

9. MODULES OVER A PID

This week we are proving the fundamental theorem for finitely generated modules over a PID, namely that they are all direct sums of cyclic modules. The proof will be in stages. On the first day I decomposed a module into a torsion and torsion-free part. The presentation was a little disorganized so that the steps do not follow one after the other but rather the other way around, i.e., to prove (1) we need to prove (2) and to prove (2) we need to prove (3), etc. I call this the “motivational order.” At the end we will go over the lemmas and put them in correct logical order.

9.1. torsion and torsion-free. Suppose that R is a PID and M is a finitely generated R -module. The main example I talked about was $R = \mathbb{Z}$ in which case $M = G$ is a f.g. abelian group.

Definition 9.1. M is *torsion-free* if $\text{ann}(x) = 0$ for all $x \neq 0$ in M .

Definition 9.2. M is *torsion* if $\text{ann}(x) \neq 0$ for all $x \neq 0$ in M .

For example, R itself is torsion-free and $R/(a)$ is torsion. In the case $R = \mathbb{Z}$, \mathbb{Z}^n and \mathbb{Q} are torsion-free additive groups. However, \mathbb{Q} is not finitely generated. The finitely generated torsion abelian groups are exactly the finite abelian groups.

The first decomposition theorem is the following.

Theorem 9.3. *Every f.g. module over a PID is a direct summand of a torsion module and a torsion-free module:*

$$M \cong tM \oplus fM$$

where tM is torsion and fM is torsion free.

The second theorem tells us what the torsion-free part looks like:

Theorem 9.4. *A f.g. module over a PID is torsion-free if and only if it is free:*

$$fM \cong R^n.$$

9.1.1. *torsion submodule.* I used two lemmas to show that the second theorem implies the first theorem. During the class we decided that these two lemmas hold over any domain. First I need a definition.

Definition 9.5. Suppose that M is a module over a domain R . Then the *torsion submodule* of M is defined to be the set of all elements of M with nonzero annihilator ideal:

$$tM := \{x \in M \mid \text{ann}(x) \neq 0\}$$

Lemma 9.6. tM is a submodule of M provided that R is a domain.

Proof. We need to show that tM contains 0 and is closed under addition and scalar multiplication.

- (1) $0 \in tM$ since $\text{ann}(0) = R$.
- (2) If $x, y \in tM$ then there are nonzero elements $a, b \in R$ so that $ax = by = 0$. Then $ab(x + y) = 0$. So, $x + y \in tM$.
- (3) If $x \in tM$ and $r \in R$ then $\text{ann}(rx) \supseteq \text{ann}(x)$ is nonzero.

In the second step we need to know that $ab \neq 0$. □

Lemma 9.7. The quotient M/tM is torsion-free provided that R is a domain.

Proof. Suppose not. Then there is a nonzero element $x + tM$ in M/tM and $a \neq 0$ in R so that $ax + tM$ is zero, i.e., $ax \in tM$. But this means there is a nonzero element $b \in R$ so that $bax = 0$. But $ba \neq 0$. So, $x \in tM$ which is a contradiction. □

It was in this proof that I mentioned the *fraction notation*:

$$(tM : x) := \{a \in R \mid ax \in tM\}.$$

Next, I showed that the second theorem (Theorem 9.4) implies the first (Theorem 9.3).

Proof of Theorem 9.4. Let $fM = M/tM$. Since this is free, there is a section $s : fM \rightarrow M$ of the projection map $M \rightarrow M/tM$. Then

$$j \oplus s : tM \oplus fM \rightarrow M$$

is an isomorphism where $j : tM \rightarrow M$ is the inclusion map. □

Next, we need to prove that f.g. torsion-free modules are free and that f.g. torsion modules are direct sums of cyclic modules. I intend to use “purity” to do both.

9.1.2. pure submodules.

Definition 9.8. We say that a submodule $N \subseteq M$ is *pure* if whenever $x \in M$ and $a \in R$ with $ax \in N$ there exists $z \in N$ so that $az = ax$. In other words: “If an element of N is divisible by $a \in R$ in M then it is divisible by a in N .”

The point is that pure submodules are direct summands in f.g. modules over PID’s. However, using this fact is a little tricky as we saw the next day.

