NORMAL SEMIMODULES: A THEORY OF GENERALIZED CONVEX CONES

DANIEL A. MARCUS

1. Introduction. In [3], C. Davis showed that if a convex polyhedral cone C (the positive span of a finite set of vectors in Euclidean space) contains no nonzero linear subspace, then C is linearly isomorphic to the set V^+ of nonnegative points in a linear subspace V of \mathbb{R}^n . Moreover n can be taken to be the number of facets (maximal proper faces) of C.

In the standard theory of convex polytopes, a convex polytope P (the convex hull of a finite set in Euclidean space) is represented by a sequence $X = (x_1, \ldots, x_n)$ of points in a real vector space of dimension n - d - 1, where n is the number of vertices and d is the dimension of P. (See [4] or [7].) X is called a *Gale diagram* of P and reflects all affine properties of P. In particular, there is a correspondence between vertices v_i of P and elements x_i of X such that a set $\{v_i: i \in I\}$ is the vertex set of a face of P if and only if the $x_i, i \notin I$, form a positive spanning set for their linear span. (By this we mean that every vector in the linear span of the $x_i, i \notin I$, can be represented in the form $\sum_{i \notin I} a_i x_i$ where the a_i are nonnegative.) It follows that for each index i_0 , the set $\{x_i: i \neq i_0\}$ is a positive spanning set for the linear span of all of the x_i . This can be regarded as the characteristic property of Gale diagrams.

A Gale diagram of P can be constructed with the aid of the representation of a convex cone as the set of nonnegative points in a linear subspace. Let P be a *d*-dimensional convex polytope in an affine subspace of \mathbf{R}^{d+1} not containing the origin. The positive cone on P

 $C = \{av: v \in P, a \in \mathbf{R}, a \ge 0\}$

is a convex polyhedral cone. Its dual

$$C^* = \{ u \in \mathbf{R}^{d+1} : (u, v) \ge 0 \forall v \in C \}$$

is also a convex polyhedral cone, where (u, v) denotes the standard inner product in \mathbf{R}^{d+1} . Moreover the number *n* of vertices of *P* is the same as the number of facets of C^* . If *V* is a subspace of \mathbf{R}^n such that C^* is isomorphic

Received December 20, 1982. This research was supported by National Science Foundation Grant MPS 75-08325.

to V^+ , then a Gale diagram of P can be constructed as the sequence of images in \mathbf{R}^n/V of the standard basis vectors of \mathbf{R}^n .

Notice that in the construction above, the cone V^+ is the kernel of the mapping

 $\left(\mathbf{R}^n\right)^+ \to \mathbf{R}^n/V.$

This mapping is surjective, since the x_i form a positive spanning set for \mathbf{R}^n/V , and in fact the characteristic property of Gale diagrams shows that each of the *n* restrictions

 $(\mathbf{R}^n)^+ \cap H_i \to \mathbf{R}^n / V$

is surjective, where H_i denotes the coordinate hyperplane

$$\{(x_1,\ldots,x_n)\in \mathbf{R}^n: x_i=0\}.$$

It is the purpose of this paper to develop a theory of generalized convex cones, in which coordinates are members of an arbitrary ordered integral domain R. The theory will apply to those generalized cones (called *normal R*-semimodules) which can be represented isomorphically as the set of nonnegative points in a submodule of a free R-module. The main result (Theorem 1) states that, for suitable rings R, such a cone is uniquely representable as the kernel of a mapping which is a generalization of the mapping

$$(\mathbf{R}^n)^+ \to \mathbf{R}^n/V$$

described above, having analogous surjective restrictions. Such mappings can be regarded as generalized Gale diagrams.

The condition placed on R is that all nonzero ideals are unbounded. Thus in particular the theory applies when R is the ring of integers Z. Normal Z-semimodules can be regarded as certain multiplicative semigroups of monomials. In that context they have arisen in the work of M. Hochster in connection with the problem of establishing sufficient conditions on a semigroup M of monomials in finitely many variables in order that the ring of polynomials A[M] be Cohen-Macaulay whenever Ais a Cohen-Macaulay ring. The sufficient condition established in [5] is that M be isomorphic to a semigroup M' of monomials in a (possibly different) finite set of variables such that if $m, m' \in M'$ and m/m' is a monomial, then $m/m' \in M'$. This, it turns out, is equivalent to M being a normal Z-semimodule. Coincidentally, M is called a normal semigroup in [5] because it generates a normal ring A[M]; in the present work, the term "normal" is suggested by the fact that a normal semimodule can be represented as the kernel of a homomorphism. Theorem 1 of the present work, for $R = \mathbb{Z}$, was used in the solution to a combinatorial problem in [6].

2. Examples of normal semimodules. Let R be an ordered integral domain. The *free semimodule* of rank n (possibly transfinite) is the direct sum of n copies of R^+ , the non-negative part of R. Each member of the direct sum has only finitely many nonzero coordinates. A *normal subsemimodule* of a free semimodule F is the intersection of F with a submodule of the corresponding free module; equivalently, it is the kernel of some R^+ -linear homomorphism from F to some R-module. A *normal semimodule* over R is any R-semimodule (i.e., a commutative semigroup on which R^+ operates by endomorphisms) which can be embedded in a free R-semimodule as a normal subsemimodule.

We give some examples:

Example 1. The set { $(m, n) \in \mathbb{Z} \oplus \mathbb{Z}:m, n \ge 0, m \equiv n \pmod{2}$ } is a normal semimodule over the ring of integers Z. More generally, so is the set of non-negative points in any *n*-dimensional integral lattice.

Example 2. The set $\{1, 2, 3, ...\}$ of positive integers is a free **Z**-semimodule of countably infinite rank with multiplicative notation. The subset $\{1, 5, 9, ..., 4n + 1, ...\}$ is a normal subsemimodule. More generally, $\{1, 5, 9, ...\}$ can be replaced by any multiplicative semigroup S of positive integers which is closed under division whenever possible: i.e., if $m, n \in S$ and m|n, then $n/m \in S$. However S need not have this property to be a normal **Z**-semimodule: for example $\{2^m3^n: 0 \le m \le n\}$ is free (with basis $\{3, 6\}$), hence a normal semimodule. But it is not a normal subsemimodule of $\{1, 2, 3, ...\}$.

