UNDERSTANDING THE STRUCTURE OF ABELIAN GROUPS (WITH MODULES!)

CHRIS JEONG, HEON LEE, KABIR NARAYANAN, KAI ZUANG

Contents

1. Smith Normal Form

In this section, we establish that for any homomorphism $\phi : N \to M$ between free R-modules where R is a Euclidean domain, a basis can be chosen such that ϕ is represented as a simple and insightful matrix, known as the Smith normal form. We introduce the following two definitions.

Definition 1.1 (Smith Normal Form [1])**.** Let R be an integral domain. A matrix A with entries in R is in **Smith normal form** if there are non-zero elements $b_1, \ldots, b_k \in R$ so that A has the form

$$\begin{pmatrix} b_1 & & & & & \\ & b_2 & & & 0 & \\ & & \ddots & & & \\ & & & b_k & & \\ & & & & 0 & \\ & 0 & & & & \ddots \\ & & & & & & 0 \end{pmatrix} \text{ and } b_1 \mid b_2 \mid \cdots \mid b_k.$$

Definition 1.2 (Elementary Matrix Operations [1])**.** Let A be a matrix with entries in R. The following are called **elementary matrix operations**:

Swap Columns: Swap any two columns of A

Swap Rows: Swap any two rows of A

Add Columns: Add an R-multiple of one column of A to any other column

Add Rows: Add an R-multiple of one row of A to any other row.

Lemma 1.3. *(Lemma 11.49 [1]) Let R be a Euclidean domain, and let A be a matrix with entries in R. Then there is a sequence of elementary operations that transforms A into a matrix $B = (b_{ij})$ in Smith normal form.*

Proof. We give a proof sketch. We can assume that A is not the zero matrix, since the zero matrix is already in the Smith normal form. We know that because R is a Euclidean domain, it is equipped with a Euclidean function $\sigma : R \setminus \{0\} \to \mathbb{Z}_+$. Then consider the map μ defined as $\mu(C) = \min\{\sigma(c_{ij}) : c_{ij} \neq 0\}$ where $C = (c_{ij})$ is a matrix with entries in R. Similarly, let $\tilde{\mu}(C) = \arg\min\{\sigma(c_{ij}) : c_{ij} \neq 0\}$.

Date: April 1, 2024.

Now, we claim (without proof) that if $\tilde{\mu}(A)$ does not divide every entry of A, then we can construct a new matrix A' using elementary operations on A so that $\mu(A') < \mu(A)$. For the proof, refer to Silverman [1].

We now describe the algorithm to transform the matrix to Smith normal form using elementary row operations. The main idea of the algorithm is to inductively place the smallest non-zero entry with respect to σ-size that divides every other entry at the top left.

Algorithm:

(1) Start with the matrix A. Perform row and column swaps to ensure that the upper-left entry a_{11} of A is $\tilde{\mu}(A)$.
(2) If any entry of A is not divisible by a_{11}, perform elementary operations to create a new matrix A' with $\mu(A') < \mu(A)$. Iterate this step until a_{11} divides every entry. We know this step must terminate in a finite number of steps since given the sequence $A_1, A_2, \ldots$ with $\mu(A) > \mu(A_1) > \mu(A_2) > \cdots$, we have a sequence of strictly decreasing nonnegative integers, which terminates. Then this step leaves us with a matrix $B = (b_{ij})$ such that $b_{11} \neq 0$ divides every entry.
(3) Subtract multiples of the first column and row of B to make $b_{i1} = b_{1j} = 0$ for all i, j, which is possible because b_{11} divides b_{i1}, b_{1j}.
(4) Repeat steps (1) to (3) with B', which is obtained by removing the first row and column of B. Note that all entries of B' are a multiple b_{11}, so $b_{11} | b'_{11}$.

By repeating until B' is either a row or column vector, the algorithm terminates, and we have transformed A into a matrix in Smith normal form.

□

2. A First Pass at the Structure Theorem

In this section we describe and prove part of a powerful theorem which decides the structure of any finitely-generated module over a Euclidean Domain. In the next section, this theorem will be refined.

Theorem 2.1. *Let R be a Euclidean domain, and M a finitely-generated (F.G.) module over R.*

Then $\exists b_1, \ldots, b_s \in R \setminus \{0_R \cup R^*\}$ such that $b_1 \mid \ldots \mid b_s$ and $\exists r \in \mathbb{Z}_{\geq 0}$ such that the following isomorphism holds:

$$M \cong \left(\prod_{i=1}^{s} \frac{R}{b_i R} \right) \times R^r$$

Moreover, the integer r and the ideals generated by $b_1, \ldots, b_s$ are unique.

Remark. *$b_1, \ldots, b_s$ are chosen to be non-zero and non-unit elements of the ring so that uniqueness hold. The zero values are included in R^r whereas $b_i = 1_R$ simply means $\frac{R}{b_i R}$ is the zero ring, so we exclude all such values. Under these assumptions r is the **rank** of M and the ideals $b_1 R, \ldots, b_s R$ are **elementary divisors** of M.*

We will reserve the proof of uniqueness for the next section, but the general idea for this proof is relatively simple.

First we make use of the natural homomorphism ϕ between R^k and M, since M is finitely-generated. Then, we establish an isomorphism between a submodule $R^k/\ker(\phi)$ and R^k, and show that $\ker(\phi)$ is F.G. Finally, we show that $\ker(\phi)$ may be written as a product of principal ideals in an appropriate basis. It is in this step, where a lovely insight (Lemmas 2.3-2.4) brings the Smith Normal Form into play.

Proof. Since M is finitely-generated, there exists $m_1, \ldots, m_k \in M$ such that $M = \mathrm{Span}(\{m_1, \ldots, m_k\})$.

Define the standard homomorphism $\phi : R^k \to M$ by

$$\phi(c_1, \ldots, c_k) = \sum_{i=1}^{k} c_i m_i$$

Which is clearly surjective since $\{m_i\}$ is a generating set.

We can achieve an isomorphism by defining the map $\tilde{\phi} : \frac{R^k}{\ker(\phi)} \to M$.

Now, our main concern will be to understand the structure of $P = \ker(\phi)$. First note that P is a submodule of R^k. R^k, as it happens, is a *Noetherian R-module*, which means all of its submodules are finitely-generated (see Lemma 2.2). It follows that P is finitely-generated.

Suppose P is generated by the set $\mathcal{P} = \{p_1, \ldots, p_l\}$.

Moreover, R^k is a free and finitely-generated module. Hence it admits a basis $\mathcal{N} = \{n_1, \ldots, n_k\}$.

Let us now introduce the matrix $A_{\mathcal{N},\mathcal{P}} \in \mathcal{M}_{k\times l}(R)$ as follows. Let $p_j = \sum_{i=1}^{k} a_{ij} n_k$., where, a_{ij} are uniquely determined by the basis $\mathcal{N}$. Then,

$$A_{\mathcal{N},\mathcal{P}} = (a_{ij})$$

Each column of this matrix corresponds to an element of the generating set for P.

Now comes the key insight of the proof. Every elementary row/column operation corresponds to a change of basis/ generating set. Thus, the existence of a finite set of operations which transforms $A_{\mathcal{N},\mathcal{P}} \mapsto \mathcal{A}'$ implies the existence of a new basis and generating set such that

$$A_{\mathcal{N}',\mathcal{P}'} = \mathcal{A}' = \begin{bmatrix} b_1' & & & & \\ & \ddots & & & \\ & & b_t' & & \\ & & & 0 & \\ & & & & \ddots \end{bmatrix}$$

. This claim is proven as a lemma afterward.

In general, $t \leq l$. The diagonal form of this matrix allows us to write: $p_i' = b_i' n_i'$, where if $i > t$, then $b_i' = 0$.

The change of basis gives us an isomorphism on $N = R^k$ which sends $(c_1, \ldots, c_k) \mapsto \sum_{i=1}^{k} c_i n_i'$. Taking the pre-image of P under the change of basis, we find:

$$P = \mathrm{Span}(\mathcal{P}') \cong \prod_{i=1}^{t} b_i' R \times \prod_{i=t+1}^{l} 0R$$

Noting that $R/0R \cong R$, we define $r = l - t$ and the rest follows straightforwardly:

$$M \cong \frac{N}{P} \cong \frac{R^k}{\prod_{i=1}^{t} b_i' R \times \prod_{i=t+1}^{l} 0R} \cong \left(\prod_{i=1}^{t} \frac{R}{b_i' R}\right) \times R^r$$

□

Note that if $b_t' \in R^*$ is a unit, then $\frac{R}{b_t' R} \cong \{0\}$, so throwing out these terms we find the $b_1', \ldots, b_s'$ where $s \leq t$ described in the theorem statement.

So far we have neither established the uniqueness of the rank nor the ideals. Before dealing with uniqueness, let us clean up the details swept under the rug.

Lemma 2.2. R^k *is a Noetherian R-module.*

Proof. R is a Euclidean domain, hence a PID, so all of its ideals are principal. In particular, this means R is a Noetherian R-module. A very nice proposition (Prop. 11.41 in [1]) tells us that a given a module M and a submodule N, M is Noetherian iff N and M/N are Noetherian. We establish the lemma by simple induction argument (we have already established the base case). If $R, \ldots, R^{k-1}$ are Noetherian. Then since $R = R^k/R^{k-1}$, the proposition tells us that R^k is Noetherian. □

Lemma 2.3. *Let $\mathcal{G}$ be a finite generating set/basis for a module M. Then $\forall i \neq j$, and $\forall c \in R$, the set $\mathcal{G}'$ obtained by swapping $g_i \leftrightarrow g_j$ or by replacing $g_j \mapsto g_j + cg_i$ is still a generating set/basis.*

Proof. The proof for a swap of elements is trivial, since addition in the module is a commutative operation. Thus we will only demonstrate the second two claims.

First suppose $\mathcal{G}$ is a generating set with n elements.

$\forall m \in M$, $\exists c_1, \ldots, c_n$ such that $m = \sum_{k=1}^{n} c_k g_k$. Then if $g'_j = g_j + cg_i$ then m is generated by $\mathcal{G}'$:

$$m = \sum_{k=1}^{n} c'_k g'_k$$

where $c'_k = c_k$ if $k \neq i$ and $c'_i = c_i - cc_j$. Morever, if $\mathcal{G}$ is a basis, then if $\sum_{k=1}^{n} c'_k g'_k = 0$ we invert the transformation of coefficients and use the linear independence of $\mathcal{G}$ to find $c_{k\neq i} = 0$ and $c_i = c'_i + cc'_j = 0$. Since $c'_j = 0$, $c'_i = 0$. We conclude $\mathcal{G}'$ is linearly independent and therefore a basis.

□

Lemma 2.4. *Let $P \subset N$ be a submodule of a free, finitely-generated module. Let $\mathcal{N}$ be a basis for N and $\mathcal{P}$ a generating set for P. Then for each elementary row/column operation that sends the matrix $A_{\mathcal{N},\mathcal{P}} \to A'$, there exists a basis and generating set $\mathcal{N}', \mathcal{P}'$ such that $A' = A_{\mathcal{N}',\mathcal{P}'}$*

Proof. This is relatively straightforward to verify, but we illustrate the idea below anway. First, consider a swap of rows. So for all $k = 1, \ldots, |\mathcal{P}|$ we send $a_{ik} \leftrightarrow a_{jk}$. Then let $\mathcal{N}'$ be formed by swapping $n_i \leftrightarrow n_j$. Then for each $p_k \in \mathcal{P}$, $p_k = \sum_{f=1}^{|\mathcal{N}|} a_{fk} n_f = \sum_{f=1}^{|\mathcal{N}|} a'_{fk} n'_f$. Thus $A' = A_{\mathcal{N}',\mathcal{P}}$. A nearly identical demonstrates the claim for a linear combination of rows.

A column operation effects an alteration in the generating set, rather than the basis. For instance sending $a_{ki} \leftrightarrow a_{kj}$ for all $k = 1, \ldots, |\mathcal{N}|$ corresponds to swapping $p_i \leftrightarrow p_j$. Now $p'_i = \sum_{f=1}^{|\mathcal{N}|} a_{fj} n_f = \sum_{f=1}^{|\mathcal{N}|} a'_{fi} n_f$. Thus $A' = A_{\mathcal{N},\mathcal{P}'}$. □

3. Structure Theorem, Take 2

In this section we present a proof of an alternative version of the theorem above. We begin by reminding ourselves of the Chinese Remainder Theorem(alternatively known as Sun Tzu's Theorem) and providing some definitions.

Theorem 3.1. *Let R be a commutative ring and* $c_1, ..., c_n \in R$ *such that whenever* $i \neq j$, $c_iR + c_jR = R$. *Let* $c = c_1c_2...c_n$. *Then there exists an isomorphism*

$\phi : R/cR \to R/c_1R \times ... \times R/c_nR$

$r \to (r \mod c_1, ..., r \mod c_n)$

Proof. Theorem 7.25/Lemma 7.26 of Silverman □

Definition 3.2 (Torsion Submodule)**.** Let M be an R-Module. The torsion submodule of M, is a submodule of M defined as

$M_{tors} = \{m \in M : am = 0 \text{ for some non-zero } a \in R\}$.

Definition 3.3 (Annihilator Ideal)**.** Let M be an R-Module. The annihilator ideal of M, is an ideal of R defined as

$Ann(M) = \{a \in R : am = 0 \text{ for all } m \in M\}$

We are now ready to restate and reprove the structure theorem.

Theorem 3.4. *Let R be a Euclidean Domain and M be a finitely generated R-Module. Then*

a. There exists a list of not necessarily distinct irreducible elements of R $\pi_1, ..., \pi_t$*, positive integers* $e_1, ..., e_t$*, and a positive integer r so that* $M \cong R/\pi_1^{e_1}R \times R/\pi_2^{e_2}R... \times R/\pi_t^{e_t}R \times R^r$

b. The integer r and the ideals $R/\pi_1^{e_1}R, ..., R/\pi_t^{e_t}R$ *are uniquely determined by M.*

Proof. We already proved above that for some list $b_1, \ldots, b_s$

$$M \cong \left(\prod_{i=1}^{s} \frac{R}{b_iR}\right) \times R^r$$

. Thus it suffices to show that for each ideal R/b_iR, we have R/b_iR is isomorphic to a product of the form $R/\pi_1^{e_1}R \times R/\pi_2^{e_2}R... \times R/\pi_t^{e_t}R$. Since R is a UFD, we can write b_i as a product of a unit and irreducibles $\pi_1^{e_1}\pi_2^{e_2}\ldots\pi_t^{e_t}$. Since R is also a PID, each $\pi_i^{e_i}R$ is a maximal ideal. So for any $i \neq k$, we have $\pi_iR + \pi_kR = R$. It follows that $\pi_i^{e_i}R + \pi_k^{e_k}R = R$. Since R is a commutative, we may apply Theorem 3.1 to get $R/b_i \cong R/\pi_1^{e_1}R \times \ldots R/\pi_j^{e_j}R$. This completes the proof of a. It remains to show that the integer r and the ideals $R/\pi_1^{e_1}R, ..., R/\pi_t^{e_t}R$ are uniquely determined by M. We first start with by showing $R/\pi_1^{e_1}R \times R/\pi_2^{e_2}R... \times R/\pi_t^{e_t}R \times 0^r \cong M_{tors}$. This is because $\pi_1^{e_1}\pi_2^{e_2}\ldots\pi_t^{e_t}$ times any element of $R/\pi_1^{e_1}R \times R/\pi_2^{e_2}R... \times R/\pi_t^{e_t}R \times 0^r$ yields us the zero element of M. Any other element of M would have a non zero component in it's free submodule thus if it were in M_{tors}, then R would have a zero divisor contradicting the fact that it is an Euclidean Domain. Now that we have shown $R/\pi_1^{e_1}R \times R/\pi_2^{e_2}R... \times R/\pi_t^{e_t}R \times 0^r \cong M_{tors}$, it follows that the quotient $M/M_{tors} \cong R^r$. Then r is uniquely determined by M since it is the R-rank of its free submodule. It remains to show that the ideals $R/\pi_1^{e_1}R, ..., R/\pi_t^{e_t}R$ are also uniquely determined by M. We start by defining the set $M(\pi) = \{m \in M : \pi^i m = 0 \text{ for some } i \geq 1\}$ where π is some irreducible element of R. Observe that we can form an R-module homomorphism

$\phi : M_{tors} \to R/\pi_1^{e_1}R \times ... \times R/\pi_m^{e_m}R \times 0^k$ by restricting ourselves to the product of quotients not formed by powers of some π'(of which there are k many). Then $M(\pi')$ is the kernel of ϕ thus it is a submodule of M_{tors}. Let l be the maximum power which π' appears. We want to show that the number of times each $R/\pi'^{e_i}R$ appears in $M(\pi')$ is uniquely determined by $M(\pi')$. We can do this by taking successive quotients $\pi'^jM(\pi')/\pi'^{j+1}M(\pi')$ for all j up to l. Let $M(\pi') = R/\pi'^{e_1}R \times \cdots \times R/\pi'^{e_n}R$. Then $\pi'^jM(\pi')/\pi'^{j+1}M(\pi') \cong \frac{\pi'^jR/\pi'^{e_1}R}{\pi'^{j+1}R/\pi'^{e_1}R} \times \cdots \times \frac{\pi'^jR/\pi'^{e_n}R}{\pi'^{j+1}R/\pi'^{e_n}R}$. For some e_i, suppose $j \geq e_i$. Then we have $\frac{\pi'^jR/\pi'^{e_1}R}{\pi'^{j+1}R/\pi'^{e_1}R} \cong \frac{\{0\}}{\{0\}} \cong \{0\}$ since

π'^{e_i} divides π'^{j}. Let $I = \pi'^{j}(\frac{R}{\pi'^{e_1}R})$. In the case where $j < e_i$, we have $\frac{\pi'^{j}R/\pi'^{e_1}R}{\pi'^{j+1}R/\pi'^{e_1}R} \cong \frac{\pi'^{j}R/\pi'^{e_1}R}{\pi'\pi'^{j}R/\pi'^{e_1}R} \cong \frac{I}{\pi'I}$. But by the 3rd Isomorphism Theorem, $I \cong \frac{\pi'^{j}R}{\pi'^{e_i}R}$ and $\pi'I \cong \frac{\pi'^{j+1}R}{\pi'^{e_i}R}$ so $\frac{I}{\pi'I} \cong \frac{\pi'^{j}R}{\pi'^{j+1}R} \cong \frac{\pi'^{j}R}{\pi'(\pi'^{j}R)}$. By the first isomorphism theorem $\frac{\pi'^{j}R}{\pi'(\pi'^{j}R)} \cong \frac{R}{\pi'R}$. Since π' is irreducible in R, $\pi'R$ is maximal thus $R/\pi'R$ is a field. Then $\frac{\pi'^{j}M(\pi')}{\pi'^{j+1}M(\pi')} \cong \frac{\pi'^{j}R/\pi'^{e_1}R}{\pi'^{j+1}R/\pi'^{e_1}R} \times \cdots \times \frac{\pi'^{j}R/\pi'^{e_n}R}{\pi'^{j+1}R/\pi'^{e_n}R} \cong (\frac{R}{\pi'R})^{x} \times 0^{y}$ for some integers x,y. Thus we have that $\frac{\pi'^{j}M(\pi')}{\pi'^{j+1}M(\pi')}$ is a x dimensional $\frac{R}{\pi'R}$ vector space and y is the number of $R/\pi^{e_i}R$ with $j \geq e_i$. Then take $\frac{\pi'^{j+1}M(\pi')}{\pi'^{j+2}M(\pi')} \cong (\frac{R}{\pi'R})^{x'} \times 0^{y'}$. Since y' is the number of $R/\pi^{e_i}R$ with $j+1 \geq e_i$, we can find the number of $R/\pi^{e_i}R$ with $j = e_i$ from $y' - y$. We have shown that the number of times each $R/\pi^{e_i}R$ is uniquely determined by $M(\pi')$. Since we can do this across all π that appears in M_{tors} we have shown that M_{tors} uniquely determines each $R/\pi_i^{e_i}R$. $\square$

4. Finitely Generated Abelian Groups

Corollary 4.1. *Lemma 11.55 of textbook:*
Let R be a Euclidean Domain, let M be a finitely generated R-module, $r \geq 0$ be an integer, and let $b_1, b_2, ..., b_s \in R$ be non-zero elements satisfying $b_1|b_2|...|b_s$.
Now suppose there is an isomorphism $M \cong R/b_1R \times ... \times R/b_sR \times R^r$.
It follows that the integer r and the ideals b_1R, b_2R, ..., b_sR are uniquely determined by M.

Proof. We have previously proved the uniqueness of r.
Thus, it suffices to show the uniqueness of ideals $b_1R, .., b_sR$.
Consider Theorem 3.4; there is a unique list of ideals such that $M_{tors} \cong R/\pi_1^{e_1}R \times ... \times R/\pi_t^{e_t}R$.
Theorem 11.54 says nothing about uniqueness, however. Similarly, some π_i in the lists may be written as a product of a list of other π_j. Thus, we must characterize the list of ideals by grouping together matching π_iR and their exponents.
Let $\pi_1^{e_1}R, ..., \pi_l^{e_l}R$ be the list of **distinct** irreducible ideals.
Now consider $e_{11} \geq e_{12} \geq ... \geq e_{1s}, ..., e_{l1} \geq e_{l2} \geq ... \geq e_{ls}$.
We get that $M_{tors} \cong \Pi_{i=1}^{l}\Pi_{j=1}^{s}R/\pi_i^{e_{ij}}R$.

Now consider $M \cong R/b_1R \times ... \times R/b_sR \times R^r$.
Please note that in the recording, it is not proven how our construction satisfies $b_1|b_2|...|b_s$.
We are very sorry for such an omission but it follows from the fact that each b_i is composed of powers of $\pi_1, ..., \pi_l$, and as we go down the list b_i, b_{i-1}, etc. the power which each π_j is raised to either remains constant or decreases; thus, $b_{i-1}|b_i$.
We get that b_sR consists of the largest powers of $\pi_1, ..., \pi_l$, so it follows that $b_sR = \pi_1^{e_{11}}...\pi_l^{e_{l1}}R$.
If $b_sR = \pi_1^{e_{11}}...\pi_l^{e_{l1}}R$, then it follows that $R/b_sR \cong R/\pi_1^{e_{11}}R \times R/\pi_2^{e_{21}}R \times R/\pi_l^{e_{l1}}R$.

We can repeat the above procedure to yield that $R/b_{s-1}R \cong R/\pi_1^{e_{12}}R \times ... \times R/\pi_l^{e_{l2}}$, etc.

□

Theorem 4.2. *Theorem 11.56 (The Structure Theorem of Finitely Generated Abelian Groups):*
Let A be a finitely generated abelian group (not necessarily finite).
Then A is isomorphic to a product of cyclic groups.
Letting $C(n)$ be a cyclic group of order n, we get that there are integers $r, s \geq 0$ and positive integers $b_1, ..., b_s \geq 2$ satisfying $b_1|b_2|...|b_s$ and $A \cong C(b_1) \times C(b_2) \times ... \times C(b_s) \times \mathbb{Z}^r$.
We also get that $r, s, b_1, ...b_s$ are uniquely determined by A.
Furthermore, there are integers $r, t \geq 0$ and prime powers $q_1, ..., q_t \in \mathbb{Z}$ uniquely determined by A such that $A \equiv C(q_1) \times C(q_2) \times ... \times C(q_t) \times \mathbb{Z}^r$.

Proof. An abelian group is a $\mathbb{Z}$-module, as proved in Chapter 11.2.
We also know that $\mathbb{Z}$ is a Euclidean domain.
Thus, Theorem 11.56 follows from Theorem 11.50 and 11.54. □

The Structure Theorem of Finitely Generated Abelian Groups allows us to identify isomorphism classes of finite groups with certain order.
For example, there are 3 isomorphism classes of finite groups with order 8: $C_8, C_4 \times C_2$, and $C_2 \times C_2 \times C_2$.
Theorem Theorem 11.56 also tells us something about the orders of elements of finite groups.
If we have a finite group A, then we get that $A \cong C(b_1) \times C(b_2) \times ... \times C(b_s)$, where $b_1|b_2|...|b_s$.
The order of any arbitrary element A must divide the orders of all groups, and it follows from $b_1|b_2|...|b_s$ that the

order of such an element divides b_s*, which is the element of highest order.*
It follows that in a finite abelian group, the order of any element divides the order of the element of the highest order.

References

[1] J. H. Silverman. *Abstract Algebra An Integrated Approach*. American Mathematical Society, 2022.