On the second day I pointed out that if P is a pure submodule of a f.g. module M over a PID, then P is a direct summand. However, we cannot use this fact to prove the main theorem because it uses the main theorem, namely that f.g. modules are direct sums of cyclic modules. However, we use the main theorem on a module with a fewer number of generators than M . So, this can be used in an inductive proof of the main theorem. The theorem is:

Theorem 9.9. *Suppose that P is a pure submodule of a f.g. module M over a PID R and M/P is a direct sum of cyclic modules. Then P is a direct summand of M .*

Proof. Suppose that M/P is a direct summand of cyclic modules. Then each summand is generated by some element $x_i + P$ with annihilator (a_i) . This means that $(x_i : P) = (a_i)$. In other words, $a_i x_i \in P$. Since P is pure, there is an element $z_i \in P$ so that $a_i z_i = a_i x_i$. But then

$$x_i + P = (x_i - z_i) + P$$

and $a_i(x_i - z_i) = 0$. So $s_i(x_i + P) = x_i - z_i$ gives a lifting $s_i : R/(a_i) \rightarrow M$ of the direct summand $R/(a_i)$ of M/P to M and, together, these give an isomorphism

$$\left(\bigoplus s_i \right) \oplus j : \bigoplus R/(a_i) \oplus P \xrightarrow{\cong} M$$

where $j : P \rightarrow M$ is the inclusion map. \square

To find the pure submodule, I need to take a maximal cyclic submodule of M . This exists because M is Noetherian. So that is next.

9.2. submodules of free modules.

Theorem 9.10. *Suppose that $M = R^n$ is a free R -module with n generators where R is a PID. Then any submodule of M is free with n or fewer generators.*

Proof. This is by induction on n . If $n = 1$ then $M = R$ and the submodules are either R or an ideal Rx . But R is a domain. So, either $x = 0$ or $\text{ann}(x) = 0$. So, Rx is free with 0 or 1 generator.

Now suppose that $n \geq 2$ and N is a submodule of R^n . Then we want to show that $N \cong R^m$ where $m \leq n$. Let e_1, \dots, e_n be the free generators of $M = R^n$. Let R^{n-1} denote the free submodule of M generated by e_1, \dots, e_{n-1} . Then, by induction on n , we have:

$$N \cap R^{n-1} \cong R^{m-1}$$

where $m \leq n$. If $N = N \cap R^{n-1}$ we are done. Otherwise, let J be the set of all e_n coordinates of all elements of N . I.e.,

$$J = \left\{ a \in R \mid (\exists x \in N) x = ae_n + \sum_{i=1}^{n-1} a_i e_i \right\}$$

We get at least one nonzero element in J since N is not contained in R^{n-1} . Then it is easy to see that J is an ideal (or all of R) since it is closed under addition and scalar multiplication and is nonempty. Therefore, $J = (b)$ is generated by one element $b \neq 0$. (So, every $a \in J$ has the form $a = rb$ where $r \in R$ is unique.)

By definition, there is an element $x_0 \in N$ so that

$$x_0 = be_n + \sum_{i=1}^{n-1} a_i e_i.$$

This can be used to define a homomorphism

$$\phi : (N \cap R^{n-1}) \oplus R \rightarrow N$$

by $\phi(y, r) = y + rx_0$. I claim that ϕ is an isomorphism.

To see that ϕ is onto, take any element $x \in N$. Then $x = ae_n +$ (some element of R^{n-1}) where $a = rb$. So,

$$x - rx_0 \in N \cap R^{n-1}$$

and $x = \phi(x - rx_0, r)$. To see that ϕ is 1-1 suppose that $\phi(y, r) = 0$. Then $y = -rx_0$. Looking at the last coordinate this gives $rb = 0 \Rightarrow r = 0 \Rightarrow y = 0$. Therefore ϕ is an isomorphism. Its inverse gives:

$$N \cong (N \cap R^{n-1}) \oplus R \cong R^{m-1} \oplus R \cong R^m$$

where $m \leq n$. □

Corollary 9.11. *If M is an R -module generated by n elements then every submodule of M is generated by $\leq n$ elements. In particular, M is Noetherian.*

Proof. If M is generated by x_1, \dots, x_n then we have an epimorphism

$$\phi : R^n \rightarrow M$$

given by $\phi(a_1, \dots, a_n) = \sum a_i x_i$. If $N \subseteq M$ then N is a quotient of $\phi^{-1}N$ which is free on $\leq n$ generators by the theorem. □

9.3. maximal cyclic submodules. Since f.g. modules are Noetherian, they have maximal cyclic submodules. This is because any sequence of cyclic submodules:

$$Rx_1 \subseteq Rx_2 \subseteq Rx_3 \subseteq \cdots \subseteq M$$

must eventually stop. (If there were no maximal cyclic submodule, I could keep going forever.)

