change that must be made in adapting this material to convex cones is the definition of minimal elements of a cone. These should now be defined as the points on 1-dimensional faces of M. Thus Theorem 4 must be reworded slightly to allow for minimal elements which are powers of each other.

As an illustration of what this shows for convex cones, consider the cone M generated over $\boldsymbol{R}^+$ by the five points in $\boldsymbol{R}^6$

$$(1, 0, 0, 1, 0, 0)$$
$$(0, 1, 0, 0, 1, 0)$$
$$(0, 0, 1, 0, 0, 1)$$
$$(1, 0, 1, 0, 1, 0)$$
$$(0, 1, 0, 1, 0, 1)\,.$$

In multiplicative notation, we represent these generators as ps, qt, ru, prt, qsu. Then M is the kernel of the mapping from the free cone $N = [p, q, r, s, t, u]$ to $\boldsymbol{R}^2$ in which the six generators go to the vertices of a regular hexagon centered at the origin. (This configuration in $\boldsymbol{R}^2$ is the Gale diagram of a triangular prism, which is the dual of a cross section of M.) To determine the splitting subcones of M, we consider subspaces H of $\boldsymbol{R}^2$. For each H, we look at the minimal elements of the kernel M_H of the mapping from N to $\boldsymbol{R}^2/H$. If the members $M_H^{\min} - M$ are pairwise relatively prime modulo powers, then they generate a free cone F which intersects M in a splitting subcone; and every splitting subcone of M is obtainable this way, possibly augmenting F by including as generators any pairwise relatively prime members of M which are relatively prime to all members of $M_H^{\min} - M$.

When $H = \boldsymbol{R}^2$, $M_H^{\min} - M$ consists of the powers of p, q, r, s, t, u. This gives the trivial splitting subcone M. When H is a line containing two opposite vertices of the hexagon (say the images of p and s), then $M_H^{\min} - M$ consists of the powers of p, s, rt, and qu. This gives the splitting subcone of M generated by ps, prt, qus, and $rtqu$. No members of M are relatively prime to all of p, s, rt, and qu, so no other splitting subcone results from this H. Two other splitting subcones are obtained from the two other pairs of opposite vertices of the hexagon. However if H is any other line through 0 in $\boldsymbol{R}^2$, then the members of $M_H^{\min} - M$, modulo powers, are not pairwise relatively prime, so H does not correspond to a splitting subcone. Finally, when $H = \{0\}$, $M_H^{\min} - M$ is empty and we obtain the trivial splitting subcone $\{1\}$ in M, corresponding to the vertex of the cone. We also obtain all subcones of M having pairwise relatively prime generators: These are the halflines $[m]$, $m \in M$; the 2-dimensional free subcones $[ps, qt]$, $[ps, ru]$, $[qt, ru]$, $[prt, qsu]$, $[ps, qt(ru)^\alpha]$, $[ps(qt)^\alpha, ru]$, and $[ps(ru)^\alpha, qt]$ for all $\alpha \in \boldsymbol{R}^+$; and the 3-dimensional free subcone $[ps, qt, ru]$.

It is interesting to interpret Theorem 2 in terms of convex cones: If K is a splitting subcone of a convex cone M and M is canonically

embedded in $(\boldsymbol{R}^+)^n$, then the GCD's (greatest lower bounds) from K form a free cone with relatively prime generators. Call this the *GCD cone* of K. In general, GCD cones are not free. For example, the points

$$(1, 0, 1, 0, 1)$$
$$(1, 0, 0, 1, 1)$$
$$(0, 1, 1, 0, 1)$$
$$(0, 1, 0, 1, 1)$$

generate a normally embedded square cone K in $(\boldsymbol{R}^+)^5$ whose GCD cone has nine minimal generators, hence the GCD cone is not free. Thus, for example, K is not a splitting subcone of any canonically embedded cone in $(\boldsymbol{R}^+)^5$.

