MT2002 Algebra 2002-3

Edmund F Robertson

September 3, 2002

Contents

About the course

These are the lecture notes for the algebra part of the MT2002 module. This part will consist of (about) 24 lectures, 10 tutorials, 2 projects using Maple and GAP, and some additional sessions.

The literature for the algebra part is as follows:

R.B.J.T. Allenby, Rings, Fields and Groups, Edward Arnold, 1983.

T.S. Blyth and E.F. Robertson, Essential Student Algebra, Volume 3: Abstract Algebra, Chapman and Hall, 1986.

T.S. Blyth and E.F. Robertson, Algebra Through Practice, Book 3: Groups, Rings and Fields, Cambridge University Press, 1984.

D.A.R. Wallace, Groups, Rings and Fields, Springer, 1998.

These books will be available on short loan in the Mathematics/Physics library, as will tutorial questions and solutions. In addition, any book containing the words 'elementary' or 'introduction' and 'algebra' or 'groups' is likely to be useful.

The assessment for this module will consist of a continuous assessment component (30%), and a three hour written exam at the end of semester (70%). The continuous assessment component will consist of two class tests, and three Microlab Assignments.

1. Introduction

Modern algebra is a study of sets with operations defined on them. It begins with the observation that certain familiar rules hold for different operations on different sets.

Let us consider the set of natural numbers $\mathbb{N}$. The operations of addition and multiplication satisfy the following rules:

$$(x+y)+z = x+(y+z), \tag{1}$$
$$(xy)z = x(yz), \tag{2}$$
$$x+y = y+x, \tag{3}$$
$$xy = yx, \tag{4}$$

as well as

$$x(y+z) = xy+xz. \tag{5}$$

Also there is a distinguished element 1, which has the property

$$1x = x. \tag{6}$$

In the sets of integers $\mathbb{Z}$, rationals $\mathbb{Q}$, reals $\mathbb{R}$ and complex numbers $\mathbb{C}$ all the above rules remain valid. In addition, in each of them there is a distinguished element 0 such that

$$0+x = x, \tag{7}$$
$$0x = 0. \tag{8}$$

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

$$x+(-x) = 0. \tag{9}$$

Moreover, in $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, for every $x \neq 0$ there is an element $1/x$ such that

$$x(1/x) = 1. \tag{10}$$

At this stage you should note that the following pairs of rules are very similar: (1) and (2); (3) and (4); (6) and (7); (9) and (10). The only difference is that they refer to different operations.

Our next example is the set $M_{n,n}$ of all $n \times n$ matrices with real number entries. Again, we can add and multiply matrices, and we have the following rules:

$$\begin{aligned}
&(A + B) + C = A + (B + C),\\
&(AB)C = A(BC),\\
&A + B = B + A,\\
&A(B + C) = AB + AC,\ (A + B)C = AC + BC.
\end{aligned}$$

This time, however, we do not have $AB = BA$. Also, we have distinguished matrices 0 (the zero matrix) and I (the identity matrix) such that

$$\begin{aligned}
&A + 0 = A,\\
&AI = IA = A.
\end{aligned}$$

For every matrix A there exists a matrix $-A$ such that

$$A + (-A) = 0.$$

However, it is not true that for every matrix there exists a matrix A^{-1} such that $AA^{-1} = A^{-1}A = I$; such a matrix exists if and only if A is invertible (i.e. if A has a non-zero determinant).

Let us now fix a set X, and consider the set $T(X)$ of all mappings $f : X \to X$. For such a mapping f and $x \in X$, we shall write the image of x under f as $f(x)$. We can compose two mappings f and g by applying first one and then the other; the resulting mapping is denoted by $g \circ f$. Thus

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

(Note that this means that we multiply mappings, slightly unnaturally, from right to left. In some books you will find mappings written to the right of their argument, i.e. $(x)f$ instead of $f(x)$; a benefit of doing this is that the composition law becomes $(x)(f \circ g) = ((x)f)g$.)

Straight from the definition it follows that

$$(f \circ g) \circ h = f \circ (g \circ h),$$

and that there exists a mapping id (the identity mapping, sending every x to itself) satisfying

$$f \circ \mathrm{id} = \mathrm{id} \circ f = f.$$

However, $f \circ g = g \circ h$ does not hold in general, and it is not true that for every mapping f there exists a mapping g such that $f \circ g = g \circ f = \mathrm{id}$.

Exercise 1.1. Find examples confirming the last two claims.

Exercise 1.2. Let X be a set, and let $\mathcal{P}(X)$ be the set of all subsets of X. List a few well known properties of the operations $\cup$ (union) and $\cap$ (intersection).

In algebra, one studies an abstract set with one or more operations defined on it. These operations are assumed to satisfy some basic properties, and the aim is to study the consequences of these properties.

2. Groups – definition and basic properties

Definition 2.1. A *group* is a set G on which a binary operation $*$ is defined, such that the following hold:

Closure: For all $x, y \in G$ we have $x * y \in G$.

Associativity: For all $x, y, z \in G$ we have $(x * y) * z = x * (y * z)$.

Identity: There exists a distinguished element e such that for all $x \in G$ we have $x * e = e * x = x$.

Inverses: For every $x \in G$ there is a distinguished element $x^{-1} \in G$ such that $x * x^{-1} = x^{-1} * x = e$.

Notation 2.2. The symbol one uses 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 $x \cdot y$, or even xy, instead of $x * y$. From time to time we will use other symbols, such as $\circ$ and $\diamond$. Probably the most confusing of all is the usage of $+$; in that case one denotes the identity element by 0 instead of e, and calls it the *neutral element*, or the *zero*; the inverse of an element is denoted by $-x$, rather than x^{-1}, and is called the *negative of* x.

Definition 2.3. A group G is said to be *commutative*, or *abelian*, if the operation $*$, in addition to the above four axioms, satisfies

Commutativity: For all $x, y \in G$ we have $x * y = y * x$.

Examples 2.4. 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). None 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.

Next we give two examples of finite groups. For a finite group G we denote by $|G|$ the number of elements in G. 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 2.5. 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. Indeed, closure is immediate, e is the identity, and every element is its own inverse. It is not so obvious that the operation is associative, but it is. (The brute force method would involve checking the equality of $4 \cdot 4 \cdot 4 = 64$ products of any three elements in any order. One can actually significantly reduce this number, 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.) The above group is called the *Klein four group*, and is denoted by K_4. It is abelian.

Example 2.6. 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, $p * q = t \neq s = q * p$.

Definition 2.7. For a group G, the number of elements of G is called the *order* of G.

We are now going to list some basic consequences of our defining axioms for groups. First of all, we note that associativity implies that in a product of any number of elements $x_1, \ldots, x_n$ in that order, the arrangement of brackets does not matter. For example, we have $(x_1(x_2x_3))(x_4x_5) = (x_1x_2)((x_3x_4)x_5)$, since

$$(x_1(x_2x_3))(x_4x_5) = ((x_1x_2)x_3)(x_4x_5) = (x_1x_2)(x_3(x_4x_5)) = (x_1x_2)((x_3x_4)x_5).$$

We can therefore omit the brackets altogether and write simply $x_1x_2 \ldots x_n$. (A rigorous proof of this is a somewhat tedious induction on n.) This, in turn means that we can use the power notation:

$$a^n = \underbrace{aa \ldots a}_{n} \ (n > 0).$$

The existence of inverses implies that we can extend this (as we do in $\mathbb{Q}$) to

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

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

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

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

Theorem 2.8. *The following statements are true in any group G.*

(i) *For all $e_1, x \in G$, $e_1x = x$ (or $xe_1 = x$) implies $e_1 = e$. (The identity is unique.)*

(ii) *For all $x, y \in G$, $xy = e$ (or $yx = e$) implies $y = x^{-1}$. (The inverse of every element is unique.)*

(iii) *For every $x \in G$ we have $(x^{-1})^{-1} = x$.*

(iv) *For all $a, b, x \in G$, $ax = bx$ (or $xa = xb$) implies $a = b$ (cancellation laws).*

(v) *For all $a, b \in G$ we have $(ab)^{-1} = b^{-1}a^{-1}$. More generally, for $a_1, \ldots, a_n \in G$ we have $(a_1a_2 \ldots a_n)^{-1} = a_n^{-1} \ldots a_2^{-1}a_1^{-1}$.*

Proof. (i) $e = xx^{-1} = (e_1x)x^{-1} = e_1(xx^{-1}) = e_1e = e_1$.

(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) $a = ae = a(xx^{-1}) = (ax)x^{-1} = (bx)x^{-1} = b(xx^{-1}) = be = b$.

(v) Since $abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$, it follows from (ii) that $(ab)^{-1} = b^{-1}a^{-1}$. Now we have

$$(a_1a_2 \dots a_n)^{-1} = (a_2 \dots a_n)^{-1}a_1^{-1} = \dots = a_n^{-1} \dots a_2^{-1}a_1^{-1},$$

as required. ■

3. Modular arithmetic

In this and the following two sections we introduce some important examples of groups.

Let $n > 0$ be a natural number, and consider the set $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$. For $a, b \in \mathbb{Z}_n$ define $a + b$ and ab by performing these operations in $\mathbb{Z}$, and the subtracting multiples of n until the result is in $\mathbb{Z}_n$. (In other words, form the sum and product of a and b as integers, divide them by n and take the remainders.) These operations are called the *addition* and *multiplication modulo n*.

Example 3.1. Let us work modulo 7. We have

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

and so on.

One can relatively easy see that the addition and multiplication modulo n satisfy the following properties:

$$\begin{aligned} &(x + y) + z = x + (y + z),\ (xy)z = x(yz), \\ &x + 0 = 0 + x = x,\ 1 \cdot x = x \cdot 1 = x, \\ &x + (n - x) = (n - x) + x = x, \\ &x + y = y + x,\ xy = yx, \\ &x \cdot 0 = 0 \cdot x = 0. \end{aligned}$$

Therefore, we immediately have

Theorem 3.2. *The set $\mathbb{Z}_n$ with the operation of addition modulo n is an abelian group.*

As for the multiplication modulo n, we have a more subtle situation. First of all we can notice that $\mathbb{Z}_n$ is never a group under multiplication modulo n, because 0 does not have an inverse. Still, with $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ in mind, we may ask whether $\mathbb{Z}_n \setminus \{0\}$ is a group.

Example 3.3. Let us write down the Cayley table for multiplication modulo 7 on the set $\mathbb{Z}_7 \setminus \{0\}$:

	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

We see that the set is closed under the operation. We also see that the inverses of 1, 2, 3, 4, 5, 6 are respectively 1, 4, 5, 2, 3, 6. We already know that the multiplication modulo n is associative and commutative, and that 1 is the identity element. We conclude that $\mathbb{Z}_7 \setminus \{0\}$ is a group under multiplication modulo 7.

