Group Theory - Week 7 - Decomposing Finitely Generated Abelian Groups

Antonio León Villares

November 2022

Contents

Based on the notes by Susan J. Sierra, Section 5.2 & 5.3

1 Recap: R-Modules

1.1 Definition: Ring

*A **ring** is a set equipped with 2 operations:*

$$(R, +, \cdot)$$

*known as **addition** and **multiplication**.*
In particular:

1. $(R, +)$ *is an **abelian group***
2. $(R, \cdot)$ *is a **monoid**:*
   - *multiplication is **associative***
   - *there is an **identity element** 1_R such that:*

   $$\forall r \in R, \quad a \cdot 1_R = 1_R \cdot a = a$$

3. *the **distributive law** holds in R:*

   $$a \cdot (b + c) = (a \cdot b) * (a \cdot a)$$

   $$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

1.2 Definition: R-Module

*An **R-module** is an **abelian group**:*

$$M = (M, +)$$

*equipped with a mapping over a **ring** R:*

$$R \times M \mapsto M$$

$$(r, m) \mapsto rm$$

such that the following hold:

1. ***Distributivity**:*

$$r(a+b) = ra + rb, \qquad \forall r \in r, \forall a, b \in M$$

$$(r+s)a = ra + sa, \qquad \forall r, s \in R, \forall a \in M$$

2. ***Associativity**:*

$$r(sa) = (rs)a, \qquad \forall r, s \in R, \forall a \in M$$

3. ***Unital**:*

$$1_R a = a, \qquad 1_R \in R, \forall a \in M$$

(Definition 5.2.1)

1.2.1 Examples

- a $\mathbb{Z}$-module is the same as an **abelian group**. If we define scalar multiplication by $\mathbb{Z}$ via:

$$na = \begin{cases} \underbrace{a + a + \ldots + a}_{n\ times}, & n > 0 \\ 0, & n = 0 \\ -(-n)a, & n < 0 \end{cases}$$

  then this is precisely the structure of an abelian group

- modules formalise many ideas, such as scalar multiplication in vectors/matrices. In fact, if K is a field (a **non-zero, commutative** ring in which every element has a **multiplicative inverse**), a K-Module is a K-vector space

1.3 Definition: Submodule

*Let M be an **R-Module**. Then, a **non-empty** subset $M' \subseteq M$ is a **submodule** if M' is also a **module** over R.*
*In particular, M' is a **submodule if and only if**:*

1. $$0_M \in M'$$

2. $$a, b \in M' \implies a - b \in M'$$

3. $$r \in R, a \in M' \implies ra \in M'$$

1.3.1 Examples

- **submodules** of vector spaces are **subscpaces**
- **submodules** of $\mathbb{Z}$-modules are **subgroups**

1.4 Definition: Free R-Module

*Let R be a **ring**, and let $n \in \mathbb{N}$.*
*A **free R-module of rank n** is the **module** R^n, obtained by applying the cartesian product n times, and endowed with the operation:*

$$r(a_1, a_2, \ldots, a_n) = (ra_1, ra_2, \ldots, ra_n), \qquad r \in R, a_i \in R$$

(Definition 5.2.4)

2 The Fundamental Theorem of Finitely Generated Abelian Groups

2.1 Theorem: Fundamental Theorem of Finitely Generated Abelian Groups

*Let A be a **finitely generated abelian group**. That is, $\exists a_1, \dots, a_s$ such that:*

$$A = \langle a_1, \dots, a_s \rangle$$

Then:

$$A \cong \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \dots \times \mathbb{Z}_{r_k} \times \mathbb{Z}^{\ell}, \qquad k, \ell \in \mathbb{N},\ r_i \in \mathbb{Z}$$

and such that:

$$r_1 \mid r_2 \mid \dots \mid r_k$$

*Here, we think of $A, \mathbb{Z}_{r_i}$ as $\mathbb{Z}$-**modules**, not abelian groups.*
(Theorem 5.2.5)

2.2 Intuition: Invertible Operations on Matrices Preserve Isomorphism

2.2.1 A Homomorphism for Finitely Generated Abelian Groups

*Let A be a **finitely generated abelian group**, such that $\exists a_1, \dots, a_s$ such that:*

$$A = \langle a_1, \dots, a_s \rangle$$

*Then θ is a $\mathbb{Z}$-**module homomorphism**:*

$$\theta : \mathbb{Z}^s \to A$$

$$(r_1, \dots, r_s) \mapsto \sum_{i=1}^{s} r_i a_i$$

This is clearly a **homomorphism**; in fact, it is **surjective**, since A is finitely generated, and θ contemplates all possible linear combinations of its generators.

