Lecture 17: Modules over a PID

Daniel Bump

June 4, 2020

Abelian groups as torsion modules over a PID

An abelian group (written additively) is the same as a $\mathbb{Z}$-module. Most of the important facts about finite abelian groups (or finitely-generated abelian groups) generalize to finitely-generated modules over a PID.

Once generalized, they have applications to linear algebra through another PID, the polynomial ring $F[X]$ where F is a field.

We begin by reviewing a fact you may know from Math 120.

Review from Math 120: Structure of finite abelian groups

Proposition

Let G be a finite abelian group.
(i) G is a direct sum of cyclic groups:

$$G \cong \bigoplus_{i=1}^{h} (\mathbb{Z}/m_i\mathbb{Z}).$$

(ii) The decomposition is unique if we assume that m_i divides m_{i+1} $(1 \leqslant i < h)$.
(iii) Alternatively, the decomposition is unique if we require the m_i to be prime powers.

The uniqueness for (ii) is not that the subgroups isomorphic to $\mathbb{Z}/m_i\mathbb{Z}$ are determined: they are not. But $m_1, \cdots, m_h$ are uniquely determined. (Similarly for (iii).)

Isomorphisms for cyclic groups

There is some freedom of choice if we do not restrict the m_i since if $(a, b) = 1$ then if $(a, b) = 1$ then

$$\mathbb{Z}/ab\mathbb{Z} \cong (\mathbb{Z}/a\mathbb{Z}) \oplus (\mathbb{Z}/b\mathbb{Z}).$$

We can use this to go back between the two decompositions. For example suppose we start with the decomposition (iii) of a group into prime powers and

$$G \cong (\mathbb{Z}/8\mathbb{Z}) \oplus (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z}).$$

Then we rewrite this

$$G \cong (\mathbb{Z}/12\mathbb{Z}) \oplus (\mathbb{Z}/24\mathbb{Z})$$

and since 12 divides 24, we have the decomposition (ii).

The generalization

The generalization to modules over principal ideal domains is as follows. We will prove this today.

Proposition

Let M be a finitely-generated torsion module over a principal ideal domain R.
(i) M is a direct sum of cyclic modules:

$$M \cong \bigoplus_{i=1}^{h} (R/m_i R).$$

(ii) The decomposition is unique if we require m_i divides m_{i+1}.
(iii) Alternatively, the decomposition is unique if we require m_i is a prime power.

Other parts of the theory

There are also direct generalizations of results for finitely generated abelian groups that are not necessarily finite to finitely generated modules that are not necessarily torsion. We will look at these generalizations on Thursday.

The assumption is that the modules are finitely generated is important. For example, $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are $\mathbb{Z}$-modules, the first torsion free, the second torsion, and these results do not apply to these groups.

A look ahead to linear algebra

Another PID is the polynomial ring $F[x]$. Examples of finitely-generated modules over $F[x]$ can be obtained as follows. Let V be a finite-dimensional vector space over $F[x]$ and let $T : V \longrightarrow V$ be a linear transformation. Make V into an $F[x]$-module by

$$f \cdot v = \sum_{k=0}^{n} a_n T^n(v), \qquad f = \sum_{k=0}^{n} a_n x^n.$$

Now the same structure theorems that gave us results about abelian groups give us results about linear algebra, such as generalized eigenspaces and the rational canonical form.

Torsion

Let R be an integral domain. If M is an R-module and $a \in M$ we say that a is a torsion element if $ra = 0$ for some nonzero $r \in R$. The reason we assume that R is an integral domain is that then the torsion elements form a submodule, M_{tor}.

On the other hand M is torsion-free if $M_{\text{tor}} = 0$. The module M/M_{tor} is torsion free. All of the above facts are very easy to prove.

Today we will study finitely generated torsion modules over a PID R. This is a generalization of the theory of finite abelian groups. Thursday we will look at finitely-generated abelian groups. Our goal today is to prove the above theorem.

Annihilators

The first fact that we want to generalize is that a finite abelian group is the direct product of its Sylow subgroups.