8. **Further results for Z-semimodules.** *Maximal common divisors.* Let K be a closed factor of M and let $k_1, \cdots, k_t \in K$. Set $f = \mathrm{GCD}(k_1, \cdots, k_t)$ and write $f = mn$, with $m \in M$ and $n \in N/M$. In other words, m is a maximal common divisor of the k_i in M.

COROLLARY 3 TO THEOREM 1. *With notation as above, $m \in K$.*

Proof. $f \equiv n (\mathrm{mod}\ M)$, hence $f \equiv n (\mathrm{mod}\ K)$ by Theorem 1. Then $m \in \langle K \rangle \cap N = K$.

Intersections. We will prove that an intersection of closed factors is a closed factor.

THEOREM 5. *Let $\{K_i : i \in I\}$ be a family or closed factors of a normal Z-semimodule M. Then $K = \bigcap_{i \in I} K_i$ is a closed factor of M. Moreover if H_i is the subgroup of $G = \langle N \rangle / \langle M \rangle$ corresponding to K_i then $H = \bigcap_{i \in I} H_i$ is the subgroup corresponding to K.*

Proof. Let F_i be the set of GCD's from K_i. By Theorem 3, all MF_i are normally embedded in N and hence so is $\bigcap_i MF_i$. We claim that this intersection is just MF, where $F = \bigcap_i F_i$.

Clearly $\bigcap_i MF_i$ contains MF. Conversely, fixing $x \in \bigcap_i MF_i$, write $x = mn$ with $m \in M$ and $n \in N/M$. Then $n \in MF_i$ for each i by normality, hence

$$n \in (MF_i)/M \subset F_i \quad \forall i \in I\,,$$

showing that $x \in MF$.

From the above we conclude that MF is normally embedded in N. Moreover F is generated by a family of pairwise relatively

prime members of N because each F_i is. (Each F_i is closed under multiplication, GCD's, and division whenever possible, hence so is their intersection; it follows as in the proof of Theorem 2 that F has relatively prime generators.) Applying Theorem 3, we conclude that $K = M \cap F$ is a closed factor of M and that F is the set of GCD's from K. Finally, the fact that $MF = \bigcap_i MF_i$ implies that $MF = M_H$, hence K corresponds to H.

Multiplicity $\geqq 2$. We establish a sufficient condition for M to have no closed factors other than M itself and the trivial factors of Example 1, §3.

Call M *irreducible* iff M has no direct product decomposition $K_1 \times K_2$, where the K_i are closed factors $\neq \{1\}$.

Define the *multiplicity* of M to be the smallest nonzero number of primes in any nontrivial congruence class mod M. Thus M has multiplicity $\geqq 2$ iff for each prime $p \in N - M$, there is a prime $q \neq p$ such tnat $q \equiv p (\mathrm{mod}\ M)$.

THEOREM 6. *If M is irreducible and has multiplicity $\geqq 2$, then all closed factors of M, other than M itself, are of the form $[m_i : i \in I]$ where the m_i are pairwise relatively prime members of M.*

Proof. Let K be a closed factor of M and let F and H be as in §6. By Theorem 4, the members of $M_H^{\min} - M$ are pairwise relatively prime. Fixing any $n \in M_H^{\min} - M$, let p be a prime divisor of n such that $p \notin M$ and let $q \neq p$ be a prime such that $q \equiv p (\mathrm{mod}\ M)$. Then $qn/p \in M_H^{\min} - M$, hence qn/p is relatively prime to n, implying $n = p$. Thus $F_0 = [M_H^{\min} - M]$ is generated by a set of primes. Moreover $F_0 \subset F$ by Theorem 4. Also note that $MF_0 = M_H$, which is normally embedded in N. Thus by Theorem 3, $K_0 = M \cap F_0$ is a closed factor of M and the complementary factor M/K_0 is equal to M/F_0. Moreover it is clear that M/F_0 is closed under multiplication. Since M is irreducible, we conclude that either $K_0 = M$, implying $K = M$, or else $K_0 = \{1\}$. In the latter case, we have $F_0 = \{1\}$ since F_0 is the set of GCD's from K_0 by Theorem 3. Then $F \subset M$, implying $K = F$.

