22 Decomposition of Modules

22.1 Classification of Abelian Groups

Last class, we proved the classification of finitely presented abelian groups (and more generally, modules over a Euclidean domain):

Theorem 22.1
Any finitely presented abelian group A is isomorphic to

$$\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z} \times \mathbb{Z}^a,$$

where $d_1 \mid d_2 \mid \cdots \mid d_n$.

The idea of the proof was to start with a presentation matrix B, and reduce it to Smith normal form (a diagonal matrix with the additional divisibility condition) by using elementary operations.

Note 22.2
The textbook describes this as diagonalization. But note that this is a *different* kind of diagonalization than the one used in Jordan normal form — in Jordan normal form we reduced the matrix to a simpler form by using conjugation, while here we're using elementary operations.

Today, we'll discuss various features of this classification.

22.1.1 Uniqueness of Subgroups

There are multiple questions we can ask about uniqueness. One is whether the numbers d_i are uniquely defined given A, and we'll see later that the answer is yes.

Meanwhile, when we write A as a product of factors, each factor is itself a *subgroup* of A — if we have the product $G \times H = \{(g, h) \mid g \in G, h \in H\}$, then G is isomorphic its subgroup consisting of the set $\{(g, 1)\}$. So this gives another question we can ask about uniqueness:

Guiding Question
Which subgroups corresponding to the factors in the decomposition of an abelian group are *uniquely determined* from A?

First, the product of all the finite factors $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$ is actually a canonically defined subgroup. It's exactly the set of all elements with finite order — if an element only has nonzero components in these factors, then it clearly has finite order; while if it has a nontrivial component in the free factor, then it can't have finite order.

Definition 22.3
The set of elements with finite order is called the **torsion subgroup** A_f, so we have

$$A_f = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}.$$

On the other hand, the free factor $\mathbb{Z}^n$ is uniquely defined up to an isomorphism, but it doesn't necessarily correspond to a uniquely defined subgroup. For example, take $A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$, so $A_f = \mathbb{Z}/2\mathbb{Z}$. Then A contains two free subgroups. It contains the subgroup

$$A_{\mathbb{Z}} = \langle (0, 1) \rangle,$$

which consists of elements $(0, n)$ for integers n — this is the obvious subgroup we'd think of as isomorphic to the free factor $\mathbb{Z}^n$ in the decomposition. But A also contains another subgroup

$$A_{\mathbb{Z}'} = \langle (\overline{1}, 1) \rangle,$$

which consists of elements $(\overline{n}, n)$ for integers n (where $\overline{n}$ represents n mod 2), and is also isomorphic to $\mathbb{Z}$. Both subgroups are complements to $\mathbb{Z}/2\mathbb{Z}$ in A, but they are not the same.

Student Question. *Why is the torsion subgroup called A_f, if it is* not *the free factor?*

Answer. *The f stands for finite, not free. It's an unfortunate coincidence that "finite" and "free" begin with the same letter.*

But it's easy to see that the rank a of the free factor *is* well-defined — we have $\mathbb{Z}^a = A/A_f$, but $\mathbb{Z}^a \not\cong \mathbb{Z}^b$ if $a \neq b$. To prove this explicitly, otherwise we would have an $a \times b$ matrix B and $b \times a$ matrix C (with integer coefficients) such that $BC = 1_a$ and $CB = 1_b$, representing the two directions of the isomorphism. This is impossible even dropping the requirement that they have integer coefficients — if $a < b$ then $\text{rank}(CB) \leq a < b = \text{rank}(1_b)$, contradiction.

22.1.2 The Torsion Subgroup

We can write another expression for the torsion subgroup A_f. By using the Chinese Remainder Theorem (which states that $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ if $\gcd(m,n) = 1$), we can split every d_i into prime powers, and write $\mathbb{Z}/d_i\mathbb{Z} \cong \prod \mathbb{Z}/p_j^{s_j}\mathbb{Z}$. So then we can write A_f as a product of cyclic groups with prime power order. We can then collect factors corresponding to the same prime, giving the decomposition

$$A_f = A_{p_1} \times A_{p_2} \times \cdots \times A_{p_m},$$

where each factor is of the form $A_p = \prod \mathbb{Z}/p^{e_i}\mathbb{Z}$.

Example 22.4
Write $\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ in this form.

Proof. We can split $36 = 4 \cdot 9$ and $6 = 2 \cdot 3$, to get $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$. □

It's easier to prove uniqueness when we write the decomposition in this form, so we'll now work with this way of writing A_f. (It's possible to use the uniqueness of this decomposition to prove uniqueness of the d_i in the original form, where $d_1 \mid \cdots \mid d_n$, as well; this will be left as an exercise.)

Note that A_p is a p-Sylow subgroup of A_f. Since the group is abelian, the Sylow subgroup is unique (in the case of a general group, all Sylow subgroups are conjugate). In fact A_p is exactly the set of elements whose order is a power of p — this is called the **p-torsion subgroup**.

Within each A_p, the set-theoretic decomposition into subgroups may not be unique, but we can show the following lemma:

Lemma 22.5
The multiplicities of the powers of p in the decomposition of A_p as a product of cyclic groups are uniquely determined by A.

For example, this means $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Note that we chose the numbers here so that it's not completely obvious — clearly if we have two isomorphic decompositions then their sizes must match. Here we do have $4 \cdot 4 = 2 \cdot 8$, but they're still not isomorphic, for more subtle reasons.

Proof. Let $A = \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_n}\mathbb{Z}$ (where $a_i \geq 1$). There are two main observations here.

