PID R, $M \cong R^n$, $N \subseteq M$ submodule.

Then N is free of rank $k \le n$, and $\exists$ basis $\{u_1, \dots, u_n\}$ in M and elements $a_1, \dots, a_k \in R$ s.t. $a_1 | a_2 | \cdots | a_k$ and $\{a_1 u_1, \dots, a_k u_k\}$ is a basis in N.

---

vector spaces

$W \subseteq V \Rightarrow \exists U$ s.t. $W \oplus U = V$.

---

in M, put $K = R\{u_{k+1}, \dots, u_n\}$. Then $M = \tilde{N} \oplus K$ where

$\tilde{N} = R\{u_1, \dots, u_k\}$ and $\tilde{N}/N$ is a torsion module.

$$\tilde{N}/N \cong R/(a_1) \oplus \cdots \oplus R/(a_k)$$

Let $\varphi: K \longrightarrow M$ be a hom-sm (M & K free of finite rank).

Let $N = \varphi(K)$.

Let $L = \operatorname{Ker}\varphi \le K$. So $\exists$ basis $\{v_1, \dots, v_m\}$ in K s.t. $\{b_1 v_1, \dots, b_\ell v_\ell\}$ is a basis in L.

but L is complete so $\{v_1, \dots, v_\ell\}$ is a basis in L

$K = L \oplus P$ and $P \cong N = \varphi(K)$.

Choose a basis in M and N as in the theorem.

take corresponding elements in P.

Then the matrix of φ will be

$$\left(\begin{array}{ccc|c} a_1 & & & \\ & \ddots & & 0 \\ & & a_k & \\ \hline & 0 & & 0 \end{array}\right)$$

So $\forall$ matrix A over R, $\exists$ invertible P & Q s.t.

$$\underset{m\times m}{P}\,\underset{m\times n}{A}\,\underset{n\times n}{Q} = \left(\begin{array}{c|c} \begin{matrix} a_1 & & \\ & \ddots & \\ & & a_k \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right)$$ and, moreover, $a_1 \mid a_2 \mid \cdots \mid a_k$.

Or: any matrix over a PID can be reduced to this form by row-column operations.

Let R be Euclidean Domain: $a, b \neq 0 \Rightarrow a = bc + r$ w/ $r = 0$ or $|r| < |b|$. ← euclidean norm

$$\left(\begin{array}{c|c} a_1 & 0 \cdots 0 \\ \hline 0 & \\ \vdots & * \\ 0 & \end{array}\right)$$

① put minimal element of matrix at $(1,1)$ by row & column switching.

② If this minimal element doesn't divide an element of first column or row, subtract a multiple of first row or column to get a smaller element

③ repeat ① and ② until $(1,1)$ element divides every element of first row & column.

④ subtract multiples of first row/column to get 0s in all $(1,j)$ and $(i,1)$ with $i \neq 1 \neq j$.

⑤ induct.

do we have $a_1 \mid a_2 \mid \cdots \mid a_k$? Not necessarily.

The algorithm must be complicated.

<u>Theorem</u>: If M is a finitely generated R-module (R is PID), then $M \cong R^\ell \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$ where $\ell = \operatorname{rank} M$ } existence

then $M \cong R^{\ell} \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$ where $\ell = \operatorname{rank} M$ and $a_1, \dots, a_m$ are nonzero, non-unit elements of R such that $a_1 | \cdots | a_m$. } existence

These numbers $a_1, \dots, a_m$ are called the invariant factors of M & are unique up to multiplication by units. } uniqueness

Special Case $R = \mathbb{Z}$. Any finitely generated abelian group is $\cong \mathbb{Z}^{\ell} \oplus \mathbb{Z}_{a_1} \oplus \cdots \oplus \mathbb{Z}_{a_m}$

with $a_1 | \cdots | a_m$

(finite $\Rightarrow \ell = 0$)

Corollary: $M \cong (\text{free module}) \oplus \operatorname{Tor}(M)$

Corollary: If M is torsion-free, M is free.

proof of existence part of Theorem: Let K be a free module of rank n such that $\varphi : K \longrightarrow M$ is epimorphism ($n = \#$ generators of M)

let $N = \operatorname{Ker} \varphi$. Find basis $\{u_1, \dots, u_n\}$ in K and $a_1, \dots, a_k \in R$ s.t. $a_1 | \cdots | a_k$ and $\{a_1 u_1, \dots, a_k u_k\}$ is a basis in N.

Then $K/N \cong R/(a_1) \oplus \cdots \oplus R/(a_k) \oplus R^{n-k}$.

if $a_i \in R^{\times}$ for some i, then $R/(a_i) = 0$ and can be removed from the sum. So

$$K/N \cong R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus R^{n-k}$$

where a_i are not units. Also, $M \cong K/N$.

$\forall i,\ a_i = p_{i,1}^{r_{i,1}} \cdot \ldots \cdot p_{i,s}^{r_{i,s}}$ – distinct primes in R

Then $R/(a_i) \cong R/(p_{i,1}^{r_{i,1}}) \oplus \cdots \oplus R/(p_{i,s}^{r_{i,s}})$

So another decomposition is

$$M = R/(p_1^{r_1}) \oplus \cdots \oplus R/(p_s^{r_s}) \oplus R^{l}$$ where

p_i are not necessarily distinct and r_i are integers.

eg $\mathbb{Z}_6 \times \mathbb{Z}_{12} = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_4$

$p_i^{r_i}$ are the elementary divisors of M, and they are uniquely defined

and <u>this</u> implies $a_1, \ldots, a_m$ are uniquely defined.