VIGRE Algebra QR Review, October 7, 2002

Modules and principal ideal domains

We review some definitions and facts about modules, but, for simplicity, we deal only with the case where the ring is commutative, with identity. A module M over a ring R is an abelian group $(M, +)$ together with a scalar multiplication, i.e., a map $R \times M \to M$ (where the value on (r, m) is denoted rm) such that for all $r, r' \in R$ and all $m, m' \in M$, $r(r'm) = (rr')m$, $r(m + m') = rm + rm'$ and $(r + r')m = rm + r'm$. A module is called *unital* if $1m = m$ for all $m \in M$ and we shall **always** assume this condition as well, i.e., all our modules are unital. A module over a field is the same thing as a vector space. Every (additive) abelian group can be made into a $\mathbb{Z}$-module in just one way: e.g., $3m = (1+1+1)m = 1m+1m+1m = m+m+m$ is forced. Thus, the study of $\mathbb{Z}$-modules coincides with the study of abelian groups.

A map $f : M \to Q$ of R-modules is called *R-linear* or an *R-module homomorphism* if it is a homomorphism of abelian groups and preserves scalar multiplication, i.e., $f(rm) = rf(m)$ for all $m \in M$. The set $\mathrm{Hom}_R(M, N)$ is again an R-module (with $(f+g)(m) = f(m)+g(m)$ and $(rf)(m) = r(f(m))$), and $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ is a noncommutative ring under composition: R maps to its center ($r \in R$ maps to multiplication by r). An R-submodule of M is an additive subgroup N closed under scalar multiplication. The kernel of an R-linear map $M \to Q$ is a submodule of M. If N is a submodule of M, then M/N (as an abelian group) also has the structure of an R-module, where $r[m] = [rm]$ (for $[m]$ we might write $m + N$). Every surjective R-linear map from M is like the map $M \to M/N$, where N is the kernel, up to isomorphism.

Direct sums and products of modules are defined as in the case of abelian groups. In products, multiplication by r is done coordinate-wise, while in direct sums one defines $r(m_1 \oplus \cdots \oplus m_k) = rm_1 \oplus \cdots \oplus rm_k$. The universal mapping properties are the same as in the case of abelian groups.

Expressions like $r_1m_1 + \cdots + r_km_k$ are called *R-linear combinations* of the m_j. Elements are called *(linearly) independent* over R if any linear combination of a subset of them that is 0 has all coefficients 0. (The empty set of elements is regarded as an independent set.) The *annihilator* of a module M is $\{r \in R : rm = 0 \text{ for all } m \in M\}$, and is an ideal of R. Elements *generate* or *span* a module M if every $u \in M - \{0\}$ is an R-linear combination of some of them. (The empty set spans the 0 module.) Equivalently, elements span the module M if M has no smaller submodule containing them all.

An R-module is called *free* if it is spanned by a set of elements linearly independent over R: this set of elements is called a *free basis*. An R-module is free if and only if it is isomorphic with a direct sum of copies of R. The cardinalities of any two free bases are the same: this number is called the *rank* of the free module.

Over a field, every set of elements that spans a module (here, one can say "vector space," but I will stick with the word "module") has a maximal subset that is independent, by Zorn's lemma, and this set will be a free basis. Thus, every module over a field is free. By Zorn's lemma, any independent set of elements can be extended to a free basis. In the case of a field, the rank of a module (they are all free) is called the *dimension* of the module (as a vector space). Also, in the case of a field, the word "basis" is used to mean free basis. But when the ring need not be a field, some authors use the word "basis" for any spanning set, and so it is better to say "free basis" if that is what is meant.

A module is called *finitely generated* if it has a finite spanning set. If such a set has n elements, the module is a quotient of a free module on n generators by some submodule. A module with just one generator is called *cyclic*, and is isomorphic with R/I, where I is the annihilator of the module.

A finitely generated free module has an ordered free basis $b_1, \ldots, b_n$ and this provides an isomorphism of the module with R^n (which we shall think of as $n \times 1$ column matrices) that sends $r_1 b_1 + \cdots + r_n b_n$ to the transpose of $(r_1 \ \cdots \ r_n)$. The R-linear maps from R^n to R^m then correspond bijectively with $m \times n$ matrices over R, where the matrix A gives an R-linear map by letting the value of the map on the column vector u be Au (matrix multiplication). With these conventions, composition of R-linear maps corresponds to matrix multiplication. The image of the map is the column space of the matrix, i.e., the linear combinations of the columns of the matrix. The cokernel M of the map is the quotient of R^m by the column space: we say that the matrix gives a *presentation* of M.

A module over an integral domain R is called *torsion-free* if whenever $rm = 0$ either $r = 0$ or $m = 0$.

A *principal ideal domain* or PID is an integral domain in which every ideal is principal, i.e., has just one generator. The integers, the polynomial ring in one variable over a field, and the ring of Gaussian integers, $\{a + bi : a,\, b \in \mathbb{Z}\}$ are examples. A domain is called a *Euclidean domain*[1] if there is a function $v : D - \{0\} \to \mathbb{N}$ such that whenever a, b are elements of the ring with $b \neq 0$ one can write $a = qb + r$ in such a way that either $r = 0$ or $v(r) < v(b)$. (Thus, Euclidean domains have something that resembles a division algorithm.) A Euclidean domain is always a PID: every nonzero ideal is generated by any element a in it such that $v(a)$ is minimum for the nonzero elements in the ideal. For the integers, one may let $v(a) = |a|$, for polynomials in one variable over a field one may let $v(a)$ be the degree, and for the Gaussian integers one may let $v(a + bi) = a^2 + b^2$: these three rings are Euclidean domains.

An element of a ring that is not 0 and not a unit (i.e., not invertible) is called *composite* if it is the product of two non-units. Otherwise, the element is called *irreducible*. In a PID, all nonzero non-units can be written as a products of irreducible elements, and this is unique except for the order of terms and the introduction of unit factors. I.e., a PID is a unique factorization domain. In a PID, irreducible elements are *prime*, i.e., if u is irreducible and divides ab, then either u divides a or u divides b. In fact, in a PID, a

[1] There are several variations on this definition in the literature. None of these variations has ever affected the solution of a qualifying review problem.

nonzero non-unit is prime if and only if it is irreducible. In a PID, every nonzero prime ideal is maximal.

Over a principal ideal domain, every finitely generated module is the direct sum of cyclic modules, and so can be represented as the direct sum of a free module (whose rank is uniquely determined) and a torsion-module, i.e., one with a nonzero annihilator. The torsion module can be written uniquely (except for the order of the terms) as a direct sum of cyclic modules R/I such that each of the ideals I is *primary*, which here means that it is generated by a power of a prime element. There is also a unique decomposition (except for the order of the terms) of the torsion module as a direct sum of terms R/I_j such that the ideals I_j occurring are linearly ordered by inclusion. E.g., when the ring is $\mathbb{Z}$, one has that $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$ (the ideals (4), (3), and (9) are primary) can also be written as $\mathbb{Z}_{12} \oplus \mathbb{Z}_{36}$. Here $(36) \subseteq (12)$. A helpful fact is that if $a_1, \ldots, a_h$ are relatively prime in pairs in the PID R, then $R/(a_1 \cdots a_h) \cong R/(a_1) \oplus \cdots \oplus R/(a_h)$, which is a form of the Chinese Remainder Theorem.

Over a PID, every submodule of a free module is free (even without assuming finite generation). Every finitely generated torsion-free module is free. (Note, however, that $\mathbb{Q}$ is a torsion-free $\mathbb{Z}$-module that is not free.)

It is standard to describe a module as the cokernel of an $m \times n$ matrix C over R (equivalently, to describe it as the quotient of R^m by a submodule spanned by n elements: make these into the columns of an $m \times n$ matrix). A change of basis in either R^n or R^m gives a new matrix for C: it will have the form ACB where C is an $m \times m$ invertible matrix and B is an $n \times n$ invertible matrix. ACB is called *equivalent* to C, and its cokernel is isomorphic with the cokernel of C. Over a principal ideal domain, every $m \times n$ matrix is equivalent to a matrix whose only nonzero entries are on the main diagonal. Such a matrix is the direct sum of m cyclic modules, $R/(d_i)$, where d_i is the entry on the diagonal in the i th row. If $m > n$, then for each $i > n$ one should take $d_i = 0$ or simply include a copy of R in the direct sum.

Over a Euclidean ring such as $\mathbb{Z}$ or $k[x]$ one can find an equivalent matrix with just one nonzero diagonal by elementary row and column operations: switching two rows (hence, any permutation), or adding (or subtracting) a multiple of one row to a different row (and similarly for columns). The effect of an elementary row operation is the same as performing the operation on the identity matrix to get a matrix E, which is invertible, and then multiplying by E on the left. (For column operations multiply on the right instead.) Thus, elementary row and column operations preserve the equivalence class of a matrix. Given an $m \times n$ matrix over a Euclidean domain with v as in the definition, do such operations until one has a nonzero entry a_{11} with $v(a_{11})$ as small as possible in the upper left corner. It follows that all the other entries of the first row (and column) must be divisible by a_{11}, and so one can get the rest of the first row to be all zeros by elementary column operations, and the rest of the first column to be zeros, using elementary row operations. After that, one may continue by working with the $m-1 \times n-1$ matrix in the lower right corner.

Given a vector space V over a field k, for any linear map $T : V \to V$ there is a unique

$k[x]$-module structure on V such that multiplication by x is the same as letting T act. This is a powerful tool in analyzing square matrices over a field — more about this later.

Problems new this week

1. Let R be the principal ideal domain $k[x]$, where k is a field and x is an indeterminate. Consider the quotient M of the free R-module R^3 by the submodule N generated by the elements $(x^2,\, x^3,\, x^4)$ and $(1,\, x+1,\, x^2)$. Express M explicitly as a direct sum of cyclic modules.

2. (a) Classify the abelian groups of order 540 up to isomorphism.

(b) Can a subgroup of the symmetric group S_9 on a nine element set act transitively on a set with 25 elements? Can a group of order 75 act doubly transitively on a set with 5 elements?

3. Let M be a module over the ring $\mathbb{Q}[x]$, and assume that M is a 3-dimensional $\mathbb{Q}$-vector spaces with basis $m_1,\, m_2,\, m_3$. Assume also that x acts on M as follows:

$$xm_1 = -m_1 - 2m_2 + 6m_3,\;\; xm_2 = -m_1 + 3m_3,\;\; xm_3 = -m_1 - m_2 + 4m_3.$$

Decompose M explicitly into a direct sum of cyclic $\mathbb{Q}[x]$-modules.

4. Let $R = \mathbb{Q}[x]$ be the polynomial ring in one variable over the rational numbers, and let M be the submodule of $R \oplus_R R = R^2$ generated by $(1,\, x)$, $(x,\, x^2 + x^3)$,and $(x^2, x^2 - x^3)$. Express $N = R^2/M$ as a direct sum of cyclic R-modules. What is its annihilator?

5. Let k be a field, and x a variable over k. (a) Let $p(x),\, q(x) \in k[x]$ be relatively prime non-zero polynomials. Viewing $\dfrac{k[x]}{(p(x))}$ and $\dfrac{k[x]}{(q(x))}$ as $k[x]$-modules in the natural way, prove that $\mathrm{Hom}_{k[x]}\left(\dfrac{k[x]}{(p(x))},\, \dfrac{k[x]}{(q(x))}\right) = 0$.

(b) Let V and W be vector spaces over k. Let $A : V \to V$ and $B : W \to W$ be k-linear endomorphisms. Make V into a $k[x]$-module so that multiplication by x is the same as the action of A, and make W into a $K[x]$-module so that multiplication by x is the same as the action of B. Given a k-linear map $T : V \to W$, give a necessary and sufficient condition on T, A, and B fo T to be a homomorphism of $k[x]$-modules.

(c) Let $A = \begin{pmatrix} 0 & 0 & 3 \\ 1 & 0 & -3 \\ 0 & 1 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. Use parts (a) and (b) to show that the only 3×3 matrix T such that $TA = BT$ is the zero matrix.

6. Each of two finitely generated abelian groups is isomorphic with a subgroup of the other. Must the two groups be isomorphic? Prove that they must be isomorphic, or give a counterexample. What happens when the groups are not abelian?

7. (a) Let $I,\, J,\, ,K$ be ideals of a principal ideal domain R. Prove that $I \cap (J + K) = (I \cap J) + (I \cap K)$. (b) Find ideals $I,\, J,\, ,K$ of $S = \mathbb{C}[x, y]/(x, y)^2$ such that $I \cap (J + K) \neq (I \cap J) + (I \cap K)$. [You may assume that $(x, y)/(x, y)^2$ is a vector space of dimension 2, thought of as a module over $\mathbb{C} \cong \mathbb{C}[x, y]/(x,\, y)$.