Lemma 9.12. *Suppose that M is torsion-free and $Rx \subseteq M$ is a maximal cyclic submodule. Then $x \notin aM$ for any nonunit $a \in R$. (I.e., $x = az \Rightarrow a$ is a unit.)*

Proof. Suppose that $x = az$. Then $Rx \subseteq Rz$. Since Rx is maximal cyclic, $Rx = Rz$ which implies that $z = bx$ for some $b \in R$. So, $x = az = abx$ which implies $(ab - 1)x = 0$. Since M is torsion-free, this implies that $ab = 1$, i.e., a is a unit. \square

Lemma 9.13. *Every maximal cyclic submodule of a torsion-free module is pure.*

Proof. Suppose that $Rx \subseteq M$ is a maximal cyclic submodule. Suppose there are elements $y \in M, a \in R$ so that $ay \in Rx$. Then $ay = bx$. We need to show that this is a times an element of Rx . In other words, we want to show that $a|b$ (a divides b). This is the same as saying that $\frac{b}{a} \in R$.

At this point I explained this equivalent formulation of divisibility. Since R is a domain, it is contained in its field of fractions: $R \subseteq Q(R)$. The fraction $\frac{b}{a}$ is an element of $Q(R)$. If $a|b$, then $b = ra$ for some $r \in R$ and

$$\frac{b}{a} = \frac{r}{1} \in R$$

and conversely. So, $a|b \Leftrightarrow \frac{b}{a} \in R$.

Let $c \in R$ be the greatest common divisor of a, b . I.e., $(a, b) = (c)$. Then $c|a$ and $c|b$. I.e., $\frac{a}{c}, \frac{b}{c} \in R$ and

$$\frac{a}{c}y = \frac{b}{c}x$$

since M is torsion-free. (c times the difference is zero. So, the difference is zero.) But $(\frac{a}{c}, \frac{b}{c}) = (1)$, i.e., there exist $s, t \in R$ so that

$$1 = \frac{a}{c}s + \frac{b}{c}t.$$

This implies that

$$x = \frac{a}{c}sx + \frac{b}{c}tx = \frac{a}{c}sx + \frac{a}{c}ty = \frac{a}{c}(sx + ty)$$

since $bx = ay$. By the previous lemma, this implies that $\frac{a}{c}$ is a unit, i.e., $\frac{c}{a} \in R$. So

$$\frac{b}{a} = \frac{b}{c} \frac{c}{a} \in R$$

as desired. \square

We need one more lemma.

Lemma 9.14. *If P is a pure submodule of a torsion-free module M then M/P is torsion-free.*

Proof. Suppose not. Then there is a nonzero element $x + P \in M/P$ so that $a(x + P) = 0 + P$. I.e., $ax \in P$. But P is pure. So, there is $z \in P$ so that $az = ax$. Then $a(x - z) = 0$ in M which implies that $x = z$ since M is torsion free. So, $x + P = z + P = P$ is the zero element of M/P which is a contradiction. \square

Now I am ready to prove Theorem 9.4: Finitely generated torsion-free modules over PID's are free, completing the proof that

$$M \cong tM \oplus fM \cong tM \oplus R^n.$$

Proof of Theorem 9.4. The proof is by induction on the number of generators. If M has one generator x then $M = Rx \cong R$ is free. So, suppose M has n generators x_1, \dots, x_n where $n \geq 2$. Since Rx_1 is a cyclic submodule of M it is contained in a maximal cyclic submodule Rx . By Lemma 9.13, Rx is pure. By Lemma 9.14, this implies that M/Rx is torsion-free. But M/Rx is generated by $n - 1$ elements (the images of the generators x_2, \dots, x_n). So, it is free, say, $M/Rx \cong R^m$. But this implies that

$$M \cong Rx \oplus R^m \cong R \oplus R^m$$

is also free. \square

It remains to show that the torsion submodule tM is also a direct sum of cyclic modules. I want to do the same proof, namely, since M is Noetherian, we can find a maximal cyclic submodule Rx . Since M/Rx will be generated by $n - 1$ elements, it is a sum of cyclic modules.

After some stumbling, I decided I need a more precise construction of a maximal cyclic submodule. I took a generator with minimal annihilator. And this works the best for p -primary modules.