Example 3. The nonzero integral ideals in a Dedekind domain form a free (multiplicative) **Z**-semimodule, of which the set of nonzero principal ideals is a normal subsemimodule. More generally the set of nonzero principal ideals in any Krull domain is a normal **Z**-semimodule under multiplication.

Example 4. The monic polynomials over any field (more generally, over any unique factorization domain) form a free \mathbb{Z} -semimodule, again multiplicative. The ones with constant term 1 form a normal subsemimodule. So do the ones whose second coefficient is 0.

Example 5. Let V be any subspace of \mathbb{R}^n . The set V^+ of non-negative points of V is a normal **R**-semimodule. For example let V be the subspace

of \mathbf{R}^4 defined by the equation $x_1 + x_2 = x_3 + x_4$. Then V^+ is easily seen to be an infinite square pyramid, or the infinite cone on a square.

Example 6. Let G be a graph, with loops and parallel edges allowed. The *circuit module* of G consists of all linear combinations of circuits in G with coefficients in Z. Regarding a circuit as a formal sum of edges, we represent the circuit module as a subgroup of the free Abelian group \mathbb{Z}^m , where m is the number of edges in G. The set S of non-negative points of the circuit module of G is a normal Z-semimodule, which we call the *circuit semimodule* of G. It should be noted that while S obviously includes all positive linear combinations of circuits, it may include other elements, as well. For example, if G is the graph with two vertices joined by three edges, the circuit semimodule of G contains 2e for each edge e.

Example 7. Let D be a digraph (graph with directed edges) and let R be an ordered domain. The nonnegative linear combinations of directed circuits in D, with coefficients in R^+ , form a normal R-semimodule S. The members of S can be regarded as the R^+ -valued circulations in D: i.e., R^+ -valued flows in D such that at each vertex the net inflow is equal to 0. For this reason we call S the *circulation semimodule* of D.

Example 8. Over an ordered field K, any finitely generated K-semimodule which contains no nonzero linear subspace is a normal K-semimodule. (See Section 6.)

Example 9. Over any ordered domain R, the nonnegative solutions to a system of linear homogeneous equations form a normal R-semimodule.

Example 10. Let G be a graph and let R be an ordered domain. A magic R^+ -labeling of G is a labeling of the edges of G by members of R^+ , such that the sum of the values at each vertex is the same. (Thus a magic labeling of a complete bipartite graph is equivalent to a "magic rectangle", or a non-negative matrix in which each row and each column have the same coordinate sum.) The magic R^+ -labelings of G form a normal R-semimodule.

Our main result (Theorem 1) is a classification of the isomorphism types of normal semimodules over a suitable ordered domain.

3. Good ordered domains. Call an ordered integral domain *good* if and only if it has no nonzero bounded ideals. Equivalently, R is good if and only if for each nonzero $\alpha \in R$ there exists $\beta \in R$ such that $\alpha\beta \ge 1$. Thus an ordered field is always good.

Every ordered domain R has a unique largest bounded ideal I, consisting of all $\alpha \in R$ for which the principal ideal αR is bounded. It is easily verified that I is a prime and that R/I, appropriately ordered, is a good ordered domain.

The ordering on an ordered domain R extends uniquely to the fraction field K of R:

$$\frac{\alpha}{\beta} \leq \frac{\gamma}{\delta} \quad (\beta, \, \delta > 0) \text{ if and only if } \alpha \delta \leq \gamma \beta.$$

It is easily seen that R is good if and only if it contains arbitrarily large members of K. Thus, for example, any subring of an archimedean ordered field is good. On the other hand if K is a nonarchimedean ordered field then the subring

$$\{\alpha \in K: -n \leq \alpha \leq n \text{ for some } n \in \mathbf{Z}\}\$$

is bad. Thus for a specific example of a bad ordered domain, order the function field $\mathbf{Q}(x)$ by setting f(x)/g(x) > 0 if and only if the leading coefficients of f and g have the same sign; then the subring

 $\{f/g: \deg(f) \leq \deg(g)\}$

is bad. This is in fact an example of a bad ordered local Dedekind domain.

We note that if R is any ordered domain, good or bad, then the polynomial ring R[x], ordered so that f(x) > 0 if and only if its leading coefficient is > 0, is good. So is any non-constant subring of R[x].

4. Normal semimodules as kernels. Let R be an ordered domain and let F be a free semimodule over R. As we have noted, a subsemimodule S is a normal semimodule of F (briefly, S is normal in F) if and only if S is the kernel of some R^+ -linear homomorphism from F to some R-module. (Clearly such homomorphisms are determined by arbitrary mappings of the basis.) Our classification of normal semimodules will involve representing them as kernels; however it will be necessary to consider representations slightly more general than the above.

Define a *semi-ideal* in R to be $I^+ = I \cap R^+$, where I is an ideal. Call a semimodule over R quasi-free if and only if it is isomorphic to a direct sum of semi-ideals. Thus free implies quasi-free, and the converse is true if and only if R is a principal ideal domain. It is easy to see that if Q is a quasi-free R-semimodule and $Q \to M$ is an R^+ -linear homomorphism to an R-module M, then the kernel S is a normal semimodule: Q can be

embedded in a free semimodule F in an obvious way (although not uniquely) such that S is normal in F. Thus up to isomorphism the normal semimodules are the same as the kernels of mappings of the form $Q \rightarrow M$. We will show that over a good ordered domain, every normal semimodule has a canonical representation as such a kernel. This will provide the classification of isomorphism types.

Thus, for a given normal semimodule S, we wish to consider embeddings $\epsilon: S \to Q$ of S into quasi-free semimodules, such that the image is normal in Q. Equivalently, the image is the kernel of some R^+ -homomorphism $Q \to M$. Call such a mapping ϵ a *normal embedding*. The following criterion will be useful:

Let $\epsilon: S \to Q$ be an R^+ -homomorphism, where S is normal and Q is quasi-free. Then ϵ is a normal embedding if and only if

$$\forall s, t \in S, \ \epsilon(s) - \epsilon(t) \in Q \Rightarrow s - t \in S.$$

It is clear that a normal embedding satisfies this condition. Conversely, assuming this condition holds, note first that ϵ must be an embedding; thus we can identify S with its image in Q. The module M can then be defined as $\langle Q \rangle / \langle S \rangle$, where $\langle Q \rangle$ is the R-module generated by Q (the obvious direct sum of ideals) and $\langle S \rangle$ is the submodule generated by S.

