Math 504, 10/14

We saw last time that any finitely generated module M over a PID R is a direct sum of quotients of $R/(d_i)$ of R, where we can arrange either that $d_1|d_2|\cdots d_n$ or that every d_i is either 0 or a power p^i of an irreducible element p of R. We now want to see that this decomposition is unique up to reordering the factors (and multiplying the powers p^i by units, which clearly does not affect $R/(p^i)$. First look at the *torsion* submodule T of M, consisting by definition of all $m \in M$ with $rm = 0$ for some $r \neq 0 \in R$. Since R is a domain this really is a submodule; passing to the quotient M/T we clearly get the sum of all the copies of R itself in the decomposition of M as a sum of quotients of R. Any two such decompositions must involve the same number of copies of R (since the rank of a free module over R is well defined); we call this number the *free rank*of M. Now let p be an irreducible element of R, m a positive integer, and look at the quotient $p^m T/p^{m+1}T$ (where $p^m T$ denotes $\{p^m t : t \in T\}$, and similarly for $p^{m+1}T$. Given a quotient $N = R/(q^r)$ of R where $q \in R$ is irreducible, one checks that $N' = p^n N/p^{n+1}N = 0$ unless $q = pu$ for some unit u in R and $r \geq n$; if $N' \neq 0$, then $N' \cong R/(p)$, a vector space of dimension one over the field $R/(p)$. Hence, for any fixed p and m, any two primary decompositions of M must involve the same number of summands isomorphic to $R/(p^k)$ for some $k \geq m$, whence any two such decompositions must involve the same number of summands isomorphic to $R/(p^m)$ itself. The upshot is that *the primary decomposition of a finitely generated R-module M is unique up to reordering the quotients of R that are the summands.* This is the uniqueness part of the classification.

The two most important applications occur when $R = \mathbf{Z}$ or $R = K[x], K$ a field. In the first case we learn that *any finitely generated abelian group is a finite direct product of cyclic groups, each either infinite or of prime-power order.* A finite abelian group iA s a finite direct product of cyclic groups, each of prime-power order. If A has at most m solutions to the equation $x^m = 1$ for all positive integers m, then it must be cyclic: no two factors can occur whose orders are powers of the same prime p, lest there be too many solutions to $x^{p^k} = 1$ for some k, so the cyclic factors have relatively prime orders and their product is again cyclic. Since there are always at most m solutions to $x^m = 1$ in any field K, it follows that *any finite subgroup of the multiplicative group K^* of a field is cyclic.* In particular, $\mathbf{Z_p}^*$ is always cyclic, as mentioned in class last week. Next, as in class, take $R = K[x]$ and let V be a finite-dimensional vector space over K equipped with a linear transformation from V to V. We make V into a $K[x]$-module by decreeing that x act on V by $T : q(x)v = q(T)v \in V$ for all $v \in V, q \in K[x]$. Then V is isomorphic to the direct sum of quotients $K[x]/(p_i^{r_i}$ for various irreducible polynomials $p_i \in K[x]$ (the quotients must all be proper since V is finite-dimensional over K). Given a single quotient $V' = K[x]/(q), q(x) = p^r(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$, the matrix of the transformation T with respect to the fairly obvious basis $1, x \ldots, x^{n-1}$ of V' has ones below the main diagonal, , last column $-a_0, \ldots, -a_{n-1}$ and zeroes elsewhere. We call this matrix the *companion matrix* $C(q)$ of q; it has minimal and characteristic polynomials both equal to q (up to sign). In general, the matrix of T with respect to a suitable basis of V will be block diagonal with blocks equal to the companion matrices attached to various powers of monic irreducible polynomials over K; this form is unique apart from reordering the blocks. If the characteristic polynomial of T happens to have all roots in K (which it always does if for example K is algebraically closed, so that all polynomials over it have a full complement of roots in it), then the powers of polynomials arising in this way all take the form $(x-a_i)^{n_i}$. In this case one generally chooses a different basis for each block, namely the powers $(x-a_i)^{n_i-1}, \ldots, x-a_i, 1$ and the corresponding matrix has a_i's on the diagonal, ones above it, and zeroes everywhere else. Such a matrix is called a *Jordan block* and the *Jordan canonical form* of a square matrix realizes it as similar to a block diagonal matrix with the blocks all Jordan blocks (possibly with different eigenvalues). In particular, *there are only finitely many similarity classes of $n \times n$ matrices having just one eigenvalue a*, for any such matrix M is similar to one in Jordan form with a's on the diagonal and so is determined by its size; the sizes involved are a set of positive integers adding to n. Such unordered sets of positive integers summing to n are called *partitions* of n and have a rich mathematical theory; they have been studied for more than two and a half centuries.