In the next section we will see how this result leads to the determination of all closed factors of any M having multiplicity $\geqq 2$.

9. Closed factors of a direct product. By a *direct product* of Z-semimodules M_i, we will always mean *restricted direct product*: The direct product $\times_{i \in I} M_i$ consists of families $(m_i)_{i \in I}$ of elements $m_i \in M_i$ such that $m_i = 1$ for all but finitely many $i \in I$. Thus we can speak of direct product decompositions of a given normal Z-

semimodule M into closed factors, possibly infinitely many. We will see that all such decompositions can be obtained from a single one by grouping factors together.

Let $M = \bigtimes_{i \in I} M_i$ be a direct product decomposition of M into closed factors M_i. It is clear that $M^{\min} \subset \bigcup_{i \in I} M_i$, and that $[M^{\min} \cap M_i] \subset M_i$. Since M is generated by the members of $M^{\min}$, we must in fact have for each i,

$$M_i = [M^{\min} \cap M_i] .$$

Thus the decomposition of M corresponds to a partition of $M^{\min}$. Moreover the partitions $M^{\min} = \bigcup_{i \in I} X_i$ which correspond to decompositions are characterized by the condition

$$\mathrm{GCD}(x_i, x_j) = 1 \quad \text{if} \quad x_i \in X_i, x_j \in X_j , \quad i \neq j .$$

(See Corollary 2, Theorem 2. GCD refers to the divisibility relation in N, where $M \subset N$ is the canonical embedding of M.)

Call a partition of $M^{\min}$ *admissible* if it has the above property. It is easy to see that there is a unique finest admissible partition of $M^{\min}$. In view of the equivalence between admissible partitions and decompositions, we obtain the following result:

THEOREM 7. *A normal Z-semimodule M has a unique finest direct product decomposition into closed factors. All other decompositions of M into closed factors $\neq \{1\}$ can be obtained from this one by grouping factors together.*

The factors in the finest decomposition of M are called the *irreducible components of M.*

COROLLARY. *A normal Z-semimodule is uniquely representable as a direct product of irreducible Z-semimodules $\neq \{1\}$.*

Next we show how all closed factors of a direct product $\bigtimes_i M_i$ can be obtained from the closed factors of the M_i.

THEOREM 8. *Let $M = \bigtimes_i M_i$ be a decomposition of a normal Z-semimodule M into closed factors M_i, and let K be a closed factor of M. For each i, set $K_i = K \cap M_{ii}$. Then*

$$K = (\bigtimes_i K_i) \times F$$

where F is free, generated by a set of pairwise relatively prime members of M which are relatively prime to all members of all K_i.

Proof. It is clear that each K_i is a closed factor of M_i, hence

$$L = \times_i K_i$$

is a closed factor of M. Since $L \subset K$, L is a closed factor of K. It remains to prove that the complementary factor K/L is free; all relative primeness statements will then follow by Corollaries 2 and 3 to Theorem 2.

First we show that $K^* = K/L$ is closed under multiplication. Clearly K^* is the intersection of the K/K_i, so it is enough to show that each K/K_i is closed. Fixing i, let $h, k \in K/K_i$ and suppose hk is divisible by $k_i \in K_i$. Since the members of M_i are relatively prime to everything in M/M_i, k_i divides

$$h\pi_{M_i}(k) .$$

Then by Propositions 2 and 3 of §6, we have

$$k_i \mid \pi_K(h\pi_{M_i}(k)) = h\pi_K\pi_{M_i}(k) = h ,$$

with the last equality following from the fact that $\pi_K\pi_{M_i}(k)$ is a divisor of k in K_i. Finally, we conclude that $k_i = 1$. That completes the proof that K^* is closed.

