Chapter 3

Integers and Abelian groups

The set integers $\mathbb{Z} = \{\ldots -2, -1, 0, 1, \ldots\}$ is obtained by adding negative numbers to the set of natural numbers. This makes arithmetic easier.

Addition satisfies the rules (1.1), (1.2), (1.3) as before. In addition, there is new operation $n \mapsto -n$ satisfying

$$\text{For each } n \in \mathbb{Z},\ n + (-n) = 0 \tag{3.1}$$

The cancellation law becomes redundant as we will see.

We will now abstract this:

Definition 3.1. *An abelian group consists of a set A with an associative commutative binary operation $*$ and an identity element $e \in A$ satisfying $a * e = a$ and such that any element a has an inverse a' which satisfies $a * a' = e$.*

Abelian groups are everywhere. Here list a few some examples.

Let $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z},\ b \neq 0\}$ be the set of rational numbers, the $\mathbb{R}$ the set of real numbers and $\mathbb{C}$ the set of complex numbers.

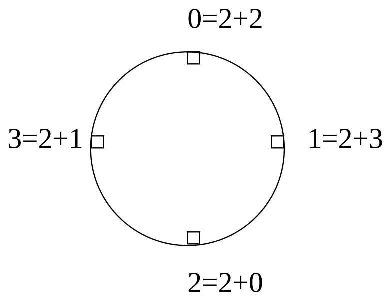
Example 3.2. *The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ with $* = +$ and $e = 0$ are abelian groups.*

Example 3.3. *The set $\mathbb{Q}^*$, (or $\mathbb{R}^*$ or $\mathbb{C}^*$) of nonzero rational (or real or complex) numbers with $* = \cdot$ (multiplication) and $e = 1$ is an abelian group. The inverse in this case is just the reciprocal.*

Example 3.4. *Let n be a positive integer. Let $\mathbb{Z}^n = \{(a_1, a_2, \ldots a_n) | a_1, \ldots a_n \in \mathbb{Z}\}$. We define $(a_1, \ldots a_n) + (b_1, \ldots b_n) = (a_1 + b_1, \ldots a_n + b_n)$ and $\mathbf{0} = (0, \ldots 0)$. Then $\mathbb{Z}^n$ becomes an abelian group. $\mathbb{Z}$ can be replaced by $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ and these examples are probably familiar from linear algebra.*

Example 3.5. *Let n be a positive integer, $\mathbb{Z}_n = \{0, 1, \ldots n-1\}$. Arrange these on the face of a "clock". We define a new kind of operation $\oplus$ called addition $\bmod n$. To compute $a \oplus b$, we set the "time" to a and then count off b hours. We'll give a more precise description later. Unlike the previous examples, this is a finite abelian group.*

Often, especially in later sections, we will simply use + instead $\oplus$ because it easier to write. We do this in the diagram below:



Here's the addition table for $\mathbb{Z}_8$.

$\oplus$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Notice that the table is symmetric (i.e. interchanging rows with columns gives the same thing). This is because the commutative law holds. The fact that 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 $0, \dots 7$ 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.

We can now define the precise addition law for $\mathbb{Z}_n$. Given $a, b \in \mathbb{Z}_n$, $a \oplus b = r(a + b, n)$, where r is the remainder introduced before.

When doing calculations in Maple, we can use the mod operator. For example to add $32 \oplus 12$ in $\mathbb{Z}_{41}$, we just type

$$32 + 12 \, mod \, 41;$$

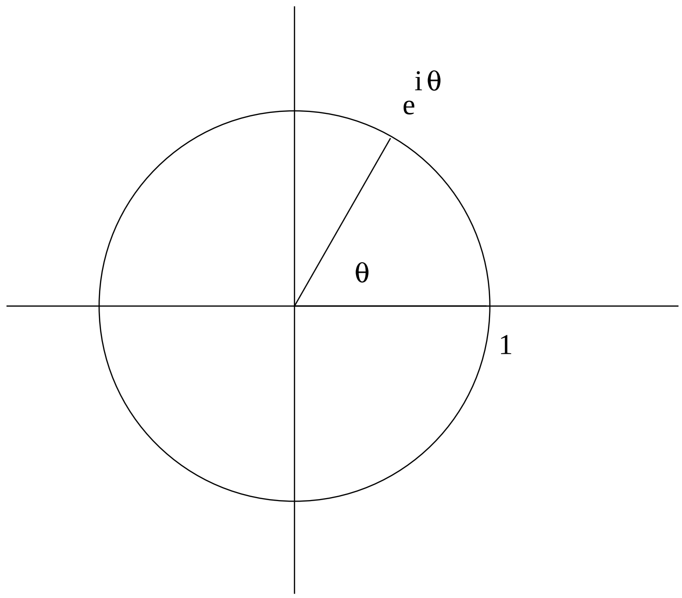
Let n be a positive integer, a complex number z is called an nth root of unity if $z^n = 1$. Let μ_n be the set of all nth roots of unity. For example, $\mu_2 = \{1, -1\}$ and $\mu_4 = \{1, -1, i, -i\}$.

