Part 3. Groups - concrete examples

4. The axioms

As mentioned above, we will see that many familiar mathematical objects are groups, such as number systems, matrices, functions and sets. We also said that a group is a set and an operation, for example, the integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ and $+$, that satisfies some conditions or rules. Before giving the precise definition of a group, we consider the example of the integers $\mathbb{Z}$ under addition $+$. In particular, let's think about what conditions (or rules) $\mathbb{Z}$ and $+$ satisfy.

The operation of addition $+$ on $\mathbb{Z}$ satisfies the following rules:

$$(x + y) + z = x + (y + z) \tag{4.1}$$

$$x + y = y + x. \tag{4.2}$$

There is a distinguished element 0, which has the property

$$0 + x = x = x + 0 \tag{4.3}$$

Also for every element x there is an element $-x$ (its negative) such that

$$x + (-x) = 0. \tag{4.4}$$

Next, let's think about the non-zero real numbers $\mathbb{R} \setminus \{0\}$ under multiplication $\times$. They satisfy the rules:

$$(x \times y) \times z = x \times (y \times z) \tag{4.5}$$

$$x \times y = y \times x. \tag{4.6}$$

There is a distinguished element 1, which has the property

$$1 \times x = x = x \times 1 \tag{4.7}$$

Also for every element x there is an element $1/x$ (its reciprocal) such that

$$x \times 1/x = 1. \tag{4.8}$$

Note that (4.1), (4.2) and (4.5), (4.6), are the same if you replace $+$ by $\times$. Also (4.3) and (4.7) are the same if you replace $+$ by $\times$ and 0 by 1. Finally, (4.4) and (4.8) are the same if you replace $+$ by $\times$, 0 by 1, and $-x$ by $1/x$.

If X is a set, for example $\mathbb{Z}$ or $\mathbb{R}$, a *binary operation on* X is just a way of combining two elements of X into one element of X. For example, $+$ and $\times$ on $\mathbb{R}$ are binary operations.

Formally, a binary operation on a set X is just a function from the set $X \times X$ of all pairs of elements in X to X.

For example, the following are binary operations on $\mathbb{R}$:

$$+ \text{ (addition)} \quad \times \text{ (multiplication)} \quad / \text{ (division)} \quad - \text{ (subtraction)}$$

The symbol used to denote the operation is unimportant. When we want to emphasise it, we will use $*$; at other times we will use ordinary multiplication notation, writing $x \cdot y$, $x \times y$ or even xy, instead of $x * y$. Sometimes we will use other symbols, such as $\circ$ and $\diamond$.

Probably the most confusing of all is the usage of $+$; in this case we denote the identity element by 0 instead of e, and say *zero* instead of identity; the inverse of an element is denoted by $-x$, rather than x^{-1}, and is called the *negative of* x.

In algebra, we study a set with one or more operations defined on it. These operations are assumed to satisfy some basic properties (called ***axioms***), and the aim is to study the consequences of these properties. The examples above motivate the definition of group.

Definition 4.1. A *group* is a set G and a binary operation $*$ on G such that the following hold:

Closure: $x * y \in G$ for all $x, y \in G$;
Associativity: $(x * y) * z = x * (y * z)$ for all $x, y, z \in G$;
Identity: there is a distinguished element $e \in G$ such that $x * e = e * x = x$ for all $x \in G$;
Inverses: for every $x \in G$ there is a distinguished element $x^{-1} \in G$ such that $x * x^{-1} = x^{-1} * x = e$.

Closure, associativity, identity, and inverses from Definition 4.1 are called the ***group axioms***.

Example 4.2. The set $\mathbb{R} \setminus \{0\}$ of real numbers under multiplication $\times$ is a group. Let's doublecheck:

Closure: $x \times y \in \mathbb{R}$ for all $x, y \in \mathbb{R}$;
Associativity: $(x \times y) \times z = x \times (y \times z)$ for all $x, y, z \in \mathbb{R}$;
Identity: the number $1 \in \mathbb{R}$ satisfies $x \times 1 = 1 \times x = x$ for all $x \in \mathbb{R}$;
Inverses: for all $x \in \mathbb{R}$ there exists $x^{-1} = 1/x \in \mathbb{R}$ such that

$$x \times (1/x) = (1/x) \times x = x/x = 1.$$

Example 4.3. The set $\mathbb{Z}$ of integers under $+$ is a group. Let's doublecheck:

Closure: $x + y \in \mathbb{Z}$ for all $x, y \in \mathbb{Z}$;
Associativity: $(x + y) + z = x + (y + z)$ for all $x, y, z \in \mathbb{Z}$;
Identity: the number $0 \in \mathbb{Z}$ satisfies $x + 0 = 0 + x = x$ for all $x \in \mathbb{Z}$;
Inverses: for all $x \in \mathbb{Z}$ there exists $-x \in \mathbb{Z}$ such that $x + (-x) = (-x) + x = 0$.

Example 4.4. Let

$$G = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R},\ a \neq 0 \right\}.$$

We will prove that G is a group under matrix multiplication.

Closure: Let

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in G$$

be arbitrary. Then

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \in G.$$

Associativity: We know that multiplication of **any** 2×2 matrices with entries in $\mathbb{R}$ is associative and so, in particular,

$$\left[\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \right] \begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \left[\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix}. \right]$$

Identity: It is true that

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{for all} \quad \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in G.$$

But

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin G$$

and so it is not the identity of G. However,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{for all} \quad \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in G$$

and since

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in G$$

it follows that it is the identity of G.

Inverses: The matrix

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in G$$

is not invertible in the sense that there exists a matrix

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix} \quad \text{such that} \quad \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}.$$

But since

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

is not the identity of G this is not relevant here. It is true that

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1/a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1/a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and so} \quad \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1/a & 0 \\ 0 & 0 \end{pmatrix} \quad \text{in } G.$$

Example 4.5. (Trivial group). Let G be any set with one element e, i.e. $G = \{e\}$, and an operation $*$ such that $e * e = e$. Then G is a group called the *trivial group*. Note that the trivial group is trivially abelian.

Example 4.6. Let $G = \{a + b\sqrt{5} : a, b \in \mathbb{Q},\ a + b\sqrt{5} \neq 0\}$ under multiplication of real numbers. We check that all of the group axioms hold:

Closure: Let $a + b\sqrt{5}, c + d\sqrt{5} \in G$. Then $(a + b\sqrt{5})(c + d\sqrt{5}) = (ac + 5bd) + (bc + ad)\sqrt{5}$. Since $a, b, c, d \in \mathbb{Q}$, it follows that $(ac + 5bd), (bc + ad) \in \mathbb{Q}$. Also since $a \neq 0$ or $b \neq 0$, it follows that $a + b\sqrt{5} \neq 0$ and similarly $c + d\sqrt{5} \neq 0$. Hence $(a + b\sqrt{5})(c + d\sqrt{5}) \neq 0$ and so $ac + 5bd \neq 0$ or $bc + ad \neq 0$. Therefore $(a + b\sqrt{5})(c + d\sqrt{5}) = (ac + 5bd) + (bc + ad)\sqrt{5} \in G$.

Associativity: We know already that multiplication of real numbers is associative.

Identity: The identity of G is $1 = 1 + 0\sqrt{5} \in G$.

Inverses: Since

$$(a + b\sqrt{5})\frac{1}{a + b\sqrt{5}} = 1,$$

it remains to show that $1/(a + b\sqrt{5}) \in G$. We see this as follows

$$\frac{1}{a + b\sqrt{5}} = \frac{1}{a + b\sqrt{5}} \cdot \frac{a - b\sqrt{5}}{a - b\sqrt{5}} = \frac{a}{a^2 - 5b^2} + \frac{-b}{a^2 - 5b^2}\sqrt{5}$$

and since $a, b \in \mathbb{Q}$, $a/(a^2 - 5b^2), -b/(a^2 - 5b^2) \in \mathbb{Q}$ and so $1/(a + b\sqrt{5}) \in G$.

Since all of the group axioms are satisfied, it follows that G is a group.

You might notice that, in addition to the 4 axioms from Definition 4.1, in Examples 4.2 and 4.3 (and several other examples also) the following rule also holds.

Definition 4.7. A group G is said to be *commutative*, or *abelian* if the operation $*$, in addition to the four axioms in Definition 4.1, satisfies:

Commutativity: $x * y = y * x$ for all $x, y \in G$.

Note that Definition 4.7 is not one of the group axioms, it is an additional property that a group can satisfy or not satisfy.