If M is a module let $\mathrm{Ann}(M) = \{x \in R | xM = 0\}$ be the annihilator. It is an ideal, and since R is a PID it has a generator a; thus if $\mathrm{Ann}(M) = aR$ we will write $a = \mathrm{Ann}(M)$ but it is understood that a is only determined up to a unit. If M is finitely generated and torsion, the annihilator is a nonzero element of R.

There is another kind of annihilator: if $a \in R$ let

$$\mathrm{Ann}_M(a) = \{m \in M | am = 0\}.$$

This is a submodule of M.

p-primary components

Now let p be a prime (irreducible element of R). Let

$$M_p = \left\{ x \in M | p^\ell x = 0 \text{ for sufficiently large } \ell \right\}.$$

This is a submodule, called the p-primary component of M. If $R = \mathbb{Z}$, so M is an abelian group, this is the p-Sylow subgroup.

Characterizatin of the p-primary components

Lemma

Let $\mathrm{Ann}(M) = p^k m$ *where* $p \nmid m$. *Then*

$$\mathrm{Ann}_M(p^k) = M_p.$$

Recall that

$$M_p = \left\{ x \in M | p^\ell x = 0 \text{ for sufficiently large } \ell \right\}.$$

Indeed, $\mathrm{Ann}_M(p^k) \subseteq M_p$ is obvious, since we can take $\ell = k$. To prove the opposite inclusion, suppose that $p^\ell x = 0$ for some sufficiently large ℓ; we must show $p^k x = 0$. Since $p^k m = \mathrm{Ann}(M)$ we have $p^k m x = 0$. Since p^ℓ and m are coprime, we may find r and s such that $1 = rp^\ell + sm$ and then

$$p^k x = rp^{k+\ell} x + sp^k mx = 0 + 0 = 0.$$

Direct sum decomposition

Lemma

Suppose that we factor the annihilator of M into two coprime factors: $\mathrm{Ann}(M) = ab$ with $(a, b) = 1$. Then

$$M = \mathrm{Ann}_M(a) \oplus \mathrm{Ann}_M(b).$$

Because $(a, b) = 1$ we may find $r, s \in R$ such that $ra + sb = 1$. Now if $x \in M$ we may write $x = rax + sbx$. Now $rax \in \mathrm{Ann}_M(b)$ since $abM = 0$, and similarly $sbx \in \mathrm{Ann}_M(a)$. This shows

$$\mathrm{Ann}_M(a) + \mathrm{Ann}_M(b) = M.$$

We also need

$$\mathrm{Ann}_M(a) \cap \mathrm{Ann}_M(b) = 0.$$

If $x \in \mathrm{Ann}_M(a) \cap \mathrm{Ann}_M(b)$, we have $x = rax + sbx = 0 + 0 = 0$.

Primary decomposition

Theorem

Let M be a finitely generated torsion module over a PID R. Then M is a direct sum (or product) of its p-primary parts, for primes p dividing $\operatorname{Ann}(M)$:

$$M = \bigoplus_{p \mid \operatorname{Ann}(M)} M_p.$$

Factor $\operatorname{Ann}(M) = \prod p^{k_p}$ into primes. By the second Lemma

$$M = \bigoplus_{p \mid \operatorname{Ann}(M)} \operatorname{Ann}_M(p^{k_p}).$$

By the first Lemma, $\operatorname{Ann}_M(p^{k_p}) = M_p$.

The real work begins

A cyclic module is one isomorphic to R/mR for some m. Our goal is to prove that M may be factored into cyclic submodules. We will have accomplished this if we prove it for p-primary modules.

Theorem

Let M be a finitely generated torsion module over the PID R. Suppose that the annihilator of M is a power p^k of a prime. Then

$$M \cong \bigoplus_{i=1}^{h} (R/p^{k_i}R)$$

where $k = \max(k_i)$.