In general, for a normal semimodule S, we let $\langle S \rangle$ denote the difference module of S (defined as the set of all differences s - t with the obvious identifications and module structure). When $S_1 \subset S_2$, we have $\langle S_1 \rangle \subset$ $\langle S_2 \rangle$ in an obvious way. It is clear that this notation is consistent with that of the previous paragraph.

5. The representation theorem. We assume in this section that R is a good ordered domain. Let Q be a quasi-free R-semimodule; i.e., Q is a direct sum $\bigoplus_p I_p^+$ where the I_p are nonzero ideals and p ranges over some index set. For each index p, let π_p denote the projection $Q \rightarrow I_p^+$ on the *pth* coordinate and let Q^p denote the kernel of this projection.

Now let $\phi: Q \to M$ be an R^+ -homomorphism from Q to some R-module M. Call ϕ strongly surjective if each Q^{ρ} maps onto M. Thus, for example, the \mathbb{Z}^+ -homomorphism $(\mathbb{Z}^+)^3 \to \mathbb{Z}$ sending (a, b, c) to a + b - c is surjective but not strongly: when the third coordinate is removed the mapping is no longer surjective.

THEOREM 1 (Representation Theorem for Normal Semimodules). Every normal semimodule S over a good ordered domain R is isomorphic to the kernel of a strongly surjective R^+ -homomorphism $\phi: Q \to M$, where Q is a quasi-free R-semimodule and M is an R-module. Moreover ϕ is unique in the sense that if S is also isomorphic to the kernel of another such mapping $\phi': Q' \to M'$, then there are isomorphisms $Q \to Q'$ and $M \to M'$ making the diagram commute:



It is helpful to establish some alternative characterizations of strong surjectivity. Let R be a good ordered domain, $Q = \bigoplus_p I_p^+$ a quasi-free Rsemimodule with all $I_p^+ \neq 0$, and adopt the following notation: For $x \in Q$, x_p denotes the *pth* coordinate $\pi_p(x)$. For $S \subset Q$, $S^p = S \cap Q^p$. Moreover Q is partially ordered in an obvious way: $x \leq y$ if and only if y = x + z for some $z \in Q$. For a finite subset $X \subset Q$, let inf (X) denote the greatest lower bound of the members of X.

LEMMA 1. Let $\phi: Q \to M$ be an R^+ -homomorphism into an R-module M and let S be the kernel of ϕ . Then the following conditions are equivalent:

(1) ϕ is strongly surjective onto a submodule of M.

(2) $\pi_p(S) = I_p^+$ for each index p, and the S^p are pairwise non-nested. (3) For each index p and for each $x \in Q$, there exists $s \in S$ such that $s \ge$

 $x \text{ and } s_p = x_p.$

(4) $\dot{Q} = \{\inf(X): X \subset S, X \text{ finite}\}.$

Proof of lemma. (1) \Rightarrow (2): Fix an index p and any $\alpha \in I_p^+$. Taking any $x \in Q$ with $x_p = \alpha$, use the strongly surjective property to obtain $y \in Q^p$ with $\phi(y) = -\phi(x)$. Then $s = x + y \in S$ and $s_p = \alpha$.

Now take any two distinct indices p and q and fix any $x \in Q^p - Q^q$. By the strongly surjective property, $-\phi(x) = \phi(y)$ for some $y \in Q^p$. Then $x + y \in S^p - S^q$.

 $(2) \Rightarrow (3)$: Start with any $t \in S$ such that $t_p = x_p$. For each index q such that $x_q > 0$, fix a member of $S^p - S^q$. The desired element s is then formed by adding a linear combination of these elements to t.

(3) \Rightarrow (4): If $x \in Q$, take any $t \in S$ such that $t \ge x$ and for each of the finitely many p for which $t_p > 0$, take s as in (3). Then x is the inf of t and these elements s.

 $(4) \Rightarrow (3)$: This is obvious.

 $(3) \Rightarrow (1)$: To show that the image of ϕ is actually a submodule of M, it is enough to show that if $\phi(Q)$ contains m then it also contains -m. Let $\phi(x) = m$ and take s as in (3). Then $y = s - x \in Q$ and $\phi(y) = -m$.

Now fix any $m \in \phi(Q)$ and any index p. Let $\phi(x) = -m$ and take s as in (3). Then $y = s - x \in Q^p$ and $\phi(y) = m$.

Proof of Theorem 1. First we establish the existence of such a ϕ . Fix a normal embedding $\epsilon: S \to Q$ of S in a quasi-free R-semimodule $Q = \bigoplus_p I_p^+$ where the I_p^+ are nonzero semi-ideals. For each set of indices E, let Q^E denote the intersection of the Q^p , $p \in E$. Then Q^E is isomorphic to the quasi-free semimodule $\bigoplus_{p \notin E} I_p^+$. There is an obvious mapping

$$\epsilon^E: S \to Q^E$$

.....

obtained by composing ϵ with the mapping $Q \rightarrow Q^E$ which replaces all E-coordinates with 0. We claim that there is a maximal subset E such that ϵ^{E} is a normal embedding.

Let $\{E_{\lambda}\}$ be a nested family such that each $\epsilon^{E_{\lambda}}$ is a normal embedding, and let E be the union of the E_{λ} . We must show that ϵ^{E} is a normal embedding. Fix $x, y \in S$ such that

$$\epsilon^{E}(x) - \epsilon^{E}(y) \in Q^{E}.$$

(As noted before, it is enough to show that $x - y \in S$ in this situation.) Letting z_p denote the *pth* coordinate of any $z \in Q$, we have

$$\epsilon(x)_p \ge \epsilon(y)_p$$
 for all $p \notin E$;

moreover $\epsilon(x)_p = \epsilon(y)_p = 0$ for all but finitely many p. It follows that some E_{λ} contains all p for which $\epsilon(x)_p < \epsilon(y)_p$. This means that

$$\epsilon^{E_{\lambda}}(x) - \epsilon^{E_{\lambda}}(y) \in Q^{E_{\lambda}}.$$

Since $\epsilon^{E_{\lambda}}$ is a normal embedding, it follows that $x - y \in S$.