Let's consider each of the group axioms separately before seeing some further examples of groups.

4.1. **Closure.** For a binary operation $*$ on a set G to be *closed* (or to satisfy the closure axiom) means that $x * y$ must be defined for all $x, y \in G$ and $x * y$ must belong to G. For example, if $*$ is division $/$ and $G = \mathbb{Z}$, then $1/0$ is not defined and $1/2 \notin \mathbb{Z}$. On the other hand, if G is the set $\mathbb{Q} \setminus \{0\}$ of non-zero rational numbers, then x/y is defined and $x/y \in G$ for all $x, y \in G$.

Example 4.8. The operations $+$ and $\times$ is well-defined and closed on the reals $\mathbb{R}$, integers $\mathbb{Z}$, natural numbers $\mathbb{N}$, rationals $\mathbb{Q}$, and complex numbers $\mathbb{C}$.

The operation $-$ is closed on $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{C}$ but is not closed on $\mathbb{N}$.

The operation $/$ is not well-defined on $\mathbb{N}$, $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{C}$; it is well-defined but not closed on $\mathbb{Z} \setminus \{0\}$, $\mathbb{N} \setminus \{0\}$; and is well-defined and closed on $\mathbb{R} \setminus \{0\}$, $\mathbb{Q} \setminus \{0\}$, and $\mathbb{C} \setminus \{0\}$.

4.2. **Associativity.** Associativity is perhaps the most subtle of the group axioms. It says that if we have a complicated expression such as:

$$x + ((y + z) + (t + u)) = ((x + y) + z) + (t + u) \text{ or } x((yz)(tu)) = ((xy)z)(tu),$$

then we may omit the brackets altogether and just write:

$$x + y + z + t + u \text{ or } xyztu.$$

So, because of associativity, the arrangements of brackets in a sum or product does not matter.

An alternative way of thinking about this is the following. If you have a complicated expression such as:

$$x + ((y + z) + y) + ((t + (u + z)) + y) + (z + y)$$

and you know the value of $z + y$ is 3, then you can ignore the brackets and just substitute in 3 every time you see an z, a $+$, and then immediately a y. For example, the expression above becomes:

$$x + y + 3 + t + u + 3 + 3.$$

One useful consequence of the associativity axiom is that we may use the power notation:

$$x^n = \underbrace{xx\cdots x}_{n} \ (n > 0).$$

The existence of inverses implies that we can extend this to

$$x^0 = e, \ x^{-n} = (x^{-1})^n.$$

With this in mind, we have the following natural rules:

$$x^i x^j = x^{i+j},$$
$$(x^i)^j = x^{ij}.$$

The proof follows straight from the definition, but one has to consider all possible cases, depending on the signs of i and j.

Example 4.9. The operations $+$ and $\times$ on $\mathbb{R}$ are associative. Composition of functions and matrix multiplication are also associative.

However, the operations $-$ and $/$ are not associative on $\mathbb{R}$. For example,

$$(5-5)-5 = 0-5 = -5 \text{ but } 5-(5-5) = 5-0 = 5$$

and

$$(1/2)/2 = 1/4 \text{ but } 1/(2/2) = 1/1 = 1.$$

The operation $x \sim y$ defined by $(x+y)/2$ on $\mathbb{R}$ is not associative. For example,

$$(2 \sim 6) \sim 6 = 4 \sim 6 = 5 \text{ but } 2 \sim (6 \sim 6) = 2 \sim 6 = 4.$$

In these examples, the brackets cannot be ignored as the outcome changes depending on where the brackets are.

Throughout this course you can use the fact that $+$ and $\times$ on $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, matrix addition and multiplication, and composition of functions are associative without proof.

If you are asked if an operation $*$ on a set G is associative, then you must either find a counter-example or give a proof. A counter-example is just a single instance of $x, y, z \in G$ where $(x*y)*z$ is not equal to $x*(y*z)$, as we saw with $/$ and $\sim$ in Example 4.9. A proof must show that associativity holds for all $x, y, z \in G$. To illustrate

$$2^{(3^2)} = 2^9 = 512 \text{ but } (2^3)^2 = 8^2 = 64$$

shows that exponentiation is not associative on $\mathbb{R}$ but the fact that

$$2^{(2^2)} = 2^4 = 16 = (2^2)^2$$

proves nothing, as the equality $(x^y)^z = x^{(y^z)}$ must hold for all x, y, z and not just some x, y, z.

4.3. **Identity.** To show that a set G and an operation $*$ has an identity, you must find one element e in G that satisfies the equalities

$$e*x = x*e = x$$

for every $x \in G$. The element x will change but the element e must be the same for every x.

Example 4.10. The identity of $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}$ under addition is 0. The identity of $\mathbb{R}\setminus\{0\}$, $\mathbb{C}\setminus\{0\}$, $\mathbb{Q}\setminus\{0\}$ under multiplication is 1.

Example 4.11. If $x \sim y$ is defined to be $(x+y)/2$ for $x, y \in \mathbb{R}$, as in Example 4.9, then $x \sim x = x$ for all $x \in \mathbb{R}$. This does not show that any $x \in \mathbb{R}$ can be the identity of $\mathbb{R}$ under $\sim$. If $x \sim y = x = y \sim x$, then $y = x$, and so no single element of $\mathbb{R}$ will satisfy the identity axiom.

Example 4.12. Let $M_{2,2}$ denote the 2×2 matrices with entries in $\mathbb{R}$. Then

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

is the identity of $M_{2,2}$ under matrix multiplication.

Under addition 0 is the identity of $\mathbb{R}$ and under multiplication 1 is the identity of $\mathbb{R}$.

4.4. **Inverses.** Unlike the identity axiom, here you must show that every element x of a set G has an inverse x^{-1} under the operation $*$ such that $x * x^{-1} = x^{-1} * x = e$ where e is the identity. As the element x changes, the element x^{-1} will also change. If there is no identity, then there are no inverses!

Example 4.13. If $a/b \in \mathbb{Q}$, then $(a/b)^{-1}$ (meaning the inverse of a/b in $\mathbb{Q} \setminus \{0\}$ under multiplication) is just $b/a \in \mathbb{Q}$ since $(a/b)(b/a) = ab/ab = 1$.

Example 4.14. The set $M_{2,2}$ of all 2×2 matrices with entries in $\mathbb{R}$ does not satisfy the axiom of inverses. For example,

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

for all

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2,2}.$$

As you already know if $A \in M_{2,2}$, then A^{-1} exists if and only if $\det(A) \neq 0$.

4.5. **Commutativity (not an axiom!)** Remember that commutativity as defined in Definition 4.7 is not one of the group axioms. It is a property that a group can either satisfy or not satisfy. To show that a group is abelian, you must check that for every pair $x, y \in G$ the equality $x * y = y * x$ holds. To show that a group is not abelian you just have to find $x, y \in G$ such that $x * y \neq y * x$.

4.6. **Further examples.**

Example 4.15. (Complex numbers.) The complex numbers $\mathbb{C} \setminus \{0\}$ is a group under $\times$. Let's doublecheck:

Closure: $x \times y \in \mathbb{C}$ for all $x, y \in \mathbb{C} \setminus \{0\}$;
Associativity: holds by assumption throughout this course;
Identity: the element $1 \in \mathbb{C} \setminus \{0\}$ satisfies the equations $x \times 1 = 1 \times x = x$ for all $x \in \mathbb{C} \setminus \{0\}$;
Inverses: for all $a + bi \in \mathbb{C} \setminus \{0\}$ there exists

$$(a + bi)^{-1} = \frac{a - bi}{a^2 + b^2} \in \mathbb{C} \setminus \{0\}$$

such that

$$(a + bi)(a + bi)^{-1} = (a + bi)\frac{a - bi}{a^2 + b^2} = \frac{a^2 + b^2}{a^2 + b^2} = 1.$$

We will show that $\mathbb{C}$ under $\times$ is not a group. It does satisfy the closure, associativity, and identity axioms for the same reasons as $\mathbb{C} \setminus \{0\}$ does. But $0 \times x = 0 \neq 1$ for every $x \in \mathbb{C}$ and so 0 has no inverse, and so the inverse axiom does not hold for $\mathbb{C}$.

Note that multiplication of complex numbers is commutative.