The proof that K^* is free is accomplished in several steps. First assume that there are only two factors: $M = M_1 \times M_2$. Then the projection mappings π_{M_1} and π_{M_2} are one-to-one on K^*: If K^* contains uv and uw with $u \in M_1$ and $v, w \in M_2$, then u, v and w are all in M/K. Then the equation

$$(uv)w = (uw)v$$

implies that $v = w$ by unique representation in $K \times (M/K)$. Thus π_{M_1} is one-to-one on K^*. Similarly, so is π_{M_2}. Thus the π_{M_i} map K^* isomorphically onto the $\pi_{M_i}(K^*)$. Moreover K^* is easily seen to be a closed factor of

$$\pi_{M_1}(K^*) \times \pi_{M_2}(K^*) .$$

LEMMA. *Let M be a normal $\mathbf{Z}$-semimodule and suppose that the diagonal*

$$D = \{(m, m): m \in M\}$$

is a factor of the direct product $M \times M$. Then M is free.

Proof. As usual, let $M \subset N$ be the canonical embedding of M. Then everything in N is a GCD from M. It follows that the set of GCD's from D is

$$D_N = \{(n, n): n \in N\} .$$

Assuming that D is a factor of $M \times M$, we have by Theorem 3

$$\pi_F(M \times M) \subset M \times M$$

where $F = D_N$. Moreover for $m_1, m_2 \in M$ we have

$$\pi_F(m_1, m_2) = (n, n)$$

where $n = \mathrm{GCD}(m_1, m_2)$. We conclude that M is closed under taking GCD's, hence $M = N$.

Applying the lemma in an obvious way, we conclude that K^* is free when $M = M_1 \times M_2$.

Next we prove by induction that K^* is free when $M = M_1 \times \cdots \times M_n$. Fixing $n \geqq 3$ and assuming the result for fewer than n factors, we have

$$K = K' \times K_3 \times \cdots \times K_n \times F$$

where F is free and $K' = K \cap (M_1 \times M_2)$. Since K' is a closed factor of $M_1 \times M_2$, we have

$$K' = K_1 \times K_2 \times F'$$

where F' is free. Then

$$K^* = F \times F' .$$

Finally we prove that K^* is free when M is decomposed into arbitrarily many factors M_i. It is sufficient to prove that any two minimal elements of K^* are relatively prime. Fixing $h, k \in (K^*)^{\min}$, we have $h, k \in M_{i_1} \times \cdots \times M_{i_n}$ for some finite set of indices $i_1, \cdots, i_n$. If we set

$$K^{**} = K^* \cap (M_{i_1} \times \cdots \times M_{i_n}) ,$$

then K^{**} is a closed factor of $M_{i_1} \times \cdots \times M_{i_n}$ intersecting each M_{i_j} trivially. From the inductive argument above we find that K^{**} is free, hence its minimal elements are pairwise relatively prime. In particular, h and k are among these minimal elements.

The proof of Theorem 8 is now complete.

COROLLARY. *If M has multiplicity $\geqq 2$, then for each closed factor K of M there is a direct product decomposition*

$$M = M_1 \times M_2$$

with M_1 and M_2 both closed, such that

$$K = M_1 \times F$$

where F is a free closed factor of M_2.

Proof. Each irreducible component of M has multiplicity $\geqq 2$, and K intersects each component in a closed factor. Let M_1 be the product of all components which are contained in K and apply Theorems 6 and 8.

A closed factor of M can have more irreducible components than M has, even if cyclic components (free semimodules of rank 1) are excluded. We give an example in which M is irreducible and K has $n \geqq 2$ noncyclic irreducible components. Let M be the kernel of the mapping

$$[p_i, q_i : i = 1, \cdots, n] \longrightarrow G = (\boldsymbol{Z}/n\boldsymbol{Z}) \oplus (\boldsymbol{Z}/2n\boldsymbol{Z})^n$$

defined by

$$p_i \longmapsto u_i$$
$$q_i \longmapsto u_0 - u_i$$

where u_0 denotes $1 \in \boldsymbol{Z}/n\boldsymbol{Z}$ and the u_i, $1 \leqq i \leqq n$, are the canonical unit vectors in $(\boldsymbol{Z}/2n\boldsymbol{Z})^n$. The product

$$m = p_1 q_1 \cdots p_n q_n$$

is in $M^{\min}$, implying that M is irreducible: m is in one irreducible component of M, hence all elements in all other irreducible components are relatively prime to m. But m is divisible by all primes in N.

