MATH 8000 HOMEWORK 11

Due on Tuesday, December 5

(1) In this problem, let R be a PID, and let $A\colon M \to N$ be a module homomorphism between free modules of ranks m and n respectively. (Recall that this means that $M \cong R^{\oplus m}$ and $N \cong R^{\oplus n}$.)

(a) Let S be the set of ideals $\varphi(A(M))$, where φ ranges over all "functionals" (that is, R-module maps from N to R). Show that S has a maximal element.

(b) Suppose that (d_1) is a maximal element of S. Then there is some $\varphi_1\colon N \to R$ such that $\varphi_1(A(M)) = (d_1)$. Let $v_1 \in M$ such that $\varphi_1(A(v_1)) = d_1$. Show that for any other functional $\varphi\colon N \to R$, we have $d_1 \mid \varphi(A(v_1))$. (Hint: consider the gcd of d and $\varphi(A(v_1))$.)

(c) Show that in fact, (d_1) is the *maximum* element of S, meaning that if (d) is any other ideal in S, then $d_1 \mid d$. (Hint: once again, consider the gcd of d and d_1.)

(d) Recall that if $\{e_1, \ldots, e_n\}$ is some free basis of N, then we have the coordinate functionals $\xi_i\colon N \to R$, such that

$$\xi_i\left(\sum_{j=1}^{n} a_j e_j\right) = a_i.$$

Use these to show that there is some $w_1 \in N$ such that $A(v_1) = d_1 w_1$.

(e) Let $\langle v_1 \rangle \subset M$ be the submodule generated by v_1, and let $\langle w_1 \in N \rangle$ be the submodule generated by w_1. Let $M' = \ker(\varphi_1 \circ A)$ and let $N' = \ker(\varphi_1)$. Show that $M = \langle v_1 \rangle \oplus M'$ and $N = \langle w_1 \rangle N'$.

(f) Check that if $m \in M$ is written as (rv_1, v_2) where $rv_1 \in \langle v_1 \rangle$ and $v_2 \in M'$, then $A(m) = (rd_1w_1, A(v_2))$ where $rd_1w_1 \in \langle w_1 \rangle$ and $A(v_2) \in N'$.

(g) Conclude by induction that for the restricted map $A\colon M' \to N'$, there is some change of basis such that the matrix of A has the following "diagonal" form $(d_2, \ldots, d_k)$:

$$\begin{pmatrix} d_2 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & d_3 & \ldots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & d_k & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 \end{pmatrix},$$

where $d_i \mid d_{i+1}$ for each $i \geq 2$. From part (c), further conclude that $d_1 \mid d_i$ for each $i \geq 2$.

(h) Conclude that there are bases for M and N in which A has the "diagonal" form $(d_1, \ldots, d_k)$, where $d_i \mid d_{i+1}$ for each $i \geq 1$.

(2) Let M be a finitely generated module over a PID R. Use the previous problem to prove that $M \cong R^r \oplus R/(d_1) \oplus R/(d_2) \oplus \cdots \oplus R/(d_k)$ where $d_i \mid d_{i+1}$ for each $i \geq 1$. (This is called an *invariant factors form* for M, and the number r is called the rank of M.)

(3) Let M be a finitely generated module over a PID R. Use the previous problem and the Chinese Remainder Theorem to show that there are primes $p_1, \ldots, p_n$ (not necessarily distinct) and powers $r_1, \ldots, r_n$ such that

$$M \cong R^r \oplus R/(p_1^{r_1}) \oplus \cdots \oplus R/(p_n^{r_n}).$$

(This is called the *elementary divisors form* for M.)