Example 4.16. (Matrices under addition.) Let $M_{2,2}$ be the set of all 2×2 matrices with real number entries under $+$ defined by

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} + \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} = \begin{pmatrix} a_1 + b_1 & a_2 + b_2 \\ a_3 + b_3 & a_4 + b_4 \end{pmatrix}.$$

Closure:

$$\begin{pmatrix} a_1 + b_1 & a_2 + b_2 \\ a_3 + b_3 & a_4 + b_4 \end{pmatrix} \in M_{2,2}$$

since $\mathbb{R}$ is closed under addition.

Associativity: follows from associativity of real number addition, and you can use this fact without proof throughout the course.

Identity: Since

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$$

for all $a_1, a_2, a_3, a_4 \in \mathbb{R}$, it follows that

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

is the identity of $M_{2,2}$.

Inverses: Since

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} + \begin{pmatrix} -a_1 & -a_2 \\ -a_3 & -a_4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} -a_1 & -a_2 \\ -a_3 & -a_4 \end{pmatrix} + \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$$

for all $a_1, a_2, a_3, a_4 \in \mathbb{R}$, it follows that every element of $M_{2,2}$ has an inverse.

Note that $M_{2,2}$ under matrix multiplication is closed, associative, and has an identity element but not every element has an inverse (see Example 4.14). It follows that $M_{2,2}$ under matrix multiplication is not a group.

Note that addition of matrices is commutative since addition of real numbers is commutative.

Example 4.17. (Subsets of a set). Let X be a set, and let $\mathcal{P}(X)$ be the set of all subsets of X. For example, if $X = \{0, 1, 2\}$, then

$$\mathcal{P}(X) = \{\varnothing, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}.$$

We will show that $\mathcal{P}(X)$ under unions $\cup$ is not a group if $|X| > 1$.

Closure: if $A, B \in \mathcal{P}(X)$, then $A, B \subseteq X$ and so $A \cup B \subseteq X$ and $A \cup B \in \mathcal{P}(X)$.
Associativity: if $A, B, C \in \mathcal{P}(X)$, then by definition $(A \cup B) \cup C = A \cup (B \cup C)$.
Identity: if $A \in \mathcal{P}(X)$, then $A \cup \varnothing = \varnothing \cup A = A$ and so $\varnothing$ is the identity of $\mathcal{P}(X)$ under unions.
Inverses: if $A \in \mathcal{P}(X)$ and $A \neq \varnothing$, then $\varnothing \neq A \subseteq A \cup B$ for all $B \in \mathcal{P}(X)$. Hence $A \cup B \neq \varnothing$ for all $B \in \mathcal{P}(X)$ and so no non-empty element of $\mathcal{P}(X)$ has an inverse.

It follows that $\mathcal{P}(X)$ under unions is not a group.

Note that unions of sets is commutative.

Example 4.18. (Functions). Let X be any set and let X^X denote the set of all mappings from X to X. For example, X could be $\mathbb{R}$ and $f \in X^X$ could be the function $(x)f = x^2$. Alternatively, $X = \{0, 1, 2\}$ and f could be the function defined by

$$f = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix}.$$

If $x \in X$, then we write the image of x under f as $(x)f$. We can compose two mappings f and g by first applying f and then g; the resulting mapping is denoted by $f \circ g$. Thus

$$(x)(f \circ g) = ((x)f)g.$$

(Note that sometimes you will find mappings written to the left of their argument, i.e. $f(x)$ instead of $(x)f$ but this means that composition is rather unnatural as it goes from right to left.)

Let's see if X^X under $\circ$ is a group.

Closure: if $f, g \in X^X$, then $f \circ g : X \longrightarrow X$ and so $f \circ g \in X^X$;
Associativity: $(x)((f \circ g) \circ h) = (((x)f)g)h = (x)(f \circ (g \circ h))$ by definition of composition (you may use this fact throughout the course without proof);
Identity: let $\mathrm{id} : X \longrightarrow X$ be defined by $(x)\mathrm{id} = x$ for all $x \in X$. Then $(x)(f \circ \mathrm{id}) = ((x)f)\mathrm{id} = (x)f = ((x)\mathrm{id})f = (x)(\mathrm{id} \circ f)$. Hence id is the identity of X^X.
Inverses: It is not true that every function on every set has an inverse. Some functions do, such as id, and some functions do not, such as

$$f = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix}.$$

It follows that X^X under composition $\circ$ is not a group.

Note that compositions of functions is not commutative since, for example, if $f, g : \mathbb{R} \longrightarrow \mathbb{R}$ is defined by $(x)f = 2$ and $(x)g = x^2$, then

$$((1)f)g = (2)g = 4 \neq 2 = (1)f = ((1)g)f.$$

So $f \circ g \neq g \circ f$.

A compendium of examples. Each of the sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ is a group with respect to addition. The set $\mathbb{N}$ is not a group with respect to addition, because no element apart from 0 has an inverse (negative). Neither of the above sets is a group with respect to multiplication, because 0 does not have a (multiplicative) inverse (there is no number x such that $0x = 1$!). However, the sets $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ and $\mathbb{C} \setminus \{0\}$ are groups, while $\mathbb{N} \setminus \{0\}$ and $\mathbb{Z} \setminus \{0\}$ are not (why?). All the above groups are abelian.

5. Cayley tables

All the examples of groups so far have been infinite groups. Next, we give two examples of finite groups.

A finite group can be given by its *multiplication table* (also called the *Cayley table*). This is a square table of size $|G| \times |G|$; the rows and columns are indexed by the elements of G; the entry in the row g and column h is $g * h$.

Example 5.1. (**Klein four group.**) The table

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

defines a group. Let's doublecheck:

Closure: No symbols other than e, a, b, and c appears in the table.

Associativity: Is not obvious or easy to check but it does hold. The brute force method would involve checking the equality of $4 \cdot 4 \cdot 4 = 64$ products of any three elements in any order. This number can be significantly reduced, but you can equally take it for granted at this stage. It is worth remembering that associativity is difficult to check from the table, and consequently Cayley tables are not as good a method for defining groups as it might at first seem.

Identity: e is the identity, since $e*a = a*e = a$, $e*e = e$, $e*b = b*e = b$, and $e*c = c*e = c$ from the table.

Inverses: Since $e * e = e$, $a * a = e$, $b * b = e$ and $c * c = e$ it follows that $e^{-1} = e$, $a^{-1} = a$, $b^{-1} = b$, and $c^{-1} = c$.

The above group is called the *Klein four group*, and is denoted by K_4. It is abelian.

Unlike associativity, various other properties of groups are easy to interpret in the Cayley table. For instance:

Closure: There is no symbol in the body of the table that does not occur as a label (i.e. in the first row and column).

Identity: There is an element e whose row and column are identical to the first row and column respectively.

Inverses: e appears in every row and every column of the table; moreover, its occurrences are symmetrical with respect to the main diagonal.

Abelian: The whole table is symmetrical with respect to the main diagonal.

Example 5.2. The table

$*$	e	p	q	r	s	t
e	e	p	q	r	s	t
p	p	e	t	s	r	q
q	q	s	e	t	p	r
r	r	t	s	e	q	p
s	s	q	r	p	t	e
t	t	r	p	q	e	s

defines a group. (What is the identity? For each element find its inverse.) It is not abelian, since, for example, $p * q = t \neq s = q * p$.

The size of a group G is sometimes called the *order* of G. For example, the order of the Klein four group is 4, and the order of the group in the previous example is 6. The number systems $\mathbb{R}$ and $\mathbb{Z}$ have infinite order.

6. Elementary properties

In this section, we explore some basic consequences of the group axioms.

Theorem 6.1. *Let G be a group. Then the following statements hold:*

(i) the identity $e \in G$ is unique, i.e. if $e' \in G$ such that $e'x = xe' = x$ for all $x \in G$, then $e = e'$;

(ii) *the inverse of every element $x \in G$ is unique, i.e. if $xy = yx = e$ for some $y \in G$, then $y = x^{-1}$;*

(iii) $(x^{-1})^{-1} = x$ *for all* $x \in G$;

(iv) $(xy)^{-1} = y^{-1}x^{-1}$ *for all* $x, y \in G$. *More generally, for* $x_1, \ldots, x_n \in G$ *we have* $(x_1 x_2 \cdots x_n)^{-1} = x_n^{-1} \cdots x_2^{-1} x_1^{-1}$.

Proof. (i) Since $x = xe'$ for all $x \in G$, in particular, $e = ee'$. Similarly, $ex = x$ for all $x \in G$ implies that $ee' = e'$ and so $e = ee' = e'$.

(ii) $y = ey = (x^{-1}x)y = x^{-1}(xy) = x^{-1}e = x^{-1}$.

