

Modules over a Principal Ideal Domain

Introduction...

For our purposes, it's safe to say that the goal of the entire section is to prove one big theorem at the end of the section (theorem IV.6.12) - *the decomposition of a module A over a PID R into a direct sum of a free R -module and a bunch of cyclic torsion R -modules*. We then use this 'structure theorem' to help us with the Jordan decomposition of a linear transformation. The main theorem should remind you of the fundamental theorem of finitely generated abelian groups, which is in fact a corollary of IV.6.12.

There are just a few things along the way we'll have to remember.

For the rest of this discussion, *let R be a principal ideal domain*. Remember that in a principal ideal domain we can speak of prime elements, and we also know what it means for one element to divide another.

Definition 1.

1. Let A be an R -module. A nonzero element $a \in A$ is a *torsion element* if there exists some nonzero $r \in R$ such that $r.a = 0$. If $r.a \neq 0$ for all $r \neq 0 \in R$, the element a is *torsion-free*.
2. The collection of all torsion elements is denoted A_t . This is actually a *submodule* of A , often called the *torsion submodule*.
3. We say A is a *torsion module* if every element of A is a torsion element ($\Leftrightarrow A_t = A$). Likewise the module A is *torsion-free* if all of its elements are ($\Leftrightarrow A_t = 0$).

(Of course, it's not always the case that either $A_t = 0$ or $A_t = A$. Sometimes the torsion module A_t is a nonzero proper submodule of A .)

Definition 2. Let a be a torsion element of the module A . The collection $\mathcal{O}_a = \{r \in R | r.a = 0\}$ is an *ideal* of R , called the *order ideal* of a .

Definition 3. A module A over R is a *cyclic module* if there exists some $a \in A$ such that $A = R.a$.

A few theorems

Recall that, in general, free modules are torsion-free, but the converse does not hold. But when R is a PID, these two notions coincide:

Theorem 1. A *finitely generated*¹ torsion-free module over R is free.

¹If we drop the 'finitely generated' hypothesis, the theorem is no longer true. A counterexample is given by the \mathbb{Z} -module \mathbb{Q} .

There's a nice corollary of this theorem worth remembering:

Corollary 1. *Let F be a free module of the PID R , and let A be a submodule of F . Then A is free.*

Another nice property of PIDs! For an arbitrary ring R it is false that submodules of free modules are free.

Theorem 2. Let A be a finitely generated module over R . then

$$A \cong F \oplus A_t;$$

where A_t is the torsion submodule of A and F is a free submodule of A , and in fact we have $F \cong A/A_t$.

Remember the *order ideal* \mathcal{O}_a we defined above for an element $a \in A$? Well, since we're in a PID, this ideal must be principally generated, right? So there exists some $r \in R$ such that $\mathcal{O}_a = (r)$. We say the element a has *order* r .

Theorem 3. Let A be a *cyclic* torsion module, so $A = R.a$ for some $a \in A$. Then $A \cong R/(r)$, where r is the order of a .

I.e., a cyclic torsion module of R is (isomorphic to) a quotient of R .

Now; not all torsion modules are cyclic. But the cyclic torsion modules are the 'tiniest' torsion modules, in the sense that an arbitrary torsion module can always be written as a direct sum of smaller cyclic torsion submodules:

Theorem 4. Let A be a torsion R -module. Then A is (isomorphic to) a direct sum of cyclic torsion R -modules:

$$A \cong R/(r_1) \oplus \dots \oplus R/(r_k).$$

Now let's put it all together. Given an arbitrary R -module A , first we use theorem 2 above to write A as the direct sum of its torsion and torsion free parts: $A \cong F \oplus A_t$. But we also know how to decompose each of *these* summands:

1. The free part F is just a direct sum of copies of R : $F \cong R \oplus \dots \oplus R$.
2. The torsion part A_t breaks down into a direct sum of *cyclic* torsion modules, according to theorem 4: $A_t \cong R/(r_1) \oplus \dots \oplus R/(r_k)$.

And so we have

$$A \cong (R \oplus \dots \oplus R) \oplus (R/(r_1) \oplus \dots \oplus R/(r_k)).$$

This is the main theorem of the section, but we need to concern ourselves with the number of direct summands of R and also with the elements r_1, \dots, r_k .

The main theorem

Theorem 5. Let A be a finitely generated module over the PID R .

1. Then there exists an integer k and elements r_1, \dots, r_m with $r_1 | r_2 \dots | r_m$ such that

$$A \cong \underbrace{(R \oplus \dots \oplus R)}_{k \text{ summands}} \oplus R/(r_1) \oplus \dots \oplus R/(r_m).$$

2. Then there exists an integer k and a list of prime-power elements $p_1^{s_1}, \dots, p_n^{s_n}$ (primes p_i not necessarily distinct) such that

$$A \cong \underbrace{(R \oplus \dots \oplus R)}_{k \text{ summands}} \oplus R/(p_1^{s_1}) \oplus \dots \oplus R/(p_n^{s_n}).$$

Remark.

1. The (uniquely determined) integer k is the *rank* of A .
2. The list of ideals $(r_1), \dots, (r_m)$ is uniquely determined. The elements r_1, \dots, r_m are called the *invariant factors* of the decomposition.
3. the list of ideals $(p_1^{s_1}), \dots, (p_n^{s_n})$ is also uniquely determined. the elements $p_1^{s_1}, \dots, p_n^{s_n}$ are called the *elementary divisors* of the decomposition.
4. It's possible, of course, for $k = 0$, in which case our module is a torsion module; or for $m = 0$ (and therefore $n = 0$), in which case our module is free.

So there are *two* ways of uniquely decomposing a finitely generated module A , the 'invariant factor way' or the 'elementary divisor way'. But once we pick one of those two ways, there's only one way to do it! Confusing? Good!

There are two applications of this theorem we'll concern ourselves with. The first will be the decomposition of a finitely generated *abelian group*, which we'll look at now just because it's a familiar example. The second will be the decomposition of a vector space under the action of a linear transformation - that's the Jordan decomposition stuff, and really the main reason we're going through all of this. More on that later. First, the easy example...

Example: decomposition of a finitely generated Abelian group

Remember that \mathbb{Z} is a PID, and abelian groups are modules over \mathbb{Z} . So here's what the above theorem has to say about finitely generated Abelian groups: they all look like direct sums of copies of \mathbb{Z} and summands of the form $\mathbb{Z}/r\mathbb{Z}$ ($\cong \mathbb{Z}_r$).

For example, here's a finitely generated Abelian group:

$$\begin{aligned} A &= \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \\ &\cong \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4. \end{aligned}$$

This is the elementary divisor decomposition of A : $k = 2$, $p_1^{s_1} = 3^1$, $p_2^{s_2} = 2^1$, and $p_3^{s_3} = 2^2$.

What about the invariant factor decomposition? Since 3 and 4 are relatively prime, $\mathbb{Z}_3 \oplus \mathbb{Z}_4 \cong \mathbb{Z}_{12}$. So I can write A as

$$A \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{12}.$$

Notice that $2 \mid 12$. I could've also written $\mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \cong \mathbb{Z}_4 \oplus \mathbb{Z}_6$, but then the numbers 4, 6 wouldn't have satisfied the divisibility condition of the 1st part of the main theorem.

One of the things that's a little tricky to get at first is this: given an invariant factor decomposition, can you write down an elementary divisor decomposition, or vice versa? There's a very straightforward little algorithm that allows one to do just that; I'll type it up some time this week.