Example 3.6. *μ_n becomes an abelian group under multiplication*

To see that this statement make sense, note that given two elements $z_1, z_2 \in \mu_n$, their product lies in μ_n since $(z_1 z_2)^n = z_1^n z_2^n = 1$ and $1/z_1 \in \mu_n$ since

$(1/z_1)^n = 1$. We can describe all the elements of μ_n with the help of Euler's formula:

$$e^{i\theta} = \cos\theta + i\sin\theta.$$



Lemma 3.7. $\mu_n = \{e^{i\theta} \,|\, \theta = 0, \frac{2\pi}{n}, \frac{4\pi}{n}, \ldots \frac{2(n-1)\pi}{n}\}$

Proof. The equation $z^n = 1$ can have at most n solutions since it has degree n (we will prove this later on). So it's enough to verify that all of the elements on the right are really solutions. Each element is of the form $z = e^{i\theta}$ with $\theta = 2\pi k/n$ with k an integer. Then

$$z^n = e^{in\theta} = \cos(2\pi k) + i\sin(2\pi k) = 1.$$

□

The lemmas says that the elements are equally spaced around the unit circle of $\mathbb{C}$.

Since $e^{i\theta_1}e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$, multiplication amounts to adding the angles. This sounds suspiciously like the previous example. We will see they are essentially the same.

Lemma 3.8. *(Cancellation) Suppose that $(A, *, e)$ is an abelian group. Then $a * b = a * c$ implies $b = c$.*

Proof. By assumption, there exists a' with $a' * a = a * a' = e$. Therefore

$$a' * (a * b) = a' * (a * c)$$

$$(a' * a) * b = (a' * a) * c$$

$$e * b = e * c$$
$$b = c.$$

□

Corollary 3.9. *Given a, there is a unique element a', called the inverse, such that $a * a' = e$.*

Lemma 3.10. *The multiplication table*

$*$	a_1	$\dots$
a_1	$\dots$	
$\vdots$		

of any abelian group $A = \{a_1, a_2, \dots\}$ forms a symmetric latin square.

Proof. The symmetry follows from the commutative law. Suppose that $A = \{a_1, a_2, \dots\}$. Then the ith row of the table consists of $a_i * a_1, a_i * a_2 \dots$. Given $a \in A$, the equation $a = a_i * (a_i' * a)$ shows that a occurs somewhere in this row. Suppose that it occurs twice, that is $a_i * a_j = a_i * a_k = a$ for $a_j \neq a_k$. Then this would contradict the cancellation lemma. □

Let $(A, *, e)$ be a group. Given $a \in A$ and $n \in \mathbb{Z}$, define a^n by

$$a^n = \begin{cases} a * a \dots a \text{ (} n \text{ times) if } n > 0 \\ e \text{ if } n = 0 \\ a' * a' \dots a' (-n \text{ times) if } n < 0 \end{cases}$$

Often the operation on A is written as $+$, in which case the inverse of a is usually written as $-a$, and we write na instead of a^n. When $A = \mathbb{Z}$, this nothing but the definition of multiplication. It's possible to prove the associative, commutative and distributive laws for $\mathbb{Z}$, but we'll skip this.

3.11 Exercises

1. Let $A = \{e, a, b\}$ with e, a, b distinct and the following multiplication table:

*	e	a	b
e	e	a	b
a	a	e	b
b	b	b	a

   Is A an abelian group? Prove it, or explain what goes wrong.

2. Let $A = \{e, a\}$ with $a \neq e$ and the following multiplication table:

*	e	a
e	e	a
a	a	e

Is A an abelian group? Prove it, or explain what goes wrong.

3. Let $(A, *, e)$ be an abelian group. Let a' denote the inverse of a. Prove that $e' = e$, $(a')' = a$ and $(a * b)' = a' * b'$.

4. With notation as above, prove that $(a^n)' = (a')^n$ for any natural number n by induction. This proves $(a^n)^{-1} = (a^{-1})^n = a^{-n}$ as one would hope.

5. Let $(A, *, e)$ and $(B, *, \epsilon)$ be two abelian groups. Let $A \times B = \{(a, b) \,|\, a \in A, b \in B\}$. Define $(a_1, b_1) * (a_2, b_2) = (a_1 * a_2, b_1 * b_2)$ and $E = (e, \epsilon)$. Prove that $(A \times B, *, E)$ is an abelian group. This is called the direct product of A and B. For example $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$.

6. Write down the multiplication tables for μ_2, μ_3, μ_4 and μ_5.

7. An element $\omega \in \mu_n$ is called a primitive root if any element can be written as a power of ω. Check that $e^{2\pi i/5} \in \mu_5$ is primitive. Determine all the others in this group.