(iii) $x = xe = x(x^{-1}(x^{-1})^{-1}) = (xx^{-1})(x^{-1})^{-1} = e(x^{-1})^{-1} = (x^{-1})^{-1}$.

(iv) Since $xyy^{-1}x^{-1} = xex^{-1} = xx^{-1} = e$, it follows from (ii) that inverses are unique and so $(xy)^{-1} = y^{-1}x^{-1}$. Hence

$$(x_1 x_2 \cdots x_n)^{-1} = (x_2 \cdots x_n)^{-1} x_1^{-1} = \cdots = x_n^{-1} \cdots x_2^{-1} x_1^{-1},$$

as required. □

Theorem 6.2. *Let G be a group and let $a, b, x \in G$.*

Right cancellativity: *if $ax = bx$, then $a = b$;*
Left cancellativity: *if $xa = xb$, then $a = b$.*

Proof. We prove right cancellativity only: $a = ae = a(xx^{-1}) = (ax)x^{-1} = (bx)x^{-1} = b(xx^{-1}) = be = b$. □

Corollary 6.3. *Let G be a group. Then every element of G appears once and only once in every row and in every column of the body of the Cayley table of G.*

Proof. The entry in the row labelled a and column b is ab. If $a, b \in G$ are arbitrary, then since $b \cdot b^{-1}a = a$, it follows that a occurs in the row labelled by b. But b was arbitrary and so a occurs at least once in every row. Similarly, since $ab^{-1} \cdot b = a$ every element occurs at least once in every column.

Assume that an element x appears in the row labelled a, in the columns labelled b and c, as in the following table:

$*$	$\cdots$	b	$\cdots$	c
$\vdots$		$\vdots$		$\vdots$
a	$\cdots$	x	$\cdots$	x

Then $ab = x = ac$ implies $a^{-1}ab = a^{-1}ac$ and so $b = c$. So, every element occurs at most once in every row (the argument for columns is similar). □

7. Modular arithmetic

In this section, we introduce an important example of groups, with which you are probably already somewhat familiar.

Let $n > 0$ be a natural number, and let

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

To define addition and multiplication of $\mathbb{Z}_n$ we require the following theorem, which is something you have probably taken for granted since you first encountered mathematics.

Theorem 7.1 (Division Algorithm)**.** *If $x, n \in \mathbb{Z}$ with $n \neq 0$, then there exists a unique remainder $r \in \mathbb{Z}$ such that*

$$x = qn + r \qquad \textbf{\textit{(dividing } x \textbf{ by } n\textit{)}}$$

where $q \in \mathbb{Z}$ and $0 \leq r < n$.

We write $x = r \pmod{n}$ and say x equals r mod n.

Proof. (Omitted from the course.) To prove that r is unique assume that

$$x = q_1 n + r_1 \quad \text{and} \quad x = q_2 n + r_2.$$

We must prove that $r_1 = r_2$. Seeking a contradiction assume that $r_1 < r_2$. It follows that $(q_1 - q_2)n = r_2 - r_1 > 0$. But then n divides $r_2 - r_1 < r_2 < n$, a contradiction.

To prove that r exists, let $M = \{\, x - qn \;:\; q \in \mathbb{Z} \,\}$ and let r be the smallest number in M such that $r \geq 0$ (exercise: why does r exist?). Then $r = x - qn$ for some $q \in \mathbb{Z}$. If $r \geq n$, then $r > r - n \geq 0$ and $r - n = x - qn - b = x - (q+1)n \in M$. Thus we have a contradiction since r is the smallest number in M with $r \geq 0$. □

We will refer to q and r from Theorem 7.1 as the *quotient* and *remainder* of x divided by n.

Example 7.2. If $x = 131$ and $n = 7$, then dividing 131 by 7 we obtain

$$131 = 18 \cdot 7 + 5$$

and so $q = 18$ and $r = 5$. Hence $131 = 5 \pmod{7}$.

If $x = 89$ and $n = 18$, then dividing 89 by 18 we obtain

$$89 = 4 \cdot 18 + 17$$

and so $q = 4$ and $r = 17$. Thus $89 = 17 \pmod{18}$.

If $x = 106$ and $n = 29$, then dividing 106 by 29 we obtain

$$106 = 3 \cdot 29 + 19$$

and so $q = 3$ and $r = 19$. Hence $106 = 19 \pmod{29}$.

If $x = -3$ and $n = 7$, then $-3 = -1 \cdot 7 + 4$, and so $-3 = 4 \pmod{7}$.

Definition 7.3. (Addition and multiplication mod n.) If $a, b \in \mathbb{Z}_n$, then we define

$$a + b \pmod{n} = r = (a + b) - qn$$

where $a + b = qn + r$ and $q \in \mathbb{Z}$ and $0 \leq r < n$ from Theorem 7.1. Likewise, we define

$$a \cdot b \pmod{n} = r = ab - qn$$

where $a \cdot b = qn + r$ and $q \in \mathbb{Z}$ and $0 \leq r < n$ from Theorem 7.1.

Modular arithmetic is the term used when referring to addition and multiplication mod n.

We refer to the operations defined in Definition 7.3 as *addition* and *multiplication modulo* n. You can calculate $a + b \pmod{n}$ and $ab \pmod{n}$ by simply subtracting n from $a + b$ or ab until you obtain a number r in $\{1, \ldots, n-1\}$.

Whether you think of it this way or not, you can already do modular arithmetic: telling time, and days of the week, is modular arithmetic.

Example 7.4. If the time is 11:00, what time will it be in 100 hours? Using modular arithmetic:

$$11 + 100 = 111 = 3 \pmod{12}$$

and so the answer is 03:00.

If today is Tuesday, then what day will it be in 10 days time? If we say Monday is 0, Tuesday is 1 and so on:

$$1 + 10 = 11 = 4 \pmod{7}$$

and so the answer is Friday.

Here are some more abstract examples.

Example 7.5.

$$\begin{aligned} n &= 0 \pmod{n} \\ 1+1 &= 2 \pmod{7} \\ 4+6 &= 3 \pmod{7} \\ 3+4 &= 0 \pmod{7} \\ 2\cdot 5 &= 3 \pmod{7} \end{aligned}$$

and so on...

When it is clear from the context we will not write $x + y \pmod{n}$ or $x \cdot y \pmod{n}$ but only $x + y$ and $x \cdot y$.

Theorem 7.6. *Let n be any positive integer. Then $\mathbb{Z}_n = \{1, \ldots, n-1\}$ with the operation of addition modulo n is an abelian group.*

Proof. We must verify that $\mathbb{Z}_n$ with addition modulo n satisfies the group axioms:

Closure: From the definition $x+y \pmod{n}$ belongs to $\{1, \ldots, n-1\}$ for all $x, y \in \{1, \ldots, n-1\}$.

Associativity: It is possible (and not too difficult) to verify that addition modulo n is associative, but we will not do this here.

Identity: Since $0 + x = x + 0 = x \pmod{n}$ for all $x \in \{1, \ldots, n-1\}$, it follows that 0 is the identity element of $\mathbb{Z}_n$.

Inverses: If $x \in \{1, \ldots, n-1\}$, then $x + (n - x) = n = 0 \pmod{n}$ it follows that $n - x$ is the inverse of x.

Hence $\mathbb{Z}_n$ is a group under addition modulo n.

We must also check that $\mathbb{Z}_n$ is commutative (which is NOT an axiom!):

Commutativity: again from the definition $x + y \pmod{n} = y + x \pmod{n}$ for all $x, y \in \{1, \ldots, n-1\}$.

Therefore $\mathbb{Z}_n$ under addition modulo n is an abelian group. □

The situation is more subtle when we use multiplication modulo n. Let's look at the axioms one by one:

Closure: From the definition $xy \pmod{n}$ belongs to $\{1, \ldots, n-1\}$ for all $x, y \in \{1, \ldots, n-1\}$.

Associativity: It is possible (and not too difficult) to verify that multiplication modulo n is associative.

Identity: Since $1 \cdot x = x \cdot 1 = x \pmod{n}$ for all $x \in \{1, \ldots, n-1\}$, it follows that 1 is the identity element of $\mathbb{Z}_n$.

Inverses: Since there is no number $x \in \{1, \ldots, n-1\}$ such that $x \cdot 0 = 1$, it follows that 0 has no inverse and so $\mathbb{Z}_n$ is not a group.

