Alg

Theorem (Smith Normal Form)
Let R be a PID, $A \in M_{m\times n}(R)$.
Then A is equivalent to a "diagonal" $m \times n$ matrix whose entries satisfy

$$d_1 \mid d_2 \mid \dots \mid d_{\min(m,n)}.$$

(This diagonal matrix is called the Smith normal form or invariant factor matrix of A.)

Proof:

Claim: A is equivalent to a matrix of the form

$$\begin{bmatrix} d_1 & \cdots \\ \hline 0 & B \end{bmatrix}$$

where

- $B \in M_{(m-1)\times(n-1)}(R)$
- $d_1 \mid b_{ij}$ $\forall i,j$.
- d_1 & all b_{ij} are R-linear combinations of a_{ij}'s.

Alg

We then iterate this until we reach

$$C_{\text{final}} = \begin{bmatrix} c_1' & \cdots & c_r' \end{bmatrix}$$

at which point we show this to be equivalent to $\begin{bmatrix} d & \bigcirc \end{bmatrix}$ with d an R-linear combination of the c_i's.

lemma

Proof of Lemma 1: Suppose C has at least two non-zero entries, c_1, c_2.

Since R is a PID, by Bézout's lemma there exist $x, y \in R$ such that

~~$d = \gcd(c_1, c_2) = xa + yb$~~.

$$d = \gcd(c_1, c_2) = xc_1 + yc_2.$$

Write $c_1 = dc_1'$, $c_2 = dc_2'$, then

$$d = d(xc_1' + yc_2') \Rightarrow xc_1' + yc_2' = 1.$$

$$\begin{bmatrix} c_1 & c_2 & \cdots & c_r \end{bmatrix} \underbrace{\left[\begin{array}{cc|c} x & -c_2' & \\ y & c_1' & \bigcirc \\ \hline 0 & & I_{r-2} \end{array}\right]}_{\text{invertible since } \det = 1} = \begin{bmatrix} d & 0 & c_3 & \cdots & c_r \end{bmatrix}$$

□

Note: $d = \gcd(c_1, \ldots, c_r)$.

So $\lambda(d) \leq \lambda(c_i)$ $\forall i$.

Back to the proof of the Theorem:

Define $\lambda : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ by

$$\lambda(r) = \begin{cases} 0 & \text{if } r \text{ is a unit} \\ k & \text{if } r \text{ is not a unit and } r = p_1 \cdots p_k \\ & \quad \text{with } p_i \text{ irred.} \end{cases}$$

If x divides y but is not associate to y, then
$\lambda(x) < \lambda(y)$.

Also $\lambda(xy) = \lambda(x) + \lambda(y)$.

Start with a matrix A. If all zero, done.
Otherwise make a_{11} nonzero. Apply lemma 1 to the first row, then the first column of A to get an equivalent matrix

$$\begin{bmatrix} d & \cdots \\ 0 & B \end{bmatrix}$$

To ensure that d divides the entries of B:
~~Arrow~~ Suppose not. Arrange that $d \nmid b_{11}$.
Add the first row of B to the first row of A:

$$\begin{bmatrix} d & b_{11} & b_{12} \cdots b_{1r} \\ 0 & b_{11} & b_{12} \cdots b_{1r} \end{bmatrix} \qquad \begin{matrix} d & 0 & b_{12} \cdots b_{1r} \\ yb_{11} & c_1' b_{11} & b_{12} \cdots b_{1r} \end{matrix}$$

Applying lemma 1, we get

$$\begin{bmatrix} d' & \cdots \\ 0 & B' \end{bmatrix}$$

with $\lambda(d') < \lambda(d)$.
So this must terminate. □

Theorem (Structure of finitely generated modules over a PID)

Let M be a finitely generated module over a PID R. Then there exist $d_1, \dots, d_k \in R$ such that

$$d_1 \mid d_2 \mid \dots \mid d_k$$

and

$$M \cong R/(d_1) \oplus R/(d_2) \oplus \dots \oplus R/(d_k)$$

Proof:

M fin. gen. so have surjective hom.

$$\varphi : R^k \longrightarrow M.$$

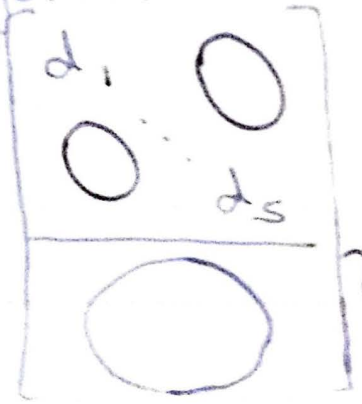
Then $N = \ker(\varphi)$ is free of rank $s \leq k$.

Choose bases for N and R^k, then

$$N \hookrightarrow R^k$$

is represented by a matrix $A \in M_{k \times s}(R)$.

But then A is equivalent to its Smith normal form



$$d_1 \mid \dots \mid d_s$$

(Alg)

So there's a basis $\{f_1, \dots, f_k\}$ of R^k such that $\{d_1 f_1, \dots, d_s f_s\}$ is a basis of $N \subseteq R^k$.

If $s < k$ let $d_{s+1} = \dots = d_k = 0$.

Define $\psi : R^k \to R/(d_1) \oplus \dots \oplus R/(d_k)$

$$\sum r_i f_i \mapsto \left(r_1 + (d_1), \dots, r_k + (d_k) \right)$$

Then ψ is surjective with kernel N, done.

□