Reading 4

Reviewing basics of abelian groups

Goals

(a) Understand $\mathbb{F}_2$ and $\mathbb{Z}$

(b) Perform computations in direct sums of the above groups

(c) Become familiar with how to think of certain homomorphisms as matrices

(d) Compute kernels and images of homomorphisms

4.1 Abelian groups and examples

Recall that an abelian group is the data of a set A and a function $A \times A \to A$ satisfying some properties.

Notation 4.1.1. It is often tradition to write this function using the plus symbol; so the image of a pair $(a, b) \in A \times A$ under this function is often written $a + b$.

Definition 4.1.2 (Abelian group)**.** An *abelian group* is a set A together with a function $+ : A \times A \to A$ satisfying the following properties:

(i) $+$ is an associative operation, meaning for every triplet $a, b, c \in A$, we have that $(a + b) + c = a + (b + c)$.

(ii) $+$ is a commutative operation, meaning that for every pair $a, b \in A$, we have that $a + b = b + a$.

(iii) $+$ has a unit, meaning that there exists an element (traditionally denoted as 0) inside of A such that, for every $a \in A$, we have $0 + a = a$.

(iv) $+$ admits inverses, meaning that for every $a \in A$, there exists an element b such that $a + b = 0$. Following tradition, this element b is usually denoted by $-a$.

Remark 4.1.3. There are various consequences of these properties. For example, there is one and only one unit – so the notation 0 is defined unambiguously – and likewise, any $a \in A$ has a *unique* inverse, so the notation $-a$ is also defined unambiguously. You should check these claims if you have not thought about them before. However, this is not a group theory class, so we will take these facts (which are proven in a standard course on group theory) for granted.

Definition 4.1.4. The element 0 is called the *additive unit*, the *additive identity*, or the *zero element*.

Given an element $a \in A$, the element $-a$ is called the *negative of* a or the *additive inverse to* a.

Notation 4.1.5 (Subtraction notation)**.** Let A be an abelian group and fix two elements $a, b \in A$. Then the expression

$$a - b$$

is shorthand for the expression $a + (-b)$.

There are two basic examples of abelian groups that begin our journey: $\mathbb{F}_2$ and $\mathbb{Z}$.

Definition 4.1.6 ($\mathbb{F}_2$)**.** We let $\mathbb{F}_2 = \{0, 1\}$ denote the set consisting of two elements 0 and 1, and we define an operation as follows:

$$0 + 0 = 0, \qquad 0 + 1 = 1, \qquad 1 + 0 = 1, \qquad 1 + 1 = 0.$$

Exercise 4.1.7. Verify that $\mathbb{F}_2$ (with the above addition) is an abelian group. In particular, make sure you understand why $-1 = 1$.

Exercise 4.1.8. Compute the following in $\mathbb{F}_2$:

(a) $1+1$

(b) $1+0$

(c) $(1+1)+1$

(d) $1+(1+1)$

(e) $1+1+1$

(f) $1+(-1)$

(g) $1-1$

(h) $-1+1$

(i) $-1+1-1+1+1$

Remark 4.1.9 (There are other notations for $\mathbb{F}_2$)**.** $\mathbb{F}_2$ also goes by other names. The most common is $\mathbb{Z}/2\mathbb{Z}$. Many topologists – especially homotopy theorists – use the notation C_2 because it is faster to write on the blackboard. The notation stands for "the cyclic group of order 2," and you do not need to know what this name literally means. Our notation, $\mathbb{F}_2$, stands for "the field with 2 elements," but you also do not need to know what a field is (in this course).

Definition 4.1.10. We let $\mathbb{Z}$ denote the usual set of integers, with addition given by the usual notion of addition.

Exercise 4.1.11. Verify that $\mathbb{Z}$ (with the above addition) is an abelian group. Make sure you understand why $-1 \neq 1$.

4.2 Making new abelian groups

Given two abelian groups A and B, we can make a new abelian group called the direct sum of A and B.

