Math 504, 10/12

Continuing from last time,let R be a PID. We will classify finitely generated R-modules; we start with submodules N of R^n. Here we find the same situation as for $\mathbf{Z}$: *any such submodule is isomorphic to R^m for some $m \leq n$.* This is also proved by induction on n, in the same way as for $\mathbf{Z}$: it is clear from the definition of PID if $n = 1$; in general, given N, look at the set I of $a \in R$ such that $(a, a_2, \ldots, a_n)$ lies in N for some $a_i \in R$ and argue that I is an ideal; if it is nonzero and generated by $a \in R$ and $v = (a, a_2, \ldots, a_n) \in N$), then N is the direct sum of the submodule generated by v and the intersection $N \cap 0 \times R^{n-1}$, with the first submodule isomorphic to R because a is a non-zero-divisor. Now let M be any R-module generated by n elements. Then is the quotient R^n/N of R^n by a submodule N, which we may take to be the column space of an $n \times m$ matrix A for some $m \leq n$. Adding columns of zeroes if necessary, we may assume that $m = n$. Now I claim that *if we replace the column space of A by that of PAQ for any $n \times n$ invertible matrices P, Q over R, then the quotient of R^n by the column space does not change, up to isomorphism.* Indeed, replacing A by AQ does not change its column space, while the column space C of PA is such that $R^n/N \cong R^n/C$ by the map sending the coset of any $v \in R^n$ to that of Pv.

We then find matrices P, Q for which the column space of PAQ is transparent. To do this, note first that any elementary column operation on A, replacing one column by the sum of itself and a multiple of another row, can be implemented by multiplying A by an invertible matrix Q_1 on the right; likewise any elementary row operation on A can be implemented by multiplying it by an invertible matrix P_1 on the left. More generally, let x, y, z, w be any elements of R such that $xw - yz = 1$. Then multiplying A on the right by the matrix Q' having x, y as the first two entires of its first column, z, w as the first two entries of its second column, with all other entries the same as the corresponding entires in the identity matrix has the effect of replacing the first two columns C_1, C_2 of A by $xC_1 + yC_2, zC_1 + wC_2$ and leaving all other columns unchanged. Doing this does not change the column space. In a similar manner, if we want to do what we just did to C_1, C_2 to some other pair of columns C_i, C_j instead, then we can do this by multiplying A on the right by a matrix agreeing with the identity matrix except in its ii, ij, ji, and jj-entries. We can do the same thing to any two rows R_i, R_j of A by multiplying it by a suitable matrix on the left. Now let a_1, a_2 be the first two entries in the first row of A.and let a be a gcd of these elements in R. There is $x, y \in R$ with $xa_1 + ya_2 = a$ and the coefficients x, y have no common factor in R, lest a proper multiple of a divide both a_1, a_2, so there are $z, w \in R$ with $xw - yz = 1$. Multiplying A on the right by the above matrix Q', we replace a_1 by a and a_2 by a multiple of a. Iterating this operation for the other rows, we can arrange to put a gcd of all entries in each row in its first coordinate. Iterating the operation for the new first column, we can put a gcd of all entries of A into its upper left corner, while all other entries are multiples of this one. Finally, performing suitable row and column operations, we can zero out the first row and column of A (except for

its $(1,1)$-entry). The upshot is a new matrix A' with $(1,1)$-entry d such that all other entries in its first row and column are 0 and all other entries anywhere are multiples of d. Iterating this procedure, we see that *we can replace A by a diagonal matrix with diagonal entries say $d_1, \ldots, , d_n$, such that $d_1 | d_2 | \cdots | d_n$.* But the quotient of R^n by the column space of this last matrix is clearly the sum of the quotients $R/(d_i)$ of R. Thus *any finitely generated R-module M is the direct sum of quotients $R/(d_i)$ of R, such that $d_1 | d_2 | \cdots | d_n$ in R. (Note that we allow some $d_i = 0$ for some i, but then all subsequent d_j must also be 0.) This is called the elementary divisor decomposition of M and is unique up to multiplying the d_i by units in R.*

There is another decomposition typically involving more but simpler summands than this one. Recall (by the Chinese Remainder Theorem) that any nonzero proper quotient $R/(a)$ is isomorphic to the direct sum of the quotients $R/(p_i^{m_i})$, where $p_1^{m_1} \ldots p_r^{m_r}$ is the irreducible factorization of a in R. Replacing each term $R/(d_i)$ in the elementary divisor decomposition as above, we get a second decomposition of M as a direct sum of quotients $R/(q_i)$ where each q_i is either 0 or a power of an irreducible element in R. This last decomposition of M is called the primary decomposition and it is unique up to reordering the summands and multiplying the q_i by units.