Proof

We will prove this by induction on the number of elements required to generate M. Thus suppose that

$$M = \langle x_1, \cdots, x_n \rangle$$

where the annihilator of x_i is p^{m_i}. This means that if $a \in R$ then $ax_i = 0$ if and only if $p^{m_i} | a$. Clearly k is the maximum of the m_i, so we will assume that $k = m_n$, and we will rename $x_n = z$. Let $\overline{M} = M/\langle z \rangle$. Let $\overline{x_i}$ be the image of x_i in $\overline{M}$. Then $\overline{M}$ has fewer than n generators (since $\bar{x}_n = 0$ is not needed) so it is a direct sum

$$\overline{M} \cong \bigoplus_{i=1}^{h-1} (R/p^{k_i}R)$$

for some h, $k_1, \cdots, k_{h-1}$. Since p^k annihilates M it annihilates $\overline{M}$ and so $k_i \leqslant k$.

Improving the generators

Let $\bar{y}_i$ be generators of the cyclic submodules $R/p^{k_i}R$ if $\overline{M}$. Let $y_i \in M$ be coset representatives.

Since $p^{k_i}\bar{y}_i = 0$ in $\overline{M} = M/\langle z \rangle$, we have $p^{k_i}y \in \langle z \rangle$, so write $p^{k_i}y_i = r_i z$. Now $p^k M = 0$ and so $0 = p^k y_i = p^{k-k_i} r_i z$. Since p^k is the annihilator of z, we have $p^k | p^{k-k_i} r_i$ and so $p^{k_i} | r_i$. Write $r_i = p^{k_i} s_i$.

Now define $x_i = y_i - s_i z$.

The new generators are very nice

Lemma

We have $p^{k_i}x_i = 0$ and $\overline{x}_i = \overline{y}_i$. If $a_i \in R$ such that $a_1x_1 + \cdots + a_{h-1}x_{h-1} \in \langle z \rangle$ then $p^{k_i}|a_i$ and $a_1x_1 + \cdots + a_nx_n = 0$.

First note that $p^{k_i}x_i = p^{k_i}y_i - r_iz = 0$. Obviously $\overline{x}_i = \overline{y}_i$. If $a_1x_1 + \cdots + a_{h-1}x_{h-1} \in \langle z \rangle$ then $\sum a_i\overline{x_i}$=0. Since $\overline{x_i} = \overline{y_i}$ and since the $\overline{M}$ spanned by the $\overline{y}_i$ is isomorphic to $\bigoplus R/p^{k_i}R$, with $\overline{y_i}$ spanning the $R/p^{k_i}R$ component, we see that $p^{k_i}|a_i$. And this implies that $a_ix_i = 0$.

Proof (concluded)

Let $N = Rx_1 + \ldots + Rx_n$. It follows from the Lemma that $N \cap \langle z \rangle = 0$. Therefore $M = N \oplus \langle z \rangle$. Furthermore the Lemma implies

$$N \cong \bigoplus_{i=1}^{h-1} R/p^{k_i}R$$

and since p^k is the annihlator of z we have $\langle z \rangle \cong R/p^kR$, so we are done with $k_h = k$.

Uniqueness

Proposition

If $k_1, \cdots, k_n$ and $\ell_1, \cdots, \ell_m$ are two sequences of nonnegative orders and

$$\bigoplus R/p^{k_i}R \cong \bigoplus R/p^{\ell_i}R$$

then $n = m$ and the k_i are the ℓ_i in some order.

To prove this, suppose

$$M = \bigoplus R/p^{k_i}R.$$

We will show that knowledge of M determines the k_i. If $j \geqslant 0$ consider

$$p^j M/p^{j+1}M.$$

The annihilator of this is p, so it is a module over the residue field R/p.

Reconstructing k_i

Lemma

The dimension of $p^j M/p^{j+1}M$ equals the number of k_i that are $\geqslant j$.

Indeed, if $U_i = R/p^{k_i}R$ then

$$p^j U_i/p^{j+1}U_i \cong \begin{cases} R/p & \text{if } j < k_i, \\ 0 & \text{if } j \geqslant k_i. \end{cases}$$

So we just have to count the number of U_i in the first case.

The Lemma shows that the k_i are intrinsically determined by M, so the $k_i = \ell_i$.