Definition 4.2.1. Fix two abelian groups A and B. The *direct sum* of A and B, as a set, is the product $A \times B$. Addition is defined by:

$$(A \times B) \times (A \times B) \to A \times B, \qquad ((a_1, b_1), (a_2, b_2)) \mapsto (a_1 + a_2, b_1 + b_2).$$

Put more succinctly,

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2).$$

We denote the direct sum of A and B by the notation

$$A \oplus B.$$

Remark 4.2.2. $A \oplus B$ is the exact same thing as $A \times B$. The former notation emphasizes the group structure on $A \oplus B$, and also emphasizes that A and B are abelian. (The notion of direct sum is typically not defined for non-abelian groups.) We will not deal too much with non-abelian groups in this course, so we will ignore this point and just be happy with the direct sum notation. It also turns out that $\oplus$ and $\times$ differ when we input infinitely many abelian groups – we will cross this bridge if we encounter it.

Example 4.2.3. The group $\mathbb{F}_2 \oplus \mathbb{F}_2$ has four elements:

$$(0,0), \qquad (1,0), \qquad (0,1), \qquad (1,1).$$

The addition in $\mathbb{F}_2 \oplus \mathbb{F}_2$ is as follows. (You should verify that there are no typos in the equations below.)

- $(0,0)+(0,0)=(0,0)$.
- $(0,0)+(1,0)=(1,0)$.
- $(0,0)+(0,1)=(0,1)$.
- $(0,0)+(1,1)=(1,1)$.
- $(1,0)+(0,0)=(1,0)$.
- $(1,0)+(1,0)=(0,0)$.
- $(1,0)+(0,1)=(1,1)$.
- $(1,0)+(1,1)=(0,1)$.
- $(0,1)+(0,0)=(0,1)$.
- $(0,1)+(1,0)=(1,1)$.
- $(0,1)+(0,1)=(0,0)$.
- $(0,1)+(1,1)=(1,0)$.
- $(1,1)+(0,0)=(1,1)$.
- $(1,1)+(1,0)=(0,1)$.
- $(1,1)+(0,1)=(1,0)$.
- $(1,1)+(1,1)=(0,0)$.

Exercise 4.2.4. What element of $\mathbb{F}_2 \oplus \mathbb{F}_2$ is the zero element? Which element is the additive inverse to $(1,1)$? Which element is the additive inverse to $(1,0)$?

Example 4.2.5. The group $\mathbb{F}_2 \oplus \mathbb{Z}$ has infinitely many elements. Here are some examples of elements:

$$(0,3), \qquad (0,-7), \qquad (1,3), \qquad (1,57788), \qquad (1,-1).$$

Exercise 4.2.6. What element of $\mathbb{F}_2 \oplus \mathbb{Z}$ is the zero element? Which element is the additive inverse to $(0,5)$? To $(0,-5)$? To $(1,-5)$? To $(1,1)$?

We can also make direct sums of more than two abelian groups.

Example 4.2.7. The group $\mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2$ has 16 elements. They are given as follows:

- $(0, 0, 0, 0)$
- $(0, 0, 0, 1)$
- $(0, 0, 1, 0)$
- $(0, 0, 1, 1)$
- $(0, 1, 0, 0)$
- $(0, 1, 0, 1)$
- $(0, 1, 1, 0)$
- $(0, 1, 1, 1)$
- $(1, 0, 0, 0)$
- $(1, 0, 0, 1)$
- $(1, 0, 1, 0)$
- $(1, 0, 1, 1)$
- $(1, 1, 0, 0)$
- $(1, 1, 0, 1)$
- $(1, 1, 1, 0)$
- $(1, 1, 1, 1)$

Here is an example of addition in $\mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2$:

$$(1, 1, 0, 1) + (0, 1, 0, 1) = (1 + 0, 1 + 1, 0 + 0, 1 + 1) = (1, 0, 0, 0).$$

When we start having many copies of an abelian group in a direct sum, we don't want to write out all the copies. So we have the following shorthand:

Notation 4.2.8. For any integer $n \geq 0$ and any abelian group A, we let

$$A^{\oplus n}$$

denote the direct sum of n copies of A.

Remark 4.2.9. By convention $A^{\oplus 0}$ is the abelian group with only one element in it, also called the trivial abelian group.

