

SMITH NORMAL FORM

THEOREM (SMITH NORMAL FORM): Let R be a PID. Let $A \in \text{Mat}_{m \times n}(R)$.

- (i) There exist invertible matrices P, Q such that
 - $PAQ = D$ is diagonal, meaning $d_{ij} = 0$ whenever $i \neq j$, and
 - $d_{11} | d_{22} | \cdots | d_{tt}$, where d_{tt} is the last nonzero diagonal entry.
- (ii) The elements d_{ii} are unique up to associate, meaning that if $D' = [d'_{ij}]$ is another diagonal matrix as in (i), then for each d'_{ii} is a unit times d_{ii} .
- (iii) If R is a Euclidean domain, then P, Q can be taken as products of elementary matrices.

STRUCTURE THEOREM FOR FINITELY GENERATED MODULES OVER PIDS (INVARIANT FACTOR FORM): Let R be a PID. Let M be a finitely generated R -module. Then there exist $r, t \geq 0$ and $a_1, \dots, a_t \in R$ such that

- $M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_t)$, and
- $a_1 | a_2 | \cdots | a_t$.

Moreover, each a_i is uniquely determined up to associates.

- (1)** Let R be a commutative ring, and $D \in \text{Mat}_{m \times n}(R)$ be a diagonal matrix with nonzero diagonal entries d_{11}, \dots, d_{tt} . Prove that the module presented by D is

$$R^{m-t} \oplus R/(d_{11}) \oplus R/(d_{22}) \oplus \cdots \oplus R/(d_{tt}).$$

- (2)** Use the Smith Normal Form Theorem to deduce the Structure Theorem for Finitely Generated Modules over PIDs (Invariant Factor Form).

- (3)** State the Structure Theorem for Finitely Generated Abelian Groups (Invariant Factor Form), and deduce it from the PID Theorem.

- (4)** Let R be a Euclidean domain. Use the Smith Normal Form Theorem to deduce that any invertible matrix over R is a product of elementary matrices.

DEFINITION: Let R be a domain and M be an R -module. We say that M is **torsionfree** if for $r \in R$ and $m \in M$, we have $rm = 0$ implies $r = 0$ or $m = 0$.

- (5)** Let R be a PID.

- (a) Show that any finitely generated torsionfree R -module is free.
- (b) Show that any submodule of a finitely generated free R -module is free.
- (c) Prove or disprove: any torsionfree R -module is free.
- (d) Prove or disprove: any submodule of a free R -module is free.

STRUCTURE THEOREM FOR FINITELY GENERATED MODULES OVER PIDS (ELEMENTARY DIVISOR FORM): Let R be a PID. Let M be a finitely generated R -module. Then there exist $r, s \geq 0$ and prime elements $p_1, \dots, p_s \in R$ such that $M \cong R^r \oplus R/(p_1^{e_1}) \oplus \dots \oplus R/(p_s^{e_s})$, and Moreover, the list $p_1^{e_1}, \dots, p_s^{e_s}$ is unique up to reordering and associates.

(6) Converting between forms:

To convert a cyclic module $R/(a)$ to elementary divisor form, write $f = p_1^{e_1} \cdots p_s^{e_s}$ as a product of prime powers, and use CRT get

$$R/a \cong R/p_1^{e_1} \oplus \dots \oplus \mathbb{Z}/p_s^{e_s}.$$

(a) Convert the $\mathbb{R}[x]$ -module

$$\mathbb{R}[x]^2 \oplus \mathbb{R}[x]/(x-1) \oplus \mathbb{R}[x]/(x-1)^2 \oplus \mathbb{R}[x]/((x-1)^2(x+1))$$

to elementary divisor form.

To convert a module from elementary divisor form to invariant factor form,

- For each distinct prime p_j occurring, take the largest power E_j it has in an elementary divisor, and combine and combine $\bigoplus_j R/p_j^{E_j} \cong \mathbb{Z}/(p_1^{E_1} \cdots p_\ell^{E_\ell})$ via CRT. If there's more than one copy of $R/p_j^{E_j}$, just take one of the copies and leave the rest.
- Repeat with the remaining factors.

(b) Convert $\mathbb{R}[x]/(x) \oplus \mathbb{R}[x]/(x^2) \oplus \mathbb{R}[x]/(x-3) \oplus \mathbb{R}[x]/(x-7)^3$ to invariant factor form.

(7) Uniqueness of Smith Normal Form:

- (a) Let D be a diagonal matrix and $d_{11} \mid d_{22} \mid \dots \mid d_{tt}$. Show that $I_r(D) = (d_{11} \cdots d_{rr})$.
- (b) Prove the uniqueness of the Smith Normal Form.