Thus by Zorn's Lemma there is a maximal E, such that ϵ^{E} is a normal embedding. This shows that there is no loss of generality in assuming from the beginning that the empty set is maximal. (In other words, throw away all factors I_p^+ , $p \in E$, and let Q denote the sum of the remaining factors.) Thus we can assume that for each p, the mapping $\epsilon^p: S \to Q^p$ fails to be normal embedding. We simplify notation further by considering S to be a subset of Q. Then the difference module $\langle S \rangle$ is contained in $\langle Q \rangle = \bigoplus_p I_p$, and we have $\langle S \rangle \cap Q = S$. We write z_p to denote the *pth* coordinate of any $z \in \langle Q \rangle$.

We can assume that each projection π_p sends $\langle S \rangle$ onto I_p . (If not, replace I_p by the image of this projection.)

Now consider the natural mapping

$$\phi: Q \to \langle Q \rangle / \langle S \rangle.$$

Clearly the kernel is S. We show that ϕ is strongly surjective by establishing condition (2) of Lemma 1.

It is helpful to observe first that for each index p, the difference module $\langle S \rangle$ contains an element u such that $u_p < 0$ while all $u_q \ge 0$ for $q \ne p$. This is because the mapping $\epsilon^p: S \rightarrow Q^p$ is not a normal embedding. By the criterion given previously, S must contain elements x and y such that

$$\epsilon^p(x) - \epsilon^p(y) \in Q^p$$
 but $x - y \notin S$.

Then u = x - y has $u_q \ge 0$ for all $q \ne p$. If also $u_p \ge 0$, then u would be in $\langle S \rangle \cap Q = S$. Thus u has the required property.

Now we show that $\pi_p(S) = I_p^+$. Taking any $\alpha \in I_p^+$, we have

 $s_p - t_p = \alpha$ for some $s, t \in S$.

Take $u \in \langle S \rangle$ as above and obtain $\beta \in R^+$ such that $\beta(-u_p) \ge 1$. Consider the element

 $v = s - (1 + \beta u_p)t + \beta t_p u.$

It is easily verified that $v_p = \alpha$ and $v \in \langle S \rangle \cap Q = S$. This proves that $\pi_p(S) = I_p^+$ for each index p.

Now fix any two indices p and q and take any $s \in S - S^q$ (which is possible since $\pi_q(S) \neq 0$). Taking u as above, set

 $t = s_p u - u_p s.$

Then $t_p = 0$ and $t \in \langle S \rangle \cap Q = S$, so $t \in S^p$. Moreover $t \notin S^q$. That completes the existence part of the proof.

For uniqueness, suppose S is the kernel of a strongly surjective R^+ -homomorphism $\phi: Q \to M$, where Q is a quasi-free R-semimodule and M is an R-module. We will reconstruct Q, M and ϕ from the internal structure of S.

Definition. A face of S is a subsemimodule U of S having the property

 $s, t \in S, s + t \in U \Rightarrow s, t \in U.$

This terminology is suggested by the case in which R is the field of real numbers and S is a convex polyhedral cone.

LEMMA 2. The faces of S are the sets $S^E = S \cap Q^E$, where E denotes a set of indices.

Proof. It is clear that each S^E is a face of S. Conversely, if U is a face of S there is a unique largest E such that $U \subset S^E$. (This is obvious since $S^{E_1 \cup E_2} = S^{E_1} \cap S^{E_2}$.) Then for each $p \notin E$ there exists an element u(p)

such that $(u(p))_p > 0$. Multiplying u(p) by an appropriate member of R^+ , we can assume that $(u(p))_p \ge 1$. Now take any $s \in S^E$. Set

$$u = \sum_{p \notin E} s_p u(p)$$

(this is a finite sum since almost all $s_p = 0$). Then

 $u \in U$ and $u - s \in \langle S \rangle \cap Q = S$.

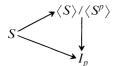
Since U is a face, we obtain $s \in U$. Thus $U = S^{E}$.

(We note for future purposes that this lemma does not depend on ϕ being strongly surjective.)

Now consider the maximal (proper) faces of S. Lemma 2 shows that each of these is of the form $S^p (= S^{\{p\}})$ for some index p, and Lemma 1 shows that the S^p are pairwise non-nested. It follows that all S^p are maximal faces. As p runs through the indices, S^p runs through the maximal faces of S. Thus, for example, the number of indices is uniquely determined by S. Much more is true, however. By Lemma 1 the *pth* coordinate mapping $\pi_p: S \to I_p^+$ is surjective; it follows that the corresponding mapping of difference modules $\langle S \rangle \to I_p$ is surjective. We claim that its kernel is just $\langle S^p \rangle$: Fixing $u, v \in S$ such that $(u - v)_p = 0$, let $x = \epsilon^p(u)$ and take s as in condition (3) of Lemma 1. Then $s \in S^p$. Moreover if we set t = s - u + v then $t_p = 0$ while $t_q \ge 0$ for all $q \neq p$. Then $t \in \langle S \rangle$ $\cap Q = S$, hence $t \in S^p$. Finally,

$$u - v = s - t \in \langle S^p \rangle.$$

We now have an isomorphism $\langle S \rangle / \langle S^p \rangle \rightarrow I_p$. Since the diagram



is commutative, it follows that the image of S in $\langle S \rangle / \langle S^p \rangle$, which we denote by $(\langle S \rangle / \langle S^p \rangle)^+$, is isomorphic to the semi-ideal I_p^+ . Recalling that the S^p are the maximal faces of $\cdot S$, we conclude that

$$Q' = \bigoplus_F (\langle S \rangle / \langle F \rangle)^+$$

where F runs through the maximal faces of S, is a quasi-free semimodule and there is an obvious isomorphism $Q' \rightarrow Q$. There is a canonical mapping $S \rightarrow Q'$, and the diagram



commutes. This shows that $S \rightarrow Q'$ is a normal embedding, hence the image of S in Q' is the kernel of the canonical mapping

$$\phi': Q' \to M' = (\bigoplus_F \langle S \rangle / \langle F \rangle) / \langle S \rangle$$

where $\langle S \rangle$ is embedded in the direct sum in the obvious way. There is an obvious isomorphism $M' \to M$, and the diagram



commutes. This proves that ϕ' is strongly surjective. Finally we note that Q', M', and ϕ' are constructed entirely from S, without reference to Q, M, and ϕ . That completes the proof.