Example 4.2.10. The abelian group in Example 4.2.7 may be written $\mathbb{F}_2^{\oplus 4}$, or $(\mathbb{F}_2)^{\oplus 4}$, or ${\mathbb{F}_2}^{\oplus 4}$.

Notation 4.2.11 (Column vector notation)**.** It is also common to denote an element of $A^{\oplus n}$ by column vectors. So the column vector

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

denotes the element $(a_1, a_2, \ldots, a_n) \in A^{\oplus n}$.

Example 4.2.12. The notation

$$\begin{pmatrix} 3 \\ -2 \\ 7 \\ 9 \end{pmatrix}$$

represents the element $(3, -2, 7, 9)$ of $\mathbb{Z}^{\oplus 4}$.

Exercise 4.2.13. Compute the following additions in ${\mathbb{F}_2}^{\oplus 4}$.

(a) $\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$

(b) $\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$

(c) $\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

(d) $\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

(e) $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

(f) $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

4.3 Group homomorphisms

Definition 4.3.1. Let A and B be abelian groups. A *group homomorphism* is a function $f : A \to B$ satisfying the following property: For every $a, a' \in A$, $f(a + a') = f(a) + f(a')$.

Intuitively, a group homomorphism is a special kind of function: one that respects addition.

Example 4.3.2. Fix your favorite integer k. Then the function $f : \mathbb{Z} to \mathbb{Z}$ sending $a \mapsto ka$ is a group homomorphism.

For example, if $k = 3$, we indeed have that $f(a+a') = 3(a+a')$, which in turn equals $3a+3a' = f(a)+f(a')$. In other words, the distributive property of multiplication over addition guarantees that multiplication by k is a group homomorphism.

Exercise 4.3.3. Write down every possible function from $\mathbb{F}_2$ to $\mathbb{F}_2$. (You should have four of them.)

Identify which of these are group homomorphisms.

Exercise 4.3.4. Show that (somewhat confusingly) the set of group homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$ is in bijection with the set of integers. (Hint: Example 4.3.2.)

More generally, if B is any group, show that the function

$$\{\text{group homomorphisms } f : \mathbb{Z} \to B\} \to B, \qquad f \mapsto f(1)$$

is a bijection.

(This is the universal property of $\mathbb{Z}$ – a homomorphism out of $\mathbb{Z}$ is uniquely determined by choosing the element of B to hit with $1 \in \mathbb{Z}$.)

4.3.1 Group isomorphisms

Definition 4.3.5. A group homomorphism $f : A \to B$ is called a group *isomorphism* if f is a bijection.

Remark 4.3.6. It is a standard fact – that you can prove! – that if f is a group isomorphism, the its inverse function is also a group homomorphism, and hence a group isomorphism.

Remark 4.3.7. You should think of a group isomorphism as a way to see that two groups are equivalent. (This is in analogy to bijection – a bijection is a way to see that two sets are equivalent in size. A group isomorphism is more – it shows not only that two abelian groups have the same size, but their additions can be translated into each other without any loss of information.)

As best as possible, you should *not* resort to being content that two groups "are isomorphic." Instead, you should always try to remember the isomorphism itself – i.e., remember the function. This is a rather sophisticated observation depending on where you are in your career, but it is true. For example, a group A can have many group isomorphisms to itself! Of course A is equivalent to itself, but each of these group isomorphisms tells us a new and equivalent way to think about A.

4.3.2 Some group homomorphisms can be thought of as matrices

When a group homomorphism is has domain $A^{\oplus m}$ and codomain $A^{\oplus n}$, one can express the group homomorphism as a matrix.

