CHAPTER 33

Modules over PIDs

Exercise 33.1. Here are some opening exercises:

(1) Let F be a field and $g \in F[t]$. Show that $g(x) = 0$ if and only if the polynomial $t - x$ divides the polynomial $g(t)$ in $F[t]$. (Hint: The division algorithm.)

(2) Fix a commutative ring R. Fix $a, b \in R$.Show

$$(a) = (b)$$

iff $a = ub$ for some unit u.

(3) Let R be a commutative ring. Prove a unit cannot be a zero divisor. What is the contrapositive?

(4) Prove that any field is a PID.

Answer:

(1) This is certainly true for $\deg g = 0$, for $g(x) = a_0 = 0$ if and only if $g = 0$, while $(t - x)0 = 0$, so $t - x$ divides g.

Now assume $\deg g \geq 1$. Use the division algorithm:

$$g = (t - x)q + r.$$

Then

$$g(x) = (x - x)q(x) + r(x) = 0q(x) + r(x) = r(x).$$

This means $r(x) = 0$. But $\deg r < \deg(t - x)$, meaning $r(x)$ must be a degree 0 polynomial for which x is a root—this means $r = 0$ as a polynomial, and

$$g = (t - x)q.$$

(2) Since $a = ub$, we see that $a \in (b)$. Thus $(a) \subset (b)$. (For if $y = ra$, then $y = rub = (ru)b$, so any multiple of a is a multiple of b.)

Likewise, $u^{-1}a = b$, so we see that $b \in (a)$, thus $(b) \subset (a)$.

(3) If x is a unit, $xy = 1$ for some $y \in R$. Then for any a, $axy = a1 = a$. On the other hand if $ax = 0$, we also have that $axy = 0y = 0$. Hence $a = 0$, so x cannot be a zero divisor.

(4) A commutative ring is a field if and only if its only ideals are $\{0\}$ and R itself. Well, $\{0\}$ is principal since $\{0\} = (0)$. Also, $R = (1)$ for any ring.

So we only need to show that there are no zero divisors aside from zero. But in a field, every non-zero element is a unit, so there are no zero divisors.

1. Review, and fixing a proof

Last time, we stated in class

Theorem 33.2 (Factorization for PIDs)**.** Let R be a PID. Then for any non-zero element $x \in R$, there exists a finite collection of distinct prime elements $p_1, \dots, p_k \in R$ so that

$$x = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}, \qquad n_i \geq 1$$

But what did the proof actually show? We showed that if we keep decomposing an element f into products, the process has to stop at some point. But there was a mistake in the proof, because the chain of thought is actually incorrect. A great teaching moment, when the teacher makes the mistake.

The core of what we proved last time was the following:

Proposition 33.3. Fix a principal ideal domain R. Assume we have an increasing sequence of ideals

$$I_1 \subset I_2 \subset \dots.$$

Then there is some finite n for which $I_n = I_{n+1} = \dots$.

Proof. As a reminder, the way this went was as follows: Let $I = \bigcup I_j$. Since R is a PID, there is a single element a that generates I, so $I = (a)$. But $a \in I$, which means $a \in I_n$ for some finite n (by definition of union). Then we'd have

$$(a) \subset I_n \subset (a)$$

so $I_n = (a)$. But if $I_n \subset I_{n+j} \subset (a) = I_n$, we have that $I_n = I_{n+j}$ for all j. □

Remark 33.4. Any commutative ring R satisfying this *ascending chain condition*—that is, the property that any ascending chain of ideals must terminate—is called *Noetherian*, after Emmy Noether (who is arguably the most famous woman in mathematics and physics). If you take any kind of course in algebraic geometry, you'll see plenty more of Noetherian rings.

Correct proof of theorem. Let $x \in R$, $x \neq 0$. If x is a prime, we're finished: Set $p_1 = x$.

Otherwise, $x = a_1 b_1$ for some non-unit elements $a_1, b_1 \in R$. If both are prime, we're done. Let's say a_1 isn't prime. Then $a_1 = a_2 b_2$, where a_2, b_2 are not units. What does this mean?

$$a_1 \in (a_2)$$

so $(a_1) \subset (a_2)$.