We claim that

$$K = \bigtimes_{i=1}^{n} [p_i^{2n} q_i^{2n}, (p_i q_i)^n]$$

is a closed factor of M. We have $K = M \cap F$ where

$$F = [p_i^n, q_i^n : 1 \leqq i \leqq n] ,$$

hence by Theorem 3 it is enough to show that MF is normally embedded in N. It is not difficult to see that $MF = M_H$, where $H = nG$. In fact the generators of M_H are the p_i^n, the q_i^n, and all products of the form

$$(p_1 q_1)^{a_1} \cdots (p_n q_n)^{a_n}$$

with $0 \leqq a_i < n$ for all i and $\Sigma_i a_i = n$. These products are all in M.

10. **The cyclic cogroup case.** It is possible to describe explicitly all closed factors of M when the cogroup of M is cyclic. In view of Theorem 8, it is sufficient to consider the case in which M is

irreducible. Moreover since all free closed factors of M are known, we consider only nonfree ones.

Throughout this section M is the kernel of a strongly surjective mapping

$$\varphi: N \longrightarrow G = \boldsymbol{Z}/n\boldsymbol{Z}$$

where n is a nonnegative integer. M is assumed to be irreducible. When $n = 0$, this assumption is equivalent to the condition that $p \notin M$ for all primes $p \in N$. For each p, let a_p be an integer representing the congruence class $\varphi(p)$ in G.

Call two primes p and p' *paired* if $pp' \in M$ and $pq, p'q \notin M$ for all other primes q. Equivalently,

$$a_p + a_{p'} \equiv 0 (\mathrm{mod}\, n)$$

and

$$a_q \not\equiv \pm a_p (\mathrm{mod}\, n) \quad \forall q \neq p, p' .$$

THEOREM 9. *Let $\{d_p\}$ be a family of positive integers satisfying the conditions*

(1) $d_p = 1$ *if p is not paired with any other prime;*

(2) *if p and p' are paired, then $d_p = d_{p'}$ and $d_p | (a_q, n)$ for all $q \neq p, p'$. Then $K = M \cap F$ is a closed factor of M, where*

$$F = [\text{all } p^{d_p}] .$$

Conversely, every nonfree closed factor of M is equal to such an intersection, where the d_p satisfy conditions (1) *and* (2).

Proof. Assuming first that the d_p satisfy conditions (1) and (2), we prove that K is a closed factor of M. By Theorem 3, it is sufficient to show that $\pi_F(M) \subset M$. For any $m \in M$, write $m = fr$ with $f \in F$ and $r \in N/F$. We claim that $r \in M$, which will imply $f \in M$. Write

$$m = \prod_{\text{all } p} p^{x_p} ;$$

then

$$r = \prod_{\text{all } p} p^{y_p}$$

where x_p reduces to $y_p \bmod d_p$, $0 \leqq y_p < d_p$. Thus $y_p = 0$ if p is not paired. For paired p, p', we have

$$a_p(x_p - x_{p'}) + \sum_{q \neq p, p'} a_q x_q \equiv 0 (\mathrm{mod}\, n) ,$$

hence

$$a_p(x_p - x_{p'}) \equiv 0 (\mathrm{mod}\, d_p) .$$

Moreover the fact that φ is surjective implies that a_p is relatively prime to d_p. (Otherwise a_p, $a_{p'}$, and all a_q would be in a proper subgroup of G.) Thus $x_p \equiv x_{p'} (\mathrm{mod}\, d_p)$, implying that

$$r = \prod_{\substack{\text{paired} \\ p\ p'}} (pp')^{y_p} \in M .$$

Now suppose that K is a nonfree closed factor of M and let F be the set of GCD's from K. Thus $K = M \cap F$ and $MF = M_H$ for some subgroup $H \subset G$. Since K is nonfree and H is the cogroup of K, H is nonzero. Thus $H = dG$ for some positive divisor d of n, $d \neq n$.