So, $\mathbb{Z}_n$ fails to be a group under multiplication since 0 does not have an inverse. The real numbers $\mathbb{R}$ is not a group under multiplication for the same reason (likewise $\mathbb{Q}$ and $\mathbb{C}$). But $\mathbb{R} \setminus \{0\}$ is a group under multiplication and so it is reasonable to ask whether $\mathbb{Z}_n \setminus \{0\}$ is a group.

Example 7.7. [**Multiplication mod 7.**] Let's write down the Cayley table for $\mathbb{Z}_7 \setminus \{0\}$ under multiplication mod 7:

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Closure: Since there are no symbols other than $1, 2, 3, 4, 5$, and 6 in the table, it follows that $\mathbb{Z}7 \setminus \{0\}$ is closed.

Associativity: We already know that multiplication modulo 7 is associative.

Identity: We already saw that 1 is the identity of $\mathbb{Z}_7$ and so it is the identity of $\mathbb{Z}7 \setminus \{0\}$. Alternatively, you can see in the table that $1 \cdot x = x \cdot 1 = x$ for all $x \in \{1, 2, \ldots, n\}$.

Inverses: To find the inverse of any element just look in the row labelled by that element and find the label of the column containing 1. For example:

$\cdot$	1	2	**3**	4	5	6
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
5	5	3	**1**	6	4	2

So, $5^{-1} = 3$. The inverses of $1, 2, 3, 4, 5, 6$ are $1, 4, 5, 2, 3, 6$, respectively.

We must also check that $\mathbb{Z}7 \setminus \{0\}$ is commutative (which is NOT an axiom!):

Commutativity: again from the table we see that $x * y = y * x$ for all $x, y \in \{1, 2, 3, 4, 5, 6\}$ (remember you can check this by making sure that the table is symmetric around the diagonal from the top left to the bottom right).

Therefore $\mathbb{Z}7 \setminus \{0\}$ under multiplication modulo 7 is an abelian group. □

Important note: when working modulo n, x^{-1} is not $1/x$!

Example 7.8. [**Multiplication mod** 10.] Let's consider $\mathbb{Z}10 \setminus \{0\}$ under multiplication modulo 10.

Closure: $2 \cdot 5 = 0 \pmod{10}$ and so $\mathbb{Z}10 \setminus \{0\}$ is not closed.

Associativity: multiplication mod n is associative for all n and you can use this fact without proof throughout the course.

Identity: since $1 \cdot x = x \cdot 1 = x$ for all x and so 1 is the identity (we've seen this several times already!).

Inverses: There is no $x \in \mathbb{Z}_{10}$ such that $2x = 1$, because $2x$ is always even. Hence, 2 does not have an inverse in $\mathbb{Z}10 \setminus \{0\}$ under multiplication mod 10.

Since $\mathbb{Z}10 \setminus \{0\}$ fails the axioms of closure and inverses, it follows that it is not a group. Remember that you only have to find one axiom that is failed to show that something is not a group.

So, a natural question is to try and determine for which n the set $\mathbb{Z}_n \setminus \{0\}$ forms a group under multiplication modulo n. As the previous two examples show, problems arise when considering closure and inverses. It will actually turn out that the latter is more serious than the former, and to resolve the problem we need to make a small detour into elementary number theory.

Definition 7.9. Let $a, b \in \mathbb{Z}$. Then the *greatest common divisor* is the largest positive integer that divides a and b; it is denoted by $\gcd(a, b)$.

Example 7.10. Let $a = 76$ and $b = 32$. Then the divisors of a are

$$1, 2, 4, 19, 38, 76$$

and the divisors of b are

$$1, 2, 4, 8, 16, 32.$$

So, the $\gcd(a, b) = 4$. How do we find x and y? We use the extended Euclidean algorithm:

a	$=$	76			
$2b$	$=$	64	32	$=$	b
$a - 2b$	$=$	12	24	$=$	$2a - 4b$
$5b - 2a$	$=$	8	8	$=$	$5b - 2a$
$3a - 5b$	$=$	4	8		
			0		

We conclude that $\gcd(76, 32) = 4 = 3 \cdot 76 - 5 \cdot 32$.

Theorem 7.11 (Bézout's identity)**.** *Let $a, b \in \mathbb{Z}$. Then $\gcd(a, b)$ is the least positive integer of the form $ax + by$ where $x, y \in \mathbb{Z}$.*

Proof. Let $x, y \in \mathbb{Z}$ such that $c = ax + by$ is the least possible positive integer and let $d = \gcd(a, b)$. We must show that $c = d$.

Since $c = ax + by$, and since d divides both a and b it follows that d also divides c and so $d \leq c$.

Using the Division Algorithm (Theorem 7.1) to divide a by c there exists $q \in \mathbb{Z}$ and $0 \leq r < c$ such that $a = qc + r$. Since $c = ax + by$, it follows that

$$r = a - qc = a - q(ax + by) = a(1 - qx) - qyb.$$

Since $1 - qx, -qy \in \mathbb{Z}$ and c is the smallest *positive* number which can be written as an integral linear combination of a and b, it follows that $r = 0$. In other words, c divides a, and, by a similar argument, c divides b. Since d is the largest positive integer dividing both a and b, it follows that $d \geq c$.

But we already showed that $d \leq c$ and so $d = c$. □

Example 7.12. Let us compute $\gcd(534, 81)$.

a	$=$	534			
$6b$	$=$	486	81	$=$	b
$a - 6b$	$=$	48	48	$=$	$a - 6b$
$-a + 7b$	$=$	33	33	$=$	$-a + 7b$
$2a - 13b$	$=$	15	30	$=$	$4a - 26b$
		15	3	$=$	$-5a + 33b$
		0			

We conclude that $\gcd(534, 81) = 3 = -5 \cdot 534 + 33 \cdot 81$.

Theorem 7.13. *Let n be any positive integer. Then the following hold:*

(i) Let $a \in \mathbb{Z}_n$ be arbitrary. Then there exists $b \in \mathbb{Z}_n$ such that $ab = 1 \pmod{n}$ if and only if $\gcd(a, n) = 1$.

(ii) $U_n = \{\, x \in \mathbb{Z}_n \,:\, \gcd(x, n) = 1 \,\}$ is a group under multiplication modulo n.

(iii) $\mathbb{Z}_n \setminus \{0\}$ is a group under multiplication modulo n if and only if n is a prime number.

Proof. **(i).** ($\Rightarrow$) If $ab = 1 \pmod{n}$, then, from the definition of multiplication modulo n,

$$ab = qn + 1$$

for some $q \in \mathbb{Z}$ and so $1 = a \cdot b + n \cdot (-q)$. By Theorem 7.11, $\gcd(a, n)$ is the least positive integer of the form $ax + ny$ for $x, y \in \mathbb{Z}$. But $1 = a \cdot b + n \cdot (-q)$ is of the form $ax + ny$ (where $x = b$ and $y = -q$) and there are no positive integers less than 1, and so $\gcd(a, n) = 1$.

($\Leftarrow$) If $\gcd(a, n) = 1$, then there exist $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Hence

$$1 = ax + ny = ax \pmod{n}$$

and so $b = x$ is the required element.

(ii). We must verify the group axioms.

Closure: Let $x, y \in U_n$. Then $\gcd(x, n) = 1 = \gcd(y, n)$ and so, by Theorem 7.13, there exist $x', y' \in \mathbb{Z}_n$ such that $xx' = 1 = yy'$. It follows that $xyx'y' = xx'yy' = 1 \cdot 1 = 1$ and so, by Theorem 7.13, $\gcd(xy, n) = 1$. Thus $xy \in U_n$, as required.

Associativity: Multiplication modulo n is associative.

Identity: We have already seen that 1 is the identity of $\mathbb{Z}n \setminus \{0\}$. Hence, since $\gcd(n, 1) = 1$, $1 \in U_n$ is the identity of U_n also.

Inverses: If $x \in U_n$, then $\gcd(x, n) = 1$ and so by part (i), there exists $x' \in \mathbb{Z}_n$ such that $xx' = 1$. It follows that $x^{-1} = x'$.

It follows that U_n is group.

(iii). ($\Rightarrow$) Assume that n is not a prime number. Then $n = ab$ for some positive integers a and b. It follows that $ab = n = 0 \pmod{n}$ and so $\mathbb{Z}_n \setminus \{0\}$ is not closed.

($\Leftarrow$) If n is a prime, then $\gcd(x, n) = 1$ for all $x \in \{1, 2, \ldots, n\} = \mathbb{Z}_n \setminus \{0\}$. Hence $U_n = \mathbb{Z}_n \setminus \{0\}$ and we know from part (ii) that U_n is a group. □

If $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$, then we say that a and b are *coprime*.

