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).

From a Lemma in class, we know that A and $PAQ = D$ present isomorphic modules. Then using the homework problem, we get that D presents a module of the form we seek.

(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).

STRUCTURE THEOREM FOR FINITELY GENERATED ABELIAN GROUPS (INVARIANT FACTOR FORM): Let M be a finitely generated abelian group. Then there exist $r, t \geq 0$ and $a_1, \dots, a_t > 0$ such that
- $M \cong \mathbb{Z}^r \oplus \mathbb{Z}/(a_1) \oplus \mathbb{Z}/(a_2) \oplus \cdots \oplus \mathbb{Z}/(a_t)$, and
- $a_1 \mid a_2 \mid \cdots \mid a_t$.

Moreover, r, t are uniquely determined.

This is a special case of the PID theorem since every abelian groups are the same thing as $\mathbb{Z}$-modules, $\mathbb{Z}$ is a PID, and unique up to associate in $\mathbb{Z}$ is same thing as unique up to sign, and since we chose positive numbers, this is actually unique.

(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.

Let A be invertible and write $PAQ = D$ following the theorem. Note that D is invertible and diagonal. We claim that D must be a square matrix with unit diagonal entries. Such

[1]Hint: Suppose that D is diagonal and invertible. What can you say about the diagonal entries of D?

a matrix is invertible, and one can check directly that if any entry is not a unit, then D is not surjective. We can choose D to be the identity matrix by using some elementary row operations. Now $A = P^{-1}IQ^{-1} = P^{-1}Q^{-1}$, and P^{-1} and Q^{-1} are products of elementary matrices, since the inverse of an elementary matrix is an elementary matrix.

(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 $m = (0, 0, \ldots, 1 + (d_n))$ in the left-hand side. Show that $\operatorname{ann}_R(\phi(m)) = (d_n)$.
(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.

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 $p_1, \ldots, p_s \in R$ 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 $p_1^{e_1}, \ldots, p_s^{e_s}$ 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.

(a) $\mathbb{R}[x]^2 \oplus (\mathbb{R}[x]/(x-1))^{\oplus 2} \oplus \mathbb{R}[x]/((x-1)^2) \oplus \mathbb{R}[x]/((x+1)^2)$
(b) $\mathbb{R}[x]/(x(x-3)) \oplus \mathbb{R}[x]/((x-3)(x^2)(x-7)^3)$