Example 3.4. Working modulo 10 we have, for example, $2 \cdot 5 = 0$. So we conclude that $\mathbb{Z}_{10} \setminus \{0\}$ is not closed for multiplication modulo 10, and that it cannot possibly be a group. Also, note that there is no $x \in \mathbb{Z}_{10}$ such that $2x = 1$, because $2x$ is always even. Hence, 2 does not have an inverse.

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 a more serious than the former, and to sort it out we need to make a small detour into elementary number theory.

The first fact is the well known fact about the division of integers with a quotient and remainder.

Theorem 3.5. *For any two integers a, b, with $b > 0$, there are unique integers q, r such that $a = bq + r$ and $0 \leq r \leq b - 1$.*

Next we recall that for two non-zero integers a and b, their *greatest common divisor* $\gcd(a, b)$ is the largest positive integer which divides (with remainder 0) both a and b. Next we give an alternative description of this number:

Theorem 3.6. *The greatest common divisor d of two non-zero integers a and b is equal to the smallest positive integer d_1 which can be written in the form $\alpha a + \beta b$ with α and β integers.*

Proof. Since $d_1 = \alpha a + \beta b$, and since d divides both a and b (we usually write this as $d|a$ and $d|b$), it follows that d also divides d_1.

Next divide a by d_1: $a = qd_1 + r$, $0 \leq r < d_1$. Since $d_1 = \alpha a + \beta b$ it follows that $r = (1 - q\alpha)a + (-q\beta)b$. Since d_1 is the smallest *positive* number which can be written as an integral linear combination of a and b it follows that r must be equal to 0. In other words, we have $d_1|a$, and, by a similar argument, $d_1|b$. Since d is the largest positive integer dividing both a and b, it follows that $d \geq d_1$.

Now from $d|d_1$ and $d \geq d_1$ we conclude that $d = d_1$, as required. ■

The above proof suggests the following algorithm for finding the greatest common divisor of two numbers a and b:

1. Divide: $a = qb + r$.
2. Rename: $a := b$, $b := r$.
3. Loop: If $r \neq 0$ then go to 1, otherwise b is the required greatest common divisor.

If at every stage you also keep track how r is expressed as a linear combination of (the original) a and b, at the end you will obtain the greatest common divisor expressed in that form as well.

Example 3.7. 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 $\gcd(534, 81) = 3 = -5 \cdot 534 + 33 \cdot 81$.

We now start returning to $\mathbb{Z}_n$.

Theorem 3.8. *For $a \in \mathbb{Z}_n$ there exists $b \in \mathbb{Z}_n$ such that $ab = 1$ if and only if $\gcd(a, n) = 1$.*

Proof. If you recall the definition of multiplication modulo n, you see that $ab = 1$ modulo n if and only if $ab = qn + 1$ (as integers), which is satisfied if and only if $\gcd(a, n) = 1$ by Theorem 3.6. ■

Example 3.9. Let us find the multiplicative inverse of 57 modulo 100.

			100	$=$	n
a	$=$	57	57	$=$	a
$-a+n$	$=$	43	43	$=$	$-a+n$
$2a-n$	$=$	14	42	$=$	$6a-3n$
		14	1	$=$	$-7a+4n$
		0			

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

Theorem 3.10. *The set $U_n = \{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}$ is a group under multiplication modulo n.*

Proof. Multiplying two numbers co-prime to n gives a number co-prime to n; subtracting a multiple of n will again yield a number co-prime to n. Hence U_n is closed. Multiplication modulo n is associative. The identity element is 1 (note that $1 \in U_n$!). The existence of inverses follows from Theorem 3.8. ■

Theorem 3.11. *The set $\mathbb{Z}_n \setminus \{0\}$ is a group under the multiplication modulo n if and only if n is a prime number.*

Proof. ($\Rightarrow$) Assume that n is not a prime number, say $n = qr$. But then, in $\mathbb{Z}_n$ we have $qr = n = 0$, i.e. closure is not satisfied.

($\Leftarrow$) If n is a prime then $U_n = \mathbb{Z}_n \setminus \{0\}$. ■

4. Permutations

In Section 1 we considered the set $T(X)$ of all mappings $X \longrightarrow X$. We saw there that the composition of mappings is associative, and that the identity mapping id is an identity for composition. However, $T(X)$ is not a group, since not every mapping has an inverse, as the next example shows.

Example 4.1. Choose two arbitrary distinct elements $a, b \in X$, and let $f : X \longrightarrow X$ be any mapping such that $f(a) = f(b) = b$. Then for any other mapping $g \in T(X)$ we have $(g \circ f)(a) = g(f(a)) = g(b) = g(f(b)) = (g \circ f)(b)$. In particular $g \circ f \neq \mathrm{id}$, and hence f does not have an inverse.

As in the previous section, we can hope that the subset of all mappings which *do* have inverses will form a group. So we want to find out which mappings have inverses. To this end we have to recall certain special kinds of mappings.

Definition 4.2. Let $f : X \longrightarrow Y$ be a mapping. We say that f is an *onto* mapping (or a *surjection*) if

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

i.e. if every element of Y is the image of some element of X. We say that f is a *one-one* mapping (or an *injection*) if

$$(\forall x_1, x_2 \in X)(f(x_1) = f(x_2) \Longrightarrow x_1 = x_2),$$

i.e. if different originals from X have different images in Y. Finally, we say that f is a *bijection* (or a *one-one correspondence*) if it is both a surjection and an injection.

Examples 4.3. The mapping $f : \mathbb{Z} \longrightarrow \mathbb{Z}_2$ defined by $f(x) = 0$ if x is even and $f(x) = 1$ if x is odd is a surjection. It is not an injection because, for example, $f(3) = f(1) = 1$. The mapping $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $f(x) = 2x$ is an injection because

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

It is not an injection because, for example, $f(x) \neq 1$ for any $x \in \mathbb{Z}$. The mapping $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $f(x) = -x$ is a bijection.

Exercise 4.4. Prove that the composition of two bijections is again a bijection.

Theorem 4.5. *For a mapping $f \in T(X)$ there exists a mapping $g \in T(X)$ such that $f \circ g = g \circ f = \mathrm{id}$ if and only if f is a bijection.*

Proof. ($\Rightarrow$) Assume that $f \circ g = g \circ f = \mathrm{id}$. Then for every $y \in X$, define $x = g(y)$, so that

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

hence f is onto. Also, for $x_1, x_2 \in X$ we have

$$\begin{aligned} f(x_1) = f(x_2) &\Rightarrow g(f(x_1)) = g(f(x_2)) \Rightarrow (g \circ f)(x_1) = (g \circ f)(x_2) \\ &\Rightarrow \mathrm{id}(x_1) = \mathrm{id}(x_2) \Rightarrow x_1 = x_2; \end{aligned}$$

hence f is one-one as well.

($\Leftarrow$) Let f be a bijection. We define $g : X \longrightarrow X$ by setting $g(x)$ to be the unique element $y \in X$ such that $f(y) = x$. It is now a routine matter to check that $f \circ g = g \circ f = \mathrm{id}$. ■

Exercise 4.6. Prove that the inverse of a bijection is again a bijection.

Theorem 4.7. *The set $S(X)$ of all bijections $X \longrightarrow X$ is a group under the composition of mappings.*

Proof. Closure follows from Exercise 4.4, we already know that the composition of mappings is associative, the identity mapping id is a bijection, and the existence of inverses follows from Theorem 4.5 and Exercise 4.6. ■

Definition 4.8. The group $S(X)$ is called the *symmetric group* on X. Its elements are called *permutations*.

If X is a finite set of size n, then without loss of generality we may take $X = \{1, \ldots, n\}$. In this case we denote $T(X)$ by T_n and $S(X)$ by S_n. A mapping $f \in T_n$ can be conveniently written as a $2 \times n$ array of originals and their images:

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

It is easy to see whether such a mapping is a permutation or not: just check whether the sequence of images $f(1), f(2), \ldots, f(n)$ contains every element of $\{1, 2, \ldots, n\}$

(and so contains it only once). In particular, we see that a mapping from T_n which is surjective must also be injective, and that a mapping that is injective must also be surjective. 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!):

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

Example 4.9. Consider the mappings

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

from T_5. Then f is not a permutation, while g and h are. Let us calculate some products and inverses:

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

(Remember that we are multiplying mappings, and hence permutations as well, from right to left.) We see that the group S_5 is not abelian.

Exercise 4.10. Prove that the group S_n is abelian only for $n = 1, 2$.

Exercise 4.11. Prove that the order of S_n is $n!(= n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1)$.

Now we describe another useful way of writing down permutations.

Definition 4.12. Let $i_1, i_2, \ldots, i_k$ be k distinct elements from $\{1, \ldots, n\}$. The *k-cycle* $(i_1\ i_2\ \ldots\ i_k)$ is the permutation mapping i_1 into i_2, i_2 into i_3, and so on, mapping i_{k-1} into i_k, mapping i_k back to i_1, and leaving all the other elements of $\{1, \ldots, n\}$ fixed.

Example 4.13. In S_5 we have

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

Definition 4.14. Two cycles $(i_1\ i_2\ \ldots\ i_k)$ and $(j_1\ j_2\ \ldots\ j_l)$ are said to be *disjoint* if $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} = \emptyset$.

Theorem 4.15. *Every permutation can be written as a composition of disjoint cycles. This decomposition is unique up to the order of cycles and presence of 1-cycles.*

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

Example 4.16. Consider the following permutation

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

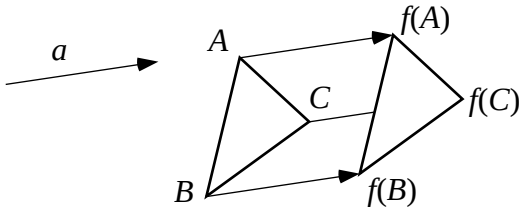

Figure 1: Translation by the vector $\vec{a}$.

from S_8. We see that $f(1) = 3$, $f(3) = 6$, $f(6) = 2$ and $f(2) = 1$; similarly, $f(5) = 7$, $f(7) = 8$ and $f(8) = 5$, while $f(4) = 4$. Hence

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

and also

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

Remark 4.17. Note that although disjoint cycles commute, arbitrary cycles do not necessarily do so (find an appropriate example).

You should be able to multiply permutations written as products of cycles, without reverting them into the two-row format. As for finding inverses, the following is of help:

$$(i_1\ i_2\ \ldots\ i_k)^{-1} = (i_k\ \ldots\ i_2\ i_1).$$

Example 4.18.

