# F1.3YR1

# ABSTRACT ALGEBRA

# INTRODUCTION TO GROUP THEORY

## LECTURE NOTES AND EXERCISES

# Contents

# Chapter 1

# Introduction and definitions

## 1.1 Introduction

Abstract Algebra is the study of algebraic systems in an abstract way. You are already familiar with a number of algebraic systems from your earlier studies. For example, in number systems such as the integers $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, the rational numbers $\mathbb{Q} = \{\frac{m}{n};\ m, n \in \mathbb{Z},\ n \neq 0\}$, the real numbers $\mathbb{R}$, or the complex numbers $\mathbb{C} = \{x+iy;\ x, y \in \mathbb{R}\}$ (where $i^2 = -1$) there are algebraic operations such as addition, subtraction, and multiplication.

There are similar algebraic operations on other objects - for example vectors can be added or subtracted, $2 \times 2$ matrices can be added, subtracted and multiplied. Sometimes these operations satisfy similar properties to those of the familiar operations on numbers, but sometimes they do not.

For example, if $a, b$ are numbers then we know that $ab = ba$. But there are examples of $2 \times 2$ matrices $A, B$ such that $AB \neq BA$:

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

Abstract Algebra studies general algebraic systems in an axiomatic framework, so that the theorems one proves apply in the widest possible setting. The most commonly arising algebraic systems are *groups, rings* and *fields*. Rings and fields will be studied in F1.3YE2 Algebra and Analysis. The current module will concentrate on the theory of groups.

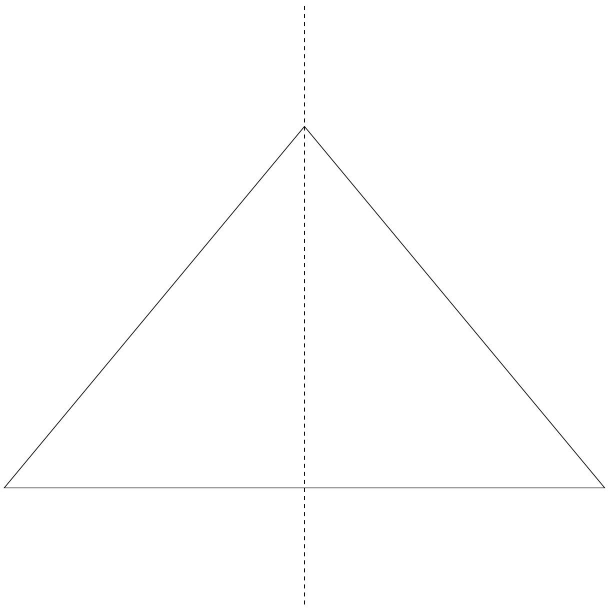
## 1.2 Examples of groups

The set of integers $\mathbb{Z}$, equipped with the operation of addition, is an example of a group. The sets $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are also groups with respect to the operation of addition of numbers.

Any vector space is a group with respect to the operation of vector addition.

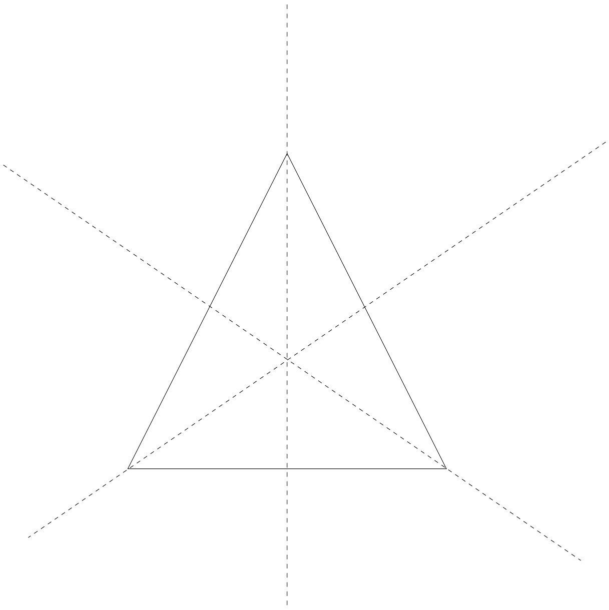
Important examples of groups arise from the symmetries of geometric objects. These can arise in all dimensions, but since we are constrained to working with 2-dimensional paper, blackboards and computer screens, I will stick to 2-dimensional examples.

Consider an isosceles triangle



This has an *axis of symmetry*, a line running across the triangle in such a way that a mirror placed on that line would reflect the triangle into itself. (Another way of thinking about this: if the triangle is drawn on paper and cut out, then turned over, it would fit back exactly into the hole in the paper.)

Other figures are more symmetric. For example, if a triangle is equilateral, then it has three axes of symmetry.



Each of these describes a different *symmetry* of the triangle, a *reflection* in the axis concerned. However, that is not the whole story. If we perform two of these reflections, one after the other, the overall effect on the triangle will be to rotate it through an angle of $2\pi/3$ (either clockwise or anti-clockwise) around its centre. These rotations are also symmetries.

Any symmetry of the triangle can be thought of as a mapping of the triangle onto itself. In all, there are 6 symmetries: three reflections, two rotations, and the identity map. The composition of two symmetries of the triangle (do one, then the other) is again a symmetry. The collection of all 6 symmetries, together with the operation of composing them together, is known as the *symmetry group* of the triangle.

## 1.3 Binary operations

The above examples of groups illustrate that there are two features to any group. Firstly we have a set (of numbers, vectors, symmetries, ...), and secondly we have a method of combining two elements of that set to form another element of the set (by adding numbers, composing symmetries, ...).

This second feature is known as a *binary operation*. The formal definition is as follows.

**Definition** Let $S$ be a set. Then a *binary operation* $*$ on $S$ is a map

$$S \times S \to S, \qquad (x, y) \mapsto x * y.$$

**Examples**

1. The arithmetic operations $+$, $-$, $\times$, are binary operations on suitable sets of numbers (such as $\mathbb{R}$).

2. Matrix addition and multiplication are binary operations on the set of all $n \times n$ matrices.

3. Vector addition and subtraction are binary operations on $\mathbb{R}^n$.

4. The vector product, or cross product, $(a, b, c) \times (x, y, z) := (bz - cy, cx - az, ay - bx)$ is a binary operation on $\mathbb{R}^3$.

5. Composition of symmetries is a binary operation on the set of symmetries of a triangle, square, cube, ...

**Remark** Part of the definition of a binary operation on a set $S$ is that it takes values in the set $S$. That is, $x * y \in S$ whenever $x \in S$ and $y \in S$. This property is sometimes expressed as: '$S$ is *closed* with respect to $*$'. The notion becomes important when we consider restricting a binary operation to subsets of the set on which it was originally defined.

If $T \subset S$ and $*$ is a binary operation on $S$, then $*$ is a map $S \times S \to S$, and $T \times T$ is a subset of $S \times S$, so we can consider the restriction of the map $* : S \times S \to S$ to $T \times T$. For $x, y \in T$, we have $x * y \in S$, but not in general $x * y \in T$. We say that a subset $T \subset S$ is *closed with respect to* $*$ if

$$\forall\, x, y \in T \quad x * y \in T.$$

If $T \subset S$ is closed with respect to $*$, then we can consider the restriction of $*$ to $T \times T$ as a map $T \times T \to T$, in other words as a binary operation on $T$.

**Examples**

1. The set $2\mathbb{Z}$ of even integers is closed with respect to the binary operation of addition. In other words, the sum of two even integers is an even integer. ($2m + 2n = 2(m + n) \in 2\mathbb{Z}$.)

2. The set $\mathbb{Z} \setminus 2\mathbb{Z}$ of all odd integers is **not** closed with respect to addition. For example, 5 and $-13$ are odd integers, but $5 + (-13) = -8$ is an even integer.

## 1.4 Cayley tables

A binary operation $*$ on a *finite* set $S$ can be displayed in the form of an array, called the *Cayley* table.

If $S$ has $n$ elements, then the Cayley table is an $n \times n$ array, with each row and each column labelled (uniquely) by an element of $S$.

The entry of the table in row $x$ and column $y$ is the element $x * y \in S$.

Here is a simple example: $S = \{0, 1\}$, and $*$ is just multiplication of numbers.

| * | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

## 1.5 Definition of a group

A *group* $(G, *)$ consists of a set $G$ and a binary operation $*$ on $G$, satisfying the following 3 axioms:

(i) $*$ is *associative.* This means that

$$(\forall\ x, y, z \in G) \quad x * (y * z) = (x * y) * z.$$

(ii) $G$ contains an element $e$ (or $e_G$) which is an *identity* for the binary operation $*$. This means that

$$(\forall x \in G) \quad x * e = x = e * x.$$

(iii) Each element $x \in G$ has an *inverse* $\overline{x}$ (or $x^{-1}$) in $G$. This means that

$$x * \overline{x} = e_G = \overline{x} * x.$$

**Remark** As mentioned above, it is implicit in the definition of a binary operation that $G$ is closed with respect to $*$. Some textbooks explicitly state as a fourth axiom in the definition of a group that $G$ is closed with respect to $*$.

**Definition** A group $(G, *)$ is said to be *abelian* if the binary operation $*$ on $G$ is *commutative.* This means that

$$(\forall\ x, y \in G) \quad x * y = y * x.$$

**Warning!** The commutative property of the binary operation is *not* one of the axioms in the definition of a group. There are many examples of groups which are not abelian. The smallest of these is the group of symmetries of an equilateral triangle. As an exercise, convince yourself of the following:

- Let $\alpha$ and $\beta$ denote the reflections in two of the axes of symmetry of an equilateral triangle. Then $\alpha \circ \beta \neq \beta \circ \alpha$.

## 1.6 Exercises

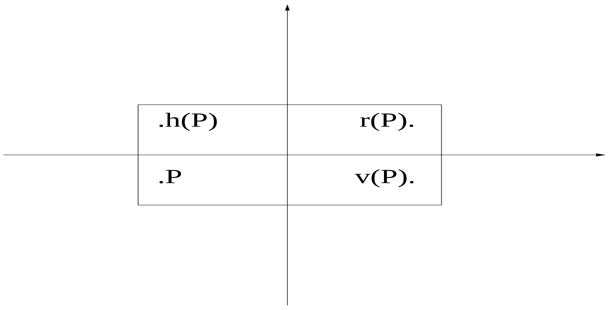
1. Which of the following binary operations on the set $\mathbb{Z}$ of integers is associative? Which is commutative? Which has an identity?

   (a) Subtraction $(x, y) \mapsto x - y$.

   (b) Exponentiation $(x, y) \mapsto x^y$.

   (c) The binary operation $*$ defined by $x * y = xy - x - y + 2$.

2. Let $R$ denote the rectangle $\{(x, y) \in \mathbb{R}^2;\ |x| \leq 2,\ |y| \leq 1\}$. in the plane.



   There are precisely four symmetries of $R$:

   (a) the identity symmetry $e : (x, y) \mapsto (x, y)$;

   (b) the reflection $h : (x, y) \mapsto (x, -y)$ in the $x$-axis;

   (c) the reflection $v : (x, y) \mapsto (-x, y)$ in the $y$-axis;

   (d) the rotation $r : (x, y) \mapsto (-x, -y)$ through $\pi$ around the origin.

   Write down the Cayley table of the symmetry group of $R$. Is this group abelian?

3. Which of the following are groups?

   (a) $(\mathbb{Z}, -)$, where $\mathbb{Z}$ is the set of integers, and $-$ is subtraction.

   (b) $(\mathbb{R}, *)$, where $\mathbb{R}$ is the set of real numbers and $*$ is the binary operation defined by $x * y := x + y - 1$.

   (c) $(G, \dagger)$, where $G$ is the set $\{1, 2, 3, 4\}$ and $x \dagger y$ is defined to be the remainder on dividing $xy$ by 5.

   (d) $(H, \ddagger)$, where $H$ is the set $\{1, 2, 3, 4, 5\}$ and $x \ddagger y$ is defined to be the remainder on dividing $xy$ by 6.

# Chapter 2

# More on groups

## 2.1 Examples of groups

1. $(\mathbb{Z}, +)$ is a group. Certainly, the sum of two integers is an integer, so $+$ is a binary operation on $\mathbb{Z}$ (ie $\mathbb{Z}$ is closed with respect to $+$). We also know that addition of numbers satisfies the associative rule. The integer 0 plays the rôle of the identity element:

   $$n + 0 = n = 0 + n \ \ \forall\, n \in \mathbb{Z}.$$

   Finally, if $n$ is an integer, then the integer $-n$ plays the rôle of its inverse:

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

   Hence $(\mathbb{Z}, 0)$ satisfies all the axioms, so it is a group. This group is abelian, since addition of numbers is commutative.

2. In the same way, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are groups. These groups are also abelian.

3. $(\mathbb{N}, +)$ is *not* a group. It does not satisfy the inverse axiom; for example, $5 \in \mathbb{N}$ has no inverse in $\mathbb{N}$ with respect to $+$.

4. The one-element set $\{e\}$ is a group with respect to the unique binary operation $(e, e) \mapsto e$ on it. This is called the *trivial group*.

5. The *cyclic group* of order $n$ is a group denoted $(\mathbb{Z}_n, +)$. As a set,

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

   The binary operation $+$ is not the usual addition of numbers, but is *addition modulo n*. To compute $a + b$ in this group, add the integers $a$ and $b$, divide the result by $n$, and take the remainder.

   The axioms for this group are easy to check. The operation $+$ is associative, because addition of numbers is associative. The element 0 acts as an identity. 0 is also the inverse of 0, and for $a \neq 0$ the inverse of $a$ is just $n - a$.

The group $(\mathbb{Z}_n, +)$ is finite, so we can write down its Cayley table. Here is what it looks like when $n = 5$:

| + | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

The group $(\mathbb{Z}_n, +)$ is abelian, since addition of numbers is commutative.

6. Let $X$ be a set, and let $S(X)$ be the set of all *permutations* of $X$, in other words, all bijective maps $X \to X$. Then $(S(X), \circ)$ is a group, where $\circ$ denotes composition of maps. The composite of two bijective maps is bijective, so $S(X)$ is closed with respect to $\circ$; we know that composition of maps is associative; the identity map $id_X : x \mapsto x \ \forall \ x \in X$ is an identity for this group; and every bijective map has an inverse, which is also bijective. So the group axioms are satisfied in this case.

   The group $(S(X), \circ)$ is called the *symmetric group on* $X$. In the case where $X$ is finite, with $n$ elements, we identify $X$ with the set $\{1, 2, \ldots, n\}$, and denote the symmetric group on $X$ by $S_n$. This group has $n!$ elements. Provided that $n > 2$, it is a nonabelian group.

   For example, consider the group of symmetries of an equilateral triangle. Any symmetry of the triangle determines a permutation of its three vertices. Conversely, any permutation of the vertices extends (uniquely) to a symmetry of the triangle, Hence the symmetry group of the equilateral triangle is essentially the same as $S_3$. (We will discuss what 'essentially the same' means in this context later.)

7. The unit circle $S^1 := \{z \in \mathbb{C} \ : \ |z| = 1\}$ in the complex plane is a group with respect to multiplication of complex numbers. The identity is the complex number 1, and the inverse of $z \in S^1$ is its complex conjugate.

8. The *general linear group* $GL_n(\mathbb{R})$ (or $GL(n, \mathbb{R})$) is the set of all invertible $n \times n$ matrices with real entries. It forms a group with respect to the binary operation of matrix multiplication. The product $AB$ of two invertible matrices is invertible, with inverse

$$(AB)^{-1} = B^{-1}A^{-1}.$$

   The group $GL_n(\mathbb{R})$ is not abelian if $n > 1$, since multiplication of matrices is not in general commutative. For example,

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

## 2.2 Cayley tables of groups

If $*$ is a binary operation on a finite set $S$, then properties of $*$ often correspond to properties of the Cayley table.

**Example** $*$ is commutative if $x * y = y * x$ for all $x, y \in S$. This means that the $(x, y)$-entry in the Cayley table is equal to the $(y, x)$-entry. In other words, the Cayley table is symmetric (assuming that the rows and columns are labelled in the same order). Conversely, if $*$ is not commutative, then the Cayley table will not be symmetric. So the Cayley table of an abelian group is symmetric, while that of a nonabelian group is not symmetric. For example, below is the Cayley tables of the nonabelian group $S_3$, also known as the symmetry group of the equilateral triangle. Here $e$ denotes the identity map, $\sigma, \tau$ are rotations, and $\alpha, \beta, \gamma$ are reflections.

| $\circ$ | $e$ | $\sigma$ | $\tau$ | $\alpha$ | $\beta$ | $\gamma$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $\sigma$ | $\tau$ | $\alpha$ | $\beta$ | $\gamma$ |
| $\sigma$ | $\sigma$ | $\tau$ | $e$ | $\beta$ | $\gamma$ | $\alpha$ |
| $\tau$ | $\tau$ | $e$ | $\sigma$ | $\gamma$ | $\alpha$ | $\beta$ |
| $\alpha$ | $\alpha$ | $\gamma$ | $\beta$ | $e$ | $\tau$ | $\sigma$ |
| $\beta$ | $\beta$ | $\alpha$ | $\gamma$ | $\sigma$ | $e$ | $\tau$ |
| $\gamma$ | $\gamma$ | $\beta$ | $\alpha$ | $\tau$ | $\sigma$ | $e$ |

A following property of Cayley tables of all groups is very useful.

**Definition** A *Latin square* of order $n$ is an $n \times n$ array, in which each entry is labelled by one of $n$ labels, in such a way that each label occurs exactly once in each row, and exactly once in each column.

Examples of Latin squares appear every day in newspapers, in the form of Sudoku puzzles. They also have more serious applications in the theory of experimental design.

**Lemma 1** *The Cayley table of any finite group is a Latin square.*

*Proof.* If the group $G$ has $n$ elements, then its Cayley table is, by definition, an $n \times n$ array, in which the entries are labelled by the $n$ elements of $G$. It remains to show that each element $g \in G$ appears exactly once in each row and in each column. We will show that $g$ appears exactly once in each row. The argument for columns is similar.

Suppose first that $g$ appears twice in row $x$. Then there are two distinct elements $y, z \in G$ such that $x * y = g = x * z$. Let $\overline{x}$ be the inverse of $x$ in $(G, *)$. Then

$$y = e_G * y = (\overline{x} * x) * y = \overline{x} * (x * y) = \overline{x} * g = \overline{x} * (x * z) = (\overline{x} * x) * z = e_G * z = z,$$

contrary to the assumption that $y, z$ are distinct.

Hence $g$ cannot appear twice in any row of the Cayley table. A similar argument applies to any other element of the group, so **no** element appears twice in the same row. But there are $n$ entries in each row, and $n$ possible labels for the entries. By the pigeonhole principle, if some label did not occur in a given row, then some other label would have to occur twice, which we have seen is impossible.

Hence each element of $G$ occurs exactly once in each row of the table. □

The Latin square property, together with the group axioms, often make it easy to complete a Cayley table given a small number of its entries. For example, consider the incomplete Cayley table for a group $(G, *)$.

| $*$ | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ |  | $a$ |  |
| $a$ |  |  |  |
| $b$ |  |  |  |

The only entry here tells us that $e * a = a$, so that $e$ must be the identity element. This allows us to fill in some more information:

| $*$ | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ |
| $a$ | $a$ |  |  |
| $b$ | $b$ |  |  |

Sudoku enthusiasts will have no difficulty completing the table now. We must put the label $b$ in one of the two empty slots in row $a$. But the $(a, b)$ slot is forbidden, since there is already a label $b$ in column $b$. So $b$ goes in the $(a, a)$ slot. There is now only one label free for the $(a, b)$ slot, namely $e$. Now each of the columns $a, b$ is complete except for one entry, and there is only one choice of label for the last empty position in each column.

The complete table is:

| $*$ | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ |
| $a$ | $a$ | $b$ | $e$ |
| $b$ | $b$ | $e$ | $a$ |

## 2.3 Homomorphisms and Isomorphisms

Here are the Cayley tables of two groups. In the group on the left, the elements are the two numbers $+1$ and $-1$, and the binary operation is multiplication. In the group on the right, the elements are the two residues $0, 1$ modulo 2, and the binary operation is addition modulo 2.

$(\{\pm 1\}, \cdot)$

| $\cdot$ | $+1$ | $-1$ |
|---|---|---|
| $+1$ | $+1$ | $-1$ |
| $-1$ | $-1$ | $+1$ |

$(\mathbb{Z}_2, +)$

| $+$ | $0$ | $1$ |
|---|---|---|
| $0$ | $0$ | $1$ |
| $1$ | $1$ | $0$ |

Although these groups are different, in the sense that the underlying sets are not equal and the binary operations are differently defined, it is clear that their Cayley tables have a similar pattern. In each case, the diagonal entries are equal to the identity element of the group, and the off-diagonal entries are equal to the non-identity element of the group.

Looked at in another way, if we relabel the elements of the first group by elements of the second group, then the Cayley table of the first will be changed to the Cayley table of the second. Thus we can think of these two groups as being really the same, up to a relabelling off the elements. When this happens, we say that the two groups are *isomorphic*, and regard them as being *essentially the same*.

The relabelling function is a bijection between the underlying sets of the two groups concerned. This function is known as an *isomorphism*. We develop a formal definition as follows.