We note that the individual factors I_p^+ of a quasi-free Q are uniquely determined as the minimal nonzero faces of Q. (This follows from Lemma 2.) This shows that strong surjectivity is an invariant property of a mapping from Q, not depending on a particular representation of Q as a direct sum. (In fact we have shown that there is only one such representation.)

Theorem 1 shows that a normal semimodule S over a good ordered domain is classified up to isomorphism by its associated strongly surjective mapping $\phi: Q \to M$ (more precisely, by the isomorphism class of ϕ). Clearly M, which we call the *comodule* of S, measures the deviation from quasi-freeness: S is quasi-free if and only if M = 0. Moreover S is free if and only if M = 0 and Q is free.

A consequence of the proof of Theorem 1 is an intrinsic criterion for a given semimodule to be a normal semimodule: S has a normal embedding in a quasi-free semimodule if and only if the mapping

 $S \to \bigoplus_F \left(\langle S \rangle / \langle F \rangle \right)^+$

is such an embedding, where F ranges over the maximal faces of S and + indicates the image of S in $\langle S \rangle / \langle F \rangle$. Thus, for example, we see that the multiplicative Z-semimodule {1, 2, 4, 6, ..., 2n, ...} is not normal, since every nontrivial face contains 2. As another example, the **R**-semimodule

$$\{(x, y) \in \mathbf{R}^2 : x, y > 0\} \cup \{(0, 0)\}$$

has no nontrivial proper faces, hence 0 is the only maximal face. But

$$(\langle S \rangle / \langle 0 \rangle)^+ = S,$$

which is not isomorphic to a semi-ideal. Hence S is not a normal semimodule. Finally, in the case of the unrestricted direct product $S = \mathbf{Z}^+ \times \mathbf{Z}^+ \times \ldots$ (in which elements can have infinitely many nonzero coordinates), the mapping

$$S \to \bigoplus_{F} \left(\langle S \rangle / \langle F \rangle \right)^+$$

cannot even be defined. In general, we have a necessary condition for a semimodule S to be normal: Each $s \in S$ must be in all but finitely many of the maximal faces.

A simpler set of criteria for normality, when S is finite dimensional, is given in Section 6.

Assume again that S is a normal semimodule isomorphic to the kernel of a strongly surjective mapping $\phi: Q \to M$. The embedding $S \to Q$ will be called the *canonical embedding* of S, and ϕ the *canonical mapping*. We describe the canonical mappings for some of the examples given earlier:

Example 1.

$$S = \{ (m, n): m \equiv n \pmod{2} \}$$
$$\mathbf{Z}^+ \bigoplus \mathbf{Z}^+ \to \mathbf{Z}_2 \text{ (integers mod 2)}$$
$$\phi(m, n) = m + n.$$

Example 2.

$$S = \{1, 5, 9, \dots\}$$

$$\{1, 3, 5, \dots\} \to \mathbb{Z}_2$$

$$\phi(n) = \begin{cases} 0 \text{ if } n \equiv 1 \pmod{4} \\ 1 \text{ if } n \equiv -1 \pmod{4} \end{cases}$$

Example 3.

 $S = \{$ nonzero principal ideals in a Dedekind domain $\}$ $\{$ all nonzero ideals $\} \rightarrow$ ideal class group $\phi(I) =$ class of I. To verify that ϕ is strongly surjective, consider condition (3) of Lemma 1. This requires that if *I* is any nonzero ideal and *P* is any prime, then *I* divides some principal ideal (α) such that both *I* and (α) are exactly divisible by the same power of *P*. Any $\alpha \in I - IP$ satisfies this condition.

The above shows that the ideal class group of a Dedekind domain and the number of primes in each class are completely determined by the multiplicative structure of the domain. In the case of the algebraic integers in a number field, each class contains infinitely many primes; thus two number fields have isomorphic ideal class groups if and only if their principal ideal semigroups (nonzero element under multiplication, modulo units) are isomorphic.

Examining the construction of the canonical embedding of S, we recall that the generators of Q correspond to maximal faces of S. In Example 3 above, these maximal faces are easily seen to be the complements of nonzero prime ideals of the Dedekind domain, modulo units. In the case of a Krull domain, the maximal faces of S are the complements of the minimal nonzero prime ideals, modulo units. Thus our construction is equivalent in this case to the well-known construction of the prime divisors of a Krull domain from the minimal nonzero prime ideals. [2, p. 486].

Example 4.

 $S = \{ \text{monic polynomials over a field } F \text{ with constant term 1} \}$ $\left\{ \begin{array}{l} \text{all monic polynomials over } F \\ \text{with } f(0) \neq 0 \end{array} \right\} \rightarrow \text{multiplicative group of } F$ $\phi(f) = f(0).$

Replacing "constant term 1" with "second coefficient 0", we have

{all monic polynomials over F} \rightarrow additive group of F

 $\phi(f) =$ second coefficient.

We leave it to the reader to verify strong surjectivity in both cases.

Example 5.

 $S = \{\text{non-negative real solutions to } x_1 + x_2 = x_3 + x_4\}$ $(\mathbf{R}^+)^4 \rightarrow \mathbf{R}$

 $\phi(x_1, x_2, x_3, x_4) = x_1 + x_2 - x_3 - x_4.$

The sequence of images (1, 1, -1, -1) of the standard basis vectors in $(\mathbf{R}^+)^4$ essentially constitutes the Gale diagram of a square cross-section of S; more precisely, they constitute the Gale diagram of the dual polytope of such a cross-section. In general, for any finitely generated normal **R**-semimodule S, the images of the standard basis vectors under the canonical mapping associated with S constitute the Gale diagram of the dual polytope of a cross-section of S. The strong surjectivity condition corresponds to the fact that the points of the Gale diagram of a convex polytope form a positive 2-spanning set for their linear span V: i.e., if any point is removed, the remaining ones span V with nonnegative coefficients. (See [4] or [7].)

Example 6. The following reduction process transforms G into a 3-edge-connected graph having, up to isomorphism, the same circuit module and circuit semimodule.

If G is not connected, fix a point in each component and identify these points;

If G is connected and contains an edge whose removal disconnects G, remove this edge and identify its endpoints;

If G is 2-edge-connected and contains two edges whose removal disconnects G, remove one of these edges and identify its endpoints.