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

5. Symmetries

We have seen number-theoretical and combinatorial examples of groups. Now we look at some geometrical ones.

Definition 5.1. A *symmetry* (or *isometry*) of the real plane $\mathbb{R}^2$ is a mapping $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ which preserves distances, i.e. a mapping satisfying that for any two points $X, Y \in \mathbb{R}^2$ we have $d(X, Y) = d(f(X), f(Y))$ (where $d(A, B)$ denotes the distance between A and B).

Examples 5.2. 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.

Below we list some facts about symmetries.

1) Every symmetry is a bijection.

2) The composition of two symmetries is again a symmetry.

3) The inverse of a symmetry is again a symmetry.

4) The set of all symmetries is a group under composition of mappings.

5) A symmetry preserves angles.

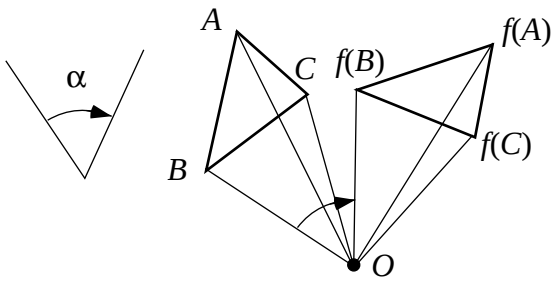

Figure 2: Rotation about the point P by the angle α.

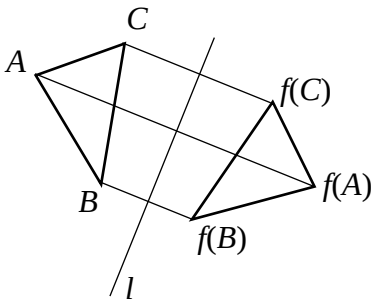

Figure 3: Reflection in the line l.

6) Every symmetry is either a translation, or a rotation, or a reflection, or a product of a translation and a reflection (called a *glide-reflection*).

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 symmetries of the plane which map this figure onto itself. It is easy to see that these symmetries also form a group; this group is called the *group of symmetries of* F. It is worth remarking here that if F is a finite (bounded) figure, then it follows from 6) that every symmetry of F is either a rotation or a reflection.

Example 5.3. Consider an equilateral triangle T (see Figure 4). It obviously has six symmetries: reflections σ_a, σ_b, σ_c in the lines a, b, c respectively, rotations ρ_{120}, ρ_{240} about O for 120^0 and 240^0 clockwise respectively, and the identity transformation id. The multiplication table is:

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

Example 5.4. An isosceles triangle (Figure 5) has only two symmetries: the identity transformation id and the reflection σ. The multiplication table is

	id	σ
id	*id*	σ
σ	σ	id

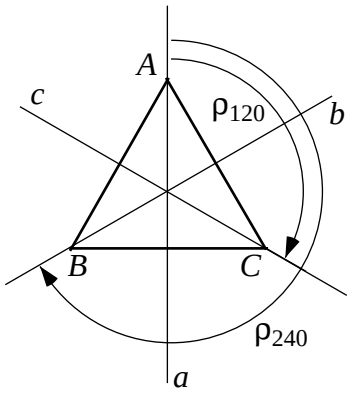

Figure 4: Symmetries of an equilateral triangle.

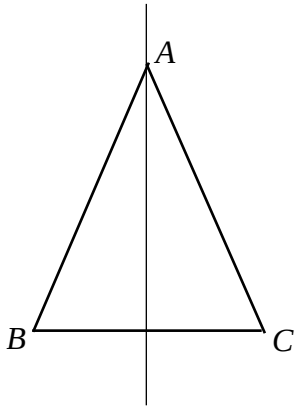

Figure 5: Symmetries of an isosceles triangle.

Example 5.5. A scalene triangle has a unique symmetry – the identity mapping id.

Example 5.6. A circle has infinitely many symmetries: 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 5.7. A non-square rectangle (Figure 6) has four symmetries – 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 5.8. A regular n-gon (Figure 7, for $n = 6$) has $2n$ symmetries: n rotations about the centre for multiples of $360^0/n$, and n reflections in lines through the centre. The group of these symmetries is called the *dihedral group* and is denoted by D_n. If ρ denotes the 'basic' rotation for $360^0/n$, then all the other rotations are powers of ρ: $\rho^0 = \text{id}$, $\rho^1 = \rho$, ρ^2,..., ρ^{n-1}, $\rho^n = \text{id}$. Moreover, if σ is one reflection,

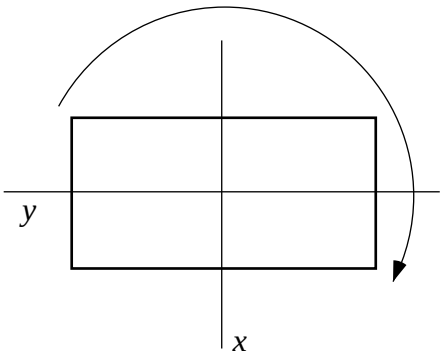

Figure 6: Symmetries of a rectangle.

then all the other reflections can be written as $\rho^i\sigma$ $(0 \leq i \leq n-1)$. In particular, we have $\sigma\rho = \rho^{n-1}\sigma = \rho^{-1}\sigma$. 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 symmetries at all. For example, in D_6 we have

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

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).

6. Order of an element

We now set on to investigate the elements and properties of general groups.

Definition 6.1. Let a be an element of a group G. The *order* of a is the smallest positive integer n such that $a^n = e$ if there is such a number, or infinite otherwise.

Examples 6.2. Every reflection has order 2. Rotation ρ in the dihedral group D_n has order n. Every non-zero element of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ has an infinite (additive) order. The identity is the only element of order 1 in any group.

Example 6.3. The orders of the elements of $\mathbb{Z}_{10}$ (under addition modulo 10) are 1, 10, 5, 10, 5, 2, 5, 10, 5, 10 respectively.

Example 6.4. Consider the permutation $\alpha = (1\ 2)(3\ 4\ 5)$ from S_5. Its powers are:

$$\begin{aligned}
\alpha^2 &= (3\ 5\ 4)\\
\alpha^3 &= (1\ 2)\\
\alpha^4 &= (3\ 4\ 5)\\
\alpha^5 &= (1\ 2)(3\ 5\ 4)\\
\alpha^6 &= \mathrm{id}.
\end{aligned}$$

Hence, the order of α is 6.

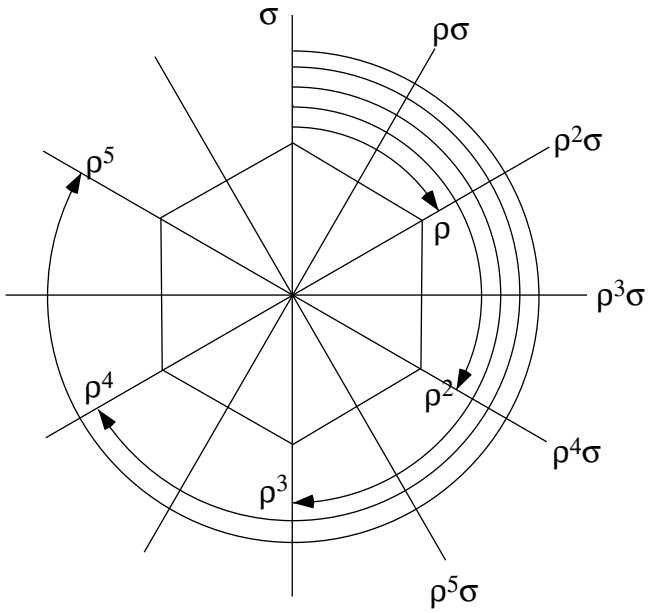

Figure 7: Symmetries of a regular hexagon.

Exercise 6.5. Find the orders of the elements of the multiplicative group $\mathbb{Z}_7 \setminus \{0\}$.

Exercise 6.6. Find the orders of elements of the dihedral group D_6.

Theorem 6.7. *If G is a finite group, then every element of G has finite order.*

Proof. Let $a \in G$ be arbitrary. Consider the elements $a, a^2, a^3, \ldots$. They certainly all belong to G. Since G is finite, there must exist two distinct i, j (say $i > j$) such that $a^i = a^j$. But then, multiplying by a^{-j}, we obtain $a^{i-j} = e$. We see that there exists a positive integer $m = i - j$ such that $a^m = e$, and it then follows that there exists the smallest such positive integer, which is then the order of a. ■

Theorem 6.8. *Let G be a group, and let a be an element of order n in G. Then for any $i, j \in \mathbb{Z}$ we have $a^i = a^j$ if and only if $n|(i-j)$. (In particular $a^i = e$ if and only if $n|i$.)*

Proof. ($\Leftarrow$) If $n|(i-j)$ then write $i - j = qn$, so that

$$a^i = a^{j+qn} = a^j (a^n)^q = a^j e^q = a^j.$$

($\Rightarrow$) Assume that $a^i = a^j$. Write $i - j = qn + r$, with $0 \leq r < n$. But then

$$a^r = a^{i-j-qn} = a^i (a^j)^{-1} (a^n)^{-q} = a^i (a^i)^{-1} e = e.$$

Since n is the order of a and $r < n$, we conclude that $r = 0$, and hence $n|(i-j)$. ■

We are now going to see how to find the orders of elements in various specific groups introduced earlier.

Theorem 6.9. *The order of an element $a \in \mathbb{Z}_n$ (under addition modulo n) is $n/\gcd(a, n)$.*

Proof. Let the order of a be m; this means that, modulo n, we have $ma = 0$, i.e. $ma = qn$ as integers for some q.

Next let $d = \gcd(a, n)$, and write $a = a_1 d$ and $n = n_1 d$. Note that $n/\gcd(a, n) = n_1$, and also that $\gcd(n_1, a_1) = 1$.

Now we have

$$n_1 a = n_1 a_1 d = n a_1 = 0 \pmod{n}.$$

Therefore $m \leq n_1$. Also, we have

$$ma = qn \Rightarrow ma_1 d = qn_1 d \Rightarrow ma_1 = qn_1 \Rightarrow n_1 | ma_1 \Rightarrow n_1 | m \Rightarrow n_1 \leq m.$$

We conclude that $m = n_1 = n/\gcd(a, n)$, as required. ■

Theorem 6.10. *The order of an l-cycle $\gamma = (i_1\ i_2\ \ldots\ i_l)$ in the symmetric group S_n is equal to l. The order of an arbitrary permutation $\alpha \in S_n$, written as a product of disjoint cycles*

$$\alpha = \gamma_1 \gamma_2 \ldots \gamma_m,$$

where γ_i has length l_i, is equal to $q = \operatorname{lcm}(l_1, \ldots, l_m)$.

