Math 122 Wednesday, December 14

R any ring, $\exists$ homomorphisms $R^n \xrightarrow{f} R^m$ of free R-modules $f(e_i) = \sum a_{ij} e_j^*$

$A = (a_{ij})$ m rows, n columns with entries in R

$A' = PAQ$ where P is an invertible $m \times m$ matrix (invertible map $R^m \rightleftarrows R^m$)
Q is an invertible $n \times n$ matrix (invertible map $R^n \rightleftarrows R^n$)
is another matrix for f wrt different bases for domain and range

Some invertible matrices include: $P = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & u_i & \\ 0 & & & \ddots \; 1 \end{pmatrix}$ $u_i \in R^\times$; P = permutation matrix with entries 0 and 1; $P = \begin{pmatrix} 1 & & c_{ij} & 0 \\ & \ddots & & \\ 0 & & & 1 \end{pmatrix}$

Left multiplication by such P performs row operations on A
i.e., multiply ith row by a unit u; permute the rows; add $c \times j^{th}$ row to ith row
Right multiplication by such Q performs column operations.

So we can obtain A' from A by a sequence of such row + column operations (note the product $P = P_1 \cdots P_k$ of invertible matrices is invertible)

Prop If R is Euclidean, A arbitrary, we can transform A to a matrix A' of the form
$A' = \begin{pmatrix} d_1 & & & 0 \\ & d_2 & & \\ & & \ddots & \\ 0 & & d_k & \\ & & & 0 \end{pmatrix}$ where $k \le \min(m,n)$ and $d_1 | d_2 | d_3 | \cdots | d_k$ (equivalently: $(d_1) \supset (d_2) \supset (d_3) \supset \cdots$) with the d_i all non-zero. Note both the d_i and k are determined by A.
Pf: For $R = \mathbb{Z}$. Here we have a natural generator for each ideal so we'll also ok $d_i \geq 1$. Use:

Lemma We can transform A to $A' = \begin{pmatrix} d & 0 \cdots 0 \\ 0 & \\ \vdots & B \\ 0 & \end{pmatrix}$ where d divides all the entries in B.

Pf: If $A = 0$ take $d = 0$, $B = 0$ done. Otherwise some $a_{ij} \neq 0$. Pick some a_{ij} to minimize $|a_{ij}| > 0$. Permute rows and columns to move this to a_{11}. Make a_{11} positive by multiplying by $\begin{pmatrix} \pm 1 & 0 \\ 0 & \ddots \; 1 \end{pmatrix}$. Now work on first row. For each a_{1i} in this row, $a_{1i} = a_{11} \cdot m + r$. If $r = 0$ the multiply the first column by m and subtract from the i-th column to get new entry $a_{1i}^* = 0$. If $r \neq 0$ do the same thing but now $a_{1i}^* = r$. But $r < a_{11}$ so permute the columns so that the a_{11} entry is r. Continue with the first row. After a finite number of steps, each decreasing the a_{11} entry or zeroing one a_{1i}, get a matrix $\begin{pmatrix} a_{11} & 0 \cdots 0 \\ a_{21} & \\ \vdots & B \\ a_{n1} & \end{pmatrix}$. Now you want to do the same thing to the first column but this is only going to work if $|a_{11}| \leq |a_{i1}|$ whenever this is non-zero. If this is false then move the a_{i1} to a_{11} and start over with the first row. Proceed as before writing $a_{i1} = m a_{11} + r$ then subtract $m \times$ row 1 from row i to replace a_{i1} with r. Then move r to a_{11}, start over with the first row and then try to make the first column zero as well. As each step decreases the $|a_{11}|$ this must eventually terminate! Check if a_{11} divides all of B. If some $b_{ij} = m a_{11} + r$, $r \neq 0$ then add 1st row to ith row, then subtract $m \times$ 1st column from jth column to change b_{ij} to r. Move r to a_{11} and start over. Eventually this all must end with A in the desired form.

Claim If $A=0$, $d=0$. If $A \neq 0$ then $d \geq 1$ is the generator of the ideal $(a_{11}, a_{12}, \dots, a_{mn}) = \gcd(a_{ij})$

To finish proof of Prop induct on the size of A. That is, perform the algorithm in the lemma on A. By hypothesis can write B in the diagonal form because it's smaller. Thus A can be written in the diagonal form and $d = d_1 | d_2 | \cdots | d_k$. QED.

ex $\begin{pmatrix} 2 & 4 & 8 \\ 12 & 16 & 20 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 \\ 12 & -8 & -28 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & -8 & -28 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix}$ $f(e_1) = 2e_1^*$, $f(e_2) = 4e_2^*$, $f(e_3) = 0$

If we choose P + Q over a Euclidean ring so that $A' = PAQ = \begin{pmatrix} d_1 & & & 0 \\ & \ddots & & \\ & & d_k & \\ 0 & & & 0 \end{pmatrix}$ then we choose new bases $e_1, \dots, e_n$ of R^n and $e_1^*, \dots, e_m^*$ of R^m, such that $f(e_1) = d_1 e_1^*, \dots, f(e_k) = d_k e_k^*, f(e_{k+1}) = \cdots = f(e_n) = 0$.

Corollary The quotient module $R^m / (\text{Image of } f(R^n))$ is isomorphic to $\underbrace{R/(d_1)}_{\text{coset of } e_1^*} + \cdots + R/(d_k) + \underbrace{R^{m-k}}_{\text{cosets of } e_{k+1}^*, \dots, e_m^*}$

This gives a classification of finitely generated R modules (R a Euclidean ring).

Let $\underset{\text{kernel of } g}{R^n} = N \xrightarrow[\text{injective}]{f} R^m \xrightarrow[\text{onto}]{g} M$ $\quad (r_i) \mapsto \sum r_i m_i$

$M \simeq R^m / (\text{kernel of } g) \simeq R^m / f(R^n)$
$\simeq R/(d_1) + \cdots + R/(d_k) + R^{m-k}$

Prop If R is Euclidean then any submodule N of a free R-module R^m is free of rank $n \leq m$

When $m=1$ submodules $N \subset R$ are ideals. Ideals are free modules of rank 1 iff they are principal, so this prop says in a Euclidean ring all ideals are principal.