Thus every circuit semimodule is isomorphic to the circuit semimodule of a 3-edge-connected graph. Assuming that G is 3-edge-connected, let I be the incidence matrix of G: We define I to have 1 in row i and column j if edge j is not a loop and is incident with vertex i, and 0 otherwise. Let x_1, \ldots, x_m denote the columns of I, considered as vectors over \mathbb{Z}_2 . The x_i are in a hyperplane $H \subset (\mathbb{Z}_2)^n$, where n is the number of vertices in G. The mapping

$$(\mathbf{Z}^+)^m \to H$$

in which the standard basis vectors go to the x_i , is the canonical mapping for the circuit semimodule S of G. In particular, S contains 2e for each edge e of G. This is a consequence of Menger's Theorem on edge-disjoint paths [1, p. 204]: the endpoints of e are joined by two edge-disjoint paths not including e.

Theorem 1 shows that if two 3-edge-connected graphs have isomorphic circuit semimodules, then there is a circuit-preserving bijection between their edge sets. (Note that this is not true if the circuit semimodule is replaced by the circuit module.)

Example 7. A digraph D is *strongly connected* if there exists a directed path from any vertex to any other vertex. D is *strongly k-edge-connected* if

it remains strongly connected after removal of any k - 1 edges. The following reduction process transforms D into a strongly 2-edge-connected digraph having, up to isomorphism, the same circulation semimodule:

Remove all edges which do not occur in directed circuits;

If D is not connected, fix a point from each component and identify these points;

If D is strongly connected and contains an edge whose removal destroys strong connectivity, remove this edge and identify its endpoints.

Assuming that D is strongly 2-edge-connected, let I be the incidence matrix of D. I has 1 (resp -1) in row i and column j if edge j is not a loop and terminates (resp. initiates) at vertex i, and 0 otherwise. The columns of I are in the submodule H of \mathbb{R}^n consisting of points whose coordinate sum is 0, and the mapping

 $(R^+)^m \to H$

(defined as in Example 6) is the canonical mapping for the circulation semimodule of D. Theorem 1 shows that if two strongly 2-edge-connected digraphs have isomorphic circulation semimodules, then there is a bijection between their edge sets which preserves directed circuits.

6. Finite dimensional normal semimodules. An R-semimodule S is *finite dimensional* if it can be embedded (not necessarily normally) in a free module R^n of finite rank. In that case the *dimension* of S is defined to be the smallest n for which such an embedding exists. For finite dimensional R-semimodules there is a relatively simple set of criteria for normality:

THEOREM 2. Let S be a finite dimensional semimodule over an ordered domain R. Then S is a normal R-semimodule if and only if

(1) $\{0\}$ is a face of S;

(2) S has a subsemimodule S_0 which is finitely generated over R^+ and such that for each $s \in S$, there exists $\alpha \in R$, $\alpha > 0$, such that $\alpha s \in S_0$;

(3) If s, $t \in S$ and $\alpha \in R$, $\alpha > 0$, such that $\alpha(s - t) \in S$, then $s - t \in S$.

Remark 1. These conditions are intrinsic, not depending on an embedding of S in a free module. The difference module $\langle S \rangle$, in which condition (3) is to be understood, depends only on S.

Remark 2. When R is a field, condition (3) become superfluous and condition (2) requires that S be finitely generated. Condition (1) says that S contains no nonzero linear subspace. These conditions for normality

170

over a field have been observed before, at least for the case $R = \mathbf{R}$ [3, Theorem 3].

Remark 3. It can be shown that every finite dimensional normal **Z**-semimodule is finitely generated over \mathbf{Z}^+ . Thus, for a semigroup of monomials in a finite set of variables, normality is equivalent to being finitely generated and satisfying the multiplicative analog of condition (3), in which α becomes a positive integral exponent. This equivalence is proved as part of Proposition 1 in [5].

Proof of Theorem 2. Assuming first that S is normal, let $S \subset (R^+)^n$ be a normal embedding of S in a free R-semimodule, so that

$$S = (R^+)^n \cap \langle S \rangle.$$

It is not assumed that n is finite, although we will see below that n can be taken to be finite.

Condition (1) is equivalent to the condition that if S contains both s and -s, then s = 0. It is clear that this holds.

To establish (2), let K be the fraction field of R and consider R^n to be embedded in the vector space K^n in the obvious way. The vector subspace V spanned by S consists of elements $(s - t)/\alpha$, where $s, t \in S$ and $\alpha \in R$, $\alpha > 0$. The fact that S is finite dimensional is easily seen to imply that V is finite dimensional. Since points of K^n have only finitely many nonzero coordinates, it follows immediately that n can be taken to be finite. It is well known that the positive cone $V^+ = V \cap (K^+)^n$ of a linear subspace V of K^n (n finite) is finitely generated over K^+ . Multiplying the members of a finite generating set by positive scalars so that they become members of S, we obtain generators for the desired S_0 .

Finally, it is clear that (3) holds.

Now suppose conditions (1)-(3) are satisfied and $S \,\subset\, \mathbb{R}^n$ is an embedding of S in a free module of finite rank. As above, we consider \mathbb{R}^n to be embedded in \mathbb{K}^n in the obvious way and define V to be the vector subspace spanned by S. Members of V are of the form $(s - t)/\alpha$ as before. Now, however, define V^+ to be the set of all s/α with $s \in S$, $\alpha \in \mathbb{R}$, $\alpha > 0$. Conditions (1) and (2) imply that V^+ is finitely generated over \mathbb{K}^+ and contains no nonzero linear subspace. It is a classical result, when $\mathbb{K} = \mathbb{R}$, that V^+ is the intersection of finitely many half-spaces in V, where by a half-space we mean one of the two closed regions bounded by a hyperplane (linear subspace of codimension 1) in V. Weyl [8] gives a proof of this which is valid over any ordered field. For each of these finitely many half-spaces H_1, \ldots, H_m , let f_i be a linear functional on V such that H_i is

the set of points at which f_i is nonnegative. Taking the f_i as coordinate mappings, we obtain a mapping

 $f: V^+ \to (K^+)^m$

which is easily seen to be a normal embedding. (The fact that it is an embedding follows from the fact that V^+ contains no nonzero linear subspace.) Identifying V^+ with its image under f, we have

$$V^+ = (K^+)^m \cap V.$$

Clearly f extends to a linear mapping on all of K^n and the image $f(R^n)$ is a finitely generated R-submodule of K^n . It follows that $\alpha f(S)$ is contained in R^m for some $\alpha \in R$, $\alpha > 0$. Replacing f with αf and identifying S with its image in R^m , we have $S \subset (R^+)^m$ since $S \subset V^+ \subset (K^+)^m$. Then

$$S \subset \langle S \rangle \cap (R^+)^m \subset \langle S \rangle \cap V \cap (K^+)^m = \langle S \rangle \cap V^+ \subset S$$

with the last containment following from condition (3).

