Chapter 4

Some finite abelian groups

We want to outline a second proof of theorem 3.12. For this proof, we assume that $X = [m]$ and $Y = [n]$ for some $m, n \in \mathbb{N}$. Then we have to construct a one to one correspondence between $[m] \times [n]$ and $[mn]$. We define a function $L(q, r) = qn + r$ from $[m] \times [n] \to \mathbb{N}$. Since $q \leq m - 1$ and $r \leq n - 1$, we have

$$L(q, r) < (m - 1)n + n = mn$$

So we can regard L is a map from $[m] \times [n] \to [mn]$ which can visualized using the table

L	0	1	...	n-1
0	0	1	...	n-1
1	n	n+1	...	2n-1
⋮	...			
m-1	(m-1)n	...		mn-1

The fact that L is a one to one correspondence is clear intuitively from the fact that every number in $[mn] = \{0, \ldots, mn - 1\}$ is listed exactly once in the table. Nevertheless, this requires proof which is provided by the next theorem which is usually called the "division algorithm". Although it's not an algorithm in the technical sense, it is the basis of the algorithm for long division that one learns in school.

Theorem 4.1. *Let $a, n \in \mathbb{N}$ with $n \neq 0$, then there exists a unique pair of natural numbers q, r satisfying*

$$a = qn + r,\ r < n$$

Furthermore if $a < mn$, then $q < m$.

Proof. Let

$$R = \{a - q'n \,|\, q' \in \mathbb{N} \text{ and } q'n \leq a\}$$

Let $r = a - qn$ be the smallest element of R. Suppose $r \geq n$. Then $a = qn + r = (q + 1)n + (r - n)$ means that $r - n$ lies in R. This is a contradiction, therefore $r < n$.

Suppose that $a = q'n + r'$ with $r' < n$. Then $r' \in R$ so $r' \geq r$. Then $qn = q'n + (r' - r)$ implies that $n(q - q') = r' - r$. So $r' - r$ is divisible by n. On the other hand $0 \leq r' - r < n$. But 0 is the only integer in this range divisible by n is 0. Therefore $r = r'$ and $qn = q'n$ which implies $q = q'$.

For the last part, suppose that $a < mn$. If $q \geq m$, then $a \geq qn \geq mn$ which is a contradiction. □

The number r is called the remainder of division of a by n, or more briefly $a \, mod \, n$; *mod* is read "modulo" or simply "mod".

This leads to a new kind of arithmetic called modular or clock arithmetic. Fix a positive number n called the modulus. Let $\mathbb{Z}_n = [n] = \{0, 1, \ldots, n-1\}$. Define the modular sum by

$$x \oplus y = (x + y) \, mod \, n$$

This an operation on $\mathbb{Z}_n$.

Theorem 4.2. *$\mathbb{Z}_n$ with this operation forms an abelian group.*

Proof. We will postpone the proof of the associative law. The rest is easy. Certainly $x \oplus 0 = x$ and $x \oplus y = y \oplus x$. If we set

$$\ominus x = \begin{cases} 0 & \text{if } x = 0 \\ n - x & \text{otherwise} \end{cases}$$

then $x \oplus (\ominus x) = 0$. □

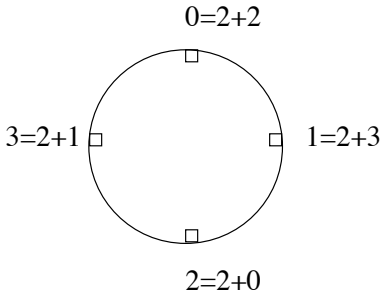
We will look at some examples. Here is the table for $n = 2$

$\oplus$	0	1
0	0	1
1	1	0

This is the simplest nonzero abelian group. A somewhat more complicated case is $n = 4$

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

These rules be understood more schematically by arranging the $0, 1, 2, 3$ on the face of a clock:



We want to observe some things about above table. First of all, it is symmetric (i.e. interchanging rows with columns gives the same thing). This is because the commutative law holds. The fact that 0 is the identity corresponds to the fact that the row corresponding 0 is identical to the top row. There is one more notable feature of this table: every row contains each of the elements $0, \dots 3$ exactly once. A table of elements with this property is called a *latin square*. As we will see this is always true for any abelian group.

In a sense, we have seen this before. If R represents a single rotation of the square, then

$\cdot$	I	R	R^2	R^3
I	I	R	R^2	R^3
R	R	R^2	R^3	I
R^2	R^2	R^3	I	R
R^3	R^3	I	R	R^2

While the entries are totally different, under the correspondence $0 \leftrightarrow I$, $1 \leftrightarrow R$, $2 \leftrightarrow R^2$, $3 \leftrightarrow R^3$, the first table goes into the second. We say two finite groups are *isomorphic* if there is a one to one correspondence between the groups, called an *isomorphism*, which takes the multiplication (or addition) table of the first group into the second. For another example, take the group $\{1, -1\}$ under multiplication.

$\cdot$	1	-1
1	1	-1
-1	-1	1

This is isomorphic to $\mathbb{Z}_2$. We will see many more examples later.

Lemma 4.3. *(Cancellation) Suppose that $(G, *, e)$ is group. Then $a * b = a * c$ implies $b = c$.*

Proof. By assumption, there exists a^{-1} with $a^{-1} * a = a * a^{-1} = e$. Therefore

$$a^{-1} * (a * b) = a^{-1} * (a * c)$$
$$(a^{-1} * a) * b = (a^{-1} * a) * c$$
$$e * b = e * c$$
$$b = c.$$

□

Lemma 4.4. *The multiplication table*

$*$	g_1	g_2	$\dots$
g_1	g_1^2	$g_1 * g_2$	$\dots$
g_2	$g_2 * g_1$	g_2^2	$\dots$
$\vdots$			

of any finite group $G = \{a_1, a_2, \dots\}$ forms a latin square. It is symmetric if and only if G is abelian.

Proof. The symmetry follows from the commutative law. Suppose that $G = \{g_1, g_2, \dots\}$. Then the ith row of the table consists of $g_i * g_1, g_i * g_2 \dots$. Given $g \in G$, the equation $g = g_i * (g_i^{-1} * g)$ shows that g occurs somewhere in this row. Suppose that it occurs twice, that is $g_i * g_j = g_i * g_k = g$ for $g_j \neq g_k$. Then this would contradict the cancellation lemma. □

As an application, we see that

Lemma 4.5. *Any group with 2 elements is isomorphic to $\mathbb{Z}_2$.*

Proof. Let $G = e, g$ be a group with two element with e is the identity. Since the e is the identity, the multiplication table is

$*$	e	g
e	e	g
g	g	?

The missing item ? has to be e in order to be latin square. Then it is isomorphic to $\mathbb{Z}_2$ via $0 \leftrightarrow e$, $1 \leftrightarrow g$. □

4.6 Exercises

1. An element $x \in \mathbb{Z}_n$ is called a generator if $\mathbb{Z}_n = \{x, x \oplus x, x \oplus x \oplus x, \dots\}$. Determine the generators of $\mathbb{Z}_4$.

2. Suppose that G has a multiplication table

$*$	e	g	h
e	e	g	h
g	g	h	e
h	h	h	g

   Is this is a group?