Example 7.14. Let us find the multiplicative inverse of 57 modulo 100.

$$\begin{array}{rcr|rcr} & & & 100 & = & n \\ a & = & 57 & 57 & = & a \\ \hline -a+n & = & 43 & 43 & = & -a+n \\ \hline 2a-n & = & 14 & 42 & = & 6a-3n \\ \hline & & 14 & 1 & = & -7a+4n \\ \hline & & 0 & & & \end{array}$$

So we see that $(-7)\cdot 57 + 4\cdot 100 = 1$, so that $57^{-1} = -7 = 93 \pmod{100}$.

The only numbers in $\mathbb{Z}_{10}\setminus\{0\}$ that are coprime to 10 are $1, 3, 7$, and 9. Hence $U_{10} = \{1, 3, 7, 9\}$. Similarly, $U_{22} = \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$ and since 7 is a prime number $U_7 = \mathbb{Z}_7 \setminus \{0\}$.

The set $\mathbb{Z}7\setminus\{0\}$ is a group under multiplication mod 7 since 7 is a prime number, but $\mathbb{Z}10\setminus\{0\}$ is not since 10 is not prime.

8. Permutations

In Example 4.18 we showed that the set X^X of all mappings from X to X under composition of functions $\circ$ is not a group since not every element has an inverse (see also Example 8.1). However, we did show that X^X under $\circ$ is closed, associative, and that the identity mapping id on X is an identity element for composition.

Example 8.1. Let $X = \{0, 1, 2\}$ and let f be the function defined by

$$f = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix}.$$

The identity mapping id is just

$$\mathrm{id} = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}.$$

If $g \in X^X$ is arbitrary, then $(0)fg = (1)g = (2)fg$ but $(0)\mathrm{id} = 0 \neq 2 = (2)\mathrm{id}$. It follows that $fg \neq \mathrm{id}$ for any $g \in X^X$ and so f does not have an inverse.

More generally, let X be any set, let $a, b \in X$ be any elements such that $a \neq b$, and let $f : X \longrightarrow X$ be any mapping such that $(a)f = (b)f = b$. Then for any other mapping $g \in X^X$ we have $(a)fg = (b)g = (b)fg$. But $(a)\mathrm{id} = a \neq b = (b)\mathrm{id}$ and so $g \circ f \neq \mathrm{id}$. Hence f does not have an inverse.

Remember that $a \in \mathbb{Z}n \setminus \{0\}$ has an inverse under multiplication modulo n if and only if $\gcd(a, n) = 1$ (Theorem 7.13). So, the elements of $\mathbb{Z}n \setminus \{0\}$ which have an inverse under multiplication modulo n are $U_n = \{\, a \in \mathbb{Z}n \setminus \{0\} \,:\, \gcd(a, n) = 1 \,\}$. In Theorem 7.13(ii), we showed that U_n is a group under multiplication modulo n. We ask: what mappings in X^X have inverses under composition of functions? And is the subset of all such mappings a group?

To answer these questions we require the follow special kinds of mappings.

Definition 8.2. Let $f : X \longrightarrow Y$ be a mapping. We say that f is an *onto* mapping if every element of Y is the image of some element of X, that is,

$$(\forall y \in Y)(\exists x \in X)((x)f = y).$$

We say that f is a *one-one* mapping if different elements of X have different images in Y, that is,

$$(\forall x, y \in X)((x)f = (y)f \Longrightarrow x = y),$$

Finally, we say that f is a *bijection* if it is both onto and 1-1.

A mapping that is *onto* may also be called *surjective* or a *surjection*. A mapping that is *one-one* may also be called *injective* or a *injection*. A bijection might also be called a *one-to-one correspondence*.

Examples 8.3. Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}_2$ be defined by

$$(x)f = \begin{cases} 0 & \text{if } x \text{ is odd} \\ 1 & \text{if } x \text{ is even.} \end{cases}$$

Then f is surjective since $\mathbb{Z}_2 = \{0, 1\}$, $(1)f = 0$, and $(2)f = 1$. It is not an injection because, for example, $(3)f = (1)f = 0$.

The mapping $g : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $(x)g = 2x$ is an injection because

$$(x)g = (y)g \Rightarrow 2x = 2y \Rightarrow x = y.$$

It is not a surjection because, for example, $(x)g \neq 1$ for any $x \in \mathbb{Z}$.

The mapping $h : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $(x)h = -x$ is a bijection.

Theorem 8.4. *Let X be a set and let $f : X \longrightarrow X$ be any function. Then the following hold:*

(i) if X is finite, then f is injective if and only if f is surjective;

(ii) there exists $g : X \longrightarrow X$ such that $f \circ g = g \circ f = \mathrm{id}$ if and only if f is a bijection.

Proof. **(i).** ($\Rightarrow$) Since f is injective, it follows that $|X| = |Xf|$ where $Xf = \{\, (x)f \,:\, x \in X \,\}$. Hence every element of X must be mapped onto by some element of X, and so f is surjective.

($\Leftarrow$) Suppose that f is not injective. Then there exist $x, y \in X$ such that $(x)f = (y)f$. It follows that $|Xf| < |X|$ and so f is not surjective, a contradiction. Hence f is injective, as required.

(ii) ($\Rightarrow$) Assume that $f \circ g = g \circ f = \mathrm{id}$. We will prove that f is a bijection by showing that f is both surjective and injective.

Surjective: Let $y \in X$ be arbitrary. Then we want to prove that there exists $x \in X$ such that $(x)f = y$. If $x = (y)g$, then

$$(x)f = ((y)g)f = (y)(g \circ f) = (y)\mathrm{id} = y$$

and so f is surjective.

Injective: If $x, y \in X$, then

$$(x)f = (y)f \quad \Rightarrow \quad ((x)f)g = ((y)f)g \quad \Rightarrow \quad (x)(f \circ g) = (y)(f \circ g)$$
$$\Rightarrow \quad (x)\mathrm{id} = (y)\mathrm{id} \quad \Rightarrow \quad x = y$$

and so f is injective.

($\Leftarrow$) Let f be a bijection. If $x \in X$ is arbitrary, then, since f is surjective there exists $y \in X$ such that $(y)f = x$. If there exists $z \in X$ such that $z \neq y$ and $(z)f = (y)f = x$, then f is not injective, which is a contradiction. So for all $x \in X$ there is a unique element $y \in X$ such that $(y)f = x$. Then we define $g : X \longrightarrow X$ by setting $(x)g$ to be the unique element $y \in X$ such that $(y)f = x$. Then

$$(x)g \circ f = ((x)g)f = (y)f = x = (x)\mathrm{id}$$

and so $g \circ f = \mathrm{id}$. Also if $(x)f = z$, then $(z)g = x$ and so

$$(z)f \circ g = ((z)f)g = (z)g = x = (x)\mathrm{id}$$

and so $f \circ g = \mathrm{id}$. □

Theorem 8.5. *Let X be a set and let S_X be the set of all bijections from X to X. Then S_X is a group under composition of mappings called the symmetric group on X; the elements of S_X are often called permutations.*

Proof. Let's consider the group axioms one by one:

Closure: Let $f, g \in S_X$. Then f and g are bijections. Hence, by Theorem 8.4($\Leftarrow$), there exist $f', g' \in S_X$ such that $f \circ f' = f' \circ f = \mathrm{id} = g \circ g' = g' \circ g$. Hence

$$(f \circ g) \circ (g' \circ f') = f \circ (g \circ g') \circ f' = f \circ \mathrm{id} \circ f' = f \circ f' = \mathrm{id}$$

and so by Theorem 8.4($\Rightarrow$), $f \circ g$ is a bijection.

Alternatively, we can prove directly that $f \circ g$ is a bijection.

Injective: if $x, y \in X$ such that $(x)fg = (y)fg$, then $((x)f)g = ((y)f)g$ and so $(x)f = (y)f$ (since g is injective), and so $x = y$ (since f is injective). Hence fg is injective.

Surjective: if $x \in X$, then (since g is surjective) there exists $y \in X$ such that $(y)g = x$. But $y \in X$ and f is surjective and so there exists $z \in X$ such that $(z)f = y$. It follows that $(z)fg = ((z)f)g = (y)g = x$ and so fg is surjective.

Associativity: We already know that composition of mappings is associative (Example 4.18).

Identity: We already know that the identity function id is an identity for all mappings and so for bijections in particular.

Inverses: If $f \in S_X$, then by Theorem 8.4 there exists $g \in S_X$ such that $f \circ g = g \circ f = \mathrm{id}$ and so $f^{-1} = g$. □

If X is a finite set of size n, then without loss of generality we may assume that $X = \{1, \ldots, n\}$. In this case we denote S_X by S_n. A mapping $f \in X^X$ can be conveniently written as a $2 \times n$ array of elements of X, i.e. 1, 2, and so on, and their images:

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ (1)f & (2)f & \ldots & (n)f \end{pmatrix}$$

For example,

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 1 & 1 & 2 & 5 & 4 & 3 & 1 \end{pmatrix}.$$

It is easy to see whether such a mapping is a permutation or not: just check whether the sequence of images $(1)f, (2)f, \ldots, (n)f$ contains every element of $\{1, 2, \ldots, n\}$ (and so contains it only once). So f in the last example is not a permutation since 6, for example, does not appear in the second row and so f is not surjective (also 1 occurs more than once and so f is not injective). On the other hand,

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 4 & 5 & 6 & 3 & 8 & 7 \end{pmatrix}.$$

is a permutation since every element of $\{1, 2, \ldots, 8\}$ appears in the second row.

It is also easy to find the inverse of a permutation written in this way: you just swap the rows (and re-order, if you are tidy!):

$$f^{-1} = \begin{pmatrix} f(1) & f(2) & \ldots & f(n) \\ 1 & 2 & \ldots & n \end{pmatrix}$$

Example 8.6. Let

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 2 & 5 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}.$$

Then f is not a permutation (since 1 does not appear in the second row, and hence 1 is not mapped onto by any element, f is not surjective), while g and h are. Let us calculate some products and inverses:

$$g^{-1} = \begin{pmatrix} 2 & 4 & 3 & 1 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}$$

$$g \circ h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix},$$

$$h \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}.$$

We see that the group S_5 is not abelian since $g, h \in S_5$ but $gh \neq hg$.

Theorem 8.7. *Let n be a positive integer. Then S_n is abelian if and only if $n = 1$ or $n = 2$.*

Proof. ($\Leftarrow$) See Problem 3 on Tutorial Sheet 3.

($\Rightarrow$) If $n \geq 3$, then the permutations

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 1 & 4 & \cdots & n \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{pmatrix} \in S_n.$$

But

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 2 & 1 & 4 & \cdots & n \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix} = f \circ g$$

and so S_n is not abelian. □

Theorem 8.8. *Let n be a positive integer. Then the order of S_n is $n! = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$, that is, $|S_n| = n!$.*

Proof. If we write an arbitrary permutation $f \in S_n$ as

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1f & 2f & 3f & \ldots & nf \end{pmatrix},$$

then recall that every element of $\{1, 2, \ldots, n\}$ must appear in $\{1f, 2f, \ldots, nf\}$ exactly once. Hence $1f$ can be any of $\{1, \ldots, n\}$, $2f$ can be any of $\{1, \ldots, n\}$ except $1f$, $3f$ can be any of $\{1, \ldots, n\}$ except $1f$ or $2f$ and so on until nf has to be the only element of $\{1, \ldots, n\}$ which is not equal to any of $1f, 2f, 3f, \ldots, (n-1)f$. So there are n choices for $1f$, $n-1$ choices for $2f$, $n-2$ choices for $3f$ and so on... Therefore $|S_n| = n \cdot n - 1 \cdot n - 2 \cdot \cdots \cdot 1 = n!$, as required. □

Example 8.9. The following is the list of all 24 elements of S_4:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

9. Disjoint cycle notation for permutations

In this section we describe a useful way of writing down permutations.

Definition 9.1. Let $i_1, i_2, \ldots, i_k$ be distinct elements from $\{1, \ldots, n\}$. The *k-cycle* $(i_1\ i_2\ \ldots\ i_k)$ is the permutation mapping i_1 to i_2, i_2 to $i_3, \ldots, i_{k-1}$ to i_k, and i_k back to i_1. The other elements of $\{1, \ldots, n\}$ are fixed by $(i_1\ i_2\ \ldots\ i_k)$.

The cycles $(i_1\ i_2\ \ldots\ i_k)$ and $(j_1\ j_2\ \ldots\ j_l)$ are said to be *disjoint* if $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} = \varnothing$.

Example 9.2. In S_5 we have

$$(2\ 4\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}.$$

Let

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 6 & 4 & 7 & 2 & 5 & 8 \end{pmatrix} \in S_8.$$

We see that $(1)f = 3$, $(3)f = 6$, $(6)f = 2$ and $(2)f = 1$; similarly, $(5)f = 7$, $(7)f = 8$ and $(8)f = 5$, while $(4)f = 4$. Hence

$$f = (1\ 3\ 6\ 2)(4)(5\ 7)(8),$$

and also

$$f = (5\ 7)(3\ 6\ 2\ 1).$$

For example, $(5\ 7\ 8)$ and $(3\ 6\ 2\ 1)$ are disjoint, whereas $(1\ 2\ 3)$ and $(1\ 3)$ are not.

Theorem 9.3. *Every permutation can be written as a composition of disjoint cycles. This decomposition is unique up to the arrangement of cycles and presence of 1-cycles.*

The proof of the above theorem, although not difficult, requires some technical attention, and it would probably not give you deeper insight than a particular example.

Example 9.4. Let us continue Example 8.9 and write all permutations of S_4 in the disjoint cycle form:

$()$	$(3\,4)$	$(2\,3)$	$(2\,3\,4)$
$(2\,4\,2)$	$(2\,4)$	$(1\,2)$	$(1\,2)(3\,4)$
$(1\,2\,3)$	$(1\,2\,3\,4)$	$(1\,2\,4\,3)$	$(1\,2\,4)$
$(1\,3\,2)$	$(1\,3\,4\,2)$	$(1\,3)$	$(1\,3\,4)$
$(1\,3)(2\,4)$	$(1\,3\,2\,4)$	$(1\,4\,3\,2)$	$(1\,4\,2)$
$(1\,4\,3)$	$(1\,4)$	$(1\,4\,2\,3)$	$(1\,4)(2\,3)$.

Note that disjoint cycles commute, for example,

$$(1\ 2)(3\ 4) = (3\ 4)(1\ 2)$$

non-disjoint cycles do not always commute, for example

$$(1\ 2)(2\ 3) = (1\ 3\ 2) \neq (1\ 2\ 3) = (2\ 3)(1\ 2).$$

If $f = (i_1\ i_2\ \ldots\ i_k)$, then $f^{-1} = (i_k\ \ldots\ i_2\ i_1)$.

$$(1\ 2\ 3)(4\ 5)(1\ 5)(2\ 4) = (1\ 4)(2\ 3\ 5)$$
$$((1\ 2\ 3)(4\ 5))^{-1} = (4\ 5)^{-1}(1\ 2\ 3)^{-1} = (5\ 4)(3\ 2\ 1).$$

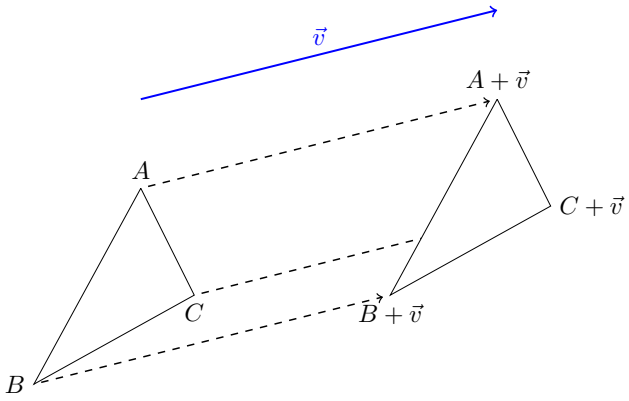

FIGURE 1. A translation of the plane $\mathbb{R}^2$ by a vector $\vec{v}$.

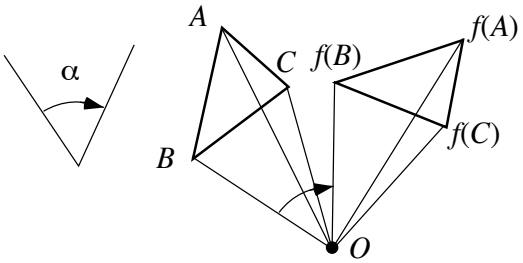

FIGURE 2. Rotation about the point P by the angle α.

10. ISOMETRIES

We have seen examples of groups arising from number systems, and Cayley tables. In this section, we consider some groups arising from geometry.

Definition 10.1. An *isometry* of the real plane $\mathbb{R}^2$ is a bijective function $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ which preserves distances.

Sometimes an isometry is called a *symmetry*; to avoid confusion with the symmetric group we will always use the term isometry. Strictly speaking a mapping $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ is an isometry if for any two points $p_1 = (x_1, y_1), p_2 = (x_2, y_2) \in \mathbb{R}^2$ we have $d(p_1, p_2) = d((p_1)f, (p_2)f)$ (where

$$d(p_1, p_2) = \sqrt{(y_2 - y_1)^2 - (x_2 - x_1)^2)}$$

is the distance between p_1 and p_2).

Examples 10.2. Translation by a vector (see Figure 1), rotation about a point by an angle (see Figure 2) and reflection in a line (see Figure 3) are well known symmetries.

Theorem 10.3. *The isometries of $\mathbb{R}^2$ form a group under composition of functions.*
Every isometry of $\mathbb{R}^2$ is either a translation, rotation, reflection, or a product of a translation and a reflection (called a glide-reflection).

Sketch of the proof. It is possible (but beyond the scope of this course) to prove that every isometry is a bijection, and to prove the following:

Closure: The composition $f \circ g$ of two isometries is an isometry.
Associativity: We have seen several times that composition of functions is associative.
Identity: The identity mapping id clearly preserves distance.
Inverses: The inverse of an isometry is an isometry. □

Now, if we are given a figure F in the plane (i.e. a set of points, like a line, or a triangle or a square, etc.) we can consider those isometries of the plane which map this figure onto itself.

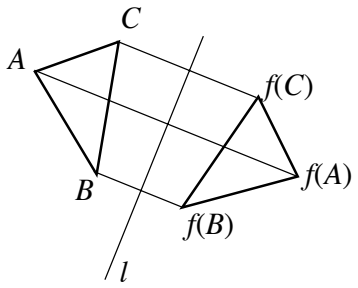

FIGURE 3. Reflection in the line l.

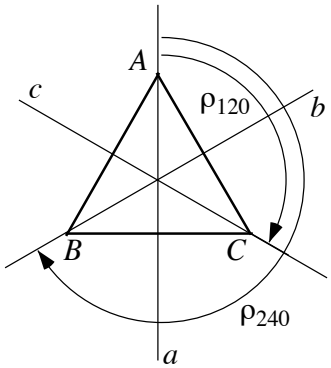

FIGURE 4. Isometries of an equilateral triangle.

Definition 10.4. If F is a figure in the plane, then isometries of $\mathbb{R}^2$ mapping F to F is called the *group of isometries of* F.

If F is a finite (bounded) figure, then it follows from Theorem 10.3 that every isometry of F is either a rotation or a reflection.

Example 10.5. Let T be an equilateral triangle (see Figure 4). Then T has six isometries:

Reflections: σ_a, σ_b, σ_c in the lines a, b, c respectively;
Rotations: ρ_{120}, ρ_{240} about the centre by 120° and 240° clockwise;
Identity: the identity id.

The multiplication table is:

	id	ρ_{120}	ρ_{240}	σ_a	σ_b	σ_c
id	id	ρ_{120}	ρ_{240}	σ_a	σ_b	σ_c
ρ_{120}	ρ_{120}	ρ_{240}	id	σ_c	σ_a	σ_b
ρ_{240}	ρ_{240}	id	ρ_{120}	σ_b	σ_c	σ_a
σ_a	σ_a	σ_b	σ_c	id	ρ_{120}	ρ_{240}
σ_b	σ_b	σ_c	σ_a	ρ_{240}	id	ρ_{120}
σ_c	σ_c	σ_a	σ_b	ρ_{120}	ρ_{240}	id

Example 10.6. An isosceles triangle (Figure 5) has only two isometries: the identity transformation id and the reflection σ. The multiplication table is

	id	σ
id	*id*	σ
σ	σ	id

Example 10.7. A scalene triangle (a triangle where all the sides have different lengths) has a unique isometry – the identity mapping id.

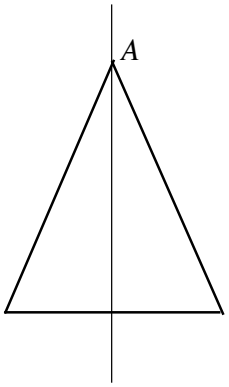

FIGURE 5. Isometries of an isosceles triangle.

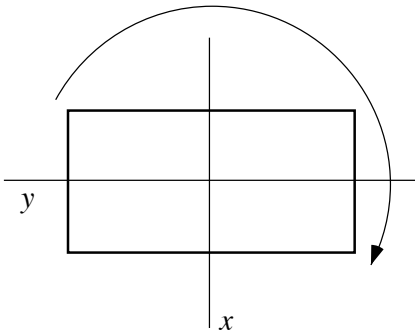

FIGURE 6. Isometries of a rectangle.

Example 10.8. A circle has infinitely many isometries: all the rotations about the centre of the circle and all the reflections in all the lines passing through the centre of the circle.

Example 10.9. A non-square rectangle (Figure 6) has four isometries – two reflections, one rotation and the identity mapping – with the multiplication table

	id	σ_x	σ_y	ρ
id	*id*	σ_x	σ_y	ρ
σ_x	σ_x	id	ρ	σ_y
σ_y	σ_y	ρ	id	σ_x
ρ	ρ	σ_y	σ_x	id

Example 10.10. (**The dihedral group.**) A regular n-gon (Figure 7 for $n = 6$ or Figure 4 for n=3) has $2n$ isometries:

Rotations: n rotations about the centre by multiples of $360°/n$;
Reflections: n reflections in the lines through the centre.

The group of these isometries is called the *dihedral group* and is denoted by D_n.

If ρ denotes the 'basic' rotation by $360°/n$, then all the other rotations are powers of ρ: $\rho^0 = \mathrm{id}$, $\rho^1 = \rho$, ρ^2,..., ρ^{n-1}, $\rho^n = \mathrm{id}$. If σ is any reflection, then all the other reflections can be written as $\sigma\rho^i$ for some i where $0 \le i \le n-1$. In particular, we have

$$\rho\sigma = \sigma\rho^{n-1} = \sigma\rho^{-1}.$$

This, together with the obvious equalities $\rho^n = \mathrm{id}$ and $\sigma^2 = \mathrm{id}$ can be used to compute products in D_n without working with isometries at all.

For example, in D_6 we have

$$\rho^3 \cdot \sigma\rho^2 = \rho^2\sigma\rho^{-1}\rho^2 = \rho^2\sigma\rho = \rho\sigma\rho^{-1}\rho = \rho\sigma = \sigma\rho^{-1} = \sigma\rho^5.$$

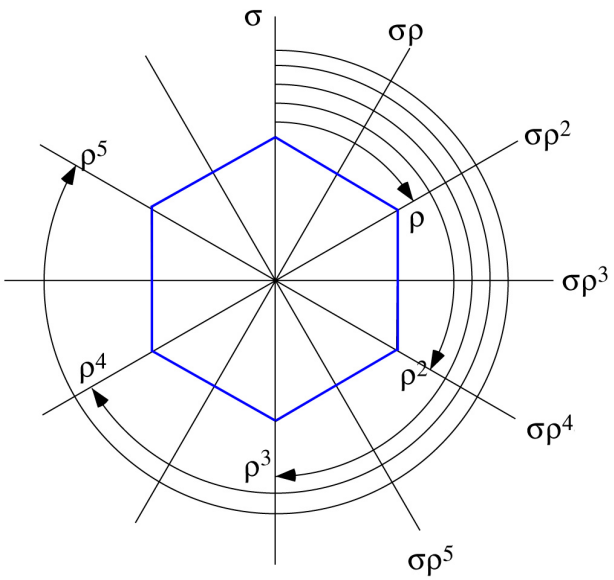

FIGURE 7. Symmetries of a regular hexagon.

Groups of symmetries of infinite figures are also of interest. Here one often considers a repeating pattern which fills a plane, rather like a wallpaper patterns. It is possible to classify all these groups, and it turns out that there are precisely 17 of them.

One can also consider the symmetries of the 3-dimensional space, rather than the plane, and also symmetries of 3-dimensional figures. Here, the analogue of wallpapers are crystals, and the classification of all possible groups arising here (there 230 of them) is a significant piece of information in the study of crystals (called *crystallography*).