We note that the vector space V and the embedding of S in V are independent of the embedding of S in \mathbb{R}^n , being equivalent to the universal construction

 $S \subset \langle S \rangle \bigotimes_R K = V.$

Moreover the dimension of V is easily seen to be equal to the dimension d of S since for any embedding $S \subset \mathbb{R}^d$, the module $\langle S \rangle$ necessarily contains nonzero points on each of the d coordinate axes R_i . (If it did not, then S would be mapped isomorphically into a quotient module $\mathbb{R}^d/\mathbb{R}_i \cong \mathbb{R}^{d-1}$.)

The last part of the proof of Theorem 2 shows that if S is a 2-dimensional normal semimodule, then in fact S has a normal embedding in $(R^+)^2$. We will use this fact in Section 7 to give an explicit classification of the 2-dimensional normal semimodules over a good ordered Dedekind domain.

7. 2-dimensional normal semimodules over a Dedekind domain. As observed in Section 6, the proof of Theorem 2 shows that every 2-dimensional normal *R*-semimodule *S* can be normally embedded in $(R^+)^2$. It follows that *S* is isomorphic to the kernel of a strongly surjective mapping

 $\phi: I^+ \oplus J^+ \to M$

where I^+ and J^+ are semi-ideals in R and M is an R-module. The strongly surjective condition says that both restrictions $I^+ \to M$ and $J^+ \to M$ are

surjective. Assuming that R is a Dedekind domain, we will describe all such mappings ϕ and give a criterion for two of these to have isomorphic kernels.

THEOREM 3. If R is a good ordered Dedekind domain, then every 2-dimensional normal R-semimodule is isomorphic to a semimodule of the form

$$S(A, I, J) = \{ (x, y) \in I^+ \oplus J^+ : x + y \in A \}$$

where A, I and J are nonzero R-ideals with I and J each relatively prime to A.

Proof. We note first that if

 $I^+ \to M$

is a surjective mapping from a semi-ideal I^+ to an *R*-module *M*, then *M* is necessarily isomorphic to R/A for some nonzero *A*. (The induced mapping $I \rightarrow M$ is surjective, hence *M* is isomorphic to I/I_0 for some ideal $I_0 \subset I$; moreover $I_0 \neq 0$ since $I^+ \rightarrow M$ is surjective. Finally, I/I_0 is isomorphic to R/A, where $I_0 = IA$.) Thus every 2-dimensional normal *R*-semimodule is isomorphic to the kernel of a strongly surjective mapping

 $\phi: I^+ \oplus J^+ \to R/A$

for some nonzero ideals I, J and A. Moreover the restrictions

 $I^+ \rightarrow R/A$ and $J^+ \rightarrow R/A$

can be assumed to be the obvious natural mappings:

LEMMA. Let A and I be nonzero ideals in a good ordered Dedekind domain R, and let

 $f:I^+ \to R/A$

be a nonzero R^+ -homomorphism. Then there is an ideal I' and an isomorphism ${I'}^+ \to I^+$ such that the composition

 $I'^+ \to I^+ \to R/A$

is the natural mapping, sending each $x \in I'^+$ to the coset x + A.

Proof. We claim first that every ideal class contains an ideal which is relatively prime to A. To see this, fix an ideal J in the inverse class and let the P_i range over the prime divisors of A. For each i, let $P_i^{a_i}||J|$ and use the Chinese remainder theorem to obtain an element $\alpha \in J$ which is not in

any of the ideals $P_i^{a_i+1}$. Write (α) = JJ'; then J' is in the original ideal class, and J' is relatively prime to A.

Using the above, obtain an ideal J' in the class of I, such that J' is relatively prime to A. Thus A + J' = R. Fix $\alpha \in A$, $\beta \in J'$ such that $\alpha + \beta = 1$, and compose f with an isomorphism $J'^+ \rightarrow I^+$ to obtain a mapping

 $f':J'^+ \to R/A.$

Extending f' to all of J' in the obvious way, we have for each $\gamma \in J'$

$$f'(\gamma) = f'((\alpha + \beta)\gamma) = \alpha f'(\gamma) + \gamma f'(\beta) = \gamma f'(\beta).$$

Write $f'(\beta) = \delta + A$ with $\delta > 0$. (This is possible because *R* is good.) Finally, set $I' = \delta J'$ and map $I'^+ \to J'^+$ by dividing everything by δ . Then the composition $I'^+ \to R/A$ is the natural mapping.

The lemma shows that we can assume that the mapping ϕ sends the pair (x, y) to the coset x + y + A. Thus the kernel of ϕ is S(A, I, J). Finally, it is clear that I and J are relatively prime to A since the natural mappings $I^+ \rightarrow R/A$ and $J^+ \rightarrow R/A$ are surjective.

Next we establish a criterion for two semimodules of the form S(A, I, J) to be isomorphic. It is clear that A is an invariant of S = S(A, I, J) since it is the annihilator of R/A, which is uniquely determined as the comodule of S. Thus it remains to determine how I and J can vary.

It is helpful to introduce the group G_A , for a given nonzero ideal A, defined as the quotient group

 $(R/A)^*/U^+$

where $(R/A)^*$ is the unit group of the quotient ring R/A, and U^+ is the subgroup consisting of the cosets u + A, where u is a positive unit in R. Let K be the fraction field of R and note that every principal fractional ideal (x) in K, relatively prime to A, determines a unique member of G_A as follows: Each such (x) can be generated by an element of the form α/β , α , $\beta \in R$, such that both (α) and (β) are relatively prime to A. (This follows from the fact that every ideal class contains an ideal which is relatively prime to A, as shown in the proof of the lemma for Theorem 3.) Moreover α/β can be taken to be positive. The elements of α and β determine members of $(R/A)^*$; take the quotient of these. Finally, reduce mod U^+ so that the result is uniquely determined by (x).

We have defined a mapping

 $\theta_A: P_A \to G_A$

where P_A is the group of principal fractional ideals in K which are relatively prime to A.