For each p, set

$$n_p = \frac{n}{(a_p, n)} , \quad d_p = \frac{d}{(a_p, d)} .$$

When $n > 0$, n_p is the additive order of $a_p \bmod n$. In all cases d_p is the additive order of $a_p \bmod d$. For all p we have

$$p^{n_p} \in M , \quad p^{d_p} \in M_H^{\min} .$$

Call p *good* iff $p^{d_p} \notin M$. When $n = 0$, it is clear that all primes are good. (Recall that M contains no primes since it is irreducible, hence all a_p are nonzero.) In all cases, p is good iff $n_p \neq d_p$.

LEMMA 1. *Let p and q be two primes, at least one of which is good. Suppose moreover that*

$$(d_p, d_q) = e > 1 .$$

Then

$$\frac{d_p}{e} a_p + \frac{d_q}{e} a_q \equiv 0 (\mathrm{mod}\, n) .$$

Proof. Set $a = a_p$, $b = a_q$, $\alpha = d_p$, $\beta = d_q$ and without loss of generality assume that p is good. Then $M_H^{\min}$ contains both p^α and q^β, and $p^\alpha \notin M$. Moreover the members of $M_H^{\min} - M$ are pairwise relatively prime by Theorem 4. It follows that whenever M_H contains an element of the form

$$p^x q^y , \quad 0 \leqq x < \alpha, 0 \leqq y < \beta$$

then M also contains this element. (If not, then some divisor of this

element would be in $M_H^{\min} - M$; this divisor could not be a power of q, since $M_H^{\min}$ contains q^β, so $M_H^{\min} - M$ would contain two multiples of p.) Equivalently, every solution of the congruence

$$ax + by \equiv 0 (\mathrm{mod}\, d)$$

with $0 \leqq x < a$ and $0 \leqq y < b$, is also a solution of

$$ax + by \equiv 0 (\mathrm{mod}\, n) .$$

Let $\langle a \rangle$ and $\langle b \rangle$ denote the subgroups of $\boldsymbol{Z}/d\boldsymbol{Z}$ generated (additively) by a and b. The intersection $\langle a \rangle \cap \langle b \rangle$ is the unique subgroup of $\boldsymbol{Z}/d\boldsymbol{Z}$ having order e. This subgroup is generated by $(\alpha/e)a$ and contains $-(\beta/e)b$, hence we can write

$$-\frac{\beta}{e} b \equiv k \frac{\alpha}{e} a (\mathrm{mod}\, d)$$

for some k, $0 \leqq k < e$. Moreover $k \neq 0$ since $e > 1$. By our observation above, the congruence

$$k \frac{\alpha}{e} a + \frac{\beta}{e} b \equiv 0$$

holds mod n, and it remains to show that $k = 1$.

The open interval $(e, 2e)$ has length $> k$, so it contains a multiple hk of k. If $k \geqq 2$, then $h < e$. Then the congruence

$$\left(hk \frac{\alpha}{e} - \alpha \right) a + h \frac{\beta}{e} b \equiv 0 ,$$

which holds mod d, also holds mod n. This implies $\alpha a \equiv 0 (\mathrm{mod}\, n)$. But then $p^\alpha \in M$, contrary to assumption.

LEMMA 2. *For all p,*

$$\left(n_p, \frac{n}{d} \right) = \frac{n_p}{d_p} .$$

Proof.

$$d \left(n_p, \frac{n}{d} \right) = (dn_p, n) = n_p (d, (a_p, n)) = n_p (d, a_p) .$$

We will use Lemmas 1 and 2 to show that no bad primes can exist.

First, suppose all primes are bad. Then $n_p = d_p \mid d$ for all p, implying

$$\frac{n}{d} \Big| \frac{n}{n_p} = (a_p, n) \mid a_p \ .$$

But then all a_p are in a proper subgroup of $\boldsymbol{Z}/n\boldsymbol{Z}$, a contradiction since φ is surjective.

