Smith Normal Form

Theorem (Smith Normal Form): Let R be a PID. Let $A \in \mathrm{Mat}_{m\times n}(R)$.

(i) There exist invertible matrices P, Q such that

- $PAQ = D$ is diagonal, meaning $d_{ij} = 0$ whenever $i \neq j$, and
- $d_{11} \mid d_{22} \mid \cdots \mid d_{tt}$, 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
- $a_1 \mid a_2 \mid \cdots \mid a_t$.

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[1] 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 $d_1 \mid \cdots \mid d_n$ and also $d'_1 \mid \cdots \mid d'_{n'}$ 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 ϕ be and isomorphism from left to right, and $m = (0, 0, \dots, 1 + (d_n))$ in the left-hand side. Show that $\mathrm{ann}_R(\phi(m)) = (d_n)$.

(c) Show that $n' > 0$ and that $d_n \mid\ d'_n$.

(d) Show that d_n and d'_n are associates.

(e) Complete the induction step and the proof.

[1] 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 $M \cong R^r \oplus R/(p_1^{e_1}) \oplus \cdots \oplus R/(p_s^{e_s})$. 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:

$\star$ 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

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

(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.

$\star$ 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.

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 $m = 0$.

(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.