**Definition** Let $(G, *)$ and $(H, \dagger)$ be groups. A *homomorphism* from $(G, *)$ to $(H, \dagger)$ is a map $f : G \longrightarrow H$ such that

$$(\forall\ x, y \in G) \quad f(x * y) = f(x) \dagger f(y).$$

An *isomorphism* from $(G, *)$ to $(H, \dagger)$ is a bijective homomorphism $f : G \longrightarrow H$. If an isomorphism from $(G, *)$ to $(H, \dagger)$ exists, then we say that the groups $(G, *)$ and $(H, \dagger)$ are *isomorphic*, which is denoted $(G, *) \cong (H, \dagger)$, or sometimes just $G \cong H$.

**Examples**

1. Let $V, W$ be two vector spaces. Then any linear map $\phi : V \longrightarrow W$ is a homomorphism from $(V, +)$ to $(W, +)$.

2. The set $\mathbb{R}_+ := \{x \in \mathbb{R}; x > 0\}$ of positive real numbers forms a group with respect to multiplication. Moreover, the exponential map $exp : \mathbb{R} \longrightarrow \mathbb{R}_+$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}_+, \cdot)$. It is certainly a bijection, with inverse $ln : \mathbb{R}_+ \longrightarrow \mathbb{R}$. The fact that is a homomorphism is just the familiar property $exp(x + y) = exp(x)exp(y)$ of exponentials.

3. If $(G, *)$ is any group, then the identity map $G \longrightarrow G$ is an isomorphism from $(G, *)$ to $(G, *)$.

4. The inclusion map $\mathbb{Z} \hookrightarrow \mathbb{R}$, $n \mapsto n$, is a homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{R}, +)$.

5. The map $f : \mathbb{Z} \to \mathbb{Z}_n$, $f(k) = k \bmod n$, is a homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}_n, +)$.

6. The set $\mathbb{R} \setminus \{0\}$ of nonzero real numbers is a group with respect to multiplication. The determinant map $det : GL_n(\mathbb{R}) \to \mathbb{R} \setminus \{0\}$ is a homomorphism. (This is just the familiar property $det(AB) = det(A)det(B)$ of determinants.

7. The map $x \mapsto (-1)^x$ is an isomorphism from $(\mathbb{Z}_2, +)$ to $(\{\pm 1\}, \cdot)$.

8. If $m \in \mathbb{Z}$, then the map $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = mn$, is a homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}, +)$.

9. If $x \in \mathbb{R} \setminus \{0\}$, then the map $f : \mathbb{R} \to \mathbb{R}$, $f(y) = xy$, is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}, +)$. The inverse isomorphism is the map $y \mapsto \frac{y}{x}$.

**Lemma 2** *Let $1 \leq n \leq 3$. Then any two groups containing exactly $n$ elements are isomorphic.*

*Proof.* I will leave most of the details of the proof as an exercise. The basic idea is that the Cayley table of a group with 3 or fewer elements is entirely determined by the Latin square property once we have decided which element is the identity in the group. (See the example at the end of the first part of these lecture notes.)

Specifically, if $n = 1$ and $G = \{e_G\}$, $H = \{e_H\}$, then the unique map $e_G \mapsto e_H$ is an isomorphism from $G$ to $H$. Similarly, if $n = 2$ and $G = \{e_G, a\}$, $H = \{e_H, x\}$ with $e_G, e_H$ the identity elements, then the map $e_G \mapsto e_H$, $a \mapsto x$ is an isomorphism from $G$ to $H$.

Finally, if $n = 3$ and $G = \{e_G, a, b\}$, $H = \{e_H, x, y\}$ with $e_G, e_H$ the identity elements, then the map $e_G \mapsto e_H$, $a \mapsto x$, $b \mapsto y$ is an isomorphism.

(Note that, in this last case, the choice of isomorphism is not unique: $e_G \mapsto e_H$, $a \mapsto y$, $b \mapsto x$ works equally well. In general, when two groups are isomorphic, there may be several choices of isomorphism between them.) □

## 2.4 Elementary properties of groups and homomorphisms

**Lemma 3** *Let $(G, *)$ be a group. Then*

1. *the identity element $e_G$ of $(G, *)$ is unique; and*

2. *for each $x \in G$, the inverse $\overline{x}$ of $x$ in $(G, *)$ is unique.*

3. (Cancellation laws) *If $a, b, c \in G$ with $a * c = b * c$, then $a = c$. Similarly, if $x, y, z \in G$ with $z * x = z * y$, then $x = y$.*

*Proof.*

1. If $e, f$ are two identity elements for $(G, *)$, then $e * f = e$ since $f$ is an identity element, while $e * f = f$ since $e$ is an identity element. Hence $e = e * f = f$.

2. Suppose that $y, z \in G$ are inverses for $x \in G$ in $(G, *)$. Then $y = y * e_G = y * (x * z) = (y * x) * z = e_G * z = z$.

3. Let $\overline{c}$ be the inverse of $c$ in $(G, *)$. If $a * c = b * c$, then $a = a * e_G = a * (c * \overline{c}) = (a * c) * \overline{c} = (b * c) * \overline{c} = b * (c * \overline{c} = b * e_G = b$. The second statement is proved in a similar way.

□

**Lemma 4** *Let $(G, *)$ and $(H, \dagger)$ be groups, and let $f : G \to H$ be a homomorphism from $(G, *)$ to $(H, \dagger)$. Then*

1. *$f(e_G) = e_H$, where $e_G, e_H$ are the identity elements for $(G, *)$ and $(H, \dagger)$ respectively.*

2. *If $\overline{x} \in G$ is the inverse of $x \in G$ in $(G, *)$, then $f(\overline{x})$ is the inverse of $f(x)$ in $(H, \dagger)$.*

*Proof.*

1. $e_G = e_G * e_G$, so $e_H * f(e_G) = f(e_G) = f(e_G * e_G) = f(e_G) \dagger f(e_G)$. By the cancellation law in $(H, \dagger)$, it follows that $e_H = f(e_G)$.

2. $f(x) \dagger f(\overline{x}) = f(x * \overline{x}) = f(e_G) = e_H$.

□

**Lemma 5** *Let $(G, *)$, $(H, \dagger)$ and $(K, \ddagger)$ be groups, and $\alpha : G \to H$, $\beta : H \to K$ be homomorphisms. Then $\beta \circ \alpha : G \to K$ is also a homomorphism. If $\alpha$ is an isomorphism, then so is $\alpha^{-1} : H \to G$. If $\alpha$ and $\beta$ are both isomorphisms, then so is $\beta \circ \alpha : G \to K$.*

*Proof.* Let $x, y \in G$. Then

$$(\beta \circ \alpha)(x * y) = \beta(\alpha(x * y)) = \beta(\alpha(x) \dagger \alpha(y)) = \beta(\alpha(x)) \ddagger \beta(\alpha(y)) = (\beta \circ \alpha)(x) \ddagger (\beta \circ \alpha)(y).$$

Hence $\beta \circ \alpha$ is a homomorphism, as claimed.

If $\alpha$ is an isomorphism, then it is a bijection, and there is an inverse map $\alpha^{-1} : H \to G$, which is also a bijection. To see that $\alpha^{-1}$ is an isomorphism, we only need to check that it is a homomorphism. With this in mind, let $x, y \in H$, and let $a = \alpha^{-1}(x)$, $b = \alpha^{-1}(y)$. Then $x = \alpha(a)$ and $y = \alpha(b)$. Since $\alpha$ is a homomorphism, we have

$\alpha(a * b) = \alpha(a) \dagger \alpha(b) = x \dagger y$. Hence $\alpha^{-1}(x \dagger y) = a * b = \alpha^{-1}(x) * \alpha^{-1}(y)$. Since this is true for arbitrary choices of $x, y \in H$, $\alpha^{-1}$ is indeed a homomorphism.

If $\alpha$ and $\beta$ are both isomorphisms, then they are both bijective, and so have inverses, $\alpha^{-1} : H \to G$ and $\beta^{-1} : K \to H$. Then

$$\alpha^{-1} \circ \beta^{-1} \circ \beta \circ \alpha = \alpha^{-1} \circ id_H \circ \alpha = \alpha^{-1} \circ \alpha = id_G,$$

and similarly $\beta \circ \alpha \circ \alpha^{-1} \circ \beta^{-1} = id_K$, so $\alpha^{-1} \circ \beta^{-1}$ is an inverse for $\beta \circ \alpha$. □

**Corollary 1** *The relation of isomorphism between groups is an equivalence relation.*

*Proof.* We need to check the three properties of equivalence relations: *reflexivity* ($G \cong G$ for any group $G$), *symmetry* ($G \cong H \Rightarrow H \cong G$), and *transitivity* ($G \cong H \cong K \Rightarrow G \cong K$).

**R** If $G$ is a group, then the identity map $id_G : G \to G$ is an isomorphism, so $G \cong G$.

**S** If $G \cong H$, then there is an isomorphism $\alpha : G \to H$, so $\alpha^{-1} : H \to G$ is also an isomorphism, and hence $H \cong G$.

**T** If $G \cong H$ and $H \cong K$, then there exist isomorphisms $\alpha : G \to H$ and $\beta : H \to K$, so $\beta \circ \alpha : G \to K$ is also an isomorphism, and hence $G \cong K$.

□

## 2.5 Exercises

1. Below is a partially completed Cayley table of a group. Fill in the missing parts of the table.

| $*$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | | | $d$ | |
| $b$ | $a$ | | | |
| $c$ | | | $b$ | |
| $d$ | | | | |

2. Which of the following maps are homomorphisms between the groups concerned?

   (a) $x \mapsto \ln|x|$, from $(\mathbb{R} \setminus \{0\}, \times)$ to $(\mathbb{R}, +)$. (Here, ln denotes the natural logarithm.)

   (b) $z \mapsto |z|$, from $(\mathbb{C}, +)$ to $(\mathbb{R}, +)$.

   (c) $x \mapsto 3x$, from $(\mathbb{Z}, +)$ to $(\mathbb{Z}, +)$.

   (d) $(x, y) \mapsto xy$, from $(\mathbb{R}^2, +)$ to $(\mathbb{R}, +)$.

   (e) $(x, y) \mapsto x - 2y$, from $(\mathbb{R}^2, +)$ to $(\mathbb{R}, +)$.

3. Given 2 groups $(G, *)$ and $(H, \dagger)$, their *direct product* is the set $G \times H$ consisting of all ordered pairs $(g, h)$ with $g \in G$ and $h \in H$, together with the binary operation $\cdot$ defined by

$$(g_1, h_1) \cdot (g_2, h_2) := (g_1 * g_2, h_1 \dagger h_2).$$

   (a) Show that $(G \times H, \cdot)$ is a group.

   (b) Show that each of the the maps

$$i_1 : G \to G \times H, \quad i_1(g) = (g, e_H),$$

$$i_2 : H \to G \times H, \quad i_2(h) = (e_G, h),$$

$$p_1 : G \times H \to G, \quad p_1(g, h) = g,$$

$$p_2 : G \times H \to H, \quad p_2(g, h) = h$$

   is homomorphism between the groups concerned.

   (c) Show that the groups $G \times H$ and $H \times G$ are isomorphic.

4. Suppose that $G$ is a finite group with $n$ elements, and $H$ is a group isomorphic to $G$. How many elements does $H$ have. Why?

5. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ and let $H = \mathbb{Z}_4$. Show that each of $G, H$ contains 4 elements. Show that each element of $G$ is its own inverse, and deduce that $G \not\cong H$.

6. Let $(G, *)$ be a *finite* group with identity $e$. If $a \in G$, write $a^2$ for $a * a$, $a^3$ for $a * a * a$, etc. Show that $a^i = a^j$ for some $i, j$ with $0 < i < j$. Deduce that $a^n = e$ for some $n > 0$.

7. Let $(G, *)$ be a group with identity $e$, containing a finite, even number of elements. By pairing off inverse elements, or otherwise, show that there is at least one element $a \neq e$ in $G$ such that $a * a = e$. [Hint: notice that $a * a = e$ if and only if $a$ is its own inverse.]

# Chapter 3

# Subgroups

## 3.1 What is a subgroup?

**Definition.** A *subgroup* of a group $(G, *)$ is a subset of $G$ which is also a group with respect to (the restriction of) the same binary operation $*$ as in $G$.

**Remark.** In particular, if $H$ is a subgroup of $(G, *)$, then the restriction of $*$ is a binary operation on $H$, in other words $H$ is closed with respect to $*$.

**Examples.**

1. $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are subgroups of $(\mathbb{C}, +)$.

2. If $n$ is a positive integer, then the set $n\mathbb{Z} := \{nk; k \in \mathbb{Z}\}$ of all multiples of $n$ is a subgroup of $(\mathbb{Z}, +)$.

3. The special linear group $SL_n(\mathbb{R})$ of $n \times n$ matrices with real entries and determinant 1 is a subgroup of the general linear group $GL_n(\mathbb{R})$ of all invertible $n \times n$ matrices with real entries.

4. We can regard the group $S_n$ of permutations of the set $\{1, 2, \ldots, n\}$ as a subgroup of the set $S_{n+1}$ of permutations of the set $\{1, 2, \ldots, n, n+1\}$, namely those permutations $\sigma \in S_{n+1}$ for which $\sigma(n+1) = n + 1$.

There is a simple way of determining when a given subset of a group is in fact a subgroup.

**Theorem 1** (The Subgroup Test) *Let $(G, *)$ be a group and $H \subset G$. Then $H$ is a subgroup of $G$ if and only if the following criteria are satisfied:*

*(i) $H$ is closed with respect to $*$, that is $(\forall\ x, y \in H)\ x * y \in H$;*

*(ii) the identity element $e_G$ of $G$ is contained in $H$;*

*(iii) for each $x \in H$, the inverse $\overline{x}$ of $x$ in $G$ is contained in $H$.*

*Proof.* Suppose first that the criteria (i), (ii) and (iii) are satisfied. Then by (i) the binary operation $*$ on $G$ restricts to a binary operation on $H$. This restriction is associative, because $*$ is associative. Since $e_G \in H$, $e_G$ acts as an identity for $(H, *)$. Finally, for each $x \in H$, since $\overline{x} \in H$, $\overline{x}$ acts as an inverse for $x$ in $(H, *)$.

Thus $(H, *)$ satisfies the axioms for a group. So $(H, *)$ is a group, in other words $H$ is a subgroup of $(G, *)$.

Conversely, suppose that $H$ is a subgroup of $(G, *)$. Then, as remarked above, $*$ must restrict to a binary operation on $H$, so $H$ must be closed with respect to $*$. Thus criterion (i) holds.

For criterion (ii), suppose that $e_H$ is the identity element of $(H, *)$. Then in $(G, *)$ we have equations

$$e_H * e_H = e_H = e_H * e_G.$$

Cancelling $e_H$ from the equation $e_H * e_H = e_H * e_G$ gives $e_H = e_G$. In particular, $e_G \in H$, so (ii) is satisfied.

Finally, suppose that $x \in H$ and let $x'$ denote the inverse of $x$ in $(H, *)$. Then in $G$ we have the equations

$$x * x' = e_H = e_G = x * \overline{x}.$$

Cancelling $x$ from the equation $x * x' = x * \overline{x}$ gives $x' = \overline{x}$. In particular, $\overline{x} \in H$, so (iii) is satisfied. □

**Examples.**

1. If $(G, *)$ is a group with identity element $e_G$, then $G$ and $\{e_G\}$ are subgroups of $(G, *)$. The criteria of the subgroup test are easily checked.

2. Let us check the criteria of the subgroup test in the case of the subgroup $n\mathbb{Z}$ of $(\mathbb{Z}, +)$, where $n$ is a positive integer. Firstly, $n\mathbb{Z}$ is closed with respect to addition, since $nk + n\ell = n(k + \ell) \in n\mathbb{Z}$. Secondly, the identity element, $0 = n \cdot 0$ belongs to $n\mathbb{Z}$. Finally, the inverse of $nk$ in $(\mathbb{Z}, +)$ is $-nk = n(-k) \in n\mathbb{Z}$.

3. Consider the cyclic group $(\mathbb{Z}_3, +)$. We already know that there are at least two subgroups of this group, namely $\mathbb{Z}_3$ itself and $\{0\}$. If $H \neq \{0\}$ is a subgroup, then $0 \in H$, so $H$ must also contain an element other than 0, ie 1 or 2. But if $1 \in H$ then $2 = 1 + 1 \in H$ since $H$ is closed. Similarly if $2 \in H$ then $1 = 2 + 2 \in H$. Thus $H = \mathbb{Z}_3$. Thus $\mathbb{Z}_3$ has precisely two subgroups, namely $\mathbb{Z}_3$ itself and the trivial subgroup $\{0\}$.

4. Now consider the cyclic group $(\mathbb{Z}_4, +)$. As in the previous example, if $H$ is a subgroup and $1 \in H$, then $2 = 1 + 1 \in H$ and $3 = 2 + 1 \in H$, so $H = \mathbb{Z}_4$. Similarly, if $3 \in H$ then $H = \mathbb{Z}_4$ since $2 = 3 + 3$ and $1 = 2 + 3$. Thus, if $H \neq \mathbb{Z}_4$ is a subgroup of $(\mathbb{Z}_4, +)$, then $\{0\} \subset H \subset \{0, 2\}$, so $H$ is either equal to the trivial

subgroup $\{0\}$ or to $\{0, 2\}$. It is easy to check that $\{0, 2\}$ satisfies the criteria of the subgroup test, so it is also a subgroup of $(\mathbb{Z}_4, +)$. Thus $(\mathbb{Z}_4, +)$ has precisely three subgroups: $\{0\}$, $\{0, 2\}$, and $\mathbb{Z}_4$.

5. Let $i \in \{1, 2, \ldots, n\}$, and define $H_i$ to be the subset $H_i = \{\sigma \in S_n;\ \sigma(i) = i\}$ of $S_n$. Then $H_i$ is a subgroup. To see this, let us check the criteria from the subgroup test

   - $H_i$ is closed: if $\sigma, \tau \in H_i$ then $(\sigma \circ \tau)(i) = \sigma(\tau(i)) = \sigma(i) = i$, so $\sigma \circ \tau \in H_i$.
   - The identity element $id$ belongs to $H_i$: $id(i) = i$.
   - if $\sigma \in H_i$, then $\sigma^{-1} \in H_i$. Suppose that $\sigma^{-1}(i) = j$. Then $\sigma(j) = i = \sigma(i)$. Since $\sigma$ is injective, $i = j$. Hence $\sigma^{-1}(i) = i$, in other words $\sigma^{-1} \in H_i$.

## 3.2 Cyclic subgroups

Let $(G, *)$ be a group and $a \in G$. In general, there are many subgroups of $(G, *)$ that contain the element $a$. However it turns out that there is a unique smallest such subgroup, which we call the *cyclic subgroup* generated by $a$.

To construct this cyclic subgroup, we first define the *powers* of $a$ in $G$, $a^n$ for $n \in \mathbb{Z}$. For $n \geq 0$, we can define $a^n$ inductively: $a^0 = e_G$, the identity element of $G$; while $a^{n+1}$ is defined to be $a^n * a$. For $n < 0$ we can define $a^n = \overline{a}^{-n}$, where $\overline{a}$ is the inverse of $a$ in $(G, *)$.

**Definition.** The *cyclic subgroup* of $(G, *)$ *generated by* $a$ is the subset

$$\langle a \rangle := \{a^n;\ n \in \mathbb{Z}\}$$

of $G$.

**Lemma 6** *$\langle a \rangle$ is a subgroup of $(G, *)$ that contains $a$. If $H$ is another subgroup of $(G, *)$ that contains $a$, then $\langle a \rangle \subset H$.*

*Proof.* To show that $\langle a \rangle$ is a subgroup of $(G, *)$, we apply the subgroup test.

- To see that $\langle a \rangle$ is closed, we prove by induction on $|n|$ that $a^m * a^n = a^{m+n} \in \langle a \rangle$. For $n = 0$ this is trivial, since $a^0$ was defined to be the identity element of $(G, *)$. If $n > 0$ and $a^m * a^n = a^{m+n}$, then

$$a^m * a^{n+1} = a^m * (a^n * a) = (a^m * a^n) * a = a^{m+n} * a = a^{m+n+1}.$$

  Similarly, if $n < 0$ and $a^m * a^n = a^{m+n}$, then

$$a^m * a^{n-1} = a^m * (a^n * \overline{a}) = (a^m * a^n) * \overline{a} = a^{m+n} * \overline{a} = a^{m+n-1}.$$

- By definition, $e_G = a^0 \in \langle a \rangle$.

- By definition, if $x = a^n \in \langle a \rangle$, then $\overline{x} = a^{-n} \in \langle a \rangle$.

Clearly, by definition, $a = a^1 \in \langle a \rangle$.

Now suppose that $H$ is a subgroup of $(G, *)$ such that $a \in H$. We show by induction on $n$ that $a^n \in H$ for all $n \geq 0$. This is true for $n = 0$ since $a^0 = e_G \in H$ by the subgroup test. If $a^n \in H$ and $a \in H$, then $a^{n+1} = a^n * a \in H$ since $H$ is closed with respect to $*$. Finally, if $x = a^n \in H$, then $a^{-n} = \overline{x} \in H$ by the subgroup test. Hence $a^n \in H$ for all $n \in \mathbb{Z}$, so $\langle a \rangle \subset H$. □

**Remark.** It follows form the above proof that the map $\mathbb{Z} \longrightarrow \langle a \rangle$ defined by $n \mapsto a^n$ is a homomorphism. (This is the statement that $a^{m+n} = a^m * a^n$.) This homomorphism is surjective by definition. If the $a^n$ are pairwise distinct, then the homomorphism is also injective, and so an isomorphism. In this case, we have an isomorphism $\langle a \rangle \cong (\mathbb{Z}, +)$.

