Math 551, Assignment 5, due Friday, November 1 in class

1. Let p be a prime and n a positive integer. Show that the number of isomorphism types of abelian groups of order p^n is equal to the number of conjugacy classes in Σ_n (i.e., the number of orbits in the action of Σ_n on itself by conjugation).

2. Show that if G, H, and K are finitely generated modules over a PID R, then $G \oplus H \cong G \oplus K$ implies $H \cong K$. Give a counterexample if the finite generation assumption is removed.

3. Show that in the ring $R = \mathbf{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbf{Z}\}$, 3 is irreducible but not prime.

4. Show that in a Euclidean domain R with rank function ν, an element $r \in R$ is a unit if and only if $r \neq 0$ and $\nu(r) = \nu(1)$.

5. Let $R = \mathbf{Z}[i] := \mathbf{Z} \oplus \mathbf{Z}i$, the ring of all complex numbers with integer real and imaginary parts. Show that $\nu(a + bi) = |a + bi|^2$ makes R a Euclidean ring. Determine which elements of R are units, and show that a prime integer $p \in \mathbf{Z}$ is prime in R if and only if p is not the sum of two squares in $\mathbf{Z}$.

6. Let R be a PID and let A be an $m \times n$ matrix with coefficients in R. An $i \times i$ minor of A is the determinant $\det B$ of an $i \times i$ matrix obtained by erasing some rows and columns of A. Let $\Delta_i(A)$ be the g.c.d. of all the nonzero $i \times i$ minors of A (and $\Delta_i(A) = 0$ if all $i \times i$ minors are 0). Also define $\Delta_0(A) = 1$. Theorem I implies (as will be discussed in class) that there exist $P \in GL_m(R)$ and $Q \in GL_n(R)$, and elements $m_1, \ldots, m_r \in R$, $r = \min(m, n)$, such that $m_1 | m_2 | \cdots | m_r$ and

$$PAQ = \begin{bmatrix} m_1 & 0 & 0 & \cdots \\ 0 & m_2 & 0 & \cdots \\ 0 & 0 & m_3 & \cdots \\ . & . & . & \cdots \end{bmatrix}.$$

Show that $\Delta_{i-1} m_i \sim \Delta_i(A)$ for any i such that $\Delta_{i-1}(A) \neq 0$. (Here $a \sim b$ means $Ra = Rb$.)

7. If the finitely generated module M over the PID R satisfies $M \cong R/p_1^{n_1}R \oplus \cdots R/p_r^{n_r}R$, where $p_1, \ldots, p_r$ are primes in R and $n_1, \ldots, n_r$ are positive integers, call

$$p_1^{n_1}, \ldots, p_r^{n_r}$$

the list of **elementary divisors** of M. (If M is the 0 module, then $r = 0$.) Thus by Theorem III the list of elementary divisors is determined up to associates, and up to reordering the list. Show that if N is a submodule of M, then lists of elementary divisors of M and N may be reordered so that the elementary divisors of N are $p_1^{k_1}, \ldots, p_s^{k_s}$ for some $0 \leq s \leq r$ and some integers $1 \leq k_i \leq n_i$, $i = 1, \ldots, s$. (Hint: it was shown in class that for any prime power p^n, $\dim_{R/pR}((p^n M[p]))$ is the number of elementary divisors which are divisible by p^{n+1}.) Show conversely that every such list of elementary divisors arises from some submodule N of M (not necessarily unique).

Prove the corresponding results for quotient modules of M. (Hint. Use $p^n M/p^{n+1}M$ instead of $p^n M[p]$.)