Proof. Clearly $\gamma^l = \mathrm{id}$. For $j < l$ we have $\gamma^j(i_1) = i_{j+1} \neq i_1$, so that $\gamma^j \neq \mathrm{id}$.

Write $q = l_i q_i$ $(i = 1, \ldots, m)$. Denote the order of α be r. Since the disjoint cycles commute, we have

$$\alpha^q = \gamma_1^q \gamma_2^q \ldots \gamma_m^q = (\gamma_1^{l_1})^{q_1} (\gamma_2^{l_2})^{q_2} \ldots (\gamma_m^{l_m})^{q_m} = \underbrace{\mathrm{id} \circ \mathrm{id} \circ \ldots \circ \mathrm{id}}_{n} = \mathrm{id}.$$

Hence $r \leq q$. On the other hand, from $\alpha^r = \mathrm{id}$, and the fact that the cycles are disjoint, it follows that $\gamma_j^r = \mathrm{id}$. By Theorem 6.8 it follows that $l_j | r$ for all $j = 1, \ldots, m$, and hence $q \leq r$. ■

Exercise 6.11. List the elements of S_3 and their orders.

7. Subgroups

A group may contain other groups within it. For example, the group $\mathbb{Q}$ (with respect to addition) contains the group $\mathbb{Z}$, in the sense that $\mathbb{Z} \subseteq \mathbb{Q}$ and that the addition in $\mathbb{Z}$ is the same as the addition in $\mathbb{Q}$ restricted to $\mathbb{Z}$.

Definition 7.1. Let G be a group. A non-empty set $H \subseteq G$ is a *subgroup* of G if it forms a group under the same operation; we denote this by $H \leq G$.

Example 7.2. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

Example 7.3. The multiplicative group $\mathbb{Q} \setminus \{0\}$ is not a subgroup of the additive group $\mathbb{Q}$, because the operations are different. Similarly, $\mathbb{Z}_m$ is not a subgroup of $\mathbb{Z}_n$ $(m < n)$.

Example 7.4. Every group G has $\{e\}$ as a subgroup; this is called the *trivial subgroup* of G. Also G itself is a subgroup of G. Any subgroup different from $\{e\}$ and G is called a *proper* subgroup.

On the face of it, to check whether a subset H of a group G is a subgroup, we have to check the four axioms for groups. In fact, this can be reduced to checking two conditions:

Theorem 7.5. *Let H be a non-empty subset of a group G. Then H is a subgroup of G if and only if for all $x, y \in H$ we have $xy \in H$ and $x^{-1} \in H$ (i.e. if and only if H is closed under multiplication and taking inverses).*

Proof. ($\Rightarrow$) This follows immediately from the definition.

($\Leftarrow$) Assume that H is closed under multiplication and taking inverses. It means that for any $a \in H$ we also have $a^{-1} \in H$, and hence $e = aa^{-1} \in H$. So, H contains the identity e. Finally, the operation is associative, because it is associative in G. ■

Example 7.6. The set $GL(n, \mathbb{R})$ of all $n \times n$ invertible matrices (i.e. the matrices with non-zero determinant) with real entries forms a group (called the *general linear group* over the reals). Consider the subset $SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) \, : \, |A| = 1\}$, where $|A|$ denotes the determinant of A. For $A, B \in SL(n, \mathbb{R})$ we have

$$|AB| = |A||B| = 1, \ |A^{-1}| = 1/|A| = 1.$$

Hence $SL(n, \mathbb{R}) \leq GL(n, \mathbb{R})$. The group $SL(n, \mathbb{R})$ is called the *special linear group* over $\mathbb{R}$. Analogous constructions can be done over $\mathbb{C}$ and $\mathbb{Q}$, giving the general and special linear groups over these sets.

Note that $\mathbb{Q} \setminus \{0\} \leq GL(2, \mathbb{Q})$.

Example 7.7. $\left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \, : \, n \in \mathbb{Z} \right\} \leq GL(2, \mathbb{Q})$.

Example 7.8. $\{0, 2, 4\}$ is a subgroup of $\mathbb{Z}_6$ under $+$.

Exercise 7.9. Let $G = \mathbb{Q} \setminus \{0\}$ under multiplication. Show that $H = \{2^n : n \in \mathbb{Z}\}$ is a subgroup.

8. Cyclic groups

Theorem 8.1. *Let G be a group, and let $a \in G$ be an arbitrary element. The set $H = \{a^i \, : \, i \in \mathbb{Z}\}$ of all powers of a is a subgroup of G. Its order is equal to the order of a.*

Proof. For $a^i, a^j \in H$ we clearly have $a^i a^j = a^{i+j} \in H$ and $(a^i)^{-1} = a^{-i} \in H$, so that $H \leq G$ by Theorem 7.5. If a has infinite order, then we have $a^i \neq a^j$ for $i \neq j$, for otherwise $a^{i-j} = e$. If a has order n, then, by Theorem 6.8, the only distinct powers of a are $e = a^0$, a, $\ldots$, a^{n-1}, so that $|H| = n$. ■

Definition 8.2. The subgroup H from the above theorem is called the *cyclic subgroup generated by a*. If $G = H$ then G is said to be a *cyclic group* (generated by a).

Example 8.3. The additive group $\mathbb{Z}$ is cyclic, generated by 1 (and also by -1!). Similarly $\mathbb{Z}_n$ is cyclic for every n. By Theorem 6.9 $a \in \mathbb{Z}_n$ generates $\mathbb{Z}_n$ if and only if $(a, n) = 1$.

Example 8.4. Consider the group $\mathbb{Z}_7 \setminus \{0\}$ under multiplication modulo 7. We have $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$. So, this group is cyclic, generated by 3. In fact, every group $\mathbb{Z}_p \setminus \{0\}$ (p prime) is cyclic – this is a non-trivial (and important) fact in number theory. It is far from obvious what its generators are.

Theorem 8.5. *Every cyclic group is abelian.*

Proof. Suppose $G = \langle a \rangle$. Then if $x, y \in G$, $x = a^i, y = a^j$ for some i, j so $xy = a^i a^j = a^{i+j} = a^j a^i = yx$ and G is abelian. ■

Example 8.6. $\mathbb{Q}$ is not cyclic. For if $q \in \mathbb{Q}$ and H is the cyclic subgroup generated by q then $H = \{nq : n \in \mathbb{Z}\}$. Hence, for $x \in H$, $|x| \geq |q|$. Thus $|q/2| \notin H$.

Theorem 8.7. *Every subgroup of a cyclic group is cyclic.*

Proof. Let G be a cyclic group generated by a, and let $H \leq G$. If H is trivial there is nothing to prove. Otherwise, let m be the smallest positive integer such that $a^m \in H$. We shall prove that H is cyclic generated by a^m. Let a^i be an arbitrary element of H. Write $i = mq + r$ with $0 \leq r \leq m - 1$. Then

$$a^r = a^{i-mq} = a^i(a^m)^{-q} \in H.$$

By the choice of m, it follows that $r = 0$, and hence $a^i = (a^m)^q$, a power of a^m. ■

Example 8.8. Let us list all subgroups of the group $\mathbb{Z}_{12}$:

$$\{0\}, \mathbb{Z}_{12},\ \{0, 2, 4, 6, 8, 10\},\ \{0, 3, 6, 9\},\ \{0, 4, 8\},\ \{0, 6\}.$$

9. Alternating groups

We are now going to introduce an important subgroup of the symmetric group S_n. First we introduce another way of writing permutations.

Theorem 9.1. *Every permutation can be written as a product of* 2*-cycles (also called* transpositions*).*

Proof. We already know that a permutation can be written as a product of (disjoint) cycles, and a cycle can be written as a product of transpositions:

$$(i_1\ i_2\ \ldots\ i_k) = (i_1\ i_2)(i_2\ i_3)\ldots(i_{k-1}\ i_k);$$

this proves the theorem. ■

A decomposition of a permutation into a product of transpositions is by no means unique; for instance

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

However, the parity of the number of transpositions in any decomposition of a given permutation does not change.

Definition 9.2. A permutation is *even* (respectively *odd*) if it can be written as a product of an even (respectively odd) number of transpositions.

Theorem 9.3. *A permutation cannot be both even and odd.*

Proof. Consider the polynomial of n variables:

$$P = P(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

For a permutation σ let

$$\sigma(P) = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Note that

$$(\sigma\tau)(P) = \sigma(\tau(P)).$$

Also note that if $\gamma = (k\ l)$ $(k < l)$ is a transposition, then

$$\gamma(P) = -P.$$

Indeed, the only factors of P that change sign when swapping x_k and x_l are $(x_k - x_l)$, $(x_k - x_i)$ and $(x_i - x_l)$ $(k < i < l)$ and there is an odd number of them.

Now assume that a permutation $\sigma \in S_n$ can be written both as a product of an even number of transpositions $\sigma = \gamma_1 \dots \gamma_{2q}$ and as a product of an odd number of transpositions $\sigma = \delta_1 \dots \delta_{2r+1}$. But then

$$P = \gamma_1(\dots(\gamma_{2q}(P))) = \sigma(P) = \delta_1(\dots(\delta_{2r+1}(P))) = -P,$$

which is a contradiction. ■

Exercise 9.4. A k-cycle is even if and only if k is odd! Hint: see the proof of Theorem 9.1.

Theorem 9.5. *The set A_n of all even permutations in S_n is a subgroup of S_n of order $n!/2$.*

Proof. For $\sigma = \gamma_1 \dots \gamma_{2k} \in A_n$ and $\tau = \delta_1 \dots \delta_{2l} \in A_n$ we have

$$\sigma\tau = \gamma_1 \dots \gamma_{2k}\delta_1 \dots \delta_{2l} \in A_n,$$
$$\sigma^{-1} = \gamma_{2k}^{-1} \dots \gamma_1^{-1} = \gamma_{2k} \dots \gamma_1 \in A_n.$$

Hence $A_n \leq S_n$.

Let O_n be the set of all odd permutations of S_n. Then clearly $S_n = A_n \cup O_n$ and $A_n \cap O_n = \emptyset$ by Theorem 9.3. Define a mapping $f : S_n \longrightarrow S_n$ by $f(\sigma) = \sigma(1\ 2)$. Then f is a bijection:

$$\sigma = \sigma(1\ 2)(1\ 2) = f(\sigma(1\ 2)),$$
$$f(\sigma_1) = f(\sigma_2) \Rightarrow \sigma_1(1\ 2) = \sigma_2(1\ 2) \Rightarrow \sigma_1 = \sigma_2.$$

Also f maps A_n into O_n and O_n into A_n. Finally $f \circ f$ is the identity transformation. We conclude that f is a bijection between A_n and O_n, so that $|A_n| = |O_n|$. Now we have $n! = |S_n| = |A_n| + |O_n| = 2|A_n|$, and hence $|A_n| = n!/2$. ■

Definition 9.6. A_n is called the *alternating group* on $\{1, \dots, n\}$.

Exercise 9.7. List the elements of A_4.

Exercise 9.8. Prove that O_n is not a subgroup of S_n.

10. Cosets and Lagrange's Theorem

Every subgroup of a group G induces an important decomposition of G.

Definition 10.1. Let G be a group, let H be a subgroup of G, and let $a \in G$ be any element. The *left coset* of H in G determined by a is the set

$$aH = \{ah \,:\, h \in H\}.$$

The *right coset* of H in G determined by a is the set

$$Ha = \{ha \,:\, h \in H\}.$$

Example 10.2. Let us find all the (left and right) cosets of the cyclic subgroup $H = \{\mathrm{id}, (1\ 2)\}$ of the symmetric group S_3:

$$\begin{array}{ll}
L_1 = \mathrm{id}H = \{\mathrm{id}, (1\ 2)\} & R_1 = H\mathrm{id} = \{\mathrm{id}, (1\ 2)\}, \\
L_2 = (1\ 2)H = \{(1\ 2), \mathrm{id}\} & R_2 = H(1\ 2) = \{(1\ 2), \mathrm{id}\}, \\
L_3 = (1\ 3)H = \{(1\ 3), (1\ 2\ 3)\} & R_3 = H(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}, \\
L_4 = (2\ 3)H = \{(2\ 3), (1\ 3\ 2)\} & R_4 = H(2\ 3) = \{(2\ 3), (1\ 2\ 3)\}, \\
L_5 = (1\ 2\ 3)H = \{(1\ 2\ 3), (1\ 3)\} & R_5 = H(1\ 2\ 3) = \{(1\ 2\ 3), (2\ 3)\}, \\
L_6 = (1\ 3\ 2)H = \{(1\ 3\ 2), (2\ 3)\} & R_6 = H(1\ 3\ 2) = \{(1\ 3\ 2), (1\ 3)\}.
\end{array}$$

Exercise 10.3. Write down the cosets of the subgroup $\{0, 3, 6, 9\}$ in $\mathbb{Z}_{12}$.

Exercise 10.4. What are the cosets of the trivial subgroup $\{e\}$ in G? What are the cosets of G in G?

Exercise 10.5. Prove that the cosets of A_n in S_n are A_n and O_n.

We see that the left and the right coset determined by the same element need not be equal. We may also notice some interesting regularities: all the cosets have equal sizes; some of them are equal (e.g. $L_3 = L_5$), and the others are disjoint (e.g. $L_3 \cap L_6 = \emptyset$). These are not accidents.

Theorem 10.6. *Let G be a group, and let H be a subgroup of G.*

(i) *H is a left coset of itself.*

(ii) *For every $a \in G$ we have $a \in aH$. (Every element belongs to the left coset determined by it.)*

(iii) *$G = \bigcup_{a \in G} aH$. (G is the union of the left cosets of H.)*

(iv) *For any two left cosets aH and bH we either have $aH = bH$, or else $aH \cap bH = \emptyset$. (Any two left cosets of H are either equal or disjoint.)*

(v) *For all $a \in G$ we have $|aH| = |H|$. (All the left cosets of H have equal size.)*

Analogous statements hold for right cosets.

Proof. (i) $H = eH$.

(ii) $a = ae \in aH$, since $e \in H$.

(iii) Clearly $aH \subseteq G$ for every $a \in G$ because of closure. Therefore $\bigcup_{a \in G} aH \subseteq G$. Conversely, since $b \in bH \subseteq \bigcup_{a \in G} aH$, it follows that $G \subseteq \bigcup_{a \in G} aH$.

(iv) Assume that $aH \cap bH \neq \emptyset$, with $z = ah_1 = bh_2 \in aH \cap bH$. We are going to prove that $aH = bH$. Let $x = ah \in aH$ be arbitrary. Write $x = ah = zh_1^{-1}h = bh_2h_1^{-1}h$. Since $h, h_1, h_2 \in H$, it follows that $x \in bH$. This shows that $aH \subseteq bH$, and the reverse inclusion can be proved by a similar argument.

(v) Define a mapping $f : H \longrightarrow aH$ be $f(x) = ax$. Then f is a bijection. Indeed, an arbitrary element of aH can be written as $ah = f(h)$ by the very definition of cosets; hence f is onto. Also

$$f(x) = f(y) \Rightarrow ax = ay \Rightarrow x = y,$$

and f is one-one. ■

Theorem 10.7 (Lagrange) *Let G be a group of finite order, and let H be a subgroup of G. Then the order of H divides the order of G.*

Proof. Let $C_1, \ldots, C_k$ be the distinct cosets of H. By Theorem 10.6 (v) we have $|C_1| = \ldots = |C_k| = |H|$. Also, by Theorem 10.6 (iii) and (iv) the cosets of H partition G, so that

$$|G| = |C_1| + \ldots + |C_k| = \underbrace{|H| + \ldots + |H|}_{k} = k|H|,$$

and the theorem follows. ■

Theorem 10.8. *Let G be a finite group, and let $a \in G$ be arbitrary. Then the order of a divides the order of G.*

Proof. The order of a is equal to the order of the cyclic subgroup of G generated by a. ■

We give one interesting application.

Theorem 10.9. *Every group of prime order is cyclic.*

Proof. Let G be a group of prime order p, and let $a \in G$ be any non-identity element. The order n of a divides p, so that $n = p$. It follows that G is cyclic generated by a. ■

11. Homomorphisms of groups

Here we study mappings between groups which respect the operations.

Definition 11.1. Let G and H be groups with operations $*$ and $\bullet$ respectively. A mapping $f : G \longrightarrow H$ is a *homomorphism* if for all $x, y \in G$ we have $f(x * y) = f(x) \bullet f(y)$.

If the operation in both groups is denoted as multiplication, then the above rule becomes $f(xy) = f(x)f(y)$. (The image of the product is the product of images.)

Example 11.2. The mapping $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ defined by $f(x) = x \pmod{n}$ is a homomorphism.

Example 11.3. For any two groups G and H the mapping $f : G \longrightarrow H$ defined by $f(x) = e_H$ (the identity of H) is a homomorphism. Indeed $f(xy) = e_H = e_H e_H = f(x)f(y)$.

Example 11.4. For any group G the identity mapping $G \longrightarrow G$ is a homomorphism.

Example 11.5. The mapping $f : GL(n, \mathbb{R}) \longrightarrow \mathbb{R} \setminus \{0\}$, given by $f(A) = |A|$ (the determinant of A, is a homomorphism from $GL(n, \mathbb{R})$ into the multiplicative group $\mathbb{R} \setminus \{0\}$, because $|AB| = |A||B|$.

Example 11.6. The mapping $f : S_n \longrightarrow \mathbb{Z}_2$ defined by

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

is a homomorphism. Indeed, note that the even and odd permutations multiply according to the rule

	even	odd
even	even	odd
odd	odd	even

Therefore, for $\sigma, \tau \in S_n$ we have

$$f(\sigma\tau) = \left\{ \begin{array}{ll} 0 & \sigma \text{ even}, \tau \text{ even} \\ 0 & \sigma \text{ odd}, \tau \text{ odd} \\ 1 & \sigma \text{ even}, \tau \text{ odd} \\ 1 & \sigma \text{ odd}, \tau \text{ even} \end{array} \right\} = f(\sigma) + f(\tau).$$

Next we derive some basic properties of homomorphisms.

Theorem 11.7. *Let G and H be two groups with identities e_G and e_H respectively. If $f : G \longrightarrow H$ is a homomorphism then*

(i) $f(e_G) = e_H$;

(ii) $f(a)^{-1} = f(a^{-1})$ *for every* $a \in G$.

Proof. (i) Take arbitrary $x \in G$. Since $xe_G = x$, it follows that $f(x) = f(xe_G) = f(x)f(e_G)$. Canceling (in H!) $f(x)$ we obtain $f(e_G) = e_H$.

(ii) From $f(a)f(a^{-1}) = f(aa^{-1}) = f(e_G) = e_H$, and the uniqueness of inverses, it follows that $f(a^{-1}) = f(a)^{-1}$. ■

We also note that there are certain natural subgroups related to homomorphisms.

Definition 11.8. Let $f : G \longrightarrow H$ be a homomorphism of groups. The set

$$\ker(f) = \{x \in G : f(x) = e_H\}$$

is called the *kernel* of f. Also for any subset $X \subseteq G$ we write

$$f(X) = \{f(x) : x \in X\}$$

for its image under f. The set $f(G)$ is also denoted by $\mathrm{im}(f)$ and is called the *image* of f.

Example 11.9. Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ be the homomorphism from Example 11.2. Then

$$m \in \ker(f) \Leftrightarrow f(m) = 0 \Leftrightarrow m = 0 \pmod{n} \Leftrightarrow n|m,$$

and hence $\ker(f) = n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$ consists of all integer multiples of n. The image of f is whole $\mathbb{Z}_n$ (i.e. f is onto).

Exercise 11.10. Prove that for the homomorphism f from Example 11.5 we have $\ker(f) = SL(n, \mathbb{R})$, and that $\mathrm{im}(f) = \mathbb{R} \setminus \{0\}$.

Exercise 11.11. Prove that for the homomorphism f from Example 11.6 we have $\ker(f) = A_n$ and $\mathrm{im}(f) = \mathbb{Z}_2$.

Theorem 11.12. *Let $f : G \longrightarrow H$ be a homomorphism of groups.*

(i) $\ker(f)$ *is a subgroup of* G.

(ii) *The image $f(K)$ of any subgroup K of G is a subgroup of H.*

Proof. (i) Let $a, b \in \ker(f)$, so that $f(a) = f(b) = e_H$. Then we have

$$f(ab) = f(a)f(b) = e_He_H = e_H \Rightarrow ab \in \ker(f),$$
$$f(a^{-1}) = f(a)^{-1} = e_H^{-1} = e_H \Rightarrow a^{-1} \in \ker(f).$$

Thus $\ker(f)$ is closed for multiplication and inverses, and hence it is a subgroup.

(ii) Let $u, v \in f(K)$, and write $u = f(x)$ and $v = f(y)$, where $x, y \in K$. Since K is a subgroup, it follows that $xy \in K$ and $x^{-1} \in K$. But then

$$uv = f(x)f(y) = f(xy) \in f(K),$$
$$u^{-1} = (f(x))^{-1} = f(x^{-1}) \in f(K).$$

Hence $f(K) \leq H$. ■

Exercise 11.13. For a homomorphism $f : G \longrightarrow H$ of groups and a subset $Y \subseteq H$ define the *inverse image* of Y to be

$$f^{-1}(Y) = \{x \in G \,:\, f(x) \in Y\}.$$

Prove that the inverse image of a subgroup of H is a subgroup of G. Also, prove that $\ker(f) = f^{-1}(\{e_H\})$.

Exercise 11.14. Prove that a homomorphism $f : G \longrightarrow H$ of groups is one-one if and only if $\ker(f) = \{e_G\}$.

12. Isomorphisms

Let us compare the group $\mathbb{Z}_3$ under addition modulo 3 with the cyclic subgroup H of S_3 generated by (1 2 3):

$\mathbb{Z}_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

H	id	(1 2 3)	(1 3 2)
id	id	(1 2 3)	(1 3 2)
(1 2 3)	(1 2 3)	(1 3 2)	id
(1 3 2)	(1 3 2)	id	(1 2 3)

We see that the two tables differ only in the names of the symbols, and not in their positions. More formally, there is mapping $f : \mathbb{Z}_3 \longrightarrow H$ (namely $f(0) = \mathrm{id}$, $f(1) = (1\ 2\ 3)$, $f(2) = (1\ 3\ 2)$) which is a bijection and satisfies $f(i+j) = f(i) \circ f(j)$.

Definition 12.1. Let G and H be two groups. A mapping $f : G \longrightarrow H$ is an *isomorphism* if it is a bijection and a homomorphism. We say that G and H are *isomorphic* if there is an isomorphism $f : G \longrightarrow H$; this is denoted $G \cong H$.

Theorem 12.2. *Let G, H and K be three groups. Then:*

(i) $G \cong G$;

(ii) $G \cong H \Longrightarrow H \cong G$;

(iii) $G \cong H \ \&\ H \cong K \Longrightarrow G \cong K$.

Proof. (i) The identity mapping on G is an isomorphism. (ii) If $f : G \longrightarrow H$ is an isomorphism, then so is $f^{-1} : H \longrightarrow G$. (iii) If $f : G \longrightarrow H$ and $g : H \longrightarrow K$ are isomorphisms, then so is their composition $g \circ f : G \longrightarrow K$. ■

It makes sense to regard isomorphic groups as identical. The main general task of group theory can be formulated as: classify all non-isomorphic groups. In general this is impossible, and one has to settle for various partial results in this direction. Probably the easiest such is the following:

Theorem 12.3. *Let G be a cyclic group. If G is infinite then $G \cong \mathbb{Z}$; if G is finite of order n then $G \cong \mathbb{Z}_n$.*

Proof. Let a be a generator for G. Assume first that G is infinite, so that all powers of a are distinct. Define $f : \mathbb{Z} \longrightarrow G$ by $f(i) = a^i$. Then f is onto, because G consists of powers of a; it is also one-one and a homomorphism because

$$f(i) = f(j) \Rightarrow a^i = a^j \Rightarrow i = j,$$
$$f(i+j) = a^{i+j} = a^i a^j = f(i)f(j).$$

Hence f is an isomorphism.

If G is finite of order n then $G = \{e, a, \ldots, a^{n-1}\}$ by Theorem 6.8. Define a mapping $f : \mathbb{Z}_n \longrightarrow G$ by $f(i) = a^i$. As above, this mapping is an isomorphism. ■

In order to prove that two groups g and H are not isomorphic, one needs to demonstrate that there is no isomorphism from G onto H. Usually, in practice, this is much easier than it sounds in general, and is accomplished by finding some property that holds in one group, but not in the other.

Example 12.4. The groups $\mathbb{Z}_4$ and $\mathbb{Z}_6$ are not isomorphic because they have different orders.

Example 12.5. $\mathbb{Z}_6 \ncong S_3$ because $\mathbb{Z}_6$ is abelian and S_3 is not (although they both have order 6).

Example 12.6. The dihedral group D_{12} is not isomorphic to S_4 because D_{12} has 13 elements of order 2 (12 reflections, and the rotation for 180^0), while S_4 has only 9 such elements (transpositions, and products of two disjoint transpositions). (Note that $|D_{12}| = |S_4| = 24$ and that they are both non-abelian.)

Exercise 12.7. Consider the group $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, where the multiplication naturally extends the rules

$$i^2 = j^2 = k^2 = -1,$$
$$ij = k,\ jk = i,\ ki = j,\ ji = -k,\ kj = -i,\ ik = -j.$$

The full Cayley table is

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

This group is called the *quaternion group*. Prove that Q_8 is not isomorphic to D_4 and $\mathbb{Z}_8$.

Finally, we prove the so called Cayley's theorem, which suggests a prominent role of the symmetric groups among all groups.

Theorem 12.8 (Cayley) *Every group G is isomorphic to a subgroup of the symmetric group $S(G)$.*

Proof. For each $a \in G$ define a mapping $\tau_a : G \longrightarrow G$ by

$$\tau_a(x) = ax.$$

Then τ_a is a permutation (i.e. bijection):

$$b = aa^{-1}b = \tau_a(a^{-1}b),$$
$$\tau_a(x) = \tau_a(y) \Rightarrow ax = ay \Rightarrow x = y.$$

Now define a mapping $f : G \longrightarrow S(G)$ by

$$f(a) = \tau_a.$$

First we prove that f is one-one:

$$f(a) = f(b) \Rightarrow \tau_a = \tau_b \Rightarrow (\forall x \in G)(\tau_a(x) = \tau_b(x)) \Rightarrow ae = be \Rightarrow a = b.$$

Next we note that

$$(\tau_a\tau_b)(x) = \tau_a(\tau_b(x)) = a(bx) = (ab)x = \tau_{ab}(x),$$

so that the mappings $\tau_a\tau_b$ and τ_{ab} are equal. Now we have

$$f(a)f(b) = \tau_a\tau_b = \tau_{ab} = f(ab),$$

and hence f is a homomorphism.

Now by Theorem 11.12 (ii), $\mathrm{im}\,(f) = \{\tau_a \ : \ a \in G\}$ is a subgroup of $S(G)$. Moreover, if we now consider f as a mapping from G into $\mathrm{im}\,(f)$, then it also becomes onto, and we conclude that $G \cong \mathrm{im}\,(f) \leq S(G)$. ■

Remark 12.9. The permutations τ_a can be read off easily from the Cayley table for G – they correspond to the rows of it. Of course, if G is finite of order n, you can rename the elements of G by numbers $1, \ldots, n$ (in an arbitrary fashion), and thus represent G as a subgroup of S_n.

Example 12.10. In the quaternion group Q_8, we have, for example,

$$\tau_i = \begin{pmatrix} 1 & -1 & i & -i & j & -j & k & -k \\ i & -i & -1 & 1 & k & -k & -j & j \end{pmatrix},$$

or, after renaming,

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

The practical use of Cayley's Theorem is limited: it is not very likely that one can obtain much useful information about groups of order, say, eight, by considering subgroups of the group S_8 of order 40320.

13. Normal subgroups

We have seen that to every homomorphism $f \ : \ G \longrightarrow H$ we can associate two distinguished subgroups: $\ker(f) \leq G$ and $\mathrm{im}\,(f) \leq H$. It is natural to ask a converse question: given a subgroup of a group G, is this subgroup the kernel or the image of some homomorphism?

It is easy that every subgroup is the image of some homomorphism. Indeed, if $K \leq G$, define $f \ : \ K \longrightarrow G$ by $f(x) = x$. Then it is clear that $\mathrm{im}\,(f) = K$.

The situation for kernels is different. In order to describe it, we introduce a special class of subgroups.

Theorem 13.1. *The following conditions are equivalent for a subgroup N of a group G:*

(i) *every left coset of N is also a right coset (and vice versa);*

(ii) *$aN = Na$ for every $a \in G$;*

(iii) *for all $a \in G$ and all $n \in N$ we have $ana^{-1} \in N$;*

(iv) *For every $a \in G$ we have $aNa^{-1} = \{a^{-1}na \ : \ n \in N\} = N$.*

Proof. (i)⇒(ii) Let $a \in G$. By (i), we have $aN = Nb$ for some $b \in G$. But then we have $a \in aN = Nb$, and also $a \in Na$. By Theorem 10.6 (iv) (for right cosets!), we conclude that $Nb = Na$, and hence $aN = Na$.

(ii)⇒(iii) Let $a \in G$ and $n \in N$. By (ii) we have $aN = Na$; hence we can write $an = n_1 a$, with $n_1 \in N$. But then

$$ana^{-1} = aa^{-1}n_1 = n_1 \in N,$$

as required.

(iii)⇒(iv) It follows immediately from (iii) that $aNa^{-1} \subseteq N$. Let now $n \in N$ be arbitrary. From (iii) (applied to a^{-1} instead of a) it follows that $a^{-1}na = n_1 \in N$. But then

$$n = aa^{-1}naa^{-1} = an_1a^{-1} \in aNa^{-1}.$$

Hence $N = aNa^{-1}$.

(iv)⇒(i) Let $a \in G$ and $n \in N$ be arbitrary. By (iv) we have $ana^{-1} = n_1 \in N$. But then $an = n_1 a \in Na$. This shows that $aN \subseteq Na$. A similar argument shows the converse inclusion. Hence $aN = Na$, and so every left coset is also a right coset. ■

Definition 13.2. A subgroup N of a group G is *normal* if it satisfies any (and hence all) of the equivalent conditions of the above theorem; this is denoted $N \trianglelefteq G$.

Example 13.3. $\{e\} \trianglelefteq G$; $G \trianglelefteq G$, as left and right cosets are obviously equal.

Example 13.4. Every subgroup of an abelian group is normal, since $aN = Na$ is obviously satisfied.

Example 13.5. The cyclic subgroup of S_3 generated by (1 2) is not normal in S_3 because the left and right cosets do not coincide; see Example 10.2.

Example 13.6. If N is a subgroup of G with exactly two left cosets, then N is normal. Indeed the left cosets are N and $G \setminus N$. But then N also must have only two right cosets, and they must be N and $G \setminus N$ as well. In particular $A_n \trianglelefteq S_n$; see Exercise 10.5.

Example 13.7. Consider the quaternion group Q_8; see Exercise 12.7. The set $N = \{1, -1\}$ is clearly a subgroup. Note that both 1 and -1 commute with every element of Q_8. Hence we have $aN = Na$ for every $a \in Q_8$, and N is normal.

We now return to our investigation of the kernels.

Theorem 13.8. *If $f : G \longrightarrow H$ is a homomorphism then $\ker(f) \trianglelefteq G$.*

Proof. Let $a \in G$ and $n \in \ker(f)$. From $f(n) = e_H$ it follows that

$$f(a^{-1}na) = f(a^{-1})f(n)f(a) = f(a)^{-1}e_H f(a) = f(a)^{-1}f(a) = e_H.$$

Hence $a^{-1}na \in \ker(f)$. ■

14. Quotient groups

We now introduce a new construction for groups, which will enable us to prove that the kernels of homomorphisms are precisely normal subgroups.

Theorem 14.1. *Let G be a group, and let $N \trianglelefteq G$. On the set $G/N = \{aN : a \in G\}$ of all cosets of N we define a binary operation by*

$$(aN)(bN) = (ab)N.$$

With this operation, G/N is a group.

Proof. First we have to prove that the above multiplication is *well defined*. The point here is that we are defining a product of two *sets*, by choosing two *elements* from them, multiplying them together, and finding the set corresponding to the product. We have to convince ourselves that the resulting set depends on the original sets, but not on the particular choices of elements.

More formally, let us assume that we have $aN = a_1N$ and $bN = b_1N$. Consider an arbitrary element abn from abN. Since $bN = b_1N$ we can write $bn = bn_1$ ($n_1 \in N$). Since $N \trianglelefteq G$ we have $b_1n_1 = n_2b_1$ for some $n_2 \in N$. From $aN = a_1N$ it follows that $an_2 = a_1n_3$ for some $n_3 \in N$. Finally, normality of N implies that $n_3b_1 = b_1n_4$ for some $n_4 \in N$. Putting all this together, we obtain

$$abn = ab_1n_1 = an_2b_1 = a_1n_3b_1 = a_1b_1n_4 \in (a_1b_1)N.$$

This shows that $(ab)N \subseteq (a_1b_1)N$. An analogous argument shows the converse inclusion, and hence $(ab)N = (a_1b_1)N$, as required.

After this, proving that G/N is a group is easy. Closure follows immediately from the definition. Associativity follows from associativity in G:

$$\begin{aligned}((aN)(bN))(cN) &= ((ab)N)(cN) = ((ab)c)N = (a(bc))N = (aN)((bc)N)\\ &= (aN)((bN)(cN)).\end{aligned}$$

The identity element is $eN = N$:

$$(eN)(aN) = (ea)N = aN = (ae)N = (aN)(eN).$$

Finally, the inverse of aN is $a^{-1}N$ since

$$(aN)(a^{-1}N) = (aa^{-1})N = eN = (a^{-1}a)N = (a^{-1}N)(aN).$$

This completes the proof. ■

Example 14.2. Consider the quaternion group G and the normal subgroup $N = \{1, -1\}$; see Example 13.7. We are going to describe the quotient Q_8/N. First we determine the cosets:

$$\begin{aligned}C_1 &= 1N = (-1)N = \{1, -1\},\\ C_2 &= iN = (-i)N = \{i, -i\},\\ C_3 &= jN = (-j)N = \{j, -j\},\\ C_4 &= kN = (-k)N = \{k, -k\}.\end{aligned}$$

According to the multiplication rule given in the theorem, we have, for example

$$\begin{aligned}C_3C_4 &= (jN)(kN) = (jk)N = iN = C_2,\\ C_4C_3 &= (kN)(jN) = (kj)N = (-i)N = C_2,\\ C_2^2 &= (iN)^2 = i^2N = (-1)N = C_1.\end{aligned}$$

(Note that $C_3C_4 = C_4C_3$ although $jk \neq kj$ in Q_8; also note that C_2 has order 2, although i has order 4.) The full multiplication table is

	C_1	C_2	C_3	C_4
C_1	C_1	C_2	C_3	C_4
C_2	C_2	C_1	C_4	C_3
C_3	C_3	C_4	C_1	C_2
C_4	C_4	C_3	C_2	C_1

.

We see that $Q_8/N \cong K_4$, the Klein four group from Exercise 2.5. (Note that Q_8/N is abelian, although Q_8 is not.)

Exercise 14.3. Describe S_n/A_n.

We return to the kernels again.

Theorem 14.4. *Let G be a group, and let $N \trianglelefteq G$. The mapping $f : G \longrightarrow G/N$ defined by $f(x) = xN$ is a homomorphism and* $\ker(f) = N$.

Proof. That f is a homomorphism follows from

$$f(xy) = (xy)N = (xN)(yN) = f(x)f(y).$$

For $n \in N$ we have $f(n) = nN = N$ (closure!); hence $N \subseteq \ker(f)$. Also, for $x \in \ker(f)$ we have $xN = f(x) = eN = N$. In particular $x = xe \in N$. Therefore $\ker(f) \subseteq N$. ■

15. The first isomorphism theorem

The connection between kernels and normal subgroups induces a connection between quotients and images.

Theorem 15.1 (The first isomorphism theorem) *If $f : G \longrightarrow H$ is a homomorphism then*

$$G/\ker(f) \cong \mathrm{im}(f).$$

Proof. For brevity denote $\ker(f)$ by N, and $\mathrm{im}(f)$ by K. Define a mapping $\phi : G \longrightarrow K$ by $\phi(aN) = f(a)$.

Again we have to prove that this mapping is well defined. To this end assume that $aN = a_1N$. In particular, $a = a_1n$ for some $n \in N$. But then

$$\phi(aN) = f(a) = f(a_1n) = f(a_1)f(n) = f(a_1)e_H = f(a_1) = \phi(a_1N).$$

If $y \in K$ is arbitrary, then there exists $x \in G$ such that $f(x) = y$. But then $\phi(xN) = f(x) = y$; hence ϕ is onto. To prove that f is one-one as well, let $aN, bN \in G/N$ be such that $\phi(aN) = \phi(bN)$. This means that $f(a) = f(b)$, and, since f is a homomorphism, we obtain $f(a^{-1}b) = e_H$. This in turn implies $a^{-1}b \in \ker(f) = N$. Write $a^{-1}b = n \in N$, so that $b = an \in aN$. Now we have $b \in aN \cap bN$, which implies $aN = bN$.

Finally, we have

$$\phi((aN)(bN)) = \phi((ab)N) = f(ab) = f(a)f(b) = \phi(aN)\phi(bN).$$

This completes the proof that ϕ is an isomorphism. ■

The importance of the first isomorphism theorem is that one may consider quotients without working with cosets.

Example 15.2. The (necessarily normal) subgroup $n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$ of $\mathbb{Z}$ is the kernel of the homomorphism $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$, $f(a) = a \pmod n$; see Examples 11.2 and 11.9. Therefore, we have

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker(f) \cong \mathrm{im}(f) = \mathbb{Z}_n.$$

16. Rings: definition and basic properties

We now give an introduction to another type of algebraic structure, called ring. The exposition here will be faster. The emphasis is on the definition of a ring and a field, understanding the few basic examples, and realising that the concepts of a subring, homomorphism and quotient can be defined in a similar way to groups.

Definition 16.1. A set R with two operations $+$ and $\cdot$ defined on it is a *ring* if the following properties are satisfied:

(I) R is an abelian group with respect to $+$ (with neutral element 0);

(II) R is closed for $\cdot$, and $\cdot$ is associative;

(III) $\cdot$ is distributive over $+$, i.e. for all $x, y, z \in R$ we have

$$x(y+z) = xy + xz, \ (x+y)z = xz + yz.$$

We will see a number of examples of rings in the next section. First we are going to list some basic consequences of the axioms. We note that many basic properties involving $+$ (such as $x + 0 = 0 + x = x$, $x + (-x) = 0$ and $-(-x) = x$) follow from the definition of a group and Theorem 2.8.

Theorem 16.2. *The following hold in any ring R:*

(i) $x0 = 0x = 0$ *for all* $x \in R$;

(ii) $(-x)y = x(-y) = -(xy)$ *and* $(-x)(-y) = xy$ *for all* $x, y \in R$.

Proof. (i) $x0 = x(0+0) = x0 + x0 \Rightarrow x0 = 0$.
(ii) $xy + (-x)y = (x + (-x))y = 0y = 0 \Rightarrow (-x)y = -(xy)$; $(-x)(-y) = -x(-y) = -(-(xy)) = xy$. ■

Exercise 16.3. Prove that for all $x, y, z, t \in R$ we have

$$(x+y)(z+t) = xz + xt + yz + yt.$$

17. Examples of rings

Example 17.1. Each of the number sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ forms a ring with respect to ordinary addition and multiplication.

Exercise 17.2. For every $m \in \mathbb{Z}$ the set $m\mathbb{Z} = \{ma : a \in \mathbb{Z}\}$ forms a ring with respect to ordinary addition and multiplication.

Example 17.3. The set $\mathbb{Z}_n$ is a ring with respect to addition and multiplication modulo n.

Example 17.4. A (real) polynomial is a formal expression of the form

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

where $a_0, \ldots, a_n \in \mathbb{R}$ and x is a variable. (It is worth emphasising that x is *not* considered to be an element of $\mathbb{R}$, but rather a formal variable.) Polynomials can be added and multiplied as usual. With these operations, the set $\mathbb{R}[x]$ of all polynomials is a ring. In fact, given any ring, one can in a similar way construct the ring $R[x]$ of polynomials over x.

Example 17.5. The set $M_n(\mathbb{R})$ of all $n \times n$ matrices with entries from $\mathbb{R}$ forms a ring with respect to the usual addition and multiplication of matrices. In fact, given an arbitrary ring R, one can consider the ring $M_n(R)$ of all $n \times n$ matrices with entries from R.

Exercise 17.6. The set

$$\left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \,:\, a, b \in \mathbb{R} \right\}$$

is a ring with respect to the ordinary matrix addition and multiplication.

Example 17.7. The set

$$\mathbb{H} = \{a_1 + a_2 i + a_3 j + a_4 k \,:\, a_1, a_2, a_3, a_4 \in \mathbb{R}\},$$

where i, j, k come from the quaternion group Q_8 (see Exercise 12.7), and multiply accordingly, forms a ring under the natural addition and multiplication. For instance, we have

$$\begin{aligned} &(2 + 3i - j + 5k) + (3 - 3i + 2j + 2k) = 5 + 0i + j + 7k, \\ &(2 + 3i - j + 5k)(3 - 3i + 2j + 2k) = 6 - 6i + 4j + 4k + 9i + 9 + 6k - 6j \\ &-3j - 3k + 2 - 2i + 15k - 15j - 10i - 10 = 7 - 9i - 20j + 22k. \end{aligned}$$

Example 17.8. Let G be any abelian group, written additively. On g define a multiplication by setting $xy = 0$ for all $x, y \in G$. This makes G into a (not very interesting!) ring.

18. Special types of rings

Definition 18.1. A ring R is said to be *commutative* if the multiplication in R is commutative, i.e. if $xy = yx$ holds for all $x, y \in R$.

Examples 18.2. The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_n$ and $\mathbb{R}[x]$ are all commutative. The rings $\mathbb{H}$ and $M_n(\mathbb{R})$ are not commutative.

Definition 18.3. A ring R is said to be a *ring with identity* if there is a neutral element (usually denoted by 1) for multiplication; thus $1x = x1 = x$ holds for all $x \in R$.

Examples 18.4. All the rings mentioned in Examples 18.2 are rings with identity. The rings from Exercises 17.2 and 17.6 are not rings with identity.

Definition 18.5. A ring R is said to be an *integral domain* if it is commutative and $xy = 0$ implies $x = 0$ or $y = 0$ for all $x, y \in R$.

Examples 18.6. All $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are integral domains. $\mathbb{Z}_n$ is an integral domain if and only if n is a prime. $M_n(\mathbb{R})$ is not an integral domain.

Definition 18.7. A ring R is a *division ring* if $R \setminus \{0\}$ forms a group with respect to multiplication, i.e. if it is a ring with identity and every non-zero element of R has a multiplicative inverse.

Definition 18.8. A ring R is a *field* if $R \setminus \{0\}$ forms an abelian group, i.e. if R is a commutative division ring.

Examples 18.9. $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields. $\mathbb{H}$ is a division ring, but not a field. Indeed, it is easy to check that the multiplicative inverse of $z = a_1 + a_2 i + a_3 j + a_4 k \neq 0$ is

$$z^{-1} = \frac{1}{a_1^2 + a_2^2 + a_3^2 + a_4^2}(a_1 - a_2 i - a_3 j - a_4 k).$$

Also $\mathbb{H}$ is obviously not commutative (e.g. $ij = k \neq -k = ji$). $\mathbb{Z}$, $M_n(\mathbb{R})$ and $\mathbb{R}[x]$ are not division rings.

Example 18.10. $\mathbb{Z}_n$ is a field if and only if n is a prime. Indeed, by Theorem 3.11, $\mathbb{Z}_n \setminus \{0\}$ is a group if and only if n is a prime.

19. Subrings, ideals and quotients

Definition 19.1. A subring of a ring R is any subset $S \subseteq R$ which forms a ring under the same operations.

Example 19.2. $\mathbb{Z}$ is a subring of $\mathbb{Q}$ is a subring of $\mathbb{R}$ is a subring of $\mathbb{C}$ is a subring of $\mathbb{H}$.

Example 19.3. Every non-trivial ring R has at least two subrings – $\{0\}$ and R; all the other subrings are called *proper*.

As in groups, we can reduce the number of axioms one has to check when proving that something is a subring.

Theorem 19.4. *A non-empty subset S of a ring R is a subring if and only if S is closed for addition ($x, y \in S \Rightarrow x + y \in S$), taking negatives ($x \in S \Rightarrow -x \in S$) and multiplication $x, y \in S \Rightarrow xy \in S$).*

Proof. ($\Rightarrow$) This is obvious.

($\Leftarrow$) The first two conditions ensure that S with respect to $+$ is a subgroup of R (see Theorem 7.5), and hence is an abelian group. The third assumption gives us that it is closed under multiplication, while the associativity, and distributivity laws are then automatically inherited from R. ■

Exercise 19.5. Prove that the set of matrices

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \,:\, a, b, c \in \mathbb{R} \right\}$$

forms a subring of the ring $M_2(\mathbb{R})$.

Example 19.6. The set of matrices

$$\left\{ \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} \,:\, a, b, c \in \mathbb{R} \right\}$$

is closed under addition and taking negatives, but is not a subring of $M_2(\mathbb{R})$ because it is not closed under multiplication (check!). The general linear group $GL(2, \mathbb{R})$ is closed under multiplication and taking negatives (!), but is not a subring of $M_2(\mathbb{R})$ because it is not closed under addition. For example, for any invertible matrix A we have $A, -A \in GL(2, \mathbb{R})$, but $A + (-A) = 0 \notin GL(2, \mathbb{R})$.

Definition 19.7. A subring I of a ring R is called an *ideal* if it satisfies

$$(\forall x \in R)(\forall y \in I)(xy, yx \in I);$$

we say that I is *stable* under multiplication from R.

Remark 19.8. Since stability implies closure under multiplication, to check that a subset I is an ideal in a ring R it is sufficient to check that I is a subgroup of the additive group R, and that it is stable.

Example 19.9. The set $m\mathbb{Z}$ is an ideal of $\mathbb{Z}$. Indeed, if $ma \in m\mathbb{Z}$ and $n \in \mathbb{Z}$ the $n(ma) = (ma)n = m(na) \in m\mathbb{Z}$.

Example 19.10. The set $x\mathbb{R}[x]$ is an ideal of $\mathbb{R}[x]$.

Example 19.11. The subring S of $M_2(\mathbb{R})$ from Exercise 19.5 is not an ideal; for example, we have

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

Example 19.12. $\{0\}$ and R are ideals of R.

Theorem 19.13. *A field F has no proper ideals.*

Proof. Let I be an ideal of F, and assume that $I \neq \{0\}$. Choose $a \in I \setminus \{0\}$. Let $b \in F$ be arbitrary. Then we have

$$b = b1 = baa^{-1} = a(ba^{-1}) \in I.$$

This proves that $I = F$. ■

Ideals play for rings the role that normal subgroups play for groups.

Theorem 19.14. *Let R be a ring, and let I be an ideal of R. The set*

$$R/I = \{a + I \,:\, a \in R\}$$

of all additive cosets of I forms a ring under the following natural operations:

$$(a + I) + (b + I) = (a + b) + I, \;\; (a + I)(b + I) = (ab) + I.$$

Proof. By Theorem 14.1 it follows that the above addition is well defined, and that it turns R/I into an abelian group.

Next we have to show that multiplication is well defined as well. To this end assume that $a + I = a_1 + I$ and $b + I = b_1 + I$. In particular, we have $a = a_1 + i$ and $b = b_1 + j$ for some $i, j \in I$. But then we have

$$\begin{aligned} (a + I)(b + I) &= ab + I = (a_1 + i)(b_1 + j) + I = (a_1b_1 + a_1j + ib_1 + ij) + I \\ &= a_1b_1 + ((a_1j + ib_1 + ij) + I) = a_1b_1 + I, \end{aligned}$$

because $a_1j, ib_1, ij \in I$.

Proving associativity and distributivity is now easy, and is left for exercise. ■

20. Homomorphisms, isomorphisms and the first isomorphism theorem for rings

Definition 20.1. Let R and S be two rings. A mapping $f : R \longrightarrow S$ is a (*ring*) *homomorphism* if for all $x, y \in R$ we have $f(x + y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$.

Example 20.2. The mapping $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ defined by $f(x) = x \pmod{n}$ is a homomorphism.

Example 20.3. The mapping $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $f(x) = 2x$ is not a homomorphism. Indeed, although $f(x+y) = 2(x+y) = 2x + 2y = f(x) + f(y)$, we have $f(xy) = 2xy \neq 4xy = f(x)f(y)$.

Example 20.4. For any two rings R and S the mapping $f : R \longrightarrow S$ defined by $f(x) = 0$ (the zero of S) is a homomorphism.

Definition 20.5. Let $f : R \longrightarrow S$ be a homomorphism of rings. The *kernel* and *image* of f are the sets:

$$\ker(f) = \{x \in R : f(x) = 0\},$$
$$\mathrm{im}(f) = \{f(x) : x \in R\}.$$

Next we prove that kernels of homomorphisms are precisely the ideals. (The corresponding results for groups are Theorems 13.8 and 14.4.)

Theorem 20.6. (I) *If $f : R \longrightarrow S$ is a homomorphism of rings then its kernel is an ideal of R.*

(II) *If I is an ideal of a ring R then the mapping $f : R \longrightarrow R/I$ defined by $f(x) = x + I$, is a homomorphism with kernel I.*

Proof. (I) That $\ker(f)$ is a subgroup of the additive group R follows from the corresponding theorem for groups (Theorem 11.12 (i)). For stability, let $x \in R$ and $y \in \ker(f)$. Now $f(y) = 0$ implies $f(xy) = f(x)f(y) = f(x)0 = 0$, and similarly $f(yx) = 0$. Therefore $\ker(f)$ is indeed an ideal.

(II) That f is a homomorphism follows from

$$f(x+y) = (x+y) + I = (x+I) + (y+I) = f(x) + f(y),$$
$$f(xy) = (xy) + I = (x+I)(y+I) = f(x)f(y).$$

Also,

$$x \in ker(f) \Leftrightarrow x + I = 0 + I \Leftrightarrow x \in I,$$

and so $\ker(f) = I$. ■

Exercise 20.7. Prove that if $f : R \longrightarrow S$ is a ring homomorphism then $\mathrm{im}(f)$ is a subring of S.

Definition 20.8. A bijective homomorphism of rings is called an *isomorphism*. Two rings R and S are isomorphic ($R \cong S$) if there is an isomorphism $f : R \longrightarrow S$.

Theorem 20.9. *If $f : R \longrightarrow S$ is a homomorphism of groups then*

$$R/\ker(f) \cong \mathrm{im}(f).$$

Proof. Denote $\ker(f)$ by I and $\mathrm{im}(f)$ by K. Let $\phi : R/I \longrightarrow K$ be defined by $\phi(a+I) = f(a)$. That this mapping is well defined, that it is bijective and that it is a homomorphism of additive groups follows from the First Isomorphism Theorem for groups. We also have

$$\phi((a+I)(b+I)) = \phi(ab+I) = f(ab) = f(a)f(b) = \phi(a+I)\phi(b+I),$$

and hence ϕ is a ring isomorphism. ■

21. Conclusion

In this course we have learnt that modern algebra is a study of sets with operations defined on them. As the main example we have started a systematic study of groups. Group theory is one of the most important areas of contemporary mathematics, with applications ranging from physics and chemistry to coding and cryptography. It is also one of the research interests in this school. Further study of groups can be undertaken in the appropriate honours modules.

As our second example, we have given a brief introduction to rings and fields. We have seen that there are some important properties which are very similar to groups. Further courses on rings are also available at the honours level.

Today, groups, rings and fields, along with vector spaces, are regarded as classical algebraic disciplines. There is also a wide variety of newer structures: semigroups, lattices, boolean algebras, etc.