What happens if the $a^n$ are not pairwise distinct?

**Lemma 7** *Let $(G, *)$ be a group and let $a \in G$. Then precisely one of the following is true:*

1. $\langle a \rangle \cong (\mathbb{Z}, +)$;

2. $\langle a \rangle \cong (\mathbb{Z}_n, +)$ *for some integer* $n > 0$.

*In the second case, $n$ is the least positive integer for which $a^n = e_G$.*

*Proof.* We have already seen that $\langle a \rangle \cong (\mathbb{Z}, +)$ in the case where the $a^n$ are pairwise distinct.

Suppose then that $a^p = a^q$ for some distinct integers $p, q$ (with $p > q$, say). Since $a^{-q}$ is the inverse of $a^q$, we can write this as $a^{p-q} = e_G$. Hence $a^k = e_G$ for some $k > 0$.

Now let $n$ be the least positive integer such that $a^n = e_G$. Then it is easy to check that the map $\mathbb{Z}_n \longrightarrow \langle a \rangle$ defined by $t \mapsto a^t$ is an isomorphism. □

## 3.3 Orders of groups and elements

**Definition.** The *order* of a group $(G, *)$, is the number of elements in the set $G$, denoted $|G|$ (which may be infinite). Note that $|G| \geq 1$, since every group contains at least one element (the identity element).

**Remark.** If $G \cong H$, then $|G| = |H|$, since any isomorphism $G \longrightarrow H$ is a bijection.

**Definition.** The *order* of an element $a \in G$ in the group $(G, *)$ is the order of the cyclic subgroup $\langle a \rangle$ of $(G, *)$ generated by $a$. We write $|a|$ for $|\langle a \rangle|$.

**Remark.** We have seen that $\langle a\rangle$ is isomorphic either to $(\mathbb{Z},+)$ or to $(\mathbb{Z}_m,+)$ for some $m$. Moreover, in the second case, $m$ is the least positive integer such that $a^m$ is the identity element of $(G,*)$. Thus we have an alternative definition for the order of $a$:

$$|a| = \begin{cases} \text{the least positive integer } m \text{ such that } a^m = e_G; \text{ or} \\ \infty, \quad \text{if no such positive integer exists.} \end{cases}$$

**Examples.**

1. $|\mathbb{Z}_m| = m$ for any positive integer $m$.

2. In $(\mathbb{Z}_4,+)$ the orders of the elements are as follows: $|0| = 1$ since 0 is the identity element; $|2| = 2$, since $2 \neq 0$ but $2+2 = 0$; $|1| = 4$ since $1+1+1+1 = 0$ but $1 \neq 0$, $1+1 \neq 0$, $1+1+1 \neq 0$; and $|3| = 4$ for similar reasons.

3. $|GL_2(\mathbb{R})| = \infty$, since there are infinitely many invertible $2 \times 2$ matrices with real entries. In $GL(_2(\mathbb{R})$ the order of $A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ is 6, since $A^6 = I_2$ but $A^k \neq I_2$ for $1 \leq k \leq 5$. (Exercise: try this and see.)

## 3.4 Orders of subgroups

Consider the group $(\mathbb{Z}_4,+)$. This group has precisely three subgroups: the trivial subgroup $\{0\}$ of order 1; the cyclic subgroup $\langle 2\rangle = \{0,2\}$ of order 2, and the whole group $\mathbb{Z}_4$ of order 4.

The group $S_3$ has one element (the identity) of order 1, three elements of order 2, and two elements of order 3 (each the inverse of the other). It therefore has cyclic subgroups of orders 1, 2 and 3. It is not difficult to convince oneself that the only non-cyclic subgroup is the whole group $S_3$, which has order 6.

In both these examples, the order of any subgroup divides the order of the whole group. This is no accident, for the following reason.

**Theorem 2** (Lagrange's Theorem) *Let $(G,*)$ be a finite group, and let $H$ be a subgroup. Then $|G|$ is a multiple of $|H|$.*

By considering cyclic subgroups, we obtain the following consequence.

**Corollary 2** *Let $(G,*)$ be a finite group, and let $a \in G$. Then $|G|$ is a multiple of $|a|$.*

In order to prove Theorem 2, we introduce the idea of a *coset* of a subgroup.

**Definition.** Let $(G,*)$ be a group, $H$ a subgroup of $(G,*)$, and $x \in G$. Then the *right coset* of $H$ in $G$ represented by $x$ is the set

$$H * x := \{h * x;\ h \in H\} \subset G.$$

Similarly, the *left coset* of $H$ in $G$ represented by $x$ is the set

$$x * H := \{x * h;\ h \in H\} \subset G.$$

**Remark.** The element $x$ representing the coset $H * x$ (resp. $x * H$) is by no means unique. For example, whenever $x \in H$, then the left and right cosets represented by $x$ are equal to the subgroup $H$ itself: $x * H = H = H * x$. (For example, if $h \in H$ then $h * x \in H$, so $H * x \subset H$; moreover $h * \overline{x} \in H$, so $h = (h * \overline{x}) * x \in H * x$, and so $H \subset H * x$.)

**Example.** In $(\mathbb{Z}, +)$ the subgroup $2\mathbb{Z}$ has precisely two (right) cosets: the set $2\mathbb{Z} = 2\mathbb{Z} + 0$ of even numbers, and the set $2\mathbb{Z} + 1 = \mathbb{Z} \setminus 2\mathbb{Z}$ of odd numbers.

We next note some elementary properties of cosets, from which we will deduce Lagrange's Theorem, Theorem 2.

**Lemma 8** *Let $(G, *)$ be a group, and let $H$ be a subgroup of $(G, *)$. Then*

1. *For any $x, y \in G$, either $H * x = H * y$ or $(H * x) \cap (H * y) = \emptyset$.*

2. *For any $x \in G$, the map $r_x : H \to H * x$ defined by $r_x(h) = h * x$ is a bijection.*

*Proof.*

1. Suppose that $H * x \cap H * y \neq \emptyset$, and let $z \in H * x \cap H * y$. Then there are elements $h_1, h_2 \in H$ such that $z = h_1 * x = h_2 * y$. An arbitrary element of $H * x$ has the form $h * x$ for some $h \in H$. If $\overline{h_1}$ is the inverse of $h_1$ in $(G, *)$ then we have
$$h * x = h * \overline{h_1} * z = (h * \overline{h_1} * h_2) * y \in H * y,$$
so $H * x \subset H * y$. By a similar argument, $H * y \subset H * x$. Hence $H * x = H * y$ as claimed.

2. By definition, any element of $H * x$ has the form $h * x = r_x(h)$ for some $h \in H$, so $r_x$ is surjective. Suppose that $h_1, h_2 \in H$ with $r_x(h_1) = r_x(h_2)$. In other words, $h_1 * x = h_2 * x$. Cancelling $x$ from this equation gives $h_1 = h_2$, so $r_x$ is also injective.

□

*Proof of Theorem 2.* Suppose that $(G, *)$ is a finite group, and $H$ is a subgroup of $(G, *)$. Then there are only finitely many right cosets of $H$ in $G$: say $H * x_1, \ldots H * x_k$. Suppose that $|H| = m$. Then by the above lemma, each right coset $H * x_i$ is in one-to-one correspondence with $H$, so contains exactly $m$ elements. Moreover, the right cosets $H * x_i$ are pairwise disjoint (by the lemma), and their union is the whole of $G$, so $|G| = km = k|H|$, as claimed. □

## 3.5 Exercises

1. Explain why each of the following subsets of $\mathbb{Z}$ is **not** a subgroup of $(\mathbb{Z},+)$:

   (a) The set $\{2n+1;\ n \in \mathbb{Z}\}$ of all odd integers;

   (b) The set $\{n \in \mathbb{Z};\ n \geq 0\}$ of all non-negative integers;

   (c) The set $\{-2,-1,0,1,2\}$;

   (d) The empty set.

2. Let $S$, $T$ be subgroups of a group $G$. Show that $S \cap T$ is a subgroup of $G$.
   Is it also true that $S\ \cup\ T$ is always a subgroup of $G$?
   (Give a proof, if true, or a counterexample, if false.)

3. Let $G$, $H$ be groups, $G_0$ a subgroup of $G$, $H_0$ a subgroup of $H$, and $\phi\ :\ G\ \rightarrow\ H$ a homomorphism. Show that

   (a) $\phi(G_0)\ =\ \{\phi(x)\ ;\ x\ \in\ G_0\}$ is a subgroup of $H$;

   (b) $\phi^{-1}(H_0)\ =\ \{x\ \in\ G\ ;\ \phi(x)\ \in\ H_0\}$ is a subgroup of $G$.

4. Determine the orders of the following groups:

   (a) $(\mathbb{Z}_5,+)$;

   (b) $(\mathbb{Z},+)$;

   (c) $S_6$;

   (d) $GL(3,\mathbb{R})$.

5. Determine the orders of the following group elements:

   (a) 2 in $(\mathbb{Z}_{10},+)$;

   (b) $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ in $GL(2,\mathbb{R})$;

   (c) the identity element $e_G$ in an arbitrary group $G$;

   (d) $\pi$ in $(\mathbb{R},+)$.

6. Determine the *index* (that is, the number of right cosets) of the following subgroups in the corresponding groups:

   (a) $\{0,2,4\}$ in $(\mathbb{Z}_6,+)$;

   (b) $\mathbb{R}$ in $(\mathbb{C},+)$;

   (c) $3\mathbb{Z}$ in $(\mathbb{Z},+)$.

# Chapter 4

# Permutations

## 4.1 Notation for permutations

In this section of the notes, we will look more closely at the group $S_n$ of all permutations of the set $\{1, 2, \ldots, n\}$. There are two common notations for permutations.

**Matrix Notation.**

This notation expresses a permutation as a $2 \times n$ matrix. Here

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

denotes the permutation $\sigma$ defined by $\sigma(1) = a_1$, $\sigma(2) = a_2$, $\ldots$, $\sigma(n) = a_n$.

In this notation, for example, the 6 elements of $S_3$ are:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

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

This notation can be used to calculate the composite of two permutations, as in the following example.

**Example.** Let $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in S_3$.

Recall that $\sigma \circ \tau$ means 'do $\tau$ first, then do $\sigma$. In other words, $(\sigma \circ \tau)(i) = \sigma(\tau(i))$ for each $i$.

Thus $(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(3) = 1$; $(\sigma \circ \tau)(2) = \sigma(\tau(2)) = \sigma(2) = 3$; and $(\sigma \circ \tau)(3) = \sigma(\tau(3)) = \sigma(1) = 2$, and this tells us that

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

We could do this calculation by rearranging the columns of $\sigma$ so that its first row matches up with the second row of $\tau$:

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 3 & 2 \end{pmatrix}.$$

We can then form a $3 \times n$ matrix whose first two rows represent $\tau$ and whose second two rows represent $\sigma$:

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

Deleting the middle row gives us

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

We can also use the matrix notation to find the inverse of a given permutation. If $\sigma(i) = j$, then $\sigma^{-1}(j) = i$. Thus to find $\sigma^{-1}(j)$, we find the entry equal to $j$ in the second row of the matrix representing $\sigma$. Then $\sigma^{-1}(j)$ is the entry immediately above it, in the first row of the matrix.

Thus, if $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, then $\sigma^{-1}(1) = 3$, $\sigma^{-1}(2) = 1$, and $\sigma^{-1}(3) = 2$, so

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

To do this calculation systematically, we can first interchange the two rows of the matrix representing $\sigma$ to get a matrix representing $\sigma^{-1}$, and then rearrange the columns so that the resulting matrix appears in the standard form (with first row $1, 2, \cdots, n$):

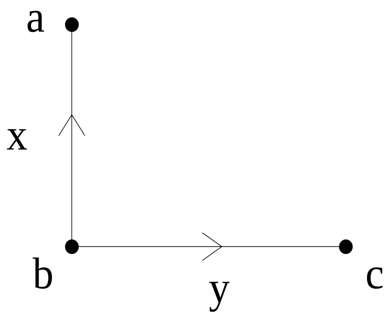
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rightarrow \quad \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} \quad \rightarrow \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

**The graph of a permutation.**

Before introducing the second type of notation for a permutation, I first want to introduce a pictorial way of representing permutations.

A *graph* consists of two sets $V, E$ of *vertices* and *edges* respectively, and two maps $i, t : E \to V$. We call $i(v)$ the *initial vertex* of the edge $e$, and $t(e)$ as the *terminal vertex* of $e$. We should think of the vertices as being points, and the edges as being line segments joining these points (with each edge carrying a specific *orientation* or *direction* from $i(e)$ towards $t(e)$). Many graphs can be drawn in the plane in this way; we usually represent the orientation of an edge by means of an arrow.

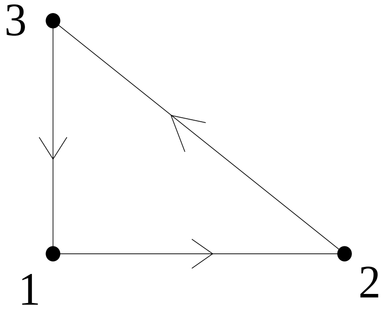
**Example.**



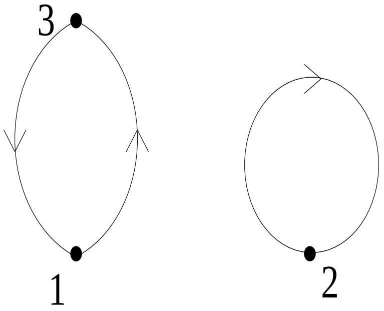
Graph with $V = \{a, b, c\}$, $E = \{x, y\}$, $i(x) = i(y) = b$, $t(x) = a$, $t(y) = c$.

Given a permutation $\sigma \in S_n$, we define the *graph* of $\sigma$ to be the graph with $V = E = \{1, 2, \ldots, n\}$, $i = id$ and $t = \sigma$.

**Example.** The graphs for the permutations $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in S_3$ look like



$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$



$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

The graph of a permutation has a special property. Because each of the maps $i = id, t = \sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ is a bijection, each vertex is the initial vertex of precisely one edge, and the terminal vertex of precisely one edge. This means that it splits naturally into a disjoint union of subgraphs known as *directed cycles.* A *directed cycle* of length $k$ is a graph with $k$ vertices $v_1, \ldots, v_k$ and $k$ edges $e_1, \ldots, e_k$, such that $i(e_j) = v_j$ for $1 \leq j \leq k$, $t(e_j) = v_{j+1}$ for $1 \leq j \leq k-1$, and $t(e_k) = v_1$.

In the above example, the graph of $\sigma$ is a single directed cycle of length 3, while the graph of $\tau$ consists of two directed cycles of length 1 and 2 respectively.

The graph of a permutation $\sigma$ indicates clearly the effect of $\sigma$ on any given element $j$ of $\{1, \ldots, n\}$: from the vertex $j$, follow the unique edge that leaves $j$. The terminal vertex of this edge is $\sigma(j)$. We can repeat this process to find $\sigma^2(j) = \sigma(\sigma(j))$: follow the unique *directed path* of length 2 that starts at $j$ (that is, the unique ordered pair $(e_1, e_2)$ of edges such that $i(e_1) = j$ and $i(e_2) = t(e_1) = \sigma(j)$). The end of this path is $t(e_2) = \sigma(i(e_2)) = \sigma(\sigma(j))$. More generally, the value of $\sigma^m(j)$ can be found by following the unique directed path of length $m$ starting at the vertex $j$ to its endpoint.

Note that this process always keeps us within the directed cycle that contains $j$. The set of vertices of this directed cycle is thus the same as the set of vertices $\{\sigma^m(j); m \geq 0\}$. This set is also called the *orbit* of $j$ under the permutation $\sigma$. The orbits of $\sigma$ form a *partition* of $\{1, \ldots, n\}$, just as the disjoint directed cycles in the graph of $\sigma$ give a partition of the vertices of that graph.

**Cycle notation.**

A permutation $\sigma \in S_n$ is a *$k$-cycle* if there are $k$ elements $a_1, a_2, \ldots, a_k \in \{1, 2, \ldots, n\}$ such that

- $\sigma(a_i) = a_{i+1}$ for $1 \leq i \leq k-1$;
- $\sigma(a_k) = a_1$;
- $\sigma(j) = j$ for all $j \notin \{a_1, a_2, \ldots, a_k\}$.

We use a shorthand notation $(a_1, a_2, \ldots, a_k)$ for the $k$-cycle $\sigma$ as described above.

Two cycles $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_\ell)$ are said to be *disjoint* if the sets $\{a_1, \ldots, a_k\}$ and $\{b_1, \ldots, b_\ell\}$ are disjoint, in other words if $(\forall\ i, j)\ a_i \neq b_j$.

**Lemma 9** *Disjoint cycles commute. If $\sigma = (a_1, \ldots, a_k)$ and $\tau = (b_1, \ldots, b_\ell)$ are disjoint cycles, then $\sigma \circ \tau = \tau \circ \sigma$.*

*Proof.* For $1 \leq i \leq k-1$ we have $\tau(a_i) = a_i$ since $a_i \notin \{b_1, \ldots, b_\ell\}$. Hence $(\sigma \circ \tau)(a_i) = \sigma(a_i) = a_{i+1}$. Also $(\tau \circ \sigma)(a_i) = \tau(a_{i+1}) = a_{i+1}$ since $a_{i+1} \notin \{b_1, \ldots, b_\ell\}$. Similar arguments show that

- $(\sigma \circ \tau)(b_j) = b_{j+1} = (\tau \circ \sigma)(b_j)$ for $1 \leq j \leq \ell - 1$;
- $(\sigma \circ \tau)(a_k) = a_1 = (\tau \circ \sigma)(a_k)$;
- $(\sigma \circ \tau)(b_\ell) = b_1 = (\tau \circ \sigma)(b_\ell)$.

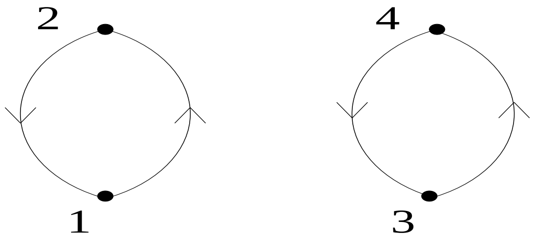
Finally, if $j \notin \{a_1, \ldots, a_k, b_1, \ldots, b_\ell\}$, then

$$(\sigma \circ \tau)(j) = \sigma(\tau(j)) = \sigma(j) = j = \tau(j) = \tau(\sigma(j)) = (\tau \circ \sigma)(j).$$

Hence $(\sigma \circ \tau)(j) = (\tau \circ \sigma)(j)$ for all $j \in \{1, \ldots, n\}$, and so $\sigma \circ \tau = \tau \circ \sigma$. □

The graph of a permutation indicates the partition of $\{1, \ldots, n\}$ into orbits of the permutation. On each orbit, the permutation acts as a cycle. Since the orbits are pairwise disjoint, they commute with one another, and their composite (in any order) is the permutation we started with.

**Example.** Consider the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$. The graph of $\sigma$ has the form



showing that $\sigma = (1,2) \circ (3,4) = (3,4) \circ (1,2)$.

**Definition.** The *cycle notation* for a permutation $\sigma$ is an expression of the form

$$(a_1, \ldots, a_k)(b_1, \ldots, b_\ell) \cdots (z_1, \ldots, z_m),$$

where

- $(a_1, \ldots, a_k), (b_1, \ldots, b_\ell) \ldots (z_1, \ldots, z_m)$ are disjoint cycles of lengths $\geq 2$; and
- $\sigma = (a_1, \ldots, a_k) \circ (b_1, \ldots, b_\ell) \circ \cdots \circ (z_1, \ldots, z_m)$.

**Remark.** In this notation, we suppress cycles of length 1, since a 1-cycle is just the identity element of $S_n$. We also suppress the binary operation $\circ$, which is understood.

**Remark.** There are two separate elements of non-uniqueness in cyclic notation.

Firstly, the order in which we write down the cycles is irrelevant, since disjoint cycles commute: $(a_1, \ldots, a_k)(b_1, \ldots, b_\ell) = (b_1, \ldots, b_\ell)(a_1, \ldots, a_k)$.

Secondly, within any given cycle, there is no fixed place to start and finish, although the *cyclic* order of elements within the cycle matters: $(a_1, a_2, a_3) = (a_2, a_3, a_1) = (a_3, a_1, a_2) \neq (a_1, a_3, a_2)$.

However, subject to these remarks, we can say that every permutation can be expressed 'essentially uniquely' in cyclic notation, ie as a product of pairwise disjoint cycles.

**Examples.**

1. Express $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix}$ in cycle notation.

   The actual cycle notation is not unique, but of all the possible choices, there is a systematic way to find the first choice in the *bibliographic* (=*dictionary*) ordering. First look at number 1. We see that $\sigma(1) \neq 1$, so 1 must appear in one of the cycles in the cycle notation for $\sigma$. We opt to write that cycle first, and to write 1 as the first entry in that cycle.