Example 4.3.8. The matrix

$$\begin{pmatrix} 0 & 1 & 3 & 5 \\ -3 & 1 & -2 & 0 \\ 1 & 2 & 1 & 19 \end{pmatrix} \tag{4.3.2.1}$$

encodes a group homomorphism from $\mathbb{Z}^{\oplus 4}$ to $\mathbb{Z}^{\oplus 3}$. The value of the group homomorphism on an element is computed by matrix multiplication. For example,

$$\begin{pmatrix} 0 & 1 & 3 & 5 \\ -3 & 1 & -2 & 0 \\ 1 & 2 & 1 & 19 \end{pmatrix} \begin{pmatrix} 9 \\ 1 \\ 7 \\ 7 \end{pmatrix} = \begin{pmatrix} 0 \cdot 9 + 1 \cdot 1 + 3 \cdot 7 + 5 \cdot 7 \\ -3 \cdot 9 + 1 \cdot 1 + -2 \cdot 7 + 0 \cdot 7 \\ 1 \cdot 9 + 2 \cdot 1 + 1 \cdot 7 + 19 \cdot 7 \end{pmatrix} = \begin{pmatrix} 57 \\ -40 \\ 151 \end{pmatrix}.$$

In other words, the group homomorphism sends the element $(9, 1, 7, 7)$ to the element $(57, -40, 151)$.

To make sure you know how matrix multiplication works, you should confirm that the element $(1, 1, 0, 0)$ is sent to $(1, -2, 3)$ under this matrix.

Remark 4.3.9. We are following the convention that, if a matrix is to be thought of as a group homomorphism, then we input a domain vector to the *right* of the matrix – meaning a matrix multiplies a vector from the left. This is to conform to the order of notation for functions and inputs. When we have a function f act on an input a, we write $f(a)$ – the function is on the left, and the input is on the right.

Exercise 4.3.10. Consider the group homomorphism given by the matrix in Example 4.3.8. Compute the image of the following elements of $\mathbb{Z}^{\oplus 4}$ under this group homomorphism:

(a) $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ (c) $\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ (e) $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$. (g) $\begin{pmatrix} 2 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ (i) $\begin{pmatrix} 19 \\ 0 \\ 8 \\ 0 \end{pmatrix}$

(b) $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ (d) $\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ (f) $\begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ (h) $\begin{pmatrix} 1 \\ -1 \\ -3 \\ 1 \end{pmatrix}$ (j) $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 9 \end{pmatrix}$.

For parts (b) through (e), what do you notice about your answers and the columns of the original matrix?

Exercise 4.3.11. ${\mathbb{F}_2}^{\oplus 3}$ has eight elements. For all eight elements, compute their images under the following matrices:

(a) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ (d) $\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$

Based on your answers, explain why the linear transformations in (a) and (b) are bijections. How about (c) and (d)?

Exercise 4.3.12. The following all encode group homomorphisms between ${\mathbb{F}_2}^{\oplus m}$ and ${\mathbb{F}_2}^{\oplus n}$.

(i) $\begin{pmatrix} 1 & 1 \\ 0 & 0 \\ 1 & 1 \end{pmatrix}$ (ii) $\begin{pmatrix} 1 & 1 \end{pmatrix}$ (iii) $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ (iv) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$

(a) For each matrix, indicate the domain and codomain. (As a hint: Matrix (i) has domain ${\mathbb{F}_2}^{\oplus 2}$ and codomain ${\mathbb{F}_2}^{\oplus 3}$.)

(b) ${\mathbb{F}_2}^{\oplus 2}$ has four elements. For all eight elements, compute their images under the above matrices.

(c) Based on your answers, explain which of the above four matrices are injections, which are surjections, and which are bijections.

4.4 Kernels

Kernels tell you a lot about a group homomorphism.

Definition 4.4.1. Let $f : A \to B$ be a group homomorphism. The *kernel* of f is the set of all elements in A that are sent to $0 \in B$. We write

$$\ker(f)$$

to denote the kernel of f.

The following is proven in a typical class involving group theory:

Proposition 4.4.2. Let $f : A \to B$ be a group homomorphism. The following are equivalent:

(a) The kernel of f consists of exactly one element.

(b) The kernel of f consists only of the element $0 \in A$.

(c) f is an injection.

Remark 4.4.3. Proposition 4.4.2 is useful for a few reasons; the biggest reason is that the proposition gives us a new way to determine whether a group homomorphism is an injection or not. Typically, to determine if f is an injection, one has to prove that $f(a) = f(a') \implies a = a'$. The proposition tells us that (if we'd like) we can instead prove that $f(a) = 0 \implies a = 0$. (Note that the two instances of 0 here mean two different things – why?)