Example

Let us do an example. Suppose that $M \cong (R/p^3R) \oplus (R/p)$. Then

$$M/pM \cong (R/p) \oplus (R/p),$$

$$pM/p^2M \cong R/p,$$

$$p^2M/p^3M \cong R/p,$$

$$p^3M/p^4M = 0$$

and from this data we can reconstruct the k_i.

The elementary divisor theorem

Theorem

Let M be a finitely-generated torsion-free module over a PID. Then we may decompose

$$M \cong \bigoplus_{i=1}^{h} (R/m_i R).$$

The decomposition is unique if we require m_i divides m_{i+1}.

Theorem 4 on page 460 of Dummit and Foote is also called the Elementary Divisor Theorem.

Proof

Indeed we have a decomposition of M into a direct sum of cyclic modules

$$\bigoplus_{p} \bigoplus_{i=1}^{h(p)} (R/p^{k_i(p)}R).$$

We may rearrange this using the identity

$$(R/aR) \oplus (R/bR) \cong R/abR$$

if $(a, b) = 1$ into terms R/m_iR where each $m_i | m_{i+1}$. We leave the uniqueness to the reader.

Algebraic integers

We will prove one more result about character. We will prove that if χ is an irreducible character of G then the degree $\chi(1)$ divides the order of the group. The same ideas lead to the Burnside $p^a q^b$ Theorem.

The proof of these results require some facts from Algebraic Number Theory.

Let R be a commutative ring, and let S be a bigger ring. An element $x \in S$ is said to be integral over R if it satisfies a monic polynomial equation

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0.$$

If $x \in \mathbb{C}$ is integral over $\mathbb{Z}$ then x is called an algebraic integer. Our first goal is to show that the algebraic integers form a ring.

A criterion for algebraic integers

Lemma

Let R be a subring of $\mathbb{C}$ that is a finitely generated $\mathbb{Z}$-module. Then every element of R is an algebraic integer.

To prove this, let $a_1, \cdots, a_N \in R$ such that every element of R is a linear combination, with integer coefficients, of the a_i Let $x \in R$. Then

$$x \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \subseteq R$$

so this vector can be expressed as a linear combination of the a_i with integer coefficients.

Proof

This means

$$x \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

with $M \in \mathrm{Mat}_n(\mathbb{Z})$. Thus x is an eigenvalue of M and a root of its characteristic equation:

$$\det(xI - M) = 0.$$

Expanding this out as a polynomial we obtain a monic polynomial with integer coefficients for x, so x is an algebraic integer.

The ring of algebraic integers

Theorem

The algebraic integers form a ring.

Let x and y be algebraic integers, say

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = y^m + b_{m-1}y^{m-1} + \cdots + b_0 = 0.$$

Let R be the $\mathbb{Z}$-module spanned by the monomials $x^i y^j$ with $i < n$ and $j < m$. Using the monic polynomials for x and y shows that $xR \subseteq R$ and $yR \subseteq R$. Therefore R is closed under multiplication and it follows that it is a ring. It contains $x + y$ and xy so these are algebraic integers.

The rational integers

Proposition

Let $x \in \mathbb{Q}$. Suppose that x is an algebraic integer. Then $x \in \mathbb{Z}$.

Because of this, the ring $\mathbb{Z}$ is sometimes called the ring of rational integers. Literally, it is the set of rational numbers that are algebraic integers.

To prove this, suppose that $x = r/s$ satisfies a monic polynomial:

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0.$$

We may assume that r and s are coprime. Clearing the denominator.

$$r^n + a_{n-1}r^{n-1}s + \cdots + a_0 s^n = 0.$$

This implies that s divides r^n. But r and s are coprime, so $s = \pm 1$ and therefore $x = \pm r \in \mathbb{Z}$.

Roots of unity and characters

Any root of unity is an algebraic integer, since it satisfies a monic polynomial $x^n = 1$.

If χ is a character of G, then $\chi(g)$ is a sum of roots of unity, so it is also an algebraic integer.

As we will see in our remaining lectures, algebraic integers are the key to proving that $\chi(1)$ divides the order of $|G|$. In fact, it always divides $[G : Z(G)]$. The same ideas are used in the proof of Burnside's $p^a q^b$ theorem.