Now suppose p is bad and q is good. Then $n_p = d_p$ and we have

$$a_p d_p \equiv 0 \ , \quad a_q d_q \not\equiv 0 (\mathrm{mod}\, n) \ .$$

Lemma 1 shows that $(d_p, d_q) = 1$. Moreover by Lemma 2,

$$\left(n_p, \frac{n_q}{d_q}\right) \Big| \left(n_p, \frac{n}{d}\right) = \frac{n_p}{d_p} = 1 \ .$$

Combining results, we obtain $(n_p, n_q) = 1$ whenever p is bad and q is good. Thus, assuming that both good and bad primes exist, $\boldsymbol{Z}/n\boldsymbol{Z}$ has a subgroup decomposition $A \times B$ such that A contains all a_p, p good, and B contains all a_p, p bad. (Note that $n > 0$ and consider the Sylow subgroup decomposition of $\boldsymbol{Z}/n\boldsymbol{Z}$. Recall that n_p is the order of a_p in $\boldsymbol{Z}/n\boldsymbol{Z}$.) Then $M = M_A \times M_B$ where

$$M_A = M \cap [p\colon p \text{ good}]$$
$$M_B = M \cap [p\colon p \text{ bad}] \ .$$

Both M_A and M_B are nontrivial since $p^n \in M$ for all p. But M was assumed to be irreducible.

We conclude that all primes are good. Thus all p^{d_p} are in $M_H^{\min} - M$ and then necessarily $F = [\text{all } p^{d_p}]$. It remains to show that the d_p satisfy conditions (1) and (2).

We claim first that for each p there is at most one $q \neq p$ such that $(d_p, d_q) > 1$. Assuming that p, q and r are distinct primes such that

$$(d_p, d_q) = e > 1 \ , \quad (d_p, d_r) = f > 1$$

and setting $\alpha = d_p$, $\beta = d_q$, $\gamma = d_r$, $a = a_p$, $b = a_q$, $c = a_r$, we have by Lemma 1

$$\frac{\alpha}{e} a + \frac{\beta}{e} b = 0 (\mathrm{mod}\, n)$$
$$\frac{c}{f} a + \frac{\gamma}{f} 0 \equiv 0 (\mathrm{mod}\, n) \ .$$

Moreover $\alpha a \equiv 0 \bmod d$ but not mod n since p is good. Fixing integers h and k such that

$$\frac{f}{2} \leqq h < e, \frac{e}{2} \leqq k < f \ ,$$

we have

$$\left(h\frac{\alpha}{e} + k\frac{\alpha}{f}\right)a + \left(h\frac{\beta}{e}\right)b + \left(k\frac{\gamma}{f}\right)c \equiv 0(\mathrm{mod}\, n) ,$$

hence the congruence

$$\left(h\frac{\alpha}{e} + k\frac{\alpha}{f} - \alpha\right)a + \left(h\frac{\beta}{e}\right)b + \left(k\frac{\gamma}{f}\right)c \equiv 0$$

holds mod d but not mod n. Denoting the coefficients of a, b, c by x, y, z respectively, we have

$$0 \leqq x < \alpha , \quad 0 \leqq y < \beta , \quad 0 \leqq z < \gamma$$

and the element

$$p^x q^y r^z$$

is in M_H but not in M. As in the proof of Lemma 1, this leads to a contradiction.

Now suppose some d_p is relatively prime to all d_q, $q \neq p$. For each $q \neq p$, we have $d_p \mid d \mid d_q a_q$, hence $d_p \mid a_q$. Thus all a_q, $q \neq p$, are in the subgroup of $\boldsymbol{Z}/n\boldsymbol{Z}$ generated by d_p. The fact that φ is strongly surjective implies that this is not a proper subgroup, so $(d_p, n) = 1$. Since $d_p \mid d \mid n$, we conclude that $d_p = 1$.

