Prerequisites:

- [[Smith reduction over a PID]]
- [[PIDs are Noetherian]]
- [[Dimension of a free module]]

Finitely generated modules over a PID

The goal is the following result:

> (Structure theorem) Let M be a finitely generated module over a PID A. Then we have an isomorphism
>
> $$M \simeq A^r \oplus A/(d_1) \oplus \ldots \oplus A/(d_k)$$
>
> with $d_1 \mid \ldots \mid d_k$ nonzero and noninvertible. The d_i's are called the invariant factors of M and are unique up to multiplication by units.

Recall that a *noetherian module* is a module such that any submodule is finitely generated. We have

> A finitely generated module M over a noetherian ring A is itself noetherian.

As we have a map $f : A^n \to M$, we can assume $M = A^n$. We argue by induction on n. The case $n = 1$ is the hypothesis.

Let N be a submodule of M, and $\pi : A^n \to A$ the projection onto the first factor. The submodule $N' = N \cap \ker(\pi) \subset \ker(\pi) = A^{n-1}$ is finitely generated by the induction hypothesis, and N/N' is isomorphic to a submodule (ideal) of A through the restriction of π to N, finitely generated by hypothesis. As both N' and N/N' are finitely generated, N is finitely generated.

This proposition applies to our case, as [[PIDs are Noetherian]], and we e may now show the

> (Adapted basis theorem) Let M be a free module of dimension n over a PID A and N a submodule of M. Then N is free and $\dim N \leq \dim M$.
> More precisely, there is a basis $(e_1, \ldots, e_n)$ of M and scalar $d_1 \mid \ldots \mid d_k$ such that $(d_1 e_1, \ldots, d_k e_k)$ is a basis of N.

As we already know that N is finitely generated, we may write down the map $i : N \hookrightarrow M$ as a rectangular matrix. Applying Smith reduction to it precisely gives the appropriate change of basis/generators system needed.

We may now prove the structure theorem. Let M be as in the statement and $f : A^n \to M$ be surjective. The 1st isomorphism theorem gives $A^n/Ker(f) \simeq M$ and the adapted basis theorem gives $Ker(f) \simeq d_1 A \oplus \ldots \oplus d_k A$. The existence part of the statement follows.

Uniqueness may be deduced from uniqueness in the Smith decomposition or done directly through a careful study of the irreducible factors involved in the decomposition, as done here.

Applications

Finitely generated abelian groups

An immediate application by setting $A = \mathbb{Z}$ is $>$ Any finitely generated abelian group is isomorphic to a group of the form

$$\mathbb{Z}^r \oplus \mathbb{Z}/d_1 \oplus \ldots \mathbb{Z}/d_s$$

with integers $1 < d_1 \mid \ldots \mid d_s$. Moreover, the d_i's satisfying this condition are unique.

Frobenius decomposition and $k[X]$-modules

When E is a finite-dimensional k-vector space, an endomorphism $\varphi \in \mathcal{L}(E)$ induces a $k[X]$-module structure on E, by setting $P \cdot v = P(\varphi)(v)$ for any $P \in k[X], v \in E$.

The structure theorem gives

$$E \simeq k[X]^r \oplus k[X]/(P_1) \oplus \ldots k[X]/(P_n)$$

with unique $P_1 \mid \ldots \mid P_n$. As E is finite dimensional, we must have $r = 0$, and we may assume the P_i are monic and non-constant.

This decomposition is in particular a k-vector space isomorphism, and the subspaces $k[X]/(P_i)$ are *cyclic* subspaces (relatively to φ). It is the Frobenius decomposition of E for φ.