9.4. p -primary decomposition. p -primary modules are generalizations of abelian p -groups. We showed that finite nilpotent groups are products of their p -Sylow subgroups. For finite abelian groups and, more generally, for torsion modules over PID's, this is very easy to prove. It follows from the unique factorization theorem. (I.e., every PID is a UFD.)

Definition 9.15. An element $x \in M$ is called p -primary if it has annihilator

$$\text{ann}(x) = (p^n)$$

for some $n \geq 0$ where $p \in R$ is irreducible. A module M is called p -primary if every element is p -primary. (Note that $0 \in M$ is p -primary for every p .)

I should have prove the following lemma first:

Lemma 9.16. *If $p^n x = 0$ where $n \geq 0$ then x is p -primary.*

Proof. Suppose $\text{ann}(x) = (a)$. Then $p^n x = 0$ implies that $p^n = ab$ for some $b \in R$. By unique factorization this implies that $a = up^k$ where u is a unit in R and $k \leq n$. But then $\text{ann}(x) = (up^k) = (p^k)$. \square

For modules over a PID, the ‘‘Sylow theorems’’ are very easy to prove:

Lemma 9.17. *The set of p -primary elements of any module M over a PID is a submodule.*

Definition 9.18. If $p \in R$ is irreducible, let M_p be the submodule of M consisting of all p -primary elements of M .

Proof. If x, y are nonzero p -primary elements of M then $p^n x = 0$ and $p^m y = 0$. Then $p^{n+r} x = 0$ for any $r \in R$ and $p^{n+m}(x+y) = 0$. Therefore, rx and $x+y$ are p -primary by the lemma. \square

Theorem 9.19. *Every torsion module M over a PID is a direct sum of p -primary modules:*

$$M = \bigoplus_p M_p.$$

Proof. First choose irreducible elements p_i so that every irreducible element of R is up_i for some unit u and some unique p_i . By the lemma, for each of these irreducibles we have a submodule $M_{p_i} \subseteq M$. By the universal property this gives a homomorphism

$$\phi : \bigoplus M_{p_i} \rightarrow M$$

I claim that this is an isomorphism.

It follows from unique factorization that this map is onto: Suppose $x \neq 0 \in M$ with annihilator $\text{ann}(x) = (a)$. Since M is torsion, $a \neq 0$. So

$$a = u \prod_{i=1}^k p_i^{n_i}$$

where u is a unit. Then, for each i ,

$$\frac{a}{p_i^{n_i}} = up_1^{n_1} \cdots \widehat{p_i^{n_i}} \cdots p_k^{n_k} \in R.$$

There is no irreducible element of R which divides each of these elements. This implies that there are elements $r_i \in R$ so that

$$1 = \sum_{i=1}^k r_i \frac{a}{p_i^{n_i}}.$$

Apply this to x to get:

$$x = \sum_{i=1}^k r_i \frac{a}{p_i^{n_i}} x = \sum_{i=1}^k r_i x_i$$

where

$$x_i = \frac{a}{p_i^{n_i}} x$$

is p_i -primary since $p_i^{n_i} x_i = ax = 0$. This shows that $x = \phi(r_i x_i)_i$ is in the image of ϕ and therefore ϕ is onto.

To show that ϕ is 1-1 suppose that $(x_i)_i$ is in the kernel of ϕ . Then

$$\sum_{i=1}^k x_i = 0$$

where x_i is p_i -primary. Thus sum is finite since the direct sum is equal to the weak product. Suppose that $\text{ann}(x_i) = (p_i^{n_i})$. Then the product $p_2^{n_2} \cdots p_k^{n_k}$ annihilates x_2, \dots, x_k and therefore annihilates their sum

$$x_2 + \cdots + x_k = -x_1$$

This implies that $p_2^{n_2} \cdots p_k^{n_k} \in (p_1^{n_1})$, i.e.,

$$p_2^{n_2} \cdots p_k^{n_k} = ap_1^{n_1}$$

for some $a \in R$. By unique factorization this is only possible if $n_1 = 0$, i.e., $x_1 = 0$. The same argument shows that $x_i = 0$ for all i . So, ϕ is a monomorphism and thus an isomorphism as claimed. \square

9.5. decomposition of p -primary modules. Now we come to the final step in the proof of the main theorem, namely, I will prove that every f.g. p -primary module is a direct sum of cyclic modules. But first some lemmas.

Lemma 9.20. *Any quotient of a p -primary module is p -primary.*

Proof. This is obvious. If $x \in M$ then $p^n x = 0$ for some n . But then $p^n(x + N) = 0$ in M/N . So, M/N is p -primary. \square

Lemma 9.21. *Suppose M is a f.g. p -primary module and $a \in R$ so that $p \nmid a$. Then, there is a $b \in R$ so that multiplication by ab is the identity on M .*

Proof. Let x_1, \dots, x_k be generators for M and suppose that $\text{ann}(x_i) = p^{n_i}$. Let $n = \max(n_i)$. Then $p^n M = 0$. Since $a \notin (p)$, $(a, p^n) = (1)$. So, there exist $b, c \in R$ so that

$$ab + p^n c = 1$$

But $p^n = 0$ on M . So, $ab = 1$ on M . \square

Theorem 9.22. *If M is a f.g. p -primary module over a PID R then M is a direct sum of cyclic p -primary modules.*

Proof. Let x_1, \dots, x_k be generators for M where k is minimal. Then we will show by induction on k that M is a direct sum of k or fewer cyclic summands. Since M/Rx_1 is generated by $k - 1$ elements, it is a direct sum of $\leq k - 1$ cyclic p -primary modules by induction. So, it suffices to show that Rx_1 is a pure submodule of M .

Let $\text{ann}(x_i) = p^{n_i}$ and let $n = \max(n_i)$. We will assume that $n = n_1$. Then $p^n M = 0$ and

$$p^{n-1}x_1 \neq 0.$$

Claim Rx_1 is a pure submodule of M .

proof: Suppose that $y \in M$ and $a \in R$ so that $ay \in Rx_1$. If $ay = 0$ then $ay = a0 \in aRx_1$. So, we may assume that $ay \neq 0$. Then $ay = bx_1$ for some $b \in R$. Write a, b as $a = p^k s, b = p^m t$ where s, t are not divisible by p . The condition $ay = p^m t x_1 \neq 0$ means that $m < n$. So,

$$n - m - 1 \geq 0.$$

By the lemma, there is an element $r \in R$ so that $sr = 1$ on M . This gives:

$$(9.1) \quad ay = p^k sy = p^m t x_1 = p^m s r t x_1$$

So, it suffices to show that $k \leq m$ since this would give $ay = a(p^{m-k} r t x_1)$. To prove that $k \leq m$ multiply both sides of Equation (9.1) by p^{n-m-1} .

This gives

$$p^{k+(n-m-1)}sy = p^{m+(n-m-1)}tx_1 = p^{n-1}tx_1 \neq 0$$

since $p^{n-1}x_1 \neq 0$ and multiplication by t is an isomorphism on M . But this implies that the left hand side is also nonzero. Since $p^n M = 0$ this implies that

$$k + n - m - 1 < n$$

In other words, $k < m + 1$ or $k \leq m$. This proves the claim and the theorem. \square

9.6. Structure theorem for f.g. modules over a PID. Now we have the complete proof of the following existence theorem.

Theorem 9.23. *Every f.g. module over a PID is a direct sum of cyclic primary modules*

$$M \cong R^r \oplus \bigoplus R/(p_i^{n_i}).$$

Proof. Here is an outline of the entire proof.

- (1) First, we defined the torsion submodule tM of M . This exists since R is a domain.
- (2) The quotient M/tM is torsion-free. Again this holds over any domain.
- (3) Since R is a PID, every submodule of a f.g. free module is f.g. free. This implies:
 - (a) M is Noetherian (all submodules are finitely generated) and
 - (b) Every f.g. torsion-free module is free.
- (4) The conclusion was that M is a direct sum of tM and a f.g. free module:

$$M \cong tM \oplus R^r$$

- (5) If $p \in R$ is irreducible, the set of p -primary elements of any module forms a submodule M_p .
- (6) It follows from unique factorization that every torsion module is a direct sum of p -primary modules:

$$tM \cong \bigoplus M_{p_i}$$

- (7) In a p -primary module M , a generator with minimal annihilator generates a pure cyclic submodule. Then we use the lemma:
- (8) If N is a pure submodule of M and M/N is a direct sum of cyclic modules then N is a direct summand of M .
- (9) Every f.g. p -primary module is a direct sum of cyclic p -primary modules.

□

The structure theorem for finitely generated modules over a PID also says the decomposition is unique:

Theorem 9.24. *For any f.g. module M over a PID, the numbers r and the sequence of pairs (p_i, n_i) are uniquely determined up to permutation of indices.*

We will prove this later using tensor products. The number $r = rk(M)$ is called the *rank* of M . It is the dimension of $Q(R) \otimes M$.