What we are more interest in is the **kernel**, $K = ker(\theta)$, since by the **First Isomorphism Theorem for Modules**:

$$A \cong \mathbb{Z}^s / K$$

which means that knowing how K "behaves" tells us everything we need to know about our **finitely generated abelian group** A.

To this regard, we need to acknowledge the fact that:

- *K is a **submodule** of A* (this is immediate from the definition of a submodule)
- *K is **finitely generated*** (this is hard to prove, so we take it as given)

2.2.2 Lemma: Automorphisms Preserve Quotients

*Let α be a $\mathbb{Z}$-**module automorphism** of $\mathbb{Z}^s$:*

$$\alpha : \mathbb{Z}^s \to \mathbb{Z}^s$$

Then:

$$\mathbb{Z}^s/K \cong \mathbb{Z}^s/\alpha(K)$$

*That is, applying an **automorphism** to a **kernel** preserves the structure of the quotient $\mathbb{Z}^s/K$.*
(Lemma 5.2.6)

Proof. Define a mapping:

$$\varphi : \mathbb{Z}^s \to \mathbb{Z}^s/\alpha(K)$$
$$z \mapsto z + \alpha(K)$$

where:

$$\alpha(K) = \{\alpha(k) \mid k \in K\}$$

and $K = ker(\theta)$, and α is an automorphism of $\mathbb{Z}^s$.

φ is well-defined (since it has the same structure as the canonical map)

We now compute the kernel. Notice, $x \in ker(\varphi)$ if and only if:

$$\varphi(x) = 0 + \alpha(K) \iff x \in \alpha(K)$$

In other words, there exists a unique $k \in ker(\theta)$ such that:

$$x = \alpha(k)$$

But α is an automorphism, so $k \in ker(\theta)$ **if and only if** $x \in ker(\theta)$. We prove this now. If $k \in ker(\theta)$, then:

$$\theta(k) = \sum_{i=1}^{s} k_i a_i = 0$$

Thus:

$$\theta(x) = \sum_{i=1}^{s} x_i a_i = \sum_{i=1}^{s} \alpha(k_i) a_i = \alpha\left(\sum_{i=1}^{s} k_i a_i\right) = 0$$

Hence, $k \in ker(\theta) \implies x = \alpha(k) \in ker(\theta)$.

Now, assume that $x = \alpha(k) \in ker(\theta)$. Then:

$$\theta(x) = \sum_{i=1}^{s} x_i a_i = 0$$

But this means that:

$$\sum_{i=1}^{s} \alpha(k_i)a_i = \alpha\left(\sum_{i=1}^{s} k_i a_i\right) = 0$$

Now, since α is an automorphism, and $\alpha(0_{\mathbb{Z}^s}) = 0_{\mathbb{Z}^s}$ (thinking about $\mathbb{Z}^s$ as a group). Hence:

$$\sum_{i=1}^{s} k_i a_i = \theta(k) = 0$$

so $k \in ker(\theta) \iff x = \alpha(k) \in ker(\theta)$

Hence, we have shown that:

$$ker(\varphi) = ker(\theta) = K$$

Moreover, φ is trivially surjective, so by the first isomorphism theorem we have:

$$\mathbb{Z}^s/K \cong \mathbb{Z}^s/\alpha(K)$$

as required.

□

2.2.3 From Kernel to Matrix

You might be wondering: what was the point of the above lemma? Well, notice, our kernel $K = ker(\theta)$ is finitely generated, say with generators $x_1, x_2, \ldots, x_r$. Then, we can write each $x_i \in \mathbb{Z}^s$ using the standard basis $\{e_j\}_{j\in[1,s]}$:

$$x_i = \sum_{j=1}^{s} a_{ij}e_j = (a_{i1}, a_{i2}, \ldots, a_{is}), \qquad a_{ij} \in \mathbb{Z},\ i \in [1, r],\ j \in [1, s]$$

This immediately reminds us of **representation matrices** in Honours Algebra.

