Chapter 12 Modules over PIDs

Basic Goal Determine & describe the structure of an R-module M. In general this is difficult, but there is a simple answer when R is a PID.

Today we will set up some preliminary ideas necessary for the main structure theorems, which we will discuss next time.

First, a certain "finiteness condition." The property of being finitely generated is a useful condition for a module to posses, but sometimes it's not enough to gain sufficient control over a module. For example a finitely generated module can have submodules that are **not** finitely generated.

Example Consider the ring $R = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots = \{(x_1, x_2, x_3, \cdots) \mid x_i \in \mathbb{Z}\}$ consisting of all infinite sequences of integers. (Multiplication and addition are componentwise.) Then R is a finitely generated, R-module, as $(1, 1, 1, 1, \cdots)$ generates all of R. Consider submodule

$$N = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \subseteq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots = R,$$

where N consists of all "eventually zero" sequences of integers. Note N is not finitely generated. Indeed any finite set $A \subseteq N$ cannot generate N because there is an index $k \in \mathbb{N}$ for which every sequence in A is zero after the k^{th} entry. Thus no linear combination of elements of A equals $(1, 1, 1, 1, \cdots 1, 0000 \cdots) \in N$, with the 1 in the $(k+1)$ th entry.

To rule out this kind of behavior, we impose the following condition, which says more than merely being finitely generated.

Definition An R-module M is **Noetherian** if every ascending chain

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq M_4 \subseteq \cdots$$

of R-submodules terminates. That is $M_i = M_{i+1}$ for all sufficiently large i. A ring R is **Noetherian** if its Noetherian as an R-module.

Example $R = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \cdots$ is **not** Noetherian because of the ascending chain $\mathbb{Z} \times 0 \times 0 \times 0 \cdots \subseteq \mathbb{Z} \times \mathbb{Z} \times 0 \times 0 \cdots \subseteq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times 0 \cdots \subseteq \cdots$ of R-modules.

Theorem 1 If M is an R-module, then the following are equivalent

1. M is Noetherian
2. Every non-empty collection of submodules of M has a maximal element under set inclusion.
3. Every submodule of M is finitely generated.

Corollary 2 Any PID R is a Noetherian Ring.

Free modules are another ingredient of our theory.

Review of Free Modules

Recall Let M be an R-module

- A subset $A \subseteq M$ is linearly independent if whenever $0 = \sum r_i a_i$ for $r_i \in R$ and $a_i \in M$, it necessarily follows that each r_i is 0.
- An R-module M is free if there is a linearly independent set $A \subseteq M$ for which $M = RA$. In other words, if each $x \in M$ has a unique expression $x = \sum r_i a_i$.
- Such a set A is called a basis for M.

- If M is free with basis A, then $M = \bigoplus_{i \in A} R$
- The rank of M is the cardinality of the largest set of linearly independent elements of M. [This term applies to any module, not just free modules]

Examples

- $\mathbb{Z}$-module $\mathbb{Z}^n$ is free with basis $A = \{(1,0,0\ldots0), (0,1,0,\ldots0), \ldots (0,0,\ldots1)\}$
- $\mathbb{Z}$-module $\mathbb{Z}_n$ is not free. Reason: It has no basis. Any single element $a \in \mathbb{Z}_n$ is not linearly independent $0 = 0a = na$ so $0 \in \mathbb{Z}_n$ does not have a unique expression as a linear combination of elements in $\{a\}$. Impossible to find a basis - none exists. Thus $\text{rank}(\mathbb{Z}_n) = 0$.
- Check: $\text{rank}(M) = 0 \iff M = \text{Tor}(M)$

Caution!

Despite their similarity to vector spaces, free R-modules don't always work the same way. Example:

Any basis for a subspace $W \subseteq V$ can be extended to a basis of V.

Not so with free-R-modules. $W = 2\mathbb{Z} \oplus 3\mathbb{Z} \subseteq \mathbb{Z} \oplus \mathbb{Z}$ has a basis $A = \{(2,0), (0,3)\}$ but this can't be extended to a basis of $\mathbb{Z} \oplus \mathbb{Z}$.

Such examples tell us that we must take care to prove even those statements that appear obvious.

Proposition 3 Suppose R is an integral domain and M is a free R-module of rank $n < \infty$. Then any set of $n+1$ elements in M is linearly dependent.

Consequence: For any submodule $N \subseteq M$ we have $\text{rank}(N) \leq \text{rank}(M)$.

Be careful with what rank(N) ≤ rank(M) is not saying. It does not say that a submodule N of a free module M is also free. In fact this is false in general:

Example Suppose R is an integral domain that's not a PID, and let $N \subseteq R$ be a non-principal ideal of R.

[For instance, $N = (2, x) \subseteq \mathbb{Z}[x] = R$]

Thus we have $N \subseteq R$ ← Free R-module with basis $A = \{1\}$.

Note that N is not free:
Take any $a, b \in N$. Then $\{a, b\}$ is linearly dependent because $-a, b \in R$ and $b \cdot a + (-a)(b) = 0$. Thus any linearly independent set in N has just one element. If N were free it would have a basis $A = \{a\}$ with $RA = Ra = (a)$, but this can't be because $Ra = (a) \neq N$. i.e. "basis" A can't span. Here rank(N) = 1.

If there is a moral to this example, it's "Avoid R-modules where R is not a PID." But the next result implies things are not so bad if R is a PID. Every submodule N of a free module is itself free, and we can, in a sense, extend a basis of N to a basis of M.

Theorem 4 Let R be a PID, and M be a free R-module of finite rank n. Suppose $N \subseteq M$ is a submodule. Then:

1. N is free and $\text{rank}(N) = n \leq m$
2. There is a basis $\mathcal{B} = \{y_1, y_2, \cdots, y_m\}$ of M and elements $a_1, a_2 \cdots a_n \in R$ such that $\{a_1 y_1, a_2 y_2 \cdots a_n y_n\}$ is a basis of N, and $a_1 \mid a_2 \mid a_3 \mid \cdots \mid a_n$

Example: $\underbrace{4\mathbb{Z} \oplus 6\mathbb{Z} \oplus 0}_{N} \subseteq \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}}_{M}$

"Standard basis" for M: $\{(1,0,0), (0,1,0), (0,0,1)\}$
"Standard basis" for N: $\{(4,0,0), (0,6,0)\}$

Theorem Guarantees: ↓

Basis for M: $\{(2,3,0), (1,1,0), (0,0,1)\}$

$(1,0,0) = -(2,3,0) + 3(1,1,0)$
$(0,1,0) = (2,3,0) - 2(1,1,0)$

$a_1 = 2 \downarrow \quad a_2 = 12 \downarrow$

Basis for N: $\{(4,6,0), (12,12,0)\}$

$(4,0,0) = -2(4,6,0) + (12,12,0)$
$(0,6,0) = 3(4,6,0) - (12,12,0)$

Next time we'll put all these pieces together to get our structure theorem for finitely generated R-modules over PIDs.