First consider A/pA. Each factor is replaced with $\mathbb{Z}/p\mathbb{Z}$ (for example, by the homomorphism theorem), so $A/pA = (\mathbb{Z}/p\mathbb{Z})^n$. This means $|A/pA| = p^n$, where n is the number of factors — so any two decompositions must have the same number of factors.

Meanwhile, we can also look at pA, which is a subgroup of A. We have $p\mathbb{Z}/p^a\mathbb{Z} \cong \mathbb{Z}/p^{a-1}\mathbb{Z}$. So replacing A with pA reduces each of the exponents by 1, and

$$pA = \prod \mathbb{Z}/p^{a_i - 1}\mathbb{Z}.$$

(It's possible that some of these factors are trivial, since $a_i - 1$ may be 0; but we can use the first observation to deal with this.)

Now use induction on $|A|$. If we can write A in two ways as

$$A \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_n}\mathbb{Z} \cong \mathbb{Z}/p^{a_1'}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_m}\mathbb{Z},$$

then we must have $n = m$ by the first observation, and

$$pA \cong \prod \mathbb{Z}/p^{a_i-1}\mathbb{Z} \cong \prod \mathbb{Z}/p^{a_i'-1}\mathbb{Z}$$

by the second. By the induction hypothesis, we can match all the nonzero $a_i - 1$ and $a_i' - 1$; so we can match all $a_i > 1$ with $a_i' > 1$. Only looking at these, we lose the information about the a_i which equal 1; but using the fact that $m = n$, we can also match the $a_i = 1$ with $a_i' = 1$. So the two decompositions must be the same. □

22.2 Polynomial Rings

This classification works for modules over any Euclidean domain. Now consider the case of $R = F[t]$, where F is a field. The theorem says that a finitely presented module over R is of the form

$$M \cong R/(P_1) \times \cdots \times R/(P_n) \times R^a,$$

where $P_1 \mid P_2 \mid \cdots \mid P_n$. Similarly to before, we can rewrite the decomposition as

$$M \cong \prod R/Q_i^{a_i} \times R^a,$$

where the Q_i are irreducible.

In particular, if the module M is finite-dimensional as a vector space over F, then there is no free factor R^a.

When we started discussing modules, we saw that a $F[t]$ module is the same as a F-vector space V, together with a linear operator $V \to V$ (the action of t). So understanding isomorphism classes of modules is the same as understanding this situation, which was studied in linear algebra with the Jordan normal form theorem.

We'd like to explicitly figure out what $R/(P)$ looks like. We can assume P is monic without loss of generality (since F is a field), so we can write $P(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$. Then $R/(P)$ has a basis consisting of $\overline{1}$, $\overline{t}$, $\ldots$, $\overline{t^{n-1}}$. Let $e_i = \overline{t^{i-1}}$. Then to describe the action of t, we have $te_i = e^{i+1}$ for $1 \le i \le n-1$, while

$$te_n = -a_0e_1 - a_1e^2 - \cdots - a_{n-1}e_n.$$

So then the matrix corresponding to t is

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_n \end{bmatrix}.$$

But we can sometimes say even more. Consider $F = \mathbb{C}$, and use the second form of the decomposition, where we quotient by powers of irreducible polynomials. The only irreducible polynomials are linear, so we have $Q_i(t) = t - \lambda_i$ for some λ_i, and in each factor we're quotienting out by some power of such a linear polynomial.

If $\lambda_i = 0$, then using the above basis, the entire right column is 0. So we get a matrix with 0's on the diagonal, 1's directly below the diagonal, and 0's everywhere else — this is the form of one Jordan block for a nilpotent matrix.

Meanwhile, in general, we can use the basis consisting of $\overline{(t-\lambda_i)^j}$ instead of $\overline{t^j}$. Then the situation is the same, except that we add a scalar to the matrix — the action of $t - \lambda_i$ corresponds to this exact matrix, and we add the scalar matrix λ_i to get the action of t. So we get the same matrix with λ_i on the diagonal instead of 0, which is a general Jordan block.

So this gives a proof of the Jordan normal form theorem, and shows that in fact, both Jordan normal form and the classification of finite abelian groups follow from the same more general theorem.

22.3 Noetherian Rings

We'll now move to the last topic about modules, Noetherian rings (named after Emmy Noether). Today we'll just see an overview of the statements, and we'll prove them next class.

Definition 22.6
A ring R is **Noetherian** if every ideal in R is finitely generated.

Example 22.7
Any field is Noetherian (since the only two ideals are the ones generated by 0 and 1), and any PID is Noetherian (since an ideal is generated by one element).

The reason the concept is useful is the following proposition:

Proposition 22.8
A ring R is Noetherian if and only if every submodule in a finitely generated R-module is itself finitely generated.

In particular, we get the following corollary:

Corollary 22.9
If R is Noetherian, every finitely generated module is finitely presented.

This explains why the notion is useful, but then we're left with the question of how to produce examples. There are some easy reductions (for example, the quotient of a Noetherian ring is Noetherian as well). But the key result is the Hilbert Basis Theorem:

Theorem 22.10 (Hilbert Basis Theorem)
If R is Noetherian, then $R[x]$ is Noetherian.

This gives a powerful tool for proving that many rings are Noetherian, and therefore that many modules are finitely generated.

Note 22.11
There is a legend about this theorem: Hilbert published this theorem in 1890. According to the legend, a famous mathematician Paul Gordan (referred to as the king of invariant theory, a branch of algebra studying such questions) ostensibly said that this is not mathematics, it's theology. At the time, people were trying to work with this case by case, to explicitly produce a finite set of generators. In contrast, this theorem has a short and very abstract proof that doesn't give much information about how to write down the actual generators.

Resource: Algebra II Student Notes

Spring 2022

Instructor: Roman Bezrukavnikov
Notes taken by Sanjana Das and Jakin Ng