Note importantly that this inclusion is *proper*, so $(a_1) \neq (a_2)$. Why is that? Otherwise, we would have

$$(a_2) \subset (a_1) \implies a_1 = ca_1b_2 = a_1cb_2 \implies (1 - cb_2)a_1 = 0. \implies (1 - cb_2) = 0$$

so b_2 would be a unit. (Note that in the last $\implies$, we're using the fact that R is a *domain.*)

And if a_2 is not prime, we would again have $a_2 = a_3b_3$, with a proper inclusion $(a_2) \subset (a_3)$. Going on in this way, each time we write $a_i = a_{i+1}b_{i+1}$, we have a chain of inclusions

$$\ldots \subset (a_i) \subset (a_{i+1}) \subset \ldots.$$

But as we saw before, at some point (a_n) must equal (a_{n+1}), which violates the proper inclusion property, for then $(a_{n+1}) \subset (a) \subset (a_n) \implies (a_{n+1}) = (a_n)$.

What this means is that some a_n *has* to be prime at a finite stage n.

What we've shown is:

(*) every non-zero element x can be written

$$x = p_1y_1$$

where p_1 is prime.

But we may have no control on y_1. Now we need to show that x can be written as a finite product of primes. (Repeating the above process, it's not clear that we get to finitely many primes in finite time!) Well, if y_1 isn't irreducible, we can write

$$y_1 = p_2y_2$$

where p_2 is a prime (by using (*) above). If y_2 isn't irreducible, we can go on in this way, and we have again a chain

$$(x) \subset (y_1) \subset (y_2) \subset \ldots$$

of proper inclusions. If y_n isn't a prime at some point we have a contradiction, since there can be no infinite ascending chain of ideals like this in a PID (as we've shown above). So set $p_{n+1} = y_n$, and we have written

$$\begin{aligned} x &= p_1y_1 \\ &= p_1p_2y_2 \\ &= \ldots \\ &= p_1p_2 \ldots p_ny_n \\ &= p_1p_2 \ldots p_np_{n+1} \end{aligned}$$

which shows any element x can be written as a product of primes. □

Chit-chat 33.5. There are other things I should prove, like unique factorization—in fact, if one writes

$$x = up_1^{n_1} \dots p_k^{n_k}$$

where u is a unit and p_i are primes, we can guarantee that each p_i is relatively prime to each other, and that the p_i are unique up to re-ordering and multiplication by units. But we won't go into that.

2. Modules over PIDs

The following is a theorem we won't prove, but I'll post further notes on the proof of it. It shows that every finitely generated module over a PID has a very simple form. (If all rings had modules as simple as this, the world would be a wonderful place.)

Theorem 33.6 (Classification of finitely generated modules over PIDs)**.** Let R be a PID, and let M be a finitely generated R-module. Then there exists a finite collection of primes $p_1, \dots, p_k \in R$, with p_i possibly equaling p_j, and numbers $n_0, \dots, n_k$ such that

$$M \cong R^{n_0} \oplus R/(p_1^{n_1}) \oplus R/(p_2^{n_2}) \oplus \dots \oplus R/(p_k^{n_k}).$$

Moreover, this decomposition is unique up to re-ordering and unit multiples of p_i.

Remark 33.7. What do we explicitly mean by uniqueness? Given some other decomposition

$$M \cong R^{m_0} \oplus R/(q_1^{m_1}) \oplus \dots \oplus R/(q_j^{m_j})$$

where each q_i is a prime, then we have

(1) $m_0 = n_0$,
(2) $j = k$, and
(3) There is some re-ordering of the i so that $n_i = m_i$, and that p_i and q_i are unit multiples of each other.

Chit-chat 33.8. I emphasize that p_i could equal p_j for $i \neq j$. In other words, modules aren't like numbers—they don't admit unique prime factorizations in which $p \cdot \ldots \cdot p$ can be grouped into p^k; the repetition of primes is important.

Example 33.9 ($R = F$ a field)**.** If F is a field, what are the prime elements? There are no prime elements, since prime elements are in particular non-zero, non-unital elements. So every finitely generated module over F must be of the form

$$M \cong F^{n_0}$$

which is just the statement that every finitely generated F-module admits a finite basis. n_0 is the dimension of the vector space.