Let $I \sim J$ indicate that two ideals I and J are in the same class. Then we have

THEOREM 4. S(A, I, J) is isomorphic to S(A', I', J') if and only if A = A' and either

(1) $I \sim I', J \sim J', and$

$$\theta_A(I/I') = \theta_A(J/J')$$

or

(2) $I \sim J', J \sim I', and$

$$\theta_A(I/J') = \theta_A(J/I').$$

Proof. By Theorem 1, the semimodules are isomorphic if and only if there are isomorphisms (the vertical mappings) making the following diagram commute:

$$I^{+} \oplus J^{+} \longrightarrow R/A$$

$$\downarrow \qquad \qquad \downarrow \qquad \qquad \downarrow$$

$$I^{\prime^{+}} \oplus J^{\prime^{+}} \longrightarrow R/A$$

Such isomorphisms require either

(1) isomorphisms $I^+ \to I'^+$ and $J^+ \to J'^+$ (necessarily multiplication by members of K^+ , each of which is a quotient α/β with α and β members of R which are relatively prime to A), both of which induce the same mapping $R/A \to R/A$ (automatically an isomorphism); or

(2) isomorphisms $I^+ \to J'^+$ and $J^+ \to I'^+$ both inducing the same mapping $R/A \to R/A$.

Finally, these isomorphisms exist if and only if the conditions of Theorem 4 are satisfied.

The result simplifies in the case of a principal ideal domain: The semimodules are isomorphic if and only if A = A' and the elements $\theta_A(I/J)$ and $\theta_A(I'/J')$ (which are always defined) are either the same or inverses of each other. Thus, over a good PID, the 2-dimensional normal semimodules are classified according to the pair

$$(A, \theta_A(I/J))$$

with two pairs (A, x) and (A', y) corresponding to isomorphic semimodules if and only if A = A' and $x = y^{\pm 1}$.

It is convenient to reformulate this result using the following notation: If α and β are nonzero relatively prime members of a good ordered PID, let $S(\alpha, \beta)$ denote the kernel of the mapping

 $(R^+)^2 \rightarrow R/(\alpha)$

under which a pair (r, s) goes to the coset containing $\beta r + s$. Thus in our previous notation we have an isomorphism

$$S(\alpha, \beta) \approx S((\alpha), (\beta), (1))$$

if $\beta > 0$; if $\beta < 0$, then

$$S(\alpha, \beta) \approx S_{-}((\alpha), (\beta), (1))$$

where in general we define

$$S_{-}(A, I, J) = \{ (x, y) \in I^+ \oplus J^+ : x - y \in A \}.$$

Note that

$$S_{-}(A, I, J) \approx S(A, I, \gamma J)$$

for any $\gamma > 0$ such that $\gamma \equiv -1 \pmod{A}$.

Combining everything we have said, we obtain

COROLLARY. Let R be a good ordered PID. Then every 2-dimensional normal R-semimodule is isomorphic to some $S(\alpha, \beta)$, and we have the following criterion for two such semimodules to be isomorphic:

 $S(\alpha, \beta)$ is isomorphic to $S(\alpha', \beta')$ if and only if $(\alpha) = (\alpha')$ and the members of $G_{(\alpha)}$ determined by β and β' are the same or inverses of each other.

(In the above, we are simply taking the cosets $\beta + (\alpha)$ and $\beta' + (\alpha)$ and reducing mod U^+ . This is not the same as applying $\theta_{(\alpha)}$ to the principal ideals unless β and β' are positive.)

Example 1. When $R = \mathbb{Z}$, the semimodules S(5, 2) and S(5, 3) are isomorphic; however S(5, 1), S(5, 2) and S(5, 4) represent distinct isomorphism classes.

Example 2. When $R = \mathbb{Z}[\sqrt{2}]$, the group $G_{(3)}$ is trivial, so up to isomorphism there is only one 2-dimensional normal *R*-semimodule having comodule R/(3). On the other hand, $G_{(3-\sqrt{2})}$ has order 2; the semimodules $S(3-\sqrt{2}, 1)$ and $S(3-\sqrt{2}, -1)$ are non-isomorphic.

Example 3. Let $R = \mathbb{Z}[\omega + \omega^{-1}]$, where ω is a primitive 7*th* root of unity. The group $(R/(7))^*$ has order 294, but the classes containing the positive units $\omega + \omega^{-1}$ and $1 + \omega + \omega^{-1}$ generate everything. Thus up to

isomorphism there is only one 2-dimensional normal *R*-semimodule having comodule R/(7). However in $(R/(\omega + \omega^{-1} - 4))^*$ only half of the 70 classes contain positive units, so $G_{(\omega + \omega^{-1} - 4)}$ has order 2. The semimodules $S(\omega + \omega^{-1} - 4, 1)$ and $S(\omega + \omega^{-1} - 4, -1)$ are non-isomorphic.

Example 4. Let R = F[x], where F is any ordered field. The ordering on R is lexicographic, beginning with the leading coefficient. The group $G_{(x^2)}$ is represented by the elements $ax \pm 1$, $a \in F$. The semimodules $S(x^2, ax \pm 1)$, with $a \in F^+$, are pairwise non-isomorphic.

REFERENCES

- 1. J. A. Bondy and U. S. R. Murty, *Graph theory with applications* (American Elsevier, New York, 1976).
- N. Bourbaki, *Elements of mathematics, commutative algebra* (Addison-Wesley, Reading, Mass., 1972).
- 3. C. Davis, Remarks on a previous paper, Michigan Math. J. 2 (1953), 23-25.
- 4. B. Grünbaum, Convex polytopes (Interscience, New York, 1967).
- 5. M. Hochster, Rings of invariants of tori, Cohen-Macaulay rings generated by monomials, and polytopes, Ann. Math. 96 (1972), 318-337.
- 6. D. Marcus, *Closed factors of normal Z-semimodules*, Pacific Journal of Mathematics 93 (1981), 121-146.
- 7. —— Gale diagrams of convex polytopes and positive spanning sets of vectors, to appear in Discrete Applied Mathematics, 1984.
- 8. H. Weyl, Elementare Theorie der konvexen Polyeder, Comm. Math. Helv., 7 (1935-36), 290-306. English translation in Contributions to the theory of games, Ann. Math. Studies 24 (Princeton, 1950), 3-18.

California State Polytechnic University, Pomona, California