Math 122 Friday, December 16

finitely generated modules over a Euclidean ring R

$R^n \xrightarrow[g]{} M = R^n/\ker g$ $\quad (r_1, \dots, r_n) \mapsto \sum r_i m_i$ where the m_i generate M.
Have such a homomorphism for any finitely generated module

Let $N = \ker g \hookrightarrow R^n$

Claim N is a free R-module of rank $m \le n$

Hence $N \cong R^m \xhookrightarrow{f} R^n$ gives a $n \times m$ matrix A

Calculate the quotient module $M \cong R^n / \text{Image } f(R^m) = R/(d_1) + \dots + R/(d_k) + R^{n-k}$

$d_1 | d_2 | \dots | d_k$ $\quad A' = PAQ$ of the form $\begin{pmatrix} d_1 & & 0 & \\ & \ddots & & \\ 0 & & d_k & \\ & & & 0 \end{pmatrix}$

Pf of claim) For R a PID, which more than suffices. We'll show any submodule of a free R-module of rank n is free of rank $m \le n$ by induction on n. When $n=1$, $N \subset R$ a submodule $\Rightarrow$ N is an ideal $\Rightarrow$ $N = aR$ as R is a PID. If $a = 0$, $N = 0$ is free of rank 0. If $a \neq 0$ then N is free of rank 1, with basis element a. $R \xrightarrow{\simeq} N$, $r \mapsto ra$
[Note this shows that claim is false if R is not a PID. A non-principal ideal will never have rank ≤ 1 and will also not be free.]

Assume true for rank $\le n-1$ and consider $N \subset R^n$. Under the map $R^n \xrightarrow{h} R^{n-1}$
$(r_1, \dots, r_n) \mapsto (r_1, \dots, r_{n-1})$. $\ker h = (0, \dots, 0, r_n) \simeq R$ a free module of rank 1. $N \mapsto h(N)$ which is a submodule of R^{n-1} so it is free of rank $\le n-1$ by induction. Let $n_1^*, \dots, n_k^*$ be the generators of $h(N)$ and choose $n_1, \dots, n_k \in N$ mapping to the $n_1^*, \dots, n_k^*$. Also kernel of $h: N \to h(N)$ is (kernel of h) $\cap N \subset R$ a submodule so this is free of rank ≤ 1.
If $\ker h$ on N is 0 then I claim $h_1, \dots, h_k$ form a basis for N. If $\ker h \cap N$ is not 0 let h_0 be a generator. Then I claim $h_0, h_1, \dots, h_k$ form a basis for N (note $k+1 \le n$).
Must show any $n \in N$ is uniquely written in the form $n = \sum_0 r_i n_i$. We know $h(n) = r_1 n_1^* + \dots + r_k n_k^*$ as the h_i^* form a basis for $h(N)$ and the r_i is unique. Consider $n - (r_1 n_1 + \dots + r_k n_k)$. This is in $N \cap \ker h$ so is either 0 (in case 1) or is written uniquely in the form $r_0 n_0$.
So $n = r_0 n_0 + \dots + r_k n_k$. Furthermore (we'll show uniqueness again), if $s_0 n_0 + \dots + s_k h_k = 0$ then apply h to see that $s_1 n_1^* + \dots + s_k n_k^* = 0 \Rightarrow s_1 = s_2 = \dots = s_k = 0$. Hence also $s_0 = 0 \Rightarrow$ unique! $\square$

Calculation of a quotient module of a map (R a Euclidean ring).

$R^m \xrightarrow{f} R^n$. Choose a new basis $e_1, \dots, e_m$ of R^m; $e_1^*, \dots, e_n^*$ of R^n so that f has matrix A', i.e., so that $f(e_1) = d_1 e_1^*, \dots, f(e_k) = d_k e_k^*$, $f(e_j) = 0$ $j > k$. So $R^n = \{a_1 e_1^* + \dots + a_n e_n^*\}$ and the Image of $f(R^m) = $ span of $f(e_i) = $ span of $d_i e_i^* = \{a_1 e_1^* + \dots + a_n e_n^* \mid a_1 \in (d_1), \dots, a_n \in (d_n)\}$. [Say $d_n = 0$ if $n > k$]
By considering the coefficients of each basis element, get $R^n / f(R^m) \simeq R/(d_1) + \dots + R/(d_k) + R^{n-k}$.

Cor Any finite abelian group is isomorphic to one of the form $M = \mathbb{Z}/d_1\mathbb{Z} + \cdots + \mathbb{Z}/d_n\mathbb{Z}$, $d_1 | d_2 | \cdots | d_n$. $d_i \geq 1$. So M is a direct sum of cyclic groups. Note $\# M = d_1 \cdots d_n$.

Say $\# M = 210 = 2 \times 3 \times 5 \times 7$. Then $M \cong \mathbb{Z}/210\mathbb{Z}$. Why? $d_1 | d_2 \Rightarrow d_1^2 | \# M$. If $\# M$ is square free then M must be cyclic.

Say M is a p-group. $\# M = p^k$.

$k=1$ $\quad \mathbb{Z}/p\mathbb{Z}$ $\qquad k=2$ $\quad \underset{d_1 = p^2}{\mathbb{Z}/p^2\mathbb{Z}}$ $\qquad \underset{d_1 = d_2 = p.}{\mathbb{Z}/p\mathbb{Z} + \mathbb{Z}/p\mathbb{Z}}$

$k=3$ $\quad \underset{d_1 = p^3}{\mathbb{Z}/p^3\mathbb{Z}}$ $\qquad \underset{d_1 = p \;\; d_2 = p^2}{\mathbb{Z}/p + \mathbb{Z}/p^2}$ $\qquad \underset{d_1 = d_2 = d_3 = p}{\mathbb{Z}/p + \mathbb{Z}/p + \mathbb{Z}/p}$

More generally the number of abelian groups of order p^k = the number of partitions of k
$k = k_1 + \cdots + k_n \rightarrow p^k = p^{k_1} \cdots p^{k_n}$. Say $k_1 \leq k_2 \leq \cdots \leq k_n$. Then $d_1 = p^{k_1} | d_2 = p^{k_2} | \cdots | d_n = p^{k_n}$.

Recall if M has order p^2 then it is abelian (by the class equation) So M is either $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} + \mathbb{Z}/p\mathbb{Z}$. Surprising fact that M is much more likely to be cyclic than not.

Should weight M by a factor $\frac{1}{\# \mathrm{Aut}\, M}$. $\quad \mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z}) = (\mathbb{Z}/p^2\mathbb{Z})^*$ has order $p^2 - p = p(p-1)$

$\mathrm{Aut}(\mathbb{Z}/p + \mathbb{Z}/p) = \mathrm{Aut}(V)$ where V where V is a 2-dim vector space over $\mathbb{Z}/p\mathbb{Z}$. So
$\mathrm{Aut}(V) = GL_2(\mathbb{Z}/p\mathbb{Z})$ which has order $\underset{\substack{\text{choices for} \\ \text{column 1}}}{(p^2-1)}\underset{\substack{\text{choices for} \\ \text{column 2}}}{(p^2-p)}$

So $\mathbb{Z}/p^2\mathbb{Z}$ has weight $\frac{1}{p^2-p}$
$\mathbb{Z}/p\mathbb{Z} + \mathbb{Z}/p\mathbb{Z}$ has weight $\frac{1}{(p^2-p)(p^2-1)}$ $\quad$ which is $\frac{1}{p^2-p}$ as likely.

Why do we weight things like this? Question for another course.