Math 504, 10/10

We now shift gears, switching to the theory of modules over rings. Let R be a ring (always assumed to have an identity, but not necessarily commutative, although for most of this course we will concentrate on the commutative case). We saw that an abelian group M is a left *R-module* if first of all the additive group R acts on M by homomorphisms, so that for every $r \in R, m \in M$ there is $rm \in M$ such that $r(m_1 + m_2) = rm_1 + rm_2, (r_1 + r_2)m = r_1m + r_2m$ and in addition $1m = m$ for all $m \in M$ and $r(sm)$ equals $(rs)m$ for all $r, s \in R, m \in M$. You should think of M as a vector space with the usual field of scalars replaced by the ring R. A subgroup N of M that is stable under the R-action is called a *submodule of M*; given any submodule N, the quotient group M/N acquires an R-module structure via $r(m + N) = rm + N$. Note that submodules of R are the same as left ideals of R, or just ideals of R, if R is commutative. Note also that an ideal I of a commutative ring R and its quotient ring R/I are both R-modules, so can to some extent be treated on an equal footing. An R-module homomorphism π from one R-module M to another one N is an additive homomorphisms that respects multiplication by R: $\pi(rm) = r\pi(m)$ for $r \in R, m \in M$. These are the analogues of linear maps between vector spaces, and indeed R-module homomorphisms are also called R-linear maps. We define the *direct sum* $M \oplus N$ of two R-modules in the same way as for groups.

The simplest kinds of modules to understand are the ones that look most like vector spaces from a first course in linear algebra, namely the *free* ones; these are modules isomorphic to the set R^n of n-tuples over R, or more generally tuples of any fixed but possibly infinite length such that all but finitely many coordinates are 0. (Such modules are also called direct sums of the appropriate number of copies of R; if we drop the requirement that only finitely many coordinates are nonzero, we get the direct *product* of the same number of copies of R.) As in linear algebra, an R-module M is free if and only if has a (free) basis B, so that every element of M is uniquely a finite linear combination of elements of B with coefficients in R. Again as in linear algebra, an R-linear map π from R^n to R^m is given by left multiplication of a column vector in R^n by an $m \times n$ matrix M with entries in R, whose ith column is the image $\pi(e_i)$ of the ith unit coordinate vector $e_i \in R^n$ under π. If $m = n$ and π is surjective, then there is a matrix N such that $MN = I$, the identity matrix. Now assume that R is commutative. Then determinants of square matrices over R are defined in the same way as in linear algebra, and continue to satisfy the product rule. Hence $\det MN = (\det M)(\det N) = 1$ in this situation, so that $\det M$ is a unit in R (note that this is a stronger condition than just $\det M \neq 0$ if R is not a field). Now there is a rather old-fashioned but very useful formula for the inverse of a square matrix over a commutative ring with determinant a unit: take the transpose N' of the cofactor matrix of M, so that the ij-entry of N' is $(-1)^{i+j}$ times the determinant of the matrix M^{ij} obtained from M by deleting its ith row and jth column, and divide each entry of N' by $\det R$ to get a matrix N. Then a direct computation using standard properties of determinants shows that $MN = NM = I$. Thus, exactly as in linear algebra, a right inverse of a square matrix is automatically a left inverse; it follows that *any* R-module surjection from R^nf to itself is an isomorphism. We also see that no R-module map from R^n to R^m with $n < m$ can be a surjection, for otherwise we could add columns of zeroes to the matrix M of such a map and get an invertible matrix, which contradicts $\det M = 0$; for homework this week you will show by a similar but more complicated argument shows that no R-module map from R^n to R^m is injective if $n > m$. In particular, $R^n \cong R^n$ *if and only* $n = m$; this completes the proof of our assertion last time that free groups on different numbers of generators cannot be isomorphic. By contrast, however, as you will see in homework this week, it is possible to have $R \cong R^2$ as R-modules if R is noncommutative, so the bizarre behavior of free groups once again rears its head for modules. We call the number n the *rank* of the free module R^n (we do not use the term "dimension" in this context).

For the next few lectures, we will specialize to the case where R is a PID (principal ideal domain); note here that every nonzero ideal of R is isomorphic to R itself, as it is generated by a single non-zero-divisor. From this we will derive a very nice classification of finitely generated R-modules that looks very much like the classification of finite-dimensional vector spaces over a field. We will assume throughout the basic structure theory of PIDs (every pair of elements a, b has a greatest common divisor that is a linear combination of them, unique factorization into irreducible elements holds, and so on).