   Now $\sigma(1) = 3$ and $\sigma(3) = 1$ - the starting point of this cycle, so we deduce that $(1,3)$ is our first cycle.

   Next, look at the lowest number not yet to have been considered: 2. We see that $\sigma(2) = 2$, and so 2 does not appear in any of the cycles of $\sigma$. We ignore this number and move on.

So far, we have considered $1, 2, 3$, but not 4. We next look at number 4, and note that $\sigma(4) \neq 4$, so we must include 4 in one of our cycles. Since it is the lowest number not yet considered, we begin the next cycle with number 4. Now we see that $\sigma(4) = 5$, $\sigma(5) = 6$, and $\sigma(6) = 4$ - the starting point of this cycle. Thus $(4, 5, 6)$ is the second cycle.

At this point, all the numbers $1, \ldots, 6$ have been considered, so we can stop, and write

$$\sigma = (1, 3)(4, 5, 6).$$

2. Express $\tau = (1, 7, 2)(3, 4)(6, 9, 8) \in S_9$ in matrix form.

   This is easy. We only need to look at the cycle notation to see that $\tau(1) = 7$, $\tau(2) = 1$, $\tau(3) = 4$, $\tau(4) = 3$, $\tau(6) = 9$, $\tau(7) = 2$, $\tau(8) = 6$, and $\tau(9) = 8$. The missing piece of information is $\tau(5)$, but the very fact that 5 does not appear in any of the cycles means that $\tau(5) = 5$. Thus we know the value of $\tau(j)$ for all $j = 1, \ldots, 9$, and the matrix notation merely records that information:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 1 & 4 & 3 & 5 & 9 & 2 & 6 & 8 \end{pmatrix}.$$

Cycle notation is also useful in other respects. The inverse of a cycle $(a_1, \ldots, a_k)$ is just the same cycle written in the opposite direction: $(a_k, \ldots, a_1)$. Since disjoint cycles commute, we can invert any permutation written in cycle notation simply by inverting each of the cycles:

**Example.** If $\tau = (1, 7, 2)(3, 4)(6, 9, 8) \in S_9$, then $\tau^{-1} = (2, 7, 1)(4, 3)(8, 9, 6)$ (or, if we prefer, $\tau^{-1} = (1, 2, 7)(3, 4)(6, 8, 9)$).

It is also easy to calculate the order of a permutation written in cyclic form. It is clear that the order of a $k$-cycle $\sigma = (a_1, \ldots, a_k)$ is precisely $k$, since $\sigma^k = id$, but $\sigma^r(a_1) = a_{r+1} \neq a_1$ for $1 \leq r \leq k - 1$. Hence, if $\tau$ is a product of $t$ disjoint cycles of lengths $k_1, \ldots, k_t$ respectively, then $\tau^n = id$ if and only if $n$ divides $k_j$ for each $j$. Thus the order of $\tau$ is the lowest common multiple of the lengths of the cycles.

**Example.** Find the order of $\tau = (1, 2, 5, 8, 13)(3, 4, 9)(10, 12) \in S_{13}$ and hence express $\tau^{245}$ in cycle notation.

The order of $\tau$ is the lowest common multiple of $5, 3, 2$, ie 30. Hence $\tau^{30} = id$, so

$$\tau^{245} = id^8 \tau^5 = \tau^5 = (1, 2, 5, 8, 13)^5 (3, 4, 9)^5 (10, 12)^5 = (3, 9, 4)(10, 12).$$

## 4.2 The sign of a permutation

**Definition.** A permutation is called a *transposition* if it is a 2-cycle, in other words $(i, j)$ for some $i, j \in \{1, \ldots, n\}$ with $i \neq j$.

**Lemma 10** *Every permutation can be expressed as a composite of transpositions.*

*Proof.* We already know that every permutation can be expressed as a composite of (disjoint) cycles, so it is sufficient to show that any $k$ cycle ($k \geq 2$) can be expressed as a composite of transpositions. We do this by induction on $k$, where the initial case $k = 2$ is trivial: $(i, j)$ is the composite of a single transposition $(i, j)$.

Suppose that the lemma is true for any $k$-cycle, and consider the $k + 1$-cycle $(a_0, a_1, \ldots, a_k)$. We claim that

$$(a_0, a_1, \ldots, a_k) = (a_0, a_1) \circ (a_1, \ldots, a_k).$$

Since $(a_1, \ldots, a_k)$ is a composite of transpositions, by inductive hypothesis, it follows that $(a_0, a_1, \ldots, a_k)$ is also a composite of transpositions.

To prove the claim, note that

- $((a_0, a_1) \circ (a_1, \ldots, a_k))(a_0) = (a_0, a_1)(a_0) = a_1 = (a_0, a_1, \ldots, a_k)(a_0)$;
- $((a_0, a_1) \circ (a_1, \ldots, a_k))(a_j) = (a_0, a_1)(a_{j+1}) = a_{j+1} = (a_0, a_1, \ldots, a_k)(a_j)$ for $1 \leq j \leq k - 1$;
- $((a_0, a_1) \circ (a_1, \ldots, a_k))(a_k) = (a_0, a_1)(a_1) = a_0 = (a_0, a_1, \ldots, a_k)(a_k)$; and
- $((a_0, a_1) \circ (a_1, \ldots, a_k))(j) = (a_0, a_1)(j) = j = (a_0, a_1, \ldots, a_k)(j)$ for $j \notin \{a_0, a_1, \ldots, a_k\}$.

**Remark.** It is not in general true that a permutation is a composite of *pairwise disjoint* transpositions. Indeed, we can see from our discussion of the order of a permutation in cycle notation that a permutation is a composite of disjoint transpositions if and only if it has order 1 or 2 in $S_n$.

**Remark.** It is also not true that the expression of a given permutation as a composite of transpositions is unique. Indeed, not even the *number* of transpositions in this expression is unique, as the following example shows.

**Example.** In $S_3$, we have

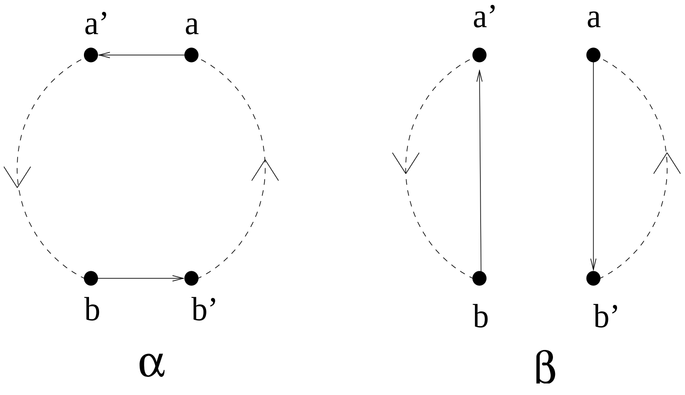
$$(1, 2) \circ (2, 3) \circ (3, 1) = (2, 3).$$

However, we can prove that the number of transpositions is unique modulo 2 (for a given permutation).

**Theorem 3** *Suppose that a permutation $\sigma \in S_n$ can be expressed as the composite of $k$ transpositions, and also as the composite of $k'$ transpositions. Then $k - k'$ is even.*

*Proof.* Suppose that $\alpha$ is a permutation, and $\tau = (a, b)$ is a transposition. The graph of $\alpha$ is a disjoint union of cycles (some of which may be cycles of length 1). Let $\ell$ be the number of cycles in the graph of $\alpha$. How many cycles does the graph of $\beta := \alpha \circ \tau$ have?

Since $\beta(j) = \alpha(j)$ for $j \notin \{a, b\}$, the graphs of $\alpha$ and $\beta$ are the same, except for the two edges beginning at $a$ and $b$. In the graph of $\alpha$, these edges go to $a' := \alpha(a), b' := \alpha(b)$ respectively, while in the graph of $\beta$ they go to $\beta(a) = \alpha(b) = b'$ and $\beta(b) = \alpha(a) = a'$ respectively.



If $a, b$ belong to the same cycle in the graph of $\alpha$ (as in the diagram above), then this cycle consists of

- a path (possibly of length 0) from $b'$ to $a$, followed by
- the edge from $a$ to $a'$, followed by
- a path (possibly of length 0) from $a'$ to $b$, followed by
- the edge from $b$ to $b'$.

In the graph of $\beta$, this cycle gets replaced by two shorter cycles, so the graph of $\beta$ has $\ell + 1$ cycles.

If, on the other hand, $a, b$ belong to different cycles in the graph of $\alpha$, then the situation is reversed: these two cycles get replaced by a single cycle in the graph of $\beta$, so the graph of $\beta$ has $\ell - 1$ cycles.

So, when we replace a permutation $\alpha$ by a new permutation $\alpha \circ \tau$ with $\tau$ a transposition, then the number of cycles in its graph changes by 1. In particular, changing the identity permutation $id \in S_n$ (whose graph consists of $n$ cycles of length 1) to a permutation $\sigma$ which is a composite of $k$ transpositions, we see that the number of cycles in the graph of $\sigma$ is congruent to $n + k$ modulo 2. Since both $n$ and the number of cycles in the graph of $\sigma$ are fixed, we see that $k \cong k'$ mod 2 if $\sigma$ can also be expressed as a composite of $k'$ transpositions. □

**Definition.** A permutation is called *even* if it is the composite of an even number of transpositions. It is called *odd* if it is the composite of an odd number of transpositions.

**Remark.** The proof that every permutation is a composite of transpositions actually shows that a $k$-cycle is a composite of $k-1$ transpositions:

$$(a_1, a_2, \dots, a_k) = (a_1, a_2) \circ \cdots \circ (a_{k-1}, a_k).$$

Hence we see that a $k$-cycle is an even permutation if and only if $k$ is an odd number.

More generally, if a permutation is expressed in cycle notation as the composite of $t$ cycles, of lengths $k_1, \dots, k_t$ respectively, then the parity of that permutation is the same as $k_1 + \cdots + k_t + t$.

**Examples.**

1. $(1,2,3) = (1,2) \circ (2,3)$ is even.
2. $(1,2,3,4,5) \circ (6,7) \circ (8,9,10,11) \circ (12,13,14,15,16,17)$ is odd.

If $\sigma \in S_n$ is a permutation, the *sign* of $\sigma$ is defined to be $\varepsilon(\sigma) = +1$ if $\sigma$ is even, and $\varepsilon(\sigma) = -1$ if $\sigma$ is odd. Recall that $\{\pm 1\}$ is a subgroup of $(\mathbb{R} \setminus \{0\}, \cdot)$: it is clear that $\varepsilon : S_n \to \{\pm 1\}$ is a homomorphism.

**Application: definition of determinant**

Let $A$ be an $n \times n$ matrix, and for each $i, j \in \{1, \dots, n\}$ let $a_{i,j}$ denote the $(i,j)$ entry of $A$. Then we can define the determinant of $A$ to be

$$det(A) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{k=1}^{n} a_{k,\sigma(k)}.$$

It is very easy to check that this definition agrees with the usual definition when $n = 2$, since $S_2 = \{id, (1,2)\}$ with $\varepsilon(id) = +1$ and $\varepsilon((1,2)) = -1$. The rule gives

$$det(A) = \varepsilon(id) a_{1,1} a_{2,2} + \varepsilon((1,2)) a_{1,2} a_{2,1} = a_{1,1} a_{2,2} - a_{1,2} a_{2,1}.$$

When $n = 3$ it is also not difficult to check that this definition agrees with the usual one:

$$\begin{gathered} det(A) = \varepsilon(id) a_{1,1} a_{2,2} a_{3,3} + \varepsilon((1,2,3)) a_{1,2} a_{2,3} a_{3,1} + \varepsilon((1,3,2)) a_{1,3} a_{2,1} a_{3,2} \\ + \varepsilon((1,2)) a_{1,2} a_{2,1} a_{3,3} + \varepsilon((1,3)) a_{1,3} a_{2,2} a_{3,1} + \varepsilon((2,3)) a_{1,1} a_{2,3} a_{3,2} \\ = a_{1,1}(a_{2,2} a_{3,3} - a_{2,3} a_{3,2}) - a_{2,1}(a_{1,2} a_{3,3} - a_{1,3} a_{3,2}) + a_{3,1}(a_{1,2} a_{2,3} - a_{1,3} a_{2,2}). \end{gathered}$$

For large $n$, a direct verification is harder, but one can check by induction on $n$ that the above definition agrees with the usual recursive definition.

## 4.3 Exercises

1. Write the following permutations in cycle notation:

$$(i)\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix};\ (ii)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 4 & 3 & 2 & 5 \end{pmatrix};\ (iii)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 3 & 6 & 2 \end{pmatrix}.$$

2. Write the following permutations in matrix notation:

$$(a)\ (1,2,3)(4,6,8);\ (b)\ (1,6)(4,2)(5,3);\ (c)\ (1,5,3);$$

$$(d)\ (2,4)(3,5,7);\ (e)\ (1,9,3)(2,6)(7,8).$$

3. Compute $\sigma \circ \tau$ and $\tau \circ \sigma$ where:

$$(a)\ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix},\ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix} \in S_5;$$

$$(b)\ \sigma = (1,2)(5,6),\ \tau = (1,3,4,6,2) \in S_6;$$

$$(c)\ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},\ \tau = (1,2)(3,4) \in S_4.$$

In each case, give your answer both in matrix and cycle notation.

4. Suppose that a permutation $\sigma$ is the product of $t$ disjoint cycles of lengths $k_1, \dots k_t$ respectively. Show that the order of $\sigma$ is the least common multiple of $k_1, \dots, k_t$. Deduce that no element of $S_5$ has order greater than 6.

5. (i) Determine how many elements of $S_3$ are cycles of length 2 and of length 3.
(ii) Show that $S_4$ contains precisely 6 cycles of length 2, 8 of length 3 and 6 of length 4.
(iii) Show that the remaining elements of $S_4$ form a subgroup $H$ of $S_4$.
(iv) What is the order of $H$? Is $H$ a cyclic group?

6. Determine which of the following permutations are even and which are odd:

$$(i)\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix};\ (ii)\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix};$$

$$(iii)\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix};\ (iv)\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 6 & 9 & 8 & 5 & 4 & 7 \end{pmatrix}.$$

7. Show that the composite of two odd permutations, or of two even permutations, is even, while the composite of an odd and an even permutation (in either order) is odd. Use this to define a surjective homomorphism $f$ from $S_n$ to the cyclic group of order 2.

# Chapter 5

# Groups of permutations

In this chapter we will consider groups of permutations of a (finite) set, which we may as well take to be $\{1, \dots, n\}$ for some $n$. Thus we are looking at subgroups of the group $S_n$ of *all* permutations of our finite set.

## 5.1 The alternating group

**Lemma 11** *Let $n \geq 2$. The set $A_n$ of all even permutations of $\{1. \dots, n\}$ is a subgroup of $S_n$. Moreover, $A_n$ has index 2 in $S_n$. (In other words, there are precisely two right cosets of $A_n$ in $S_n$.)*

*Proof.* We use the subgroup test to show that $A_n$ is a subgroup of $S_n$. Certainly $A_n$ is closed: if $\sigma, \tau$ are composites of $2k$, $2\ell$ transpositions respectively, then $\sigma \circ \tau$ is a composite of $2(k + \ell)$ transpositions. The identity permutation is the composite of 0 transpositions. Finally, if $\sigma$ is a composite $\tau_1 \circ \cdots \circ \tau_{2k}$ of $2k$ transpositions, then so is $\sigma^{-1} = \tau_{2k} \circ \cdots \circ \tau_1$.

Thus $A_n$ is a subgroup. If $\tau$ is a transposition, then for any odd permutation $\alpha$ we have $\beta := \alpha \circ \tau \in A_n$, and $\alpha = \beta \circ \tau$ (since $\tau^2 = id$). Hence the coset $A_n \circ \tau$ contains all odd permutations. Since $A_n$ contains all even permutations, $A_n \cup A_n \circ \tau = S_n$, so the only two right cosets of $A_n$ in $S_n$ are $A_n$ and $A_n \circ \tau = S_n \setminus A_n$. □

**Example.** $S_3 = \{id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$.

$A_3 = \{id, (1,2,3), (1,3,2)\} = \langle (1,2,3) \rangle \cong \mathbb{Z}_3$.

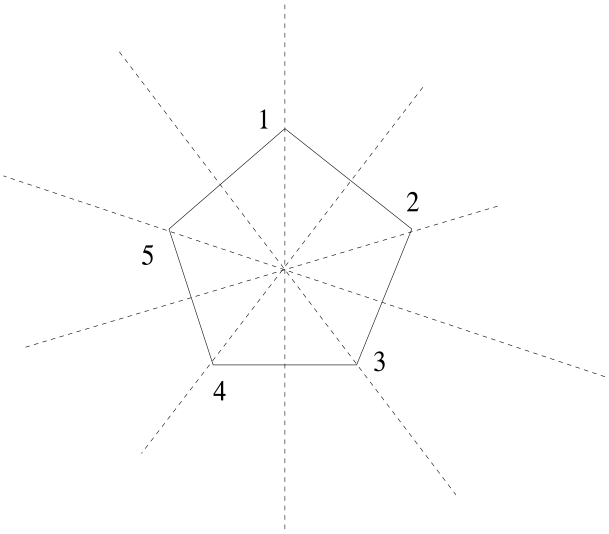
The group $A_n$ is know as the *alternating group of degree n*. It has order $n!/2$, since it is a subgroup of index 2 in the group $S_n$ of order $n!$.

## 5.2 The dihedral groups.

Let $n \geq 3$ be an integer, and let $P_n$ be a regular $n$-gon in the euclidean plane $\mathbb{R}^2$. Then there are precisely $2n$ symmetries of $P_n$: $n$ rotations around the centre of $P_n$

(including the identity element) and $n$ reflections in axes of symmetry of $P_n$. The group of symmetries of $P_n$ is denoted $D_n$, and called the *dihedral group* of order $2n$.

**Example.** Consider the regular pentagon $P_5$, with vertices numbered $1, 2, 3, 4, 5$ as in the diagram below.



The symmetry group of $P_5$ is the dihedral group $D_5$ of order 10. Any symmetry of $P_5$ restricts to a permutation of the 5 vertices of $P_5$, and indeed is determined by that permutation. Thus we can identify $D_5$ with a subgroup of $S_5$.

In these terms, the ten elements of $D_5$ are the identity element, the four nontrivial rotations $(1, 2, 3, 4, 5)$, $(1, 3, 5, 2, 4)$, $(1, 4, 2, 5, 3)$, $(1, 5, 4, 3, 2)$, and the five reflections $(1, 2)(3, 5)$, $(1, 3)(4, 5)$, $(1, 4)(2, 3)$, $(1, 5)(2, 4)$, $(2, 5)(3, 4)$.

Note also that $D_5$ contains an element of order 5, namely any of its rotations. Hence it contains a cyclic subgroup $C_5 = \langle(1, 2, 3, 4, 5)\rangle$ of order 5. This subgroup therefore has index 2: there are precisely two (right) cosets, $C_5$ and $C_5 \circ \rho$, where $\rho$ is any one of the reflections. (Indeed, the coset $C_5 \circ \rho$ consists precisely of the set of five reflections in $D_5$.)

More generally, the dihedral group $D_n$ of order $2n$ contains a rotation $a$ through an angle of $2\pi/n$. Thus $a$ has order $n$ in $D_n$, and so generates a cyclic subgroup $C_n = \langle a \rangle$ of order $n$ and index 2 in $D_n$. If $\tau$ is any of the reflections in $D_n$, then the coset $C_n \circ \tau = D_n \smallsetminus C_n$ consists of all the reflections in $D_n$. We can deduce two things from this:

- Every element of $D_n$ can be expressed uniquely as $a^k$ or $a^k \circ \tau$ for some $k = 0, 1, \ldots, n-1$.

- Each $a^k \circ \tau$ is a reflection in $D_n$, so has order 2. It follows that $\tau \circ a^{n-k}$, the inverse of $a^k \circ \tau$, is also equal to $a^k \circ \tau$. This in turn tells us how to compose arbitrary elements of $D_n$: for example, $(a^k \circ \tau) \circ (a^\ell \circ \tau) = a^{k-\ell}$ (where $k - \ell$ is computed modulo $n$).