Indeed, define the matrix:

$$M = (a_{ij}) \in \mathbb{Z}^{r\times s}$$

In this way, the **kernel** M can be represented by a matrix M (notice, M won't be unique, since the generators $x_1, \ldots, x_r$ need not be unique, so many possible a_{ij} may be used). However, we can easily go from kernel (or more generally, **submodule**) to matrix, and from **matrix** to kernel/submodule:

$$(b_{ij}) \iff y_i = \sum b_{ij}e_j$$

Again, you might **still** be wondering how these 2 are related. Well, one particular instance of an **automorphism** on $\mathbb{Z}^s$ (thinking about $\mathbb{Z}^s$ as a vector) is **matrix multiplication** (by invertible matrices). What the Lemma above tells us is that we can apply matrix multiplication (or in general, some invertible transformation) to our representative matrix M, which won't affect the structure of the quotient:

$$\mathbb{Z}^s/K \cong \mathbb{Z}^s/\alpha(K)$$

In particular, if we are clever, we can "chain" automorphisms α, such that $K' = \alpha(K)$ corresponds with a "convenient" matrix for computation, which will then give us an equivalent, but more convenient way of looking at:

$$A \cong \mathbb{Z}^s / K$$

This is all rather abstract, so lets consider a particular example. Suppose we have a submodule K of $\mathbb{Z}^2$ generated by $x_1 = (0,6), x_2 = (6,8), x_3 = (3,1)$. In terms of **groups**:

$$K = \langle (0,6), (6,8), (3,1) \rangle$$

and in terms of **modules**:

$$K = \mathbb{Z}(0,6) + \mathbb{Z}(6,8) + \mathbb{Z}(3,1)$$

Now, the representative matrix for K will be:

$$M = \begin{pmatrix} 0 & 6 \\ 6 & 8 \\ 3 & 1 \end{pmatrix}$$

Now, we consider the effect of applying **invertible** row operations to M, and how these affect the corresponding **submodule** associated to the matrix.

① **Row Swap**

Say we act on M by swapping it's first 2 rows:

$$M \overset{R_1 \leftrightarrow R_2}{\mapsto} M' = \begin{pmatrix} 6 & 8 \\ 0 & 6 \\ 3 & 1 \end{pmatrix}$$

It is easy to M' has the same **row space** as M, so by swapping rows we preserve the submodule, since we operate over abelian groups over addition:

$$K = \mathbb{Z}(0,6) + \mathbb{Z}(6,8) + \mathbb{Z}(3,1) = \mathbb{Z}(6,8) + \mathbb{Z}(0,6) + \mathbb{Z}(3,1)$$

② **Row Addition**

Say we act on M by adding it's first 2 rows:

$$M \overset{R_1 + R_2}{\mapsto} M' = \begin{pmatrix} 6 & 14 \\ 6 & 8 \\ 3 & 1 \end{pmatrix}$$

Again, is easy to M' has the same **row space** as M, so by adding rows we preserve the submodule. In particular, the submodule associated to M' is:

$$K' = \mathbb{Z}(6,14) + \mathbb{Z}(6,8) + \mathbb{Z}(3,1)$$

but:

$$\mathbb{Z}(0,6) = \mathbb{Z}(6,14) - \mathbb{Z}(6,8) \qquad \mathbb{Z}(6,14) = \mathbb{Z}(0,6) + \mathbb{Z}(6,8)$$

which means that:

$$K = K'$$

In general, **invertible row operations** won't change the submodule K: they simply change the **generators** we use. This is the same as the linear algebra statement "row equivalent matrices have the same row space".

Moreover, notice these invertible row operations can be represented by **left matrix multiplication**. For example, **swapping** the first 2 rows is given by:

$$DM = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 6 \\ 6 & 8 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 8 \\ 0 & 6 \\ 3 & 1 \end{pmatrix} = M'$$

and **row addition**:

$$DM = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 6 \\ 6 & 8 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 14 \\ 6 & 8 \\ 3 & 1 \end{pmatrix} = M'$$

Indeed, these matrix multiplications represent **automorphisms** of $\mathbb{Z}^s$, so we'd expect that:

$$\mathbb{Z}^s/K \cong \mathbb{Z}^s/K'$$

but in the case of **invertible row operations**, we get the bonus that our submodule doesn't even change!

> *Notice, we aren't including scalar multiplication as part of our invertible operations. This is because we are operating over $\mathbb{Z}$-modules, whereby the inverse of a product is not always defined (i.e $4^{-1} \notin \mathbb{Z}$).*
> ***However**, performing operations of the form $R_i + zR_j$ **is** invertible (just subtract zR_j from the resulting R_i).*

Now, what happens to our **submodule** K if we apply **invertible column operations** to our matrix M?