Example 4.4.4. Consider the group homomorphism $f : {\mathbb{F}_2}^{\oplus 3} \to {\mathbb{F}_2}^{\oplus 2}$ given by the following matrix:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

What does it mean for an element $(a, b, c) \in {\mathbb{F}_2}^{\oplus 3}$ to be in the kernel? It means precisely that

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Computing the righthand side, we find that $(a, b, c) \in \ker(f)$ if and only if the following equations are satisfied:

$$a + b + c = 0 \qquad \text{and} \qquad a + c = 0.$$

Subtracting the second equation from the first, we find that

$$\begin{aligned} (a + b + c) - (a + c) &= 0 - 0 \\ b &= 0. \end{aligned} \tag{4.4.0.1}$$

Now, because a and c are elements of $\mathbb{F}_2$, of course $a + c = 0$ is equivalent to saying $a = c$. In other words, we find that $(a, b, c) \in \ker(f)$ if and only if (i) $a = c$ and $b = 0$. We conclude there are two elements in the kernel:

$$(1, 0, 1) \qquad \text{and} \qquad (0, 0, 0).$$

By Proposition 4.4.2, we conclude that f is not an injection.[1]

Remark 4.4.5. An efficient way to identify the kernel of a matrix is by computing the reduced row echelon form. We will not go over this, and you also will not need it to compute kernels in this class.

Exercise 4.4.6. (a) Compute the kernels of all the group homomorphisms in Exercise 4.3.3.

(b) Compute the kernels of all the group homomorphisms in Exercise 4.3.11.

(c) Compute the kernels of all the group homomorphisms in Exercise 4.3.12.

4.5 Images

Definition 4.5.1. The *image* of a homomorphism $f : A \to B$ is the image of f as a function. (That is, the set of all elements $b \in B$ for which there exists an $a \in A$ with $f(a) = b$.)

Here is a fact that is proven in linear algebra and some group theory classes:

Proposition 4.5.2. If a homomorphism f is given by a matrix, the image of f is generated by the columns of the matrix.

Remark 4.5.3. Here, by *generated*, we mean that the entire image can be obtained by some linear combination of the columns. For example, given the matrix (4.3.2.1), any element of its image can be written as a summation

$$a \begin{pmatrix} 0 \\ 3 \\ -1 \end{pmatrix} + b \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix} + c \begin{pmatrix} 3 \\ -2 \\ 1 \end{pmatrix} + d \begin{pmatrix} 5 \\ 0 \\ 19 \end{pmatrix}$$

where a, b, c, d are integers. Indeed, given values of a, b, c, d, the element above is the image of the element $(a, b, c, d) \in \mathbb{Z}^{\oplus 4}$.

Remark 4.5.4. Instead of "generated," we sometimes say "spanned." So the image of a matrix is spanned by its columns.

[1] In fact, just knowing the domain and codomain of f, one can see that f cannot be an injection. Why?

Example 4.5.5. Consider the homomorphism $f : \mathbb{F}_2{}^{\oplus 3} \to \mathbb{F}_2{}^{\oplus 2}$ given by the following matrix:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

By Proposition 4.5.2, the image of f is spanned by the columns of the matrix. Hence, any element of the image is of the form

$$a \begin{pmatrix} 1 \\ 1 \end{pmatrix} + b \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

(Note that I am ignoring repeated columns, for obvious reasons.) Of course, in $\mathbb{F}_2$, adding something an even number of times results in zero, so the only interesting values of a and b are 0 and 1 – meaning there are only 4 elements in the image. Let's compute each one:

- $(a = 0, b = 0)$. $0 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$
- $(a = 1, b = 0)$. $1 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$
- $(a = 0, b = 1)$. $0 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + 1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
- $(a = 1, b = 1)$. $\begin{pmatrix} 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$

So we conclude that all four elements of $\mathbb{F}_2^{\oplus 2}$ are in the image. In particular, f is a surjection.

Remark 4.5.6. One nice thing about working with $\mathbb{F}_2$ is that $\mathbb{F}_2$ is finite – unlike $\mathbb{Z}$. Especially as you are starting out playing with abelian groups and matrices, this can give some sense of solace.