The above remarks allow us to compute the complete Cayley table of $D_n$. In the case $n = 5$ this looks like:

| $\circ$ | $id$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $\tau$ | $a \circ \tau$ | $a^2 \circ \tau$ | $a^3 \circ \tau$ | $a^4 \circ \tau$ |
|---|---|---|---|---|---|---|---|---|---|---|
| $id$ | $id$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $\tau$ | $a \circ \tau$ | $a^2 \circ \tau$ | $a^3 \circ \tau$ | $a^4 \circ \tau$ |
| $a$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $id$ | $a \circ \tau$ | $a^2 \circ \tau$ | $a^3 \circ \tau$ | $a^4 \circ \tau$ | $\tau$ |
| $a^2$ | $a^2$ | $a^3$ | $a^4$ | $id$ | $a$ | $a^2 \circ \tau$ | $a^3 \circ \tau$ | $a^4 \circ \tau$ | $\tau$ | $a \circ \tau$ |
| $a^3$ | $a^3$ | $a^4$ | $id$ | $a$ | $a^2$ | $a^3 \circ \tau$ | $a^4 \circ \tau$ | $\tau$ | $a \circ \tau$ | $a^2 \circ \tau$ |
| $a^4$ | $a^4$ | $id$ | $a$ | $a^2$ | $a^3$ | $a^3 \circ \tau$ | $a^4 \circ \tau$ | $\tau$ | $a \circ \tau$ | $a^2 \circ \tau$ |
| $\tau$ | $\tau$ | $a^4 \circ \tau$ | $a^3 \circ \tau$ | $a^2 \circ \tau$ | $a \circ \tau$ | $id$ | $a^4$ | $a^3$ | $a^2$ | $a$ |
| $a \circ \tau$ | $a \circ \tau$ | $\tau$ | $a^4 \circ \tau$ | $a^3 \circ \tau$ | $a^2 \circ \tau$ | $a$ | $id$ | $a^4$ | $a^3$ | $a^2$ |
| $a^2 \circ \tau$ | $a^2 \circ \tau$ | $a \circ \tau$ | $\tau$ | $a^4 \circ \tau$ | $a^3 \circ \tau$ | $a^2$ | $a$ | $id$ | $a^4$ | $a^3$ |
| $a \circ \tau$ | $a^3 \circ \tau$ | $a^2 \circ \tau$ | $a \circ \tau$ | $\tau$ | $a^4 \circ \tau$ | $a^3$ | $a^2$ | $a$ | $id$ | $a^4$ |
| $a^4 \circ \tau$ | $a^4 \circ \tau$ | $a^3 \circ \tau$ | $a^2 \circ \tau$ | $a \circ \tau$ | $\tau$ | $a^4$ | $a^3$ | $a^2$ | $a$ | $id$ |

where, for example, we take $a = (1, 2, 3, 4, 5)$ and $\tau = (1, 2)(3, 5)$.

**Remark.** If we place our regular $n$-gon $P_n$ in the plane with its centre at the *origin* – that is, the vector $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ – then symmetries of $P_n$ extend to linear maps $\theta : \mathbb{R}^2 \to \mathbb{R}^2$ of a certain type known as *rigid motions*. This means that the map preserves the euclidean distance between points:

$$||\theta(u) - \theta(v)|| = ||u - v||.$$

A linear map is determined by a matrix: $\theta(v) = Av$ where $A \in GL_2(\mathbb{R})$, and rigid motions are defined by matrices which are *orthogonal*: $A^T A = I_2 = AA^T$, where $A^T$ denotes the transpose of $A$. The orthogonality of $A$ means that $A$ preserves the *inner product* (also known as the *dot product*) of vectors: $(Au)^T(Av) = u^T A^T Av = u^T v$, and hence also the norm, and hence also the euclidean distance.

Note also that an orthogonal matrix $A$ satisfies

$$det(A)^2 = det(A^T)det(A) = det(A^T A) = det(I_2) = 1,$$

so $det(A) = \pm 1$. In particular, $2 \times 2$ orthogonal matrices fall into two categories: the *rotation matrices*

$$\begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix},$$

of determinant $+1$, and the *reflection* matrices

$$\begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix},$$

of determinant $-1$.

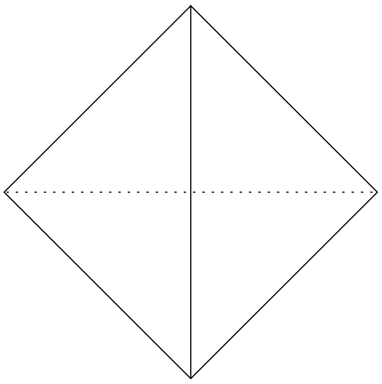
For example, if $P_3$ is an equilateral triangle with centre at the origin, such that the $y$-axis is an axis of symmetry, then the 6 matrices defining symmetries of $P_3$ are:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

## 5.3 Symmetry groups of 3-dimensional figures

Just as the symmetries of polygons in the plane are determined by their action on the vertices of the polygon, the same applies to symmetries of 3-dimensional polyhedra, so the symmetry groups of the polyhedra can be identified with subgroups of the appropriate $S_n$.

**Example.** Let $T$ be a *regular tetrahedron* in $\mathbb{R}^3$. This is a pyramid whose base is an equilateral triangle, and all its sides are also equilateral triangles. For example, there is such a $T$ with vertices $(1,1,1)$, $(1,-1,-1)$, $(-1,1,-1)$ and $(-1,-1,1)$ (any two of which are $2\sqrt{2}$ apart) and centre of gravity at the origin.



Any symmetry of $T$ determines a permutation of its four vertices, and conversely any permutation of the vertices extends uniquely to a symmetry of $P$. Hence the symmetry group of $T$ is isomorphic to $S_4$.

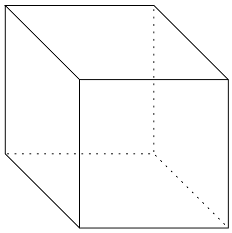
Just as in the 2-dimensional case, symmetries of $T$ can be represented by orthogonal $3 \times 3$ matrices, so we can also identify the symmetry group of $T$ with a subgroup of $GL_3(\mathbb{R})$. For example, the orthogonal matrix

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

represents a symmetry of $T$.

**Exercise:** Work out how this matrix permutes the vertices of $T$.

**Example.** Let $C = [-1,1]^3$. In other words, $C$ is the cube with vertices $(\pm 1, \pm 1, \pm 1)$. As in the previous example, any symmetry of $C$ determines a permutation of the 8 vertices of $C$, so we can identify the symmetry group of $C$ with a subgroup of $S_8$. In this case, however, it is not the whole of $S_8$: not every permutation of the vertices extends to a symmetry of the cube because, for example, symmetries also have to map edges to edges, and faces to faces.



Indeed, a symmetry of $C$ also permutes the six faces of $C$, so we can equally well consider the symmetry group to be a subgroup of $S_6$. Again, it is not the whole of $S_6$, because for example a symmetry has to map a pair of opposite faces to a pair of opposite faces, and not every permutation of faces will have that property.

Again, the symmetries of $C$ can be defined by orthogonal matrices, so the symmetry group is isomorphic to a subgroup of $GL_3(\mathbb{R})$.

Can we get a clearer understanding of what this symmetry group looks like? For example, what is its order? One way to work this out is to consider a face $F$ of $C$. Then $F$ is a square, so the symmetry group of $F$ is the dihedral group $D_4$ of order 8. Every symmetry of $F$ can be extended (uniquely) to a symmetry of $C$, so there is a subgroup $H$ of the symmetry group of $C$ that is isomorphic to $D_4$. Indeed, $H$ is the subgroup of symmetries $\alpha$ such that $\alpha(F) = F$. Since symmetries of $C$ permute the 6 faces of $C$, the subgroup $H = \{\alpha; \alpha(F) = F\}$ has index 6, so the whole symmetry group has order $6 \cdot 8 = 48$.

If $G$ is the symmetry group of $C$, consider the following two homomorphisms. Firstly, we get a (surjective) homomorphism $\phi : G \to S_4$ by noticing that symmetries of $C$ permute the four diagonals of $C$. Secondly, we get a homomorphism $\psi : G \to \{\pm 1\}$ by letting $\psi(\alpha) = \pm 1$ be the determinant of the orthogonal matrix representing $\alpha$. It turns out that, by putting these together, we get an isomorphism $G \to S_4 \times \{\pm 1\}$, $\alpha \mapsto (\phi(\alpha), \psi(\alpha))$.

## 5.4 Cayley's Theorem

The following result tells us that, in one sense, the whole of group theory is about understanding the subgroups of permutation groups.

**Theorem 4** *Let $(G, *)$ be a group. Then there is a set $X$ such that $(G, *)$ is isomprohic to a subgroup of the group $(S(X), \circ)$ of all permutations of $X$. If $|G| < \infty$ then $X$ may be chosen to be a finite set (so that $(G, *)$ is isomorphic to a subgroup of $S_n$ for some integer $n$).*

*Proof.* We choose $X$ to be the set $G$. Suppose that $g \in G$, and consider the map $\lambda_g : X \to X$ defined by $\lambda_g(x) = g * x$. (In other words, $\lambda_g$ is 'left multiplication by $g$'.)

First note that $\lambda_g$ is injective, by the cancellation property:

$$\lambda_g(x_1) = \lambda_g(x_2) \Rightarrow g * x_1 = g * x_2 \Rightarrow x_1 = x_2.$$

It is also true that $\lambda_g$ is surjective: if $y \in X$ and $\overline{g}$ is the inverse of $g$ in $(G, *)$, then

$$y = g * \overline{g} * y = \lambda_g(\overline{g} * y).$$

Hence $\lambda_g$ is a permutation of $X$.

Secondly, we claim that all the permutations of $X$ that arise in this way form a subgroup $H$ of $(S(X), \circ)$. This follows easily from the subgroup test.

- $(\lambda_g \circ \lambda_h)(x) = g * h * x = \lambda_{g*h}(x)$ for all $x \in X$, so $\lambda_g \circ \lambda_h = \lambda_{g*h}$, and $H$ is closed with respect to $\circ$.
- If $e$ is the identity element of $G$, then $\lambda_e(x) = e * x = x$ for all $x \in X$, so $\lambda_e = id$, the identity element of $(S(X), \circ)$.
- If $\overline{g}$ is the inverse of $g$ in $(G, *)$, then $(\lambda_g \circ \lambda \overline{g})(x) = g * \overline{g} * x = x$ for all $x \in X$, so $\lambda_g \circ \lambda_{\overline{g}} = id$. Similarly, $\lambda_{\overline{g}} \circ \lambda_g = id$, so $\lambda_{\overline{g}}$ is the inverse of $\lambda_g$ in $(S(X), \circ)$.

Finally, we claim that this subgroup $H$ of $(S(X), \circ)$ is isomorphic to $(G, *)$. The map $\theta : G \to H$ defined by $\theta(g) = \lambda_g$ for all $g \in G$ is surjective, since $H$ is by definition the set of all the $\lambda_g$. But $\theta$ is also injective, because

$$\theta(g) = \theta(h) \Rightarrow g = \theta(g)(e) = \theta(h)(e) = h.$$

We have already noted that

$$\theta(g) \circ \theta(h) = \lambda_g \circ \lambda_h = \lambda_{g*h} = \theta(g * h),$$

in other words, $\theta$ is a homomorphism from $(G, *)$ to $(H, \circ)$. Thus $\theta$ is a bijective homomorphism, ie an isomorphism, and $G \cong H$ as claimed. □

**Remark.** This result is interesting from a theoretical point of view, but in practice it does not help us to understand a particular group, because the size of the set $X$ arising in the proof of the theorem is usually much bigger than is really necessary. For example, in the case of the group of symmetries of a cube (which has order 48), the proof of Cayley's Theorem tells us that this group is isomorphic to a subgroup of $S_{48}$ – a group of order $48! \sim 10^{61}$.

However, we have already noticed that symmetries of the cube permute the faces of the cube, so that the group of symmetries is isomorphic to a subgroup of $S_6$. Since $S_6$ has order only 720, we have more chance of understanding $S_6$ than $S_{48}$. Moreover, we have also seen that the group of symmetries of a cube is isomorphic to $S_4 \times \mathbb{Z}_2$, in which form it is even easier to understand.

## 5.5 Exercises

1. How many elements of order 2 are there in each of the following groups: (i) $\mathbb{Z}_6$; (ii) $S_3$; (iii) $A_4$; (iv) $D_5$; (v) $D_6$. How many elements of order 3 are there in the same groups?

2. Show that the group $A_5$ contains no elements of order 4, and precisely 15 elements of order 2. How many elements of are there of orders 1, 2, 3, 6 respectively? What is the order of $A_5$?

3. In the dihedral group $D_n$, suppose that $\alpha$ is a rotation and that $\rho$ is a reflection. Use the fact that $\alpha \circ \rho$ is also a reflection, together with the fact that reflections have order 2, to show that $\alpha \circ \rho \circ \alpha$ is the inverse of $\rho$.

4. Suppose that $n \geq 3$ and that $\phi : S_n \to \mathbb{Z}_3$ is a homomorphism. Show that $\phi(\tau) = 0$ for every transposition $\tau \in S_n$, and deduce that $\phi(\sigma) = 0$ for all $\sigma \in S_n$.

5. Let $C$ be the group of symmetries of a cube, and let $v$ be one of the vertices of the cube. Show that the set of symmetries $\alpha$ that *fix* $v$ (in other words, such that $\alpha(v) = v$) forms a subgroup $H$ of $C$. Calculate the index of $H$ in $C$ and hence (using Lagrange's Theorem) the order of $H$. Can you find an isomorphism from $H$ to a symmetric group $S_n$ for some $n$?

6. The four-dimensional cube $[-1, 1]^4 \subset \mathbb{R}^4$ has 8 faces, each of which is a three-dimensional cube. (One example is $\{1\} \times [-1, 1]^3$.) What is the order of the symmetry group of the four-dimsnional cube? Suggest a formula for the order of the symmetry group of the $n$-dimensional cube $[-1, 1]^n \subset \mathbb{R}^n$ that would apply for all $n \geq 1$.

7. Let $A$ be an abelian group and $n$ a positive integer. Define $A^n$ to be the subset $\{a^n \; ; \; a \in A \}$ of $A$. Show that $A^n$ is a subgroup of $A$. Is the corresponding statement true for all groups?
(Hint: consider the case $A = S_3$, $n = 3$).

# Chapter 6

# More on homomorphisms

## 6.1 The image and kernel of a homomorphism

**Definition.** Let $f : G \to H$ be a homomorphism from a group $(G, *)$ to a group $(H, \dagger)$. The *image* of $f$ is the subset

$$\mathrm{Im}(f) := \{f(g);\ g \in G\}$$

of $H$.

**Example.** Let $f : \mathbb{R} \to \mathbb{R} \smallsetminus \{0\}$ be the exponential map. Then

$$\mathrm{Im}(f) = \mathbb{R}_+ = \{x \in \mathbb{R},\ x > 0\}.$$

**Lemma 12** $\mathrm{Im}(f)$ *is a subgroup of* $(H, \dagger)$.

*Proof.* Use the subgroup test:

- If $x = f(a), y = f(b) \in \mathrm{Im}(f)$, then $x \dagger y = f(a) \dagger f(b) = f(a * b)$ since $f$ is a homomorphism. Hence $\mathrm{Im}(f)$ is closed with respect to †.
- If $e_G, e_H$ are the identity elements of $G, H$ respectively, then $f(e_G) = e_H$ since $f$ is a homomorphism. hence $e_H \in \mathrm{Im}(f)$.
- If $x = f(a) \in \mathrm{Im}(f)$ and $\overline{a}$ is the inverse of $a$ in $(G, *)$, then the inverse of $x = f(a)$ in $(H, \dagger)$ is $f(\overline{a}) \in \mathrm{Im} f$.

□

We have already seen the image of a homomorphism arising implicitly in the proof of Cayley's Theorem. Given a group $(G, *)$ we defined a homomorphism $\theta : G \to S(G)$ by $\theta(g) = \lambda_g$ (the permutation $x \mapsto g * x$). We showed that $\theta$ defined an isomorphism from $G$ to a certain subgroup $H$ of $S(G)$. In fact, $H$ was just the image of the homomorphism $\theta$. (Look back at the proof of Cayley's Theorem and check this.)

The idea used in the proof of Cayley's Theorem applies more generally:

**Lemma 13** *Let $f : G \to H$ be an injective homomorphism. Then $f$ defines an isomorphism from $G$ onto* $\mathrm{Im}(f)$.

*Proof.* This is more or less obvious. Since by definition $f(g) \in \mathrm{Im}(f)$ for all $g \in G$, we can regard $f$ as a function $G \to \mathrm{Im}(f)$. This function is now surjective as well as being injective by hypothesis, so it is bijective. It is also a homomorphism, since $f$ is a homomorphism from$G$ to $H$ and $\mathrm{Im}(f)$ has the same binary operation as $H$ (being a subgroup of $H$). □

Most homomorphisms are not injective. What happens then? Let us investigate. If $f : G \to H$ is a homomorphism that is not injective, then there are two distinct elements $g_1 \neq g_2$ of $G$ such that $f(g_1) = f(g_2)$. Let us write $*$ for the binary operation in $G$, and $\overline{g_2}$ for the inverse of $g_2$ in $(G, *)$. If $\dagger$ is the binary operation in $H$, and $\widehat{h}$ denotes the inverse in $(H, \dagger)$ of an arbitrary element $h \in H$, then the rules for a homomorphism say that

$$f(g_1 * \overline{g_2}) = f(g_1)\dagger f(\overline{g_2}) = f(g_2)\dagger\widehat{f(g_2)} = e_H,$$

where $e_H$ denotes the identity element in $(H, dag)$. Thus there is an element $x := g_1 * \overline{g_2} \neq e_G$ of $G$ such that $f(x) = e_H$.

In some sense the number of elements $x \in G$ with this property measures how far the homomorphism $f$ is from being injective.

**Definition.** Let $f : G \to H$ be a homomorphism from $(G, *)$ to $(H, \dagger)$. Then the *kernel* of $f$ is the subset

$$\mathrm{Ker}(f) := \{x \in G;\ f(x) = e_H\}$$

of $G$, where $e_H$ denotes the identity element of $(H, \dagger)$.

**Example.** Let $f : \mathbb{Z} \to \mathbb{Z}_3$ be the homomorphism $f(n) = n \bmod 3$ from $(\mathbb{Z}, +)$ to $(\mathbb{Z}_3, +)$. Then $\mathrm{Ker}(f)$ is the set of integers congruent to 0 modulo 3, ie $\mathrm{Ker}(f) = 3\mathbb{Z}$.

**Lemma 14** *Let $f : G \to H$ be a homomorphism. Then* $\mathrm{Ker}(f)$ *is a subgroup of $G$.*

*Proof.* As usual, we apply the subgroup test

- Let $*, \dagger$ denote the binary operations in $G, H$ respectively, and let $e_H$ denote the identity element of $(H, \dagger)$. If $x, y \in \mathrm{Ker}(f)$, then $f(x) = f(y) = e_H$, so $f(x * y) = f(x)\dagger f(y) = e_h\dagger e_H = e_H$. Hence $x * y \in \mathrm{Ker}(f)$, and so $\mathrm{Ker}(f)$ is closed with respect to $*$.
- Let $e_G$ be the identity element of $(G, *)$. Then $f(e_G) = e_H$ so $e_G \in \mathrm{Ker}(f)$.
- Let $x \in \mathrm{Ker}(f)$ and let $\overline{x}$ denote the inverse of $x$ in $(G, *)$. Then $f(\overline{x})$ is the inverse in $(H, \dagger)$ of $f(x) = e_H$. But the inverse of $e_H$ is $e_H$, so $f(\overline{x}) = e_H$, so $\overline{x} \in \mathrm{Ker}(f)$, as required.

□

**Examples.**

1. Recall that the sign $\epsilon(\sigma)$ of a permutation $\sigma$ is $+1$ if $\sigma$ is even, or $-1$ if $\sigma$ is odd. We can think of $\epsilon$ as a homomorphism from $S_n$ onto the group $\{\pm 1\}$ with binary operation multiplication. Its kernel is therefore the set of all even permutations, $A_n$

2. Consider the determinant map $det : GL_n(\mathbb{R}) \to \mathbb{R} \smallsetminus \{0\}$. This is a homomorphism from $GL_n(\mathbb{R})$ to the group $(\mathbb{R} \smallsetminus \{0\}, \cdot)$, whose identity element is the number 1. Thus
$$\mathrm{Ker}(det) = \{A \in GL_n(\mathbb{R});\ det(A) = 1\} = SL_n(\mathbb{R}).$$

3. Let $K$ denote the cyclic subgroup of $S_3$ generated by the transposition $(1, 2)$. That is, $K = \{id, (1, 2)\}$. Then $K$ is not the kernel of any homomorphism defined on $S_3$.

   To see this, suppose that $(H, \dagger)$ is a group, and $f : S_3 \to H$ is a homomorphism such that $K \subset \mathrm{Ker}(f)$. Then $f((1, 2)) = e_H$, the identity element of $(H, \dagger)$. In $S_3$ we have an equation
$$(1, 3) \circ (1, 2) \circ (1, 3) = (2, 3),$$
   so
$$f((2, 3)) = f((1, 3)) \dagger f((1, 2)) \dagger f((1, 3)) = f((1, 3)) \dagger e_H \dagger f((1, 3))$$
$$= f((1, 3)) \dagger f((1, 3)) = f((1, 3) \circ (1, 3)) = f(id) = e_H.$$
   Hence $(2, 3) \in \mathrm{Ker}(f)$.

This last example shows us that not all subgroups can arise as kernels of homomorphisms. In what way are kernels of homomorphisms special?

## 6.2 Normal subgroups

**Definition.** Let $(G, *)$ be a group, and for any $g \in G$ let $\overline{g}$ denote the inverse of $g$ in $(G, *)$. Then a subgroup $N$ of $G$ is said to be *normal* if $g * x * \overline{g} \in N$ for every $g \in G$ and every $n \in N$.

**Examples.**

1. If $(G, *)$ is an abelian group, then *every* subgroup of $(G, *)$ is normal, since $g * x * \overline{g} = x * g * \overline{g} = x \in N$.