We have shown that for each p with $d_p > 1$, there is a unique $p' \neq p$ such that $(d_p, d_{p'}) > 1$. We show now that in fact p and p' are paired. For each $q \neq p, p'$ we have $d_p \mid a_q$ since $d_p \mid d \mid d_q a_q$ and $(d_p, d_q) = 1$. It follows that d_p must be relatively prime to $a_{p'}$ since otherwise all a_q, $q \neq p$, would be in a proper subgroup of G, contradicting strong surjectivity. Thus from $d_p \mid d \mid d_{p'} a_{p'}$ we obtain $d_p \mid d_{p'}$. By symmetry, $d_p = d_{p'}$. Applying Lemma 1, we obtain the fact that

$$a_p + a_{p'} \equiv 0(\mathrm{mod}\, n) .$$

Moreover for $q \neq p, p'$

$$a_q \not\equiv \pm a_p(\mathrm{mod}\, n)$$

since $d_q \neq d_p$. We conclude that p and p' are paired. Also note that we have shown that $d_p \mid a_q$ for all $q \neq p, p'$.

It follows easily from the above that the d_p satisfy conditions (1) and (2). That completes the proof of Theorem 9.

As an application of this result, consider Example 4 of §4. The primes p and q are paired, and so are r and s. Theorem 9 shows that all nonfree closed factors of M have the form

$$M \cap [p^a, q^a, r^b, s^b]$$

where $a \mid 2$ and $b \mid 3$, and that every such intersection is a closed factor. The closed factor in Example 4 was the case $a = 2, b = 3$.

11. Conjecture on arbitrary factorizations. Let $\{K_i: i \in I\}$ be a nested, well-ordered family of closed factors of a normal Z-semimodule M such that $K_0 = M$ and $\cap K_i = \{1\}$. (I is a well-ordered index set whose initial element is 0.) Then there is a factorization

$$M = \bigtimes_{i \in I} (K_i/K_{i+1})$$

where $i + 1$ denotes the successor of i. Every partition of I into subsets I_j leads to a factorization

$$M = \bigtimes_j A_j ,$$

where for each j

$$A_j = \bigtimes_{i \in I_j} (K_i/K_{i+1}) .$$

Conjecture: Every factorization of M comes from a nested family of closed factors K_i by the above construction.

This was proved in [6] for all free Z-semimodules and in [7] for all normal Z-semimodules of multiplicity $\geqq 3$. Moreover it was shown that if N is countable, then the index set I can be taken to be the nonnegative integers.

REFERENCES

1. N. G. DeBruijn, *On bases for the set of integers*, Publ. Math., (Debrecen) **1** (1950), 232-242.
2. ———, *On number systems*, Nieuw Arch. Wisk., **4** (1956), 15-17.
3. ———, *Some direct decompositions of the set of integers*, Math. Comp., **18** (1964), 537-546.
4. R. T. Hansen, *Complementing pairs of subsets of the plane*, Duke Math. J., **36** (1969), 441-449.
5. C. T. Long, *Addition theorems for sets of integers*, Pacific J. Math., **23** (1967), 107-112.
6. D. Marcus, *Direct decompositions in free commutative monoids*, J. Combinatorial Theory, **16** (1974), 286-312.
7. ———, *Direct decompositions of commutative monoids*, doctoral dissertation, Harvard U., 1972.
8. ———, *Normal semimodules: a theory of generalized convex cones*, to appear.
9. I. Niven, *A characterization of complementing sets of pairs of integers*, Duke Math. J., **38** (1971), 193-203.
10. S. K. Stein, *Algebraic tiling*, Amer. Math. Monthly, **81** (1974), 445-462.
11. ———, *Factors of some direct products*, Duke Math. J., **41** (1974), 537-539.
12. C. Swenson, *Direct sum subset decompositions of Z*, Pacific J. Math., **53** (1974), 629-632.

Received August 2, 1979. This research was supported by National Science Foundation Grant MPS 75-08325.

CALIFORNIA STATE POLYTECHNIC UNIVERSITY
POMONA, CA 91768

PACIFIC JOURNAL OF MATHEMATICS

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics
Vol. 93, No. 1 March, 1981