

## 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,  $r, t$  are uniquely determined, and each  $a_i$  is uniquely determined up to associates.

- (1) Use the SMITH NORMAL FORM THEOREM and a homework problem to deduce the existence part of the STRUCTURE THEOREM FOR FINITELY GENERATED MODULES OVER PIDs (INVARIANT FACTOR FORM).
- (2) Remember/state the STRUCTURE THEOREM FOR FINITELY GENERATED ABELIAN GROUPS (INVARIANT FACTOR FORM), and deduce it from the STRUCTURE THEOREM FOR FINITELY GENERATED MODULES OVER PIDs (INVARIANT FACTOR FORM).
- (3) Let  $R$  be a Euclidean domain. Use the SMITH NORMAL FORM THEOREM to deduce<sup>1</sup> that any invertible matrix over  $R$  is a product of elementary matrices.
- (4) Proof of the uniqueness part of the STRUCTURE THEOREM FOR FINITELY GENERATED MODULES OVER PIDs (INVARIANT FACTOR FORM): Suppose that

$$R^m \oplus R/(d_1) \oplus \cdots \oplus R/(d_n) \cong R^{m'} \oplus R/(d'_1) \oplus \cdots \oplus R/(d'_{n'})$$

and  $d_1 | \cdots | d_n$  and also  $d'_1 | \cdots | d'_{n'}$  with  $n \geq n'$ . We proceed by induction on  $n$ .

- (a) Deal with the base case  $n = 0$  (so  $n' = 0$ ).
- (b) Suppose that  $n > 0$ . Let  $\phi$  be an isomorphism from left to right, and  $m = (0, 0, \dots, 1 + (d_n))$  in the left-hand side. Show that  $\text{ann}_R(\phi(m)) = (d_n)$ .
- (c) Show that  $n' > 0$  and that  $d_n | d'_{n'}$ .
- (d) Show that  $d_n$  and  $d'_{n'}$  are associates.
- (e) Complete the induction step and the proof.

---

<sup>1</sup>Hint: Suppose that  $D$  is diagonal and invertible. What can you say about the diagonal entries of  $D$ ?

**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  $M \cong R^r \oplus R/(p_1^{e_1}) \oplus \dots \oplus R/(p_s^{e_s})$ . Moreover, the number  $r$  is uniquely determined and the list  $p_1^{e_1}, \dots, p_s^{e_s}$  is unique up to reordering and associates.

**CRT (FROM 817 HW):** Let  $R$  be a commutative ring, and  $I, J$  ideals such that  $I + J = R$ . Then  $R/IJ \cong R/I \times R/J$  as rings, and hence also as  $R$ -modules.

**(5) 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 to get

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

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

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

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  $\bigoplus_j R/p_j^{E_j} \cong R/(p_1^{E_1} \cdots p_\ell^{E_\ell})$  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  $\mathbb{R}[x]/(x) \oplus \mathbb{R}[x]/(x^2) \oplus (\mathbb{R}[x]/(x - 3))^{\oplus 2} \oplus \mathbb{R}[x]/((x - 7)^3)$  to invariant factor form.**

**(6) 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.