2. For every positive integer $n$, $A_n$ is a normal subgroup of $S_n$. Suppose $\alpha \in S_n$ is a composite of $k$ transpositions: $\alpha = \tau_1 \circ \cdots \circ \tau_k$. Then so is its inverse: $\alpha^{-1} = \tau_k \circ \cdots \circ \tau_1$. If $\sigma \in A_n$ then $\sigma$ is even - say a composite of $2\ell$ transpositions. But then $\alpha \circ \beta \circ \alpha^{-1}$ is a composite of $k + 2\ell + k = 2(k + \ell)$ transpositions, so it is also even.

3. In the dihedral group $D_n$, the cyclic subgroup $C_n$ consisting of all the rotations is normal. If $\rho$ is a reflection, and $\sigma$ is a rotation in a clockwise direction through an angle of $\theta$, then $\rho \circ \sigma \circ \rho$ is a rotation in an anti-clockwise direction through the same angle $\theta$.

There is an alternative characterisation of normal subgroups: namely those for which the left and right cosets coincide:

**Lemma 15** *Let $(G, *)$ be a group, and $H$ a subgroup. Then $H$ is normal if and only if, for each $x \in G$, the left coset $x * H$ is equal to the right coset $H * x$.*

*Proof.* First suppose that $x * H = H * x$ for each $x \in G$. Let $x \in G$ and $h \in H$. Then $x * h \in x * H = H * x$, so there is an element $h' \in H$ such that $h' * x = x * h$. If $\overline{x}$ is the inverse of $x$ in $(G, *)$, then it follows that

$$x * h * \overline{x} = h' * x * \overline{x} = h' \in H.$$

Hence $H$ is normal in $(G, *)$.

Conversely, suppose that $H$ is normal, and let $x \in G$. If $h \in H$ then $h' := x*h*\overline{x} \in H$ and $h'' := \overline{x} * h * x \in H$, so $x * h = h' * x \in H * x$, while $h * x = x * h'' \in x * H$.

Since $x * h \in H * x$ for all $h \in H$, we have $x * H \subseteq H * x$. Since $h * x \in x * H$ for all $h \in H$, we have $H * x \subseteq x * H$. Hence $x * H = H * x$, as claimed. □

**Corollary 3** *Any subgroup of index 2 in a group $(G, *)$ is normal.*

*Proof.* Let $(G, *)$ be a group, $H$ a subgroup of index 2, and $x \in G \setminus H$. Then the two right cosets of $H$ in $G$ are $H$ and $H * x = G \setminus H$. For any $y \in G$, the left coset $y * H = \{y * h;\ h \in H\}$ consists of the inverses $(\overline{\overline{h} * \overline{y}})$ of elements of the right coset $H * \overline{y}$, so there are also precisely two left cosets, namely $H$ and $x * H = G \setminus H$. In particular, each left coset is also a right coset, and *vice versa.*

By Lemma 15, this means that $H$ is normal. □

**Lemma 16** *If $K$ is the kernel of a homomorphism from $(G, *)$ to $(H, \dagger)$, then $K$ is a normal subgroup of $(G, *)$.*

*Proof.* We have already seen that $K$ is a subgroup of $(G, *)$. We need to show that this subgroup is normal.

If $g \in G$, $\overline{g}$ is its inverse, and $x \in K$, then

$$f(g * x * \overline{g}) = f(g) \dagger e_H \dagger f(\overline{g}) = f(g) \dagger f(\overline{g}) = f(g * \overline{g}) = e_H,$$

and so $g * x * \overline{g} \in \mathrm{Ker}(f)$, as required. □

We will shortly see that this last result has a converse: every normal subgroup arises as the kernel of some homomorphism.

## 6.3 Quotient groups

Suppose that $(G, *)$ is a group, and $N$ is a normal subgroup of $(G, *)$. We construct a new group, called the *quotient group* of $(G, *)$ over $N$, as follows.

The underlying set of the new group, denoted $G/N$, is defined to be the set of left cosets of $N$ in $G$:

$$G/N := \{x * N;\ x \in G\}.$$

**Remark.** By Lemma 15, this is the same as the set of right cosets of $N$ in $G$. Notice also that, while we define a left coset $x*N$ using a specific representative element $x \in G$, there will in general be many coset representatives defining a single coset. Thus, for example, in $\mathbb{Z}/3\mathbb{Z}$ there are precisely three elements, since there are only three distinct (left) cosets of $3\mathbb{Z}$ in $\mathbb{Z}$.

The binary operation on $G/N$ is defined using the binary operation $*$ of $G$ as follows. Let us denote this new binary operation $\oplus$. Then the definition is

$$(x * N) \oplus (y * N) := (x * y) * N.$$

**Theorem 5** *With the above definition, $\oplus$ is a well-defined binary operation on $G/N$, and $(G/N, \oplus)$ is a group.*

*Proof.* The hardest part of the proof is that $\oplus$ is well-defined. In other words, the definition does not depend on the choices of coset representatives $x, y$. Suppose that $x' \in x * N$, $y' \in y * N$ are alternative choices for these coset representatives. If we substituted these for $x, y$ respectively in the definition of $\oplus$, then the result would be $(x' * y') * N$ instead of $(x * y) * N$. Thus we need to check that $(x' * y') * N = (x * y) * N$, or equivalently $x' * y' \in (x * y) * N$.

Since $x' \in x * N$, we can write $x' = x * n_1$ for some $n_1 \in N$. Similarly $y' = y * n_2$ for some $n_2 \in N$. Now $n_1 * y \in N * y = y * N$, so $n_1 * y = y * n_3$ for some $n_3 \in N$. Hence

$$x' * y' = x * n_1 * y * n_2 = x * y * n_3 * n_2 \in (x * y) * N.$$

Hence $\oplus$ is well-defined, as claimed. It is also a binary operation on $G/N$, since it is defined for any pair of elements from $G/N$, and the result is also an element of $G/N$.

Next we must check the axioms for a group.

- $\oplus$ is associative. Let $x * N, y * N, z * N \in G/N$, in other words, let $x, y, z \in G$. Then

  $$((x * N) \oplus (y * N)) \oplus (z * N) = ((x * y) * N) \oplus (z * N) = ((x * y) * z) * N.$$

  Similarly,

  $$(x * N) \oplus ((y * N) \oplus (z * N)) = (x * N) \oplus ((y * z) * N) = ((x * (y * z)) * N.$$

  But $(x * y) * z = x * (y * z)$ since $*$ is associative. Hence

  $$((x * N) \oplus (y * N)) \oplus (z * N) = (x * N) \oplus ((y * N) \oplus (z * N)),$$

  and so $\oplus$ is associative.

- Let $e_G$ be the identity element of $(G, *)$. Then $e_G * N$ is an identity element for $(G/N, \oplus)$. To see this, take an arbitrary element $x * N \in G/N$, and calculate

  $$(e_G * N) \oplus (x * N) = (e_G * x) * N = x * N.$$

  Similarly

  $$(x * N) \oplus (e_G * N) = (x * e_G) * N = x * N.$$

  Hence $e_G * N$ is indeed an identity element, as claimed.

- If $\overline{x}$ is the inverse for $x$ in $(G, *)$, then $\overline{x} * N$ is an inverse for $x * N$ in $(G/N, \oplus)$. To see this, calculate

  $$(\overline{x} * N) \oplus (x * N) = (\overline{x} * x) * N = e_G * N,$$

  and similarly

  $$(x * N) \oplus (\overline{x} * N) = (x * \overline{x}) * N = e_G * N.$$

□

**Remark.** Note that the above proof uses in an essential way the hypothesis that the subgroup $N$ is normal - namely the property that $N * y = y * N$ in the proof that $\oplus$ is well-defined. If we tried to do this construction for a non-normal subgroup, then the proof would break down at that point.

**Examples.**

1. The quotient group $\mathbb{Z}/n\mathbb{Z}$ consists of the $n$ cosets $n\mathbb{Z}$, $1 + 2\mathbb{Z}$, …, $(n-1) + n\mathbb{Z}$ of $n\mathbb{Z}$ in $\mathbb{Z}$. The binary operation $\oplus$ is defined by $(x + n\mathbb{Z}) \oplus (y + n\mathbb{Z}) = z + n\mathbb{Z}$, where $z \cong x + y$ mod $n$. In other words, it just corresponds to adding the coset representatives $0, 1, \ldots, n-1$ modulo $n$. Thus $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to the cyclic group $\mathbb{Z}_n$.

2. In $S_n$, we have seen that the subgroup $A_n$ of even permutations is normal (of index 2). The two cosets are the set $A_n$ of even permutations, and the set $S_n \smallsetminus A_n$ of odd permutations. Thus we can write $S_n/A_n = \{even, odd\}$, with binary operation $\oplus$ defined by $even \oplus even = even = odd \oplus odd$; $even \oplus odd = odd = odd \oplus even$.

**Lemma 17** *Let $(G*)$ be a group, and $N$ a normal subgroup. Then the map $f : G \to G/N$ defined by $f(g) = g * N$ is a surjective homomorphism with kernel $N$.*

*Proof.* The fact that $f$ is a homomorphism follows immediately from the definition of the binary operation $\oplus$ on the quotient group $G/N$:

$$f(x * y) = (x * y) * N = (x * N) \oplus (y * N) = f(x) \oplus f(y).$$

The fact that $f$ is surjective also follows immediately from the definition of $G/N$: every element of $G/N$ has the form $g * N = f(g)$ for some $g \in G$.

Finally,

$$\mathrm{Ker}(f) = \{x \in G;\ f(g) = e_G * N\} = \{x \in G;\ x * N = e_G * N\} = N.$$

□

## 6.4 The First Isomorphism Theorem

**Theorem 6** (The First Isomorphism Theorem) *Let $f : G \to H$ be a homomorphism from a group $(G, *)$ to a group $(H, \dagger)$. Then*

$$\frac{G}{\mathrm{Ker}(f)} \cong \mathrm{Im}(f).$$

*Proof.* We need to define an isomorphism $\theta : G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$. There is only one sensible way to do this, namely:

$$\theta(g * \ker(f) := f(g).$$

First, we need to check that $\theta$ is well-defined, in other words that $\theta(g * \mathrm{Ker}(f))$ does not depend on the choice $g$ of coset representative from the coset $g * \mathrm{Ker}(f)$. To see this, suppose that $g' \in g * \mathrm{Ker}(f)$. Then $g' = g * x$ for some $x \in \mathrm{Ker}(f)$, so

$$f(g') = f(g * x) = f(g) \dagger f(x) = f(g) \dagger e_H = f(g).$$

Hence $\theta(g * \mathrm{Ker}(f)) = f(g)$ is well-defined, as required.

Secondly, we should check that $\theta$ is a homomorphism.

$$\theta((g * \mathrm{Ker}(f)) \oplus (h * \mathrm{Ker}(f))) = \theta((g * h) * \mathrm{Ker}(f)) = f(g * h)$$

$$= f(g)\dagger f(h) = \theta(g * \mathrm{Ker}(f))\dagger\theta(h * \mathrm{Ker}(f)).$$

Hence $\theta$ is a homomorphism, as required.

Next, to see that $\theta$ is injective, suppose that $\theta(g*\mathrm{Ker}(f)) = \theta(h*\mathrm{Ker}(f))$. In other words, $f(g) = f(h)$. Then $f(\overline{g}*h) = e_H$, where $\overline{g}$ is the inverse of $g$ in $(G, *)$, and $e_H$ is the identity element of $(H, \dagger)$. But then $x := \overline{g} * h \in \mathrm{Ker}(f)$, so $h = g * x \in g * \mathrm{Ker}(f)$. Hence $h * \mathrm{Ker}(f) = g * \mathrm{Ker}(f)$, so $\theta$ is injective.

Finally, to see that $\theta$ is surjective, if $a \in \mathrm{Im}(f)$, then there is an element $g \in G$ with $a = f(g) = \theta(g * \mathrm{Ker}(f))$. □

**Examples.**

1. Let $f : \mathbb{Z} \to \mathbb{Z}_n$ be the homomorphism $f(k) = k \bmod n$. Then $\mathrm{Im}(f) = \mathbb{Z}_n$, $\mathrm{Ker}(f) = n\mathbb{Z}$, and the First Isomorphism Theorem tells us that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$, as we have already seen.

2. The determinant map $det : GL_n(\mathbb{R}) \to \mathbb{R}\setminus\{0\}$ is a surjective homomorphism with kernel $SL_n(\mathbb{R})$, so the First Isomorphism Theorem tells us that $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R} \setminus \{0\}$.

3. Let $f : \mathbb{R} \to \mathbb{C} \setminus \{0\}$ be the map $f(t) = exp(2\pi it)$. Then $f$ is a homomorphism, since
$$f(s+t) = exp(2\pi i(s+t)) = exp(2\pi is)exp(2\pi it) = f(s)f(t).$$
Moreover, $\mathrm{Im}(f) = \{exp(2\pi it);\ t \in \mathbb{R}\} = \{z \in \mathbb{C};\ |z| = 1\} = S^1$ (the circle group), and $\mathrm{Ker}(f) = \{t \in \mathbb{R};\ exp(2\pi it) = 1\} = \mathbb{Z}$. Thus the First Isomorphism Theorem tells us that $\mathbb{R}/\mathbb{Z} \cong S^1$.

4. Recall that we may identify the symmetric group $S_4$ with the group of symmetries of a regular tetrahedron, since such symmetries correspond to permutations of the vertices of the tetrahedron.

   To be specific, let $T$ be the regular tetrahedron with vertices $(1, 1, 1)$, $(1, -1, -1)$, $(-1, 1, -1)$, and $(-1, -1, 1)$. The midpoint of the edge joining the first two of these vertices is $(1, 0, 0)$, while the midpoint of the edge joining the last two vertices is $(-1, 0, 0)$. Note that both these points lie on the $x$-axis. Thus the $x$-axis passes through the midpoints of an opposite pair of edges of $T$. In all, $T$ has 6 edges, which occur in three opposite pairs. A similar analysis shows that the $y$-axis also passes through the midpoints of a pair of opposite edges of $T$, as does the $z$-axis.

   Hence any symmetry of $T$ induces a permutation of the three coordinate axes in $\mathbb{R}^3$. This gives rise to a homomorphism $f : S_4 \to S_3$. What does the First Isomorphism Theorem tell us about this situation?

   Firstly, we should determine the image of $f$. If $F$ is a face of $T$, and $V$ is the vertex of $T$ that is not in $F$, then $F$ is an equilateral triangle, and any symmetry of $F$ extends (uniquely) to a symmetry of $T$ which maps $V$ to $V$. Each coordinate axis meets $F$ in the midpoint of one of its edges. Since any permutation of these edges is achievable by a symmetry of $F$, it follows that any permutation of the three coordinate axes is achievable by a symmetry of $T$. Thus $f : S_4 \to S_3$ is surjective, ie. $\mathrm{Im}(f) = S_3$.

The First Isomorphism Theorem thus tells us that $S_4/\mathrm{Ker}(f) \cong S_3$.

Secondly, we should determine $\mathrm{Ker}(f)$. The index of $\mathrm{Ker}(f)$ in $S_4$ is $|S_3| = 6$, so $|\mathrm{Ker}(f)| = |S_4|/6 = 4$. Clearly the identity element of $S_4$ must belong to $\mathrm{Ker}(f)$, but what are the other three elements?

Consider the rotation $\sigma$ through an angel of $\pi$ around the $x$-axis, $\sigma(x, y, z) = (x, -y, -z)$. It is easy to check that $\sigma$ permutes the four vertices of $T$, and so is a symmetry of $T$. It is also easy to check that $\sigma$ maps each coordinate axis to itself, so $\sigma \in \mathrm{Ker}(f)$. In a similar way, the rotations through $\pi$ around the $y$- and $z$-axes, $(x, y, z) \mapsto (-1, y, -z)$ and $(x, y, z) \mapsto (-x, -y, z)$, also give elements of $\mathrm{Ker}(f)$.

These three rotations, together with the identity element, form $\mathrm{Ker}(f)$. In terms of permutations, $\mathrm{Ker}(f) = \{id, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$.

This normal subgroup of $S_4$ is known as the *Klein 4-group* after Felix Klein, the 19th century German geometer and inventor of the Klein bottle, who laid much of the early foundations of the theory of groups – see `http://www-history.mcs.st-andrews.ac.uk/history/Biographies/Klein.html` for more details. If we call it $K$, then we have the equation $S_3 \cong S_4/K$.

As a group in its own right, $K$ is abelian but not cyclic. It is in fact isomorphic to the direct product $\mathbb{Z}_2 \times \mathbb{Z}_2$. (Exercise: find a specific isomorphism $K \to \mathbb{Z}_2 \times \mathbb{Z}_2$.)

## 6.5 More Isomorphism Theorems

The First Isomorphism Theorem has two corollaries, known as the Second and Third Isomorphism Theorems. Here they are.

**Theorem 7** (Second Isomorphism Theorem) *Let $(G, *)$ be a group, $H$ a subgroup of $G$, and $N$ a normal subgroup of $G$. Then the subset $H * N := \{n * h,\ n \in N, h \in H\}$ of $G$ is a subgroup of $(G, *)$ containing $N$ as a normal subgroup, $N \cap H$ is a normal subgroup of $H$, and*

$$\frac{H}{H \cap N} \cong \frac{H * N}{N}.$$

*Proof.* We can easily check that $H * N$ is a subgroup of $G$, using the subgroup test and the fact that $N$ is normal in $G$:

- If $h_1 {*} n_1, h_2 {*} n_2 \in H {*} N$, with $h_1, h_2 \in H$ and $n_1, n_2 \in N$, then $(h_1 {*} n_1) {*} (h_2 {*} n_2) = (h_1 * h_2) * (n_3 * n_2) \in H * N$, where $n_3 = \overline{h_2} * n_1 * h_2 \in N$ since $N$ is normal (and where, as usual, $\overline{h_2}$ denotes the inverse of $h_2$ in $(G, *)$). Hence $H * N$ is closed with respect to $*$.

- Clearly $e_G = e_G * e_G \in H * N$.

- If $h * n \in H * N$ with $h \in H$ and $n \in N$, then the inverse of $h * n$ is $\overline{n} * \overline{h} = \overline{h} * \overline{n'}$, where $n' = h * n * \overline{h} \in N$ since $N$ is normal. Hence the inverse of $h * n$ belongs to $H * N$.

It is clear that $N \subset H * N$: $n = e_G * n \in H * N$ for all $n \in N$. It is also clear that $N$ is a subgroup of $H * N$, since it is a group with respect to the binary operation $*$. That it is normal follows from the fact that it is normal in the larger group $G$: if $g \in H * N$ and $n \in N$ then $g \in G$ so $g * n * \overline{g} \in N$.

Define $f : H \to G/N$ to be the composite of the inclusion homomorphism $H \to G$ and the quotient homomorphism $G \to G/N$. In other words, define $f(h) = h * N \in G/N$ for all $h \in H$. Then $f$ is certainly a homomorphism, from the definition of the binary operation in the quotient group $G/N$. The First Isomorphism Theorem tells us that $H/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$, so it remains to interpret each side of that equation.

Firstly, $\mathrm{Ker}(f) = \{h \in H;\ f(h) = e_G * N = N\} = \{h \in H;\ h \in N\} = H \cap N$.

Secondly, $\mathrm{Im}(f) = \{f(h);\ h \in H\} = \{h * N;\ h \in H\} = \{(h * n) * N;\ h \in H, n \in N\} = (H * N)/N$.

Putting these three equations together gives the result. □

**Theorem 8** (Third Isomorphism Theorem) *Let $(G, *)$ be a group, and let $K, N$ be normal subgroups of $G$, such that $K \subset N$. Then $N/K$ is a normal subgroup of $G/K$, and*

$$\frac{G/K}{N/K} \cong \frac{G}{N}.$$

*Proof.* Define $f : G/K \to G/N$ by $f(g * K) = g * N$. Then $f$ is well-defined, since if $g' \in g * K$ then $g' \in g * N$. Moreover, $f$ is a homomorphism by the definitions of the binary operations in the quotient groups $G/K$ and $G/N$.

Clearly $f$ is surjective, since $g * N \in \mathrm{Im}(f)$ for all $g \in G$. In other words, $\mathrm{Im}(f) = G/N$.

Finally, $\mathrm{Ker}(f) = \{g * K;\ f(g * K) = e_G * N\} = \{g * K;\ g \in N\} = N/K$.

The result follows. □

**Example.** Let $G = \mathbb{Z}$ with binary operation $+$, let $K = 2\mathbb{Z}$ and $N = 6\mathbb{Z}$. Then $G/N \cong \mathbb{Z}_6$, under an isomorphism mapping $K/N$ onto the index 2 subgroup $2\mathbb{Z}_6 = \{0, 2, 4\} \subset \mathbb{Z}_6$. The Third Isomorphism Theorem tells us that

$$\frac{\mathbb{Z}_6}{2\mathbb{Z}_6} \cong \frac{\mathbb{Z}/6\mathbb{Z}}{2\mathbb{Z}/6\mathbb{Z}} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \cong \mathbb{Z}_2.$$

## 6.6 Exercises

1. Which of he following subsets of $S_4$ is (i) a normal subgroup; (ii) a subgroup, but not normal; (iii) not a subgroup at all?

