Lecture 10-9: Free modules and linear algebra over commutative rings

October 9, 2024

The analogy between modules over rings and vector spaces over fields is especially strong for free modules over commutative rings. I will indicate the extent to which familiar linear algebra can be carried over to the setting of commutative ring rather than a field of scalars.

Last time I defined a free module of rank n over a ring R to be one isomorphic to R^n. Unlike the situation for free groups, it turns out that the rank of a free module is not well defined in general: in homework this week you will show that there is a ring R such that $R \cong R^2$ as an R-module, so that the rank of R as a module over itself could be taken to be any positive integer. For *commutative* rings R, however, this kind of bad behavior cannot occur: not only is the rank of a free module uniquely determined, but the rank of a free submodule of a free module M cannot exceed the rank of M (again unlike the situation for free groups, but this time better than that situation).

I begin by observing that, just as for vector spaces over a field, any R-homomorphism ϕ from a free R-module F to another R-module N is completely determined by the image $\phi(B)$ of a free basis B of F, which can be any subset of N (Theorem 6, p. 354); indeed, given $\phi(b_i)$ for $b_i \in B$, one can and must take $\phi(\sum_i r_i b_i)$ to be $\sum_i r_i \phi(b_i)$ for $r_i \in R$. If F has rank n and the codomain N of ϕ is also free, say of rank m, then it is convenient to encode ϕ by an $m \times n$ matrix, just as one would for a linear transformation between finite-dimensional vector spaces over a field. Fixing bases $B = \{b_1, \ldots, b_n\}$ and $B' = \{c_1, \ldots, c_m\}$ of F and N respectively, write $\phi(b_j) = \sum_{i=1}^{m} m_{ij} c_j$ for $m_{ij} \in R$. The matrix M with ijth entry m_{ij} is then called the matrix of ϕ (with respect to B and B').

The special case where $n = m$, so that the matrix M is square, is the most important one, for it turns out that the definition and basic properties of the determinant of a square matrix over a field extends without change to matrices over commutative rings (see Theorem 24, Chapter 11, p. 437). Thus $\det M$ can be inductively defined as $\sum_{j=1}^{n}(-1)^{i+j}m_{ij}\det M_{ij}$ for any fixed i, where M_{ij} denotes the cofactor matrix obtained from M by omitting its ith row and jth column; this amounts to expanding $\det M$ along the ith row of M (Theorem 29, p. 438).

Similarly, we have $\det M = \sum_{i=1}^{n} (-1)^{i+j} m_{ij} \det M_{ij}$ for any fixed j, expanding $\det M$ along its jth column. If any two rows or any two columns of M are equal, then $\det M = 0$ (Corollary 27, p. 438). One also has the product rule $\det AB = (\det A)(\det B)$ (Theorem 28, p. 439). Finally, a somewhat arcane formula from linear algebra turns out be very important in the current setting: given M, if we define the square matrix N by decreeing that its jith entry $n_{ji} = (-1)^{i+j} \det M_{ij}$, then $MN = NM = (\det M)I$, where I is the identity matrix (Theorem 30. p. 440).

Using this last formula, you will prove in homework this week that the span over R of the columns of M is all of R^n if and only if M is invertible (in the obvious sense), or if and only if $\det M$ is a unit in R (it is *not* enough for $\det M$ to be nonzero). Also you will show that the columns of M are linearly independent over R (again in the obvious sense) if and only if $\det M$ is a zero divisor in R (but $\det M$ need not be 0).

It follows easily that the span of fewer than n elements of R^n cannot be all of R^n and that no set of $m > n$ elements of R^n spans a free submodule of it. In particular, as claimed above, $R^m \cong R^n$ if and only if $m = n$ and no free submodule of R^n has rank larger than n. In particular the $\mathbb{Z}$-modules $\mathbb{Z}^m$ and $\mathbb{Z}^n$, called free abelian groups (see p. 355) are isomorphic if and only if $m = n$. What is *not* true, however, even over $\mathbb{Z}$, is that the only free submodule of $\mathbb{Z}^n$ of rank n is $\mathbb{Z}^n$ itself: clearly the submodule $(2\mathbb{Z})^n$ consisting of all elements with even coordinates is proper and isomorphic to $\mathbb{Z}^n$.

These results extend beyond the setting of free modules. Let F be any R-module generated by $f_1, \ldots, f_n$ and let ϕ lie in the endomorphism ring End F. We can define a matrix M of F by decreeing that its ijth entry is m_{ij}, where $\phi(f_j) = \sum_{i=1}^{n} m_{ij} f_j$; here the matrix M is not uniquely determined by ϕ, even if the generators f_i are fixed, since these generators need not form a free basis of F. Make F into a module over $R[t]$, the polynomial ring in one variable over R, as in the example on p. 340, by decreeing that $tf = \phi(f)$ for any $f \in F$.

The matrix $M - tI$ over $R[t]$ then acts on F by 0, in the sense that it sends the column vector with coordinates $(r_1, \ldots, r_n)$, representing $\sum r_i f_i$ to $(\phi - \phi)(\sum_{i=1}^{n} r_i f_i) = 0$. Letting N_t be the transpose of the cofactor matrix of $M - tI$, we find as in the proof of Theorem 30 on p. 440 (mentioned above) that $N_t(M - tI) = (M - tI)N_t = 0 = \det(M - tI)I$, so that $\det(M - tI) = 0$, interpreting t as the endomorphism ϕ. This is the famous Cayley-Hamilton Theorem proved on p. 478 (by a very different method) for square matrices over fields; but one now sees that it holds for square matrices over any commutative ring. In particular, given the formula for the determinant, we see that ϕ satisfies a monic polynomial equation with coefficients in R; that is, one with leading coefficient 1. I will use this fact on several occasions later this year.

Lest you get the impression that free modules over commutative rings behave *exactly* like vector spaces, I should point out that submodules of free modules, even over commutative rings, need not be free. For example, the polynomial ring $R = F[x, y]$ in two variables over a field F, is free of rank one as a module over itself, but the ideal $I = (x, y)$ generated by x and y clearly is not singly generated, so that it is not free of rank one. Nor is it free of any higher rank, since any two nonzero polynomials $p, q \in R$ satisfy the dependence relation $qp - pq = 0$, so that these polynomials cannot lie in a free basis of any submodule of R. All free submodules of R have rank 0 or 1, but most submodules of R are not free.

I will show later in the course that any submodule of the polynomial ring $R = F[x_1, \ldots, x_n]$ in a finite number of variables over a field F is at least finitely generated; but there is no bound on the number of generators required if $n \geq 2$. Moreover, a submodule of a free module, even of rank one, need not be finitely generated. Letting $R = F[x_1, x_2, \ldots]$ be the polynomial ring in infinitely many variables x_i, the submodule I generated by the x_i is not finitely generated, since any finite subset of I can involve only finitely many variables. Thus free modules overall behave better than free groups in some ways, but worse in others.

I should also mention that endomorphisms ϕ of free modules R^n over *noncommutative* rings R also have $n \times n$ matrices M defined as above. In this setting the determinant of M can also be defined, at least if $R = D$ is a division ring (satisfying all axioms of a field except for commutativity of multiplication). The theory of such determinants, called Dieudonné determinants, is however not nearly as powerful as the theory of determinants in the commutative case. For example, the determinant of M, if nonzero, lies in the quotient $D^*/[D^*, D^*]$ of the multiplicative group D^* of nonzero elements of D by its commutator subgroup, rather than in D^* itself. Notice that R^n is a right module over R as well as a left module; it is possible for a set of vectors in it to be linearly independent with respect to the left R-action but not the right one.