Example 33.10 ($R = \mathbb{Z}$)**.** What are the primes of $\mathbb{Z}$? Numbers of the form $\pm p$ for p a prime number. (Note that $(p) = (-p)$.) So the above theorem is stating that any finitely generated $\mathbb{Z}$-module—that is, any finitely generated *abelian group*—is of the form

$$M \cong \mathbb{Z}^{n_0} \oplus \mathbb{Z}/p_1^{n_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p_k^{n_k}\mathbb{Z}.$$

Uniqueness means, for example, that

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \qquad (p_1 = p_2 = 2, \text{ while } n_0 = 0,\ n_1 = n_2 = 1.\ )$$

and

$$\mathbb{Z}/4\mathbb{Z} \qquad (p_1 = 2, \text{ while } n_0 = 0,\ n_1 = 2.\ )$$

are not isomorphic $\mathbb{Z}$-modules (i.e., not isomorphic abelian groups). This, we already knew—for instance, $\mathbb{Z}/4\mathbb{Z}$ is cyclic, while the former group is not. Note that the former group is also an example of when $p_i = p_j$ for $i \neq j$.

Example 33.11. Again let $R = \mathbb{Z}$. We can classify every abelian group of order 8 now:

	n_0	$p_1, p_2, \ldots, p_k$	$n_1, \ldots, n_k$
$\mathbb{Z}/8\mathbb{Z}$	0	2	3
$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	0	2, 2	2, 1
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	0	2, 2, 2	1, 1, 1

Example 33.12. As another example, let $M = \mathbb{Z}/6\mathbb{Z}$. This is not of the form stated in the theorem. In fact, M is isomorphic to

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

as you've proven in homework.

3. When the PID is a polynomial ring

The only other PID we've talked about is $R = F[t]$. What are the primes of $F[t]$? In general, this is a hard question. A first prerequisite for f to be a prime is that it have no roots in F—otherwise, as we saw earlier, f can be factored by a linear polynomial, which is not a unit in $F[t]$.

But there are a class of fields in which you can characterize the irreducible elements of $F[t]$ easily:

Definition 33.13. A field F is called *algebraically closed* if every polynomial $f \in F[t]$ has a root.

The obvious example is $F = \mathbb{C}$. The perhaps surprising theorem is:

Theorem 33.14. Any field F admits an injective ring homomorphism into an algebraically closed field.

Remark 33.15. Note that not every field F admits an injective ring homomorphism into $\mathbb{C}$. For instance, if $F = \mathbb{Z}/2\mathbb{Z}$, the multiplicative unit $\overline{1}$ satisfies the property that $\overline{1} + \overline{1} = 0$. Any ring homomorphism $\phi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{C}$ must satisfy the property that $\phi(\overline{1}) + \phi(\overline{1}) = \phi(0)$, which is impossible, since a ring homomorphism must also satisfy the constraint that $\phi(\overline{1}) = 1_{\mathbb{C}}$.

In other words, there must be some *other field*, other than $\mathbb{C}$, which has a root to any polynomial, and which admits an injective map from $\mathbb{Z}/2\mathbb{Z}$. Seems mysterious, doesn't it?

We'll talk about this a little bit more later. Regardless, your mind can have in mind $\mathbb{C}$ for now.

Proposition 33.16. If F is algebraically closed, the only irreducible elements of $F[t]$ are (non-zero) linear polynomials.

Proof. We know already that any non-zero linear polynomial is irreducible—for any pair $f = ab$ either a or b must have degree 0, meaning any factorizations of f involves a unit.

On the other hand, if f has degree ≥ 2, we know f has a root by definition of algebraically closed field, so we can always write

$$f = (t - x)q$$

for some q with degree $\deg f - 1$. Neither $t - x$ nor q can be units since they are not constant polynomials (they have non-zero degree) so no polynomial of higher degree can be a prime. □

Corollary 33.17. If F is algebraically closed, then any finitely generated module over F is isomorphic to

$$F[t]^{n_0} \oplus F[t]/(t - \lambda_1)^{n_1} \oplus \ldots \oplus F[t]/(t - \lambda_k)^{n_k}$$

for some choice of elements $\lambda_i \in F$ and integers $n_1, \ldots, n_k \geq 1$.

Why might this be helpful for us? Well, a good example of an $F[t]$-module is an F-vector space V together with a linear map $A : V \to V$. In other words, this helps us classify linear maps A!

You've already seen ways to think about linear maps A, by using change-of-bases, and eigenvectors and all that. We'll see that this decomposition gives us a powerful change-of-basis next class.