① **Column Swap**

Say we act on M by swapping its 2 columns:

$$M \overset{C_1 \leftrightarrow C_2}{\mapsto} M' = \begin{pmatrix} 8 & 6 \\ 6 & 0 \\ 1 & 3 \end{pmatrix}$$

Now, whilst the **column space** is preserved, its **row space** changes completely. Indeed, the associated **submodule** will be:

$$K' = \mathbb{Z}(8,6) + \mathbb{Z}(6,0) + \mathbb{Z}(1,2)$$

This is completely different from K. For instance:

$$(6,0) = 0(8,6) + 1(6,0) + 0(1,3) \in K'$$

but $(6,0) \notin K$, since $K = \mathbb{Z}(0,6) + \mathbb{Z}(6,8) + \mathbb{Z}(3,1)$, so we'd require:

$$\begin{aligned} & x(0,6) + y(6,8) + z(3,1) = (6,0) \\ \implies & 6y + 3z = 6 \qquad 6x + 8y + z = 0 \\ \implies & 6x + 8y + 2 - 2y = 0 \\ \implies & 6x + 6y = -2 \\ \implies & 6(x+y) = -2 \end{aligned}$$

and there is no integer satisfying $6a = -2$.

However, not all hope is lost. After all, **invertible column operations** can be represented by **right matrix multiplication** with an invertible matrix. For instance, to swap the columns:

$$M' = MD = \begin{pmatrix} 0 & 6 \\ 6 & 8 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 8 & 6 \\ 6 & 0 \\ 1 & 3 \end{pmatrix}$$

D is an automorphism of $\mathbb{Z}^s$, and we can indeed see that:

$$KD = \mathbb{Z}(0,6)D + \mathbb{Z}(6,8)D + \mathbb{Z}(3,1)D = \mathbb{Z}(8,6) + \mathbb{Z}(6,0) + \mathbb{Z}(1,2) = K'$$

so by our Lemma:

$$\mathbb{Z}^s/K \cong \mathbb{Z}^s/K' = \mathbb{Z}^s/KD$$

Hence, whilst **invertible column operations** do change our **submodule** K, they don't change the **isomorphism class**:

$$A \cong \mathbb{Z}^s/K \cong \mathbb{Z}^s/KD$$

Since all we care about is A, we can change K as much as we want, so long as this doesn't affect the **structure** of $\mathbb{Z}^s/K$.

All this discussion then leads to the following proposition.

2.2.4 Proposition: Invertible Operations on Matrices Preserve Isomorphism

*Suppose that M is the $r \times s$ matrix corresponding to the **finitely generated submodule**:*

$$K = \sum_{i=1}^{r} \mathbb{Z}x_i \subseteq \mathbb{Z}^s$$

*If we change $M \to M'$ via **invertible row and column** operations, then M' corresponds to a **submodule** K' of $\mathbb{Z}^s$, such that:*

$$\mathbb{Z}^s/K \cong \mathbb{Z}^s/K'$$

(Proposition 5.2.7)

2.3 Proof: Fundamental Theorem of Finitely Generated Abelian Groups

*Using the discussions above, we have now developed a sufficient amount of linear algebra to prove the **Fundamental Theorem of Finitely Generated Abelian Groups**. We restate it:*

*Let A be a **finitely generated abelian group**. That is, $\exists a_1, \dots, a_s$ such that:*

$$A = \langle a_1, \dots, a_s \rangle$$

Then:

$$A \cong \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \dots \times \mathbb{Z}_{r_k} \times \mathbb{Z}^{\ell}, \qquad k, \ell \in \mathbb{N},\ r_i \in \mathbb{Z}$$

and such that:

$$r_1 \mid r_2 \mid \dots \mid r_k$$

*Here, we think of $A, \mathbb{Z}_{r_i}$ as $\mathbb{Z}$-**modules**, not abelian groups.*
(Theorem 5.2.5)

Proof. Let K be the kernel of the $\mathbb{Z}$-module homomorphism:

$$\theta : \mathbb{Z}^s \to A$$

$$(r_1, \dots, r_s) \mapsto \sum_{i=1}^{s} r_i a_i$$

such that:

$$A = \mathbb{Z}^s/K$$

Moreover, let M be the matrix associated to K, where K is finitely generated by:

$$x_i = (a_{i1}, \dots, a_{is})$$

such that:

$$M = (a_{ij})$$

We then perform the following algorithm:

1. Apply invertible row and column operations on M to ensure that $a_{11} = r_1 = gcd(\{a_{ij}\})$ (this will always be possible, using Bezout's lemma)

2. Perform further IRCs, to "clean" the first row and columns. That is turn the first row into:

$$\begin{pmatrix} r_1 & 0 & \dots & 0 \end{pmatrix}$$

   and the first column into:

$$\begin{pmatrix} r_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

   (again, this will always be possible, since r_1 will divide all other entries in the matrix)

3. Repeat this procedure, until M becomes a diagonal matrix:

$$M = \begin{pmatrix} r_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & r_2 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & r_k & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

But then this tells us that:

$$K' = \mathbb{Z}(r_1, 0, \dots, 0) + \mathbb{Z}(0, r_2, \dots, 0) + \dots + \mathbb{Z}(0, 0, \dots, r_k, \dots, 0)$$

and

$$A \cong \mathbb{Z}^s / K \cong \mathbb{Z}^s / K'$$

We now claim that this implies that:

$$A \cong \mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}_{r_k} \times \mathbb{Z}^{s-k}$$

To this regard, consider a mapping:

$$\varphi : \mathbb{Z}^s \to \mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}_{r_k} \times \mathbb{Z}^{s-k}$$

Define:

$$[x]_n = x \ (mod \ n)$$

and define φ as:

$$(z_1, \dots, z_s) \mapsto ([z_1]_{r_1}, [z_2]_{r_2}, \dots, [z_k]_{r_k}, z_{k+1}, \dots, z_s)$$

This is clearly a homomorphism, since $z_i \mapsto [z_i]_{r_i}$ is a homomorphism (and the trivial map $z_i \mapsto z_i$ is too). Moreover, it is clearly surjective.

Now, lets compute $ker(\varphi)$. We claim that $ker(\varphi) = K'$. Indeed:

$$\begin{aligned} & z \in ker(\varphi) \\ \iff & \varphi(z) = (0, 0, \dots, 0) \\ \iff & z = (a_1 r_1, a_2 r_2, \dots, a_k r_k, 0, \dots, 0), \quad a_i \in \mathbb{Z} \\ \iff & z \in K' \end{aligned}$$

where we can rewrite:

$$\begin{aligned} K' &= \mathbb{Z}(r_1, 0, \dots, 0) + \mathbb{Z}(0, r_2, \dots, 0) + \dots + \mathbb{Z}(0, 0, \dots, r_k, \dots, 0) \\ &= \mathbb{Z}(r_1, 0, \dots, 0) + \mathbb{Z}(0, r_2, \dots, 0) + \dots + \mathbb{Z}(0, 0, \dots, r_k, \dots, 0) \\ &+ \underbrace{\mathbb{Z}(0, 0, \dots, 0) + \dots + \mathbb{Z}(0, 0, \dots, 0)}_{s-k \ times} \end{aligned}$$

Hence, by the First Isomorphism Theorem:

$$\mathbb{Z}^s / K' \cong \mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}_{r_k} \times \mathbb{Z}^{s-k}$$

Hence, we have that:

$$A \cong \mathbb{Z}^s / K \cong \mathbb{Z}^s / K' \cong \mathbb{Z}_{r_1} \times \dots \times \mathbb{Z}_{r_k} \times \mathbb{Z}^{s-k}$$

as required.

We prove uniqueness in the following proposition.

□

2.3.1 Proposition: FTFGAG Provides a Unique Decomposition

Let p be prime, and let:

$$a_1 \geq a_2 \geq \dots \geq a_m$$

$$b_1 \geq b_2 \geq \dots \geq b_n$$

be ***positive integers****. If:*

$$A = C_{p^{a_1}} \times \dots \times C_{p^{a_m}} \cong B = A = C_{p^{b_1}} \times \dots \times C_{p^{b_n}}$$

then:

$$m = n \qquad \forall i \in [1, m], a_i = b_i$$

If this is true, then by FTFAG from last week, each $\mathbb{Z}_{r_i}$ will decompose uniquely into cyclic groups of prime power order, so our decomposition for A in terms of $\mathbb{Z}_{r_i}$, will be unique.
(Proposition 5.3.2)