   (a) $\{\mathrm{id}, (1\ 3\ 4), (1\ 4\ 3)\}$;

   (b) $\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$;

   (c) $\{\mathrm{id}, (1\ 2\ 3\ 4), (1\ 4\ 3\ 2), (1\ 3)(2\ 4)\}$;

   (d) $\{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2), (2\ 3\ 4), (2\ 4\ 3)\}$;

2. There is a homomorphism $f$ from $(\mathbb{Z}_{12}, +)$ to $(\mathbb{C} \setminus \{0\}, \cdot)$ defined by $f(k) = i^k$ for all $k \in \mathbb{Z}_{12}$ (where $i = \sqrt{-1} \in \mathbb{C}$). List all the elements of

   (a) $\mathrm{Im}(f)$, the image of $f$;

   (b) $\mathrm{Ker}(f)$, the kernel of $f$;

   (c) the quotient group $\mathbb{Z}_{12}/\mathrm{Ker}(f)$.

   Write down the Cayley tables of $\mathbb{Z}_{12}/\mathrm{Ker}(f)$ and $\mathrm{Im}(f)$. Look at them carefully, and convince yourself that these two groups are indeed isomorphic (as promised by the First Isomorphism Theorem).

3. For each of the following homomorphisms, determine the kernel and image, and write down the isomorphism equation given by the First Isomorphism Theorem.

   (a) $n \mapsto 2n$, from $\mathbb{Z}$ to $\mathbb{Z}$;

   (b) $x \mapsto e^{ix}$, from $(\mathbb{R}, +)$ to $(\mathbb{C} \setminus \{0\}, \cdot)$;

   (c) $(m, n) \mapsto \sigma^m \circ \tau^n$, from $(\mathbb{Z} \times \mathbb{Z}, +)$ to $S_4$, where $\sigma = (1\ 2)(3\ 4)$ and $\tau = (1\ 3)(2\ 4)$;

   (d) det, from $GL(3, \mathbb{R})$ to $(\mathbb{C} \setminus \{0\}, \cdot)$.

4. Let $f : \mathbb{Z} \longrightarrow (\mathbb{Z}_2 \times \mathbb{Z}_3)$ be the map defined by $f(n) = (n_2, n_3)$, where $n_2 \in \{0, 1\}$ is $n$ modulo 2 and $n_3 \in \{0, 1, 2\}$ is $n$ modulo 3. Show that $f$ is a homomorphism (where the binary operations on $\mathbb{Z}$, $\mathbb{Z}_2$ and $\mathbb{Z}_3$ are all addition).
   Determine the image and kernel of $f$. Use the First Isomorphism Theorem to show that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is isomorphic to a cyclic group.

5. Suppose that $A$ is a finite abelian group such that each element of $A$ has order 1 or 3. If $B$ is a subgroup of $A$, show that each element of $B$ has order 1 or 3, and each element of $A/B$ has order 1 or 3.
   Use induction on $|A|$ to show that $|A| = 3^k$ for some natural number $k$.

# Chapter 7

# Abelian Groups

## 7.1 Abelian Groups

For the next part of the course, we will restrict our attention to abelian groups, in other words groups in which the binary operation is commutative. Our aim will be to understand the structure of a large class of abelian groups, including all finite abelian groups.

When studying abelian groups, we will adopt the convention (which is quite standard) of using additive notation. This means that the binary operations in our abelian groups will be denoted $+$, the identity element will be denoted $0$ (or $0_A$ if we wish to emphasise the specific abelian group $A$), and the inverse of an element $x$ will be denoted by $-x$.

Since we will always be using the same symbol $+$ for our binary operations, we will usually just refer to the abelian group $A$ rather than the abelian group $(A, +)$. Thus, for example, in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ it is understood that the binary operation is the usual addition of numbers; in $\mathbb{R}^n$ or $\mathbb{C}^n$ it is the usual vector addition.

A first observation is that, without some sort of restriction, there are too many abelian groups to have any hope of classifying them up to isomorphism. A simple analogy is the classification of (real) vector spaces. A theorem states that every vector space has a basis, and another theorem states that two vector spaces are isomorphic (as vector spaces) if and only if there is a bijection from a basis of one to a basis of the other. Thus the classification of vector spaces up to isomorphism reduces to the classification of sets up to bijection, which sounds easy but in fact depends on the axiomatic foundations of set theory.

On the other hand, if we restrict our attention to *finite-dimensional* vector spaces, then the classification could not be simpler: there is precisely one (real) vector space of dimension $n$ (up to isomorphism) for each natural number $n \in \{0, 1, 2, 3, 4, \ldots\}$, namely $\mathbb{R}^n$.

We will impose a similar restriction on the abelian groups that we investigate, and will obtain a classification that is slightly more subtle than that of finite-dimensional vector spaces.

**Example.** Consider the abelian group $\mathbb{Q}$ of rational numbers, $\mathbb{Q} = \{\frac{a}{b},\ a, b \in \mathbb{Z},\ b > 0\}$. It can be shown that $\mathbb{Q}$ has the same *cardinality* $\aleph_0$ as the set $\mathbb{N}$ of natural numbers. In other words there is a bijection $\mathbb{N} \to \mathbb{Q}$. We also know that there is an infinite set $P$ of prime numbers, which we can list $\{p_0, p_1, p_2, \ldots\}$ and which therefore also has cardinality $\aleph_0$.

Now let $\Pi$ be a subset of $P$, and let $A_\Pi$ be the set of all rational numbers $\frac{a}{b}$ such that all the prime factors of the denominator $b$ belong to the set $\Pi$.

**Exercise:** Show that $A_\Pi$ is a subgroup of $\mathbb{Q}$.

It can also be shown that the subgroups $A_\Pi$ for different subsets $\Pi \subset P$ are pairwise nonisomorphic. Hence the set of isomorphism classes of subgroups of $\mathbb{Q}$ has cardinality $2^{\aleph_0}$, which is much bigger than that of the natural numbers.

Thus even if we restrict ourselves to subgroups of a rather easy group $\mathbb{Q}$, the classification up to isomorphism could be very hard.

## 7.2 Cyclic Groups

Let us say that a group is *cyclic* if it is a cyclic subgroup of itself. We have seen that any cyclic subgroup is isomorphic either to $\mathbb{Z}$ or to $\mathbb{Z}_n$ for some $n$. On the other hand, $\mathbb{Z} = \langle 1 \rangle$ is cyclic, and $\mathbb{Z}_n = \langle 1 \rangle$ is cyclic for each $n$.

Hence the cyclic groups are classified up to isomorphism by their order.

Cyclic groups are abelian, but of course not every abelian group is cyclic.

**Example.** The Klein 4-group $K = \mathbb{Z}_2 \times \mathbb{Z}_2$ of order 4 is abelian. It cannot be cyclic because it does not contain an element of order 4.

Here are some elementary properties of cyclic groups.

**Lemma 18** *Every subgroup of a cyclic group is cyclic. Every quotient group of a cyclic group is cyclic.*

*Proof.* Let $H$ be a subgroup of $\mathbb{Z}$. If $H = \{0\}$ then $H = \langle 0 \rangle$ is cyclic. If $H \neq \{0\}$ then $H$ contains at least one positive integer. Let $n$ be the least positive integer contained in $H$. Then $\langle n \rangle = n\mathbb{Z} \subset H$. If $H \neq n\mathbb{Z}$, then there is an integer $k \in H$ with $k \notin n\mathbb{Z}$. Dividing $k$ by $n$, we find $k = nq + r$ with $q, r \in \mathbb{Z}$ and $0 < r < n$. But then $r = k - nq \in H$, contradicting the choice of $n$. Hence $H = n\mathbb{Z} = \langle n \rangle$ is cyclic.

Now let $H$ be a subgroup of $\mathbb{Z}_n$ for some $n$, and let $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ be the quotient homomorphism ($f(k) = k \bmod n$). Then $\widehat{H} := \{k \in \mathbb{Z},\ f(k) \in H\}$ is a subgroup of $\mathbb{Z}$, so cyclic. Say $\widehat{H} = \langle m \rangle = m\mathbb{Z}$. Then $H = f(\widehat{H}) = m\mathbb{Z}_n = \langle m \rangle$ is a cyclic subgroup of $\mathbb{Z}_n$.

If $Q$ is a quotient group of $\mathbb{Z}$, then $Q = \mathbb{Z}/K$ where $K$ is a subgroup of $\mathbb{Z}$. Either $K = \{0\}$, in which case $\mathbb{Z}/K \cong \mathbb{Z}$ is infinite cyclic, or $K = n\mathbb{Z}$ for some $n > 0$, in which case $\mathbb{Z}/K \cong \mathbb{Z}_n$ is cyclic of order $n$.

Finally, if $Q$ is a quotient group of $\mathbb{Z}_n$, then there are surjective homomorphisms $\mathbb{Z} \to \mathbb{Z}_n \to Q$. The composite of these homomorphisms is also surjective, so $Q$ is also a quotient group of $\mathbb{Z}$. We have just shown that such groups are cyclic. □

**Lemma 19** *Any group whose order is a prime number is cyclic.*

*Proof.* Suppose that $(G, *)$ is a group whose order is a prime number $p$. (Note that we cannot *a priori* assume that the group is abelian, since it is not part of the hypothesis.)

Since $|G| = p > 1$, there is at least one element $a \in G$ which is not the identity element, and hence has order greater than 1.

By Lagrange's Theorem, the order of $a$ divides the prime number $p$, and hence it must be equal to $p$. Thus the cyclic subgroup $\langle a \rangle$ has order $p = |G|$, so $G = \langle a \rangle$ is a cyclic group. □

Here is a slightly less elementary property. Two positive integers $m, n$ are said to be *coprime* if they have no common prime factors. For example, 24 and 35 are coprime, while 77 and 224 are not coprime (both being divisible by 7).

**Theorem 9** (The Chinese Remainder Theorem) *Let $n_1, n_2, \dots, n_k$ be positive integers which are pairwise coprime – that is, $n_i$ and $n_j$ are coprime whenever $1 \le i < j \le k$. Let $N = n_1 n_2 \cdots n_k$ be their product. Then*

$$\mathbb{Z}_N \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}.$$

*Proof.* It suffices to prove this result in the case where $k = 2$. The general case follows by induction on $k$: assume inductively that $\mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k} \cong \mathbb{Z}_{N'}$, where $N' = n_2 \cdots n_k = N/n_1$. Note that $n_1$ and $N'$ are coprime, so by the case $k = 2$ we have $\mathbb{Z}_{n_1} \times \mathbb{Z}_{N'} \cong \mathbb{Z}_N$.

Hence we may assume that $m, n$ are coprime positive integers, and we are required to prove that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

Recall that $\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$, and similarly $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$. Define a homomorphism $f : \mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ by $f(t) = (t + m\mathbb{Z}, t + n\mathbb{Z})$. Then $\mathrm{Ker}(f) = \{t \in \mathbb{Z};\ t \in m\mathbb{Z}\ \&\ t \in n\mathbb{Z}\} = m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$. (Since $m, n$ are coprime, an integer $t$ is divisible by $m$ and by $n$ if and only if it is divisible by $mn$.)

By the First Isomorphism Theorem, $\mathrm{Im}(f) \cong \mathbb{Z}/\mathrm{Ker}(f) = \mathbb{Z}/mn\mathbb{Z}$, which has order $mn$. But $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ also has order $mn$. Hence $\mathrm{Im}(f)$ is the whole of $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$. Thus

$$\mathbb{Z}_{mn} \cong \mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}_m \times \mathbb{Z}_n.$$

□

## 7.3 Generating sets

Since we are using additive notation for abelian groups, let us write $n.a$ in stead of $a^n$ when $a$ is an element of an abelian group $(A, +)$ and $n \in \mathbb{Z}$. Thus, for example, $3a$ means $a + a + a$, $-2a$ means $(-a) + (-a)$, and so on.

In this notation, the cyclic subgroup of $A$ generated by $a$ is $\langle a \rangle = \{n.a;\ n \in \mathbb{Z}\}$. As we have seen, this is the smallest subgroup of $A$ that contains the element $a$. It can also be thought of as the image of the homomorphism $\mathbb{Z} \to A$ that sends $n \in \mathbb{Z}$ to $n.a \in A$.

More generally, given any subset $X$ of $A$, we can consider the smallest subgroup of $A$ that contains $X$. This is called the *subgroup generated by* $X$, and sometimes denoted $\langle X \rangle$. It is well-defined for any $X$, but we shall only be concerned with the case where $X$ is a finite subset of $A$. Let us first consider the case where $X$ has two elements: $X = \{a, b\}$.

Now, any subgroup $H$ containing $X$ must contain $a$, and so must contain $\langle a \rangle$. Thus $m.a \in H$ for all $m \in \mathbb{Z}$. Similarly, $n.b \in H$ for all $n \in \mathbb{Z}$. Since $H$ is closed with respect to $+$, it follows that $m.a + n.b \in H$ for all $m, n \in \mathbb{Z}$.

Now consider the abelian group $\mathbb{Z} \times \mathbb{Z} = \{(m, n);\ m, n \in \mathbb{Z}\}$. Let $f : \mathbb{Z} \times \mathbb{Z} \to A$ be the function $f(m, n) := m.a+n.b$. This is a homomorphism, since if $(m_1, n_1), (m_2, n_2) \in \mathbb{Z} \times \mathbb{Z}$, then

$$f((m_1, n_1) + (m_2, n_2)) = f(m_1 + m_2, n_1 + n_2) = (m_1 + m_2)a + (n_1 + n_2)b$$

$$= (m_1a + n_1b) + (m_2a + m_2b) = f(m_1, n_1) + f(m_2, n_2).$$

(Note that this argument makes use of the fact that $(A, +)$ is abelian.)

It follows that the image of $f$ – that is, the set $\{m.a+n.b;\ m, n \in \mathbb{Z}\}$ – is a subgroup of $A$ containing $X = \{a, b\}$. But we have shown above that any subgroup of $A$ that contains $X$ must contain this set, so $\langle X \rangle = \langle a, b \rangle = \mathrm{Im}(f)$.

In a similar way one can show that, if $X = \{a, b, c\}$ is a three-element subset of $A$, then the map $f$ from $\mathbb{Z}^3 = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ to $A$ defined by $f(m, n, p) = m.a + n.b + p.c \in A$ is a homomorphism with $\mathrm{Im}(f) = \langle X \rangle$.

**Definition.** Let $A$ be an abelian group, and let $X$ be a subset of $A$. We say that $X$ *generates* $A$, or is a *generating set* for $A$, if $A = \langle X \rangle$. An abelian group $A$ is said to be *finitely generated* if it has a finite generating set.

**Lemma 20** *An abelian group $A$ is finitely generated if and only if there is a surjective homomorphism $\mathbb{Z}^n \to A$ for some natural number $n$.*

*Proof.* Suppose that $A$ has a finite generating set $X = \{a_1, \ldots, a_n\}$. Let $f : \mathbb{Z}^n \to A$ denote the homomorphism

$$f(m_1, m_2, \ldots, m_n) = m_1a_1 + m_2a_2 + \cdots + m_na_n.$$

Then $a_1 = f(1, 0, \ldots, 0) \in \mathrm{Im}(f)$, and similarly $a_2, \ldots, a_n \in \mathrm{Im}(f)$. Hence $X \subset \mathrm{Im}(f)$, and so $A = \langle X \rangle \subseteq \mathrm{Im}(f)$. In other words, $f$ is surjective.

Conversely, suppose that $f : \mathbb{Z}^n \to A$ is a surjective homomorphism. For each $i = 1, \ldots, n$, let $e_i$ denote the vector in $\mathbb{Z}^n$ whose $i$th coordinate is 1 and whose other coordinates are zero. (For example, $e_2 = (0, 1, 0, \ldots, 0) \in \mathbb{Z}^n$.) Now define $a_i = f(e_i) \in A$, and let $X$ be the finite subset $\{a_1, \ldots, a_n\}$ of $A$.

Suppose that $\alpha \in A$. Then, since $f$ is surjective, there is a vector

$$\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n) = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_n e_n \in \mathbb{Z}^n$$

such that

$$\alpha = f(\lambda) = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n \in \langle X \rangle.$$

Hence $A = \langle X \rangle$ is finitely generated. □

**Corollary 4** *Let $A$ be a finitely generated abelian group. Then there is a natural number $n$ and a subgroup $K$ of $\mathbb{Z}^n$ such that $A \cong \mathbb{Z}^n / K$.*

*Proof.* By the Lemma, there is a homomorphism $f : \mathbb{Z}^n \to A$, for some $n$, which is surjective, that is $A = \mathrm{Im}(f)$. By the First Isomorphism Theorem, $A = \mathrm{Im}(f) \cong \mathbb{Z}^n / \mathrm{Ker}(f)$, so the result follows by taking $K = \mathrm{Ker}(f)$. □

This last corollary tells us that we can understand all finitely generated abelian groups, provided that we can understand all the subgroups of the groups $\mathbb{Z}^n$. The first thing to note is that all such subgroups are themselves finitely generated.

**Lemma 21** *If $H$ is a subgroup of $\mathbb{Z}^n$, then $H$ has a generating set with $n$ or fewer elements. Indeed, $H \cong \mathbb{Z}^m$ for some $m \leq n$.*

*Proof.* The proof is by induction on $n$. In the case $n = 1$, the result is just the fact (which we proved earlier) that every subgroup of $\mathbb{Z}$ is cyclic. The trivial subgroup of $\mathbb{Z}$ is isomorphic to $\mathbb{Z}^0$, while any nontrivial subgroup is infinite cyclic, so is isomorphic to $\mathbb{Z} = \mathbb{Z}^1$.

For the inductive step, let $B$ be the cyclic subgroup of $\mathbb{Z}^n$ generated by $(0, \ldots, 0, 1)$., and note that $B$ is the kernel of the homomorphism $\mathbb{Z}^n \to \mathbb{Z}^{n-1}$ defined by

$$(\lambda_1, \ldots, \lambda_{n-1}, \lambda_n) \mapsto (\lambda_1, \ldots, \lambda_{n-1}).$$

Since $B$ is cyclic, so is $H \cap B$, so let us choose a generator $h_0$ of $H \cap B$.

By inductive hypothesis, the subgroup $(H + B)/B$ of $\mathbb{Z}^n / B \cong \mathbb{Z}^{n-1}$ is isomorphic to $\mathbb{Z}^k$ for some $k \leq n - 1$, and so has a generating set with $k$ elements – say $\{h_1 + B, \ldots, h_k + B\}$, where $h_1, \ldots, h_k \in H$.

If $h_0 = 0$, then $H \cap B = \{0\}$, and the Third Isomorphism Theorem says that

$$\mathbb{Z}^k \cong \frac{(H + B)}{B} \cong \frac{H}{H \cap B} \cong H.$$

The result follows in this case.

Now suppose that $h_0 \neq 0$, and let $\phi : \mathbb{Z}^k \to (H+B)/B$ be an isomorphism. For $i = 1, \dots k$, let $e_k \in \mathbb{Z}^k$ be the element whose $i$th coordinate is 1 and whose other coordinates are 0, and choose $h_i \in H$ such that $\phi(e_i) = h_i + B \in (H+B)/B$. Define $\theta : \mathbb{Z}^{k+1} \to H$ by

$$\theta(\lambda_0, \lambda_1, \dots, \lambda_k) = \lambda_0 h_0 + \lambda_1 h_1 + \cdots \lambda_k h_k.$$

Then $\theta$ is a group homomorphism, since $H$ is abelian. It is also injective, which we can see as follows. If $\theta(\lambda_0, \lambda_1, \dots, \lambda_k) = 0$ then $\phi(\lambda_1, \dots, \lambda_k) = -\lambda_0 h_0 + B = 0 + B$, whence $\lambda_1 = \cdots = \lambda_k = 0$, since $\phi$ is injective. But then $0 = \theta(\lambda_0, 0, \dots, 0) = \lambda_0 h_0 \Rightarrow \lambda_0 = 0$. Hence $\mathrm{Ker}(\theta) = \{0\}$.

Finally, to see that $\theta$ is surjective, let $h \in H$, let $(\lambda_1, \dots, \lambda_k) = \phi^{-1}(h+B)$ in $\mathbb{Z}^k$. Then $y = h - \lambda_1 h_1 - \cdots - \lambda_k h_k \in H \cap B = \langle h_0 \rangle$, so $y = \lambda_0 h_0$ for some $\lambda_0 \in \mathbb{Z}$, and then

$$\theta(\lambda_0, \lambda_1, \dots, \lambda_k) = \lambda_0 h_0 + \lambda_1 h_1 + \cdots + \lambda_k h_k = h.$$

□

**Example.** Let $f : \mathbb{Z}^2 \to \mathbb{Z}$ be the homomorphism defined by $f(m,n) = 2m + 3n$. Then $\mathrm{Ker}(f)$ is cyclic, with generator $(-3, 2)$. Certainly $f(-3,2) = 0$ from the definition of $f$, so the cyclic subgroup generated by $(-3,2)$ must be contained in the kernel of $f$. Conversely, if $2m + 3n = f(m,n) = 0$, then $3n = -2m$ is even, so $n$ must be even – say $n = 2k$, where $k \in \mathbb{Z}$. Then $2m = -3n = -6k$ implies that $m = -3k$, so $(m,n) = (-3k, 2k) = k(-3,2) \in \langle(-3,2)\rangle$. This confirms that $\mathrm{Ker}(f) = \langle(-3,2)\rangle$.

The groups $\mathbb{Z}^n$ for $n = 0, 1, 2, \dots$ clearly play a big part in the understanding of all finitely generated abelian groups. This rôle is in some ways analogous to that of the vector spaces $\mathbb{R}^n$ in linear algebra. On the other hand, while every finite-dimensional real vector space is isomorphic to $\mathbb{R}^n$ for some $n$, it is not true that every finitely generated abelian group is isomorphic to $\mathbb{Z}^n$ for some $n$ - the finite abelian groups are counterexamples. The groups $\mathbb{Z}^n$ are special and have a name to match.

**Definition.** A group $(A, +)$ is *free abelian* if it is isomorphic to $(\mathbb{Z}^n, +)$ for some natural number $n$. The number $n$ is called the *rank* of the free abelian group $A$.

As indicated above, free abelian groups have many features in common with vector spaces. Here is one more.

**Definition.** A subset $X = \{x_1, \dots, x_n\}$ of an abelian group $(A, +)$ is *linearly independent* if, whenever $\lambda_1, \dots, \lambda_n \in \mathbb{Z}$ with $\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$, then $\lambda_1 = \cdots = \lambda_n = 0$. Equivalently, $X$ is linearly independent if the homomorphism $\theta : \mathbb{Z}^n \to A$ defined by $\theta(\lambda_1, \dots, \lambda_n) = \lambda_1 x_1 + \cdots + \lambda_n x_n$ is injective. A *basis* for $A$ is a linearly independent generating set. Equivalently, $X$ is a basis for $A$ if the map $\theta : \mathbb{Z}^n \to A$ defined above is an isomorphism.

Thus, only free abelian groups have bases. By the previous result, every subgroup of a free abelian group is free abelian, and hence has a basis. How can we find such a basis in practice? Let us first consider the case of the free abelian group of rank 1, namely $\mathbb{Z}$. Suppose that we are given a finite subset $X \subset \mathbb{Z}$. We know that $\langle X \rangle$ is a cyclic subgroup of $\mathbb{Z}$. How can we find a generator?

In the simplest case, $X = \{m, n\}$. Suppose that $\langle m, n \rangle = \langle k \rangle = k\mathbb{Z}$. Then $m, n \in k\mathbb{Z}$, so each of $m, n$ is a multiple of $k$. We also say that $k$ is a *common divisor* of $m, n$. Conversely, if $\ell$ is a common factor of $m, n$, then $m, n \in \ell\mathbb{Z}$, and so $k\mathbb{Z} = \langle X \rangle \subset \ell\mathbb{Z}$. In particular, $k \in \ell\mathbb{Z}$, so $k$ is a multiple of $\ell$. Assuming that $k \geq 0$ (which we may do, since $\langle -k \rangle = \langle k \rangle$), we see that $k$ is greater than any other common divisor of $m, n$. This $k$ is called the *greatest common divisor* (gcd) of $m, n$. There is an effective algorithm to find the gcd of two integers $m, n$.

## The Euclidean Algorithm

```
Input: $m, n \in \mathbb{Z}$;
Replace $m$ by $|m| \geq 0$, $n$ by $|n| \geq 0$;
If $n < m$, then interchange $m, n$; endif;
If $m = 0$ then OUTPUT $n$ and STOP; endif;
(*): Divide $n$ by $m$ to get $n = qm + r$ with $0 \leq r \leq m - 1$;
If $r = 0$ then OUTPUT $m$ and STOP; endif;
Replace $m$ by $r$ and replace $n$ by $m$;
GOTO (*)
```

**Example.** Find the gcd of 1755 and 432.
Since $1755 > 432$, we interchange them, so that $(m, n) = (432, 1755)$.
$1755 = 432 \times 4 + 27$, so we replace $(432, 1755)$ by $(27, 432)$.
$432 = 27 \times 16 + 0$, so we stop and deduce that 27 is the gcd of 1755 and 432.

We can find the gcd of three or more integers by repeated use of the algorithm. For example, to find the gcd of three integers $m, n, p$, we can first find the gcd of $m, n$ – $q$, say – and then find the gcd of $p, q$.

Here is another way to look at the Euclidean Algorithm. Consider a 2 × 1 matrix with integer entries, $\begin{pmatrix} m \\ n \end{pmatrix}$. The algorithm operates on this matrix using elementary row operations of two types: (i) interchange the two rows (interchange $m$ and $n$); (ii) subtract an integer multiple of one row from the other row (replace $n$ by $r = n - qm$). The output of the algorithm is then $\begin{pmatrix} k \\ 0 \end{pmatrix}$, where $k$ is the gcd of $m, n$.

More generally, suppose that $X$ is a finite subset of $\mathbb{Z}^n$. We can regard the elements of $X$ as row vectors of length $n$ with integer entries, which we can lay out as an $m \times n$ matrix, where $m = |X|$.

**Lemma 22** *Suppose that $M_1, M_2$ are two $m \times n$ matrices, such that $M_2$ can be obtained from $M_1$ by a sequence of elementary row operations of types* (i) *and* (ii) *above. Then the subgroup $H_1 \subset \mathbb{Z}^n$ generated by the rows of $M_1$ is equal to the subgroup $H_2 \subset \mathbb{Z}^n$ generated by the rows of $M_2$.*

*Proof.* By induction on the number of row operations used, it is enough to prove the result in the case where $M_2$ is obtained from $M_1$ by a single row operation of type (i) or (ii).

But a type (i) operation is just a permutation of the rows of the matrix, so does not change the generating set. Hence it also does not change the subgroup generated by that set.

Suppose then that $M_2$ is obtained from $M_1$ by a single operation of type (ii). Without loss of generality this operation subtracts an integer multiple of the second row of $M_1$ from the first row. Thus if the rows of $M_1$ are $v_1, v_2, \dots, v_m$, then the rows of $M_2$ are $v_1 - qv_2, v_2, \dots, v_m$, with $q \in \mathbb{Z}$. Now $v_1, v_2 \in H_1$, so $v_1 - qv_2 \in H_1$ since $H_1$ is a subgroup. Since also $v_2, \dots, v_m \in H_1$, $H_1$ contains the generating set of $H_2$, and hence $H_2 \subset H_1$.

Conversely, since $v_1 - qv_2 \in H_2$, $v_2 \in H_2$ and $H_2$ is a subgroup, $v_1 = (v_1 - qv_2) + qv_2 \in H_2$. Since also $v_2, \dots, v_m \in H_2$, $H_2$ contains the given generating set of $H_1$, so $H_1 \subset H_2$. Hence $H_1 = H_2$, as claimed. □

Hence we may adapt the Euclidean Algorithm to find a basis for the subgroup $\langle X \rangle$ of $\mathbb{Z}^n$, for any given finite set $X \subset \mathbb{Z}^n$ as follows. As before, express $X$ as the rows of an $m \times n$ matrix $M$.

```
(a) Use row operations (i) and (ii) to change $M$ to a matrix whose
first nonzero column contains only one nonzero entry, in the first row.
...
(b) Leaving the first row unchanged, use more row operations (i) and
(ii) until the first column of $M$ to contain a nonzero entry below the
first row contains only one such entry, in the second row.
...
(c) Continue until $M$ is in row echelon form.
(The nonzero rows are then linearly independent, so form a basis for
the subgroup that they generate.)
```

**Example.** Find a basis for the subgroup $H$ of $\mathbb{Z}^3$ generated by $\{(0,3,8), (2,6,4), (4,9,0)\}$.

$$\begin{pmatrix} 0 & 3 & 8 \\ 2 & 6 & 4 \\ 4 & 9 & 0 \end{pmatrix} \to \begin{pmatrix} 2 & 6 & 4 \\ 4 & 9 & 0 \\ 0 & 3 & 8 \end{pmatrix} \to \begin{pmatrix} 2 & 6 & 4 \\ 0 & -3 & -8 \\ 0 & 3 & 8 \end{pmatrix} \to \begin{pmatrix} 2 & 6 & 4 \\ 0 & -3 & -8 \\ 0 & 0 & 0 \end{pmatrix}.$$

So $\{(2,6,4), (0,-3,-8)\}$ is a basis for $H$.

## 7.4 Exercises

1. Which of he following groups are abelian?

   (a) $(\mathbb{C}^2, +)$;

   (b) $A_4$;

   (c) $D_7$;

   (d) $\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \subset S_4$;

   (e) $(\mathbb{R} \smallsetminus \{0\}, \cdot)$;

   (f) The group $SL(2, \mathbb{Z})$ of $2 \times 2$ matrices with integer entries and determinant 1 (where the binary operation is matrix multiplication).

2. Suppose that $(A, +)$ is an abelian group. Show that $f : A \to A$, $f(a) = a + a$ for all $a \in A$, is a homomorphism. Deduce that $2A := \{a + a;\ a \in A\}$ is a subgroup of $(A, +)$.
   Show that every element of the quotient group $A/2A$ has order 1 or 2.

3. How many elements of order 2 are there in each of the following abelian groups? (i) $\mathbb{Z}_4$; (ii) $\mathbb{Z}_{10}$; (iii) $\mathbb{Z}_{1000}$; (iv) $\mathbb{Z}_{999}$; (v) $\mathbb{Z}_4 \times \mathbb{Z}_4$; (vi) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
   Deduce that $\mathbb{Z}_4 \times \mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

4. Use the Euclidean algorithm to find the highest common factor of 768 and 666. Given that $768 \times 666 = 511488$, find the order of the subgroup of $\mathbb{Z}_{511488}$ generated by $\{768, 666\}$.

5. Find a basis for the subgroup of $\mathbb{Z} \times \mathbb{Z}$ generated by $\{(6, 6), (11, 15), (16, 18)\}$.

6. Let $(G, *)$ be a group (not necessarily abelian) and let $a, b \in G$. If $f : \mathbb{Z} \times \mathbb{Z} \to G$ is a homomorphism such that $f(1, 0) = a$ and $f(0, 1) = b$, show that $a, b$ commute in $G$ (that is, $a * b = b * a$).

   Conversely, if $a * b = b * a$, can you find a homomorphism $f : \mathbb{Z} \times \mathbb{Z} \to G$ such that $f(1, 0) = a$ and $f(0, 1) = b$?

# Chapter 8

# More on Abelian Groups

## 8.1 Finitely Generated Abelian Groups

If $A$ is a finitely generated abelian group, then we have seen that there is a natural number $n$ and a subgroup $K$ of $\mathbb{Z}^n$ such that $A \cong \mathbb{Z}^n/K$. Moreover, $K$ is free abelian of rank $m \leq n$. A basis for $K$ can be expressed as the set of rows of an $m \times n$ matrix: such a matrix is known as a *presentation matrix* for $A$.

**Example.**

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix}$$

is a presentation matrix for $A = \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}$, since the subgroup $K$ of $\mathbb{Z}^3$ generated by the rows of the matrix is

$$K = \{(3m, 4n, 0);\ m, n \in \mathbb{Z}\} = 3\mathbb{Z} \times 4\mathbb{Z} \times 0\mathbb{Z}$$

and so

$$\frac{\mathbb{Z}^3}{K} = \frac{\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}}{3\mathbb{Z} \times 4\mathbb{Z} \times 0\mathbb{Z}} = \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{0\mathbb{Z}} \cong \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}.$$

Of course, since $\mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_{12}$, it follows that

$$\begin{pmatrix} 12 & 0 \end{pmatrix}$$

is another presentation for $A \cong \mathbb{Z}_{12} \times \mathbb{Z}$.

**Lemma 23** *Let the $m \times n$ matrix $M$ be a presentation matrix for a finitely generated abelian group $A$. If $m = n$ then $A$ is finite, of order $|\det(M)|$, where $M$ is any presentation matrix for $A$. Otherwise there exists a surjective homomorphism $A \to \mathbb{Z}$.*

*Proof.* Since the rows of $M$ represent a basis for $K$, they are linearly independent. Suppose first that $m = n$. Then the euclidean algorithm will transform $M$ into a new presentation matrix $M'$ which is *upper triangular* in the sense that the entries below the diagonal are all 0: $m_{i,j} = 0$ for $i > j$.

The elementary row operations used in the euclidean algorithm do not alter the fact that the rows are linearly independent. Moreover, the only effect they have on the determinant is to multiply it by 1 or $-1$, so $|\det(M)| = |\det(M')| = |\mu_1 \cdots \mu_n|$, where $\mu_1, \ldots, \mu_n$ are the diagonal entries in $M'$.

Let $B$ be the cyclic subgroup of $A$ generated by $e_n = (0, \ldots, 0, 1)$. Then $B$ has order $|\mu_n|$ in $A$, since $(0, \ldots, 0, \mu_n) = \mu_n e_n$ is one of the rows of the presentation matrix $M'$. Moreover, $A/B$ is generated by $e_1, \ldots, e_{n-1}$, and we can get a presentation matrix $M$" for $A/B$ by removing the $n$th row and the $n$th column from $M'$. By induction on $n$ we can assume that $A/B$ is finite of order $|\mu_1 \cdots \mu_{n-1}|$, and it follows that $A$ is finite of order $|A/B| \cdot |B| = |\mu_1 \cdots \mu_n|$.

Now assume that $m < n$. For any vector $v = (v_1, \ldots, v_n) \in \mathbb{Z}^n$, we can define a homomorphism $\phi_v : \mathbb{Z}^n \to \mathbb{Z}$ by $\phi_v(u) = u.v = u_1 v_1 + \cdots + u_n v_n$. Suppose that $u.v = 0$ whenever $u$ is one of the rows of the presentation matrix $M$ for $A$. Then each row of $M$ belongs to $\mathrm{Ker}(\phi_v)$. Hence the subgroup $K$ of $\mathbb{Z}^n$ generated by the rows of $M$ is also contained in $\mathrm{Ker}(\phi_v)$, and we may then define a homomorphism $\theta_v : A = \mathbb{Z}^n/K \to \mathbb{Z}$ by $\theta_v(u + K) = u.v = \phi_v(u)$.

We have an $n$-parameter family $\phi_v$, $v = (v_1, \ldots, v_n) \in \mathbb{Z}^n$ of homomorphisms $\mathbb{Z}^n \to \mathbb{Z}$, and a family of $m$ linear equations $u.v = 0$ that determine which of the $\phi_v$ give rise to homomorphisms $\theta_v : A \to \mathbb{Z}$. Since $m < n$, there is at least one nonzero solution to this family of simultaneous equations, and so at least one nonzero homomorphism $\theta_v : A \to \mathbb{Z}$.

Of course, the homomorphism $\theta_v$ is not necessarily surjective. However, since it is nonzero, its image $\mathrm{Im}(\theta_v)$ has the form $k\mathbb{Z}$ for some $k > 0$, so $\theta : A \to \mathbb{Z}$ defined by $\theta(u) = \theta_v(u)/k$ is surjective. □

**Example.** Let

$$M = \begin{pmatrix} 4 & 3 \\ 5 & 2 \end{pmatrix}$$

be a presentation matrix for a finitely generated abelian group $A$. Then $\det(M) = 8 - 5 = -7$, so $A$ has order 7, which is a prime number, and hence $A \cong \mathbb{Z}_7$. To see this isomorphism more directly, we can use row operations to put $M$ into row echelon form, for example:

$$\begin{pmatrix} 4 & 3 \\ 5 & 2 \end{pmatrix} \to \begin{pmatrix} 5 & 2 \\ 4 & 3 \end{pmatrix} \to \begin{pmatrix} 1 & -1 \\ 4 & 3 \end{pmatrix} \to \begin{pmatrix} 1 & -1 \\ 0 & 7 \end{pmatrix}$$

Then the subgroup $K$ generated by the rows of $M$ is also generated by the rows of the new matrix, $(1, -1) = e_1 - e_2$, and $(0, 7) = 7e_2$. The group $A = \mathbb{Z}^2/K$ is generated by two elements, $a_1 = e_1 + K$ and $a_2 = e_2 + K$. But the fact that $e_1 - e_2 \in K$ means that $a_1 - a_2 = 0$ in $A$, ie $a_1 = a_2$, so $A$ is cyclic. The fact that $7e_2 \in K$ means that $7a_2 = 0$ in $A$, so $A$ is cyclic of order dividing 7. On the other hand, the order of $A$ must be greater than 1, since no $\mathbb{Z}$-linear combination of the rows of $M$ contains $e_2$, so $e_2 \notin K$, so $a_2 \neq 0$ in $A$. Thus $A \cong \mathbb{Z}_7$, as promised by the Lemma.

**Example.** Let

$$M = \begin{pmatrix} 1 & 4 & 3 \\ 0 & 5 & 2 \end{pmatrix}$$

be a presentation matrix for a finitely generated abelian group $A$. Since $M$ has fewer rows than columns, the Lemma tells us that there must be a surjective homomorphism $f : A \to \mathbb{Z}$. Now $A = \mathbb{Z}^3/K$, where $K$ is the subgroup generated by the rows of $M$, and so $A$ is generated by $a_1 = e_1 + K$, $a_2 = e_2 + K$ and $a_3 = e_3 + K$. To find a homomorphism $f$, we need to define $f(a_1) = u_1$, $f(a_2) = u_2$ and $f(a_3) = u_3$, where $u_1, u_2, u_3 \in \mathbb{Z}$ are solutions of the simultaneous linear equations

$$1.u_1 + 4.u_2 + 3.u_3 = 0,$$

$$0.u_1 + 5.u_2 + 2.u_3 = 0.$$

A nonzero solution to the second equation can be obtained by putting $u_2 = 2$ and $u_3 = -5$. We may than substitute these values back into the first equation to get $u_1 = 7$.

**Lemma 24** *Let $A$ be an abelian group, and let $\theta : A \to \mathbb{Z}$ be a surjective homomorphism. Then $A \cong \mathrm{Ker}(\theta) \times \mathbb{Z}$.*

*Proof.* Choose $a \in A$ such that $\theta(a) = 1 \in \mathbb{Z}$. Define $\phi : \mathrm{Ker}(\theta) \times \mathbb{Z} \to A$ by $\phi(x, n) = x + na$.

Then $\phi$ is a homomorphism, since

$$\phi((x_1, n_1) + (x_2, n_2)) = \phi(x_1 + x_2, n_1 + n_2) = x_1 + x_2 + (n_1 + n_2)a$$

$$= (x_1 + n_1 a) + (x_2 + n_2 a) = \phi(x_1, n_1) + \phi(x_2, n_2).$$

Moreover, if $(x, n) \in \mathrm{Ker}(\phi)$ then

$$n = \theta(na) = \theta(x) + \theta(na) = \theta(x + na) = \theta(\phi(x, n)) = \theta(0) = 0,$$

and hence also $x = \phi(x, 0) = \phi(x, n) = 0$. Thus $\ker(\phi) = \{(0, 0)\}$ and so $\phi$ is injective.

Finally, if $\alpha \in A$, let $m = \theta(\alpha) \in \mathbb{Z}$, and let $y = \alpha - ma$. Then $\theta(y) = \theta(\alpha) - m\theta(a) = m - m = 0$, so $y \in \mathrm{Ker}(\theta)$. Moreover, $\phi(y, m) = y + ma = \alpha$. Hence $\phi$ is also surjective.

Thus $\phi$ is an isomorphism from $\mathrm{Ker}(\theta) \times \mathbb{Z}$ to $A$, as required. □

**Corollary 5** *Let $A$ be a finitely generated abelian group. Then there is a finite subgroup $A_0$ of $A$ and an integer $m \geq 0$ such that $A \cong A_0 \times \mathbb{Z}^m$.*

*Proof.* We know that $A \cong \mathbb{Z}^n/K$ for some integer $n \geq 0$ and some subgroup $K \subset \mathbb{Z}^n$, where $K$ is free abelian of rank $r \leq n$. If $r = n$ then we know from Lemma 23 that $A$ is finite, so we can take $A_0 = A$. Otherwise we know – also from Lemma 23 – that there exists a surjective homomorphism $f : A \to \mathbb{Z}$. Composing $f$ with the surjective quotient map $\mathbb{Z}^n \to A$, we also get a surjective homomorphism $\phi : \mathbb{Z}^n \to \mathbb{Z}$.

By the last Lemma, $A \cong \mathrm{Ker}(f) \times \mathbb{Z}$, and similarly $\mathbb{Z}^n \cong \mathrm{Ker}(\phi) \times \mathbb{Z}$. Since we also know that $\mathrm{Ker}(\phi) \subset \mathbb{Z}^n$ is free abelian of rank $t \leq n$, it follows that $t = n - 1$. Also $\mathrm{Ker}(f) \cong \mathrm{Ker}(\phi)/K$. By induction on $n-r$, we may assume that $\mathrm{Ker}(f) \cong A_0 \times \mathbb{Z}^{n-1-r}$ for some finite subgroup $A_0$, and hence $A \cong \mathrm{Ker}(f) \times \mathbb{Z} \cong A_0 \times \mathbb{Z}^{n-r}$. □

## 8.2 Finite Abelian Groups

Corollary 5 reduces the classification of finitely generated abelian groups to that of finite abelian groups.

The next step is to simplify further. We start with a result similar to the Chinese Remainder Theorem.

**Lemma 25** *Let $A$ be a finite abelian group of order $mn$, where $m, n$ are positive integers which are* coprime *– in other words $hcf(m,n) = 1$. Then $A \cong mA \times nA$.*

*Proof.* The map $f : A \to mA \times nA$ defined by $f(a) = (ma, na)$ is a homomorphism, since

$$f(a+b) = (m(a+b), n(a+b)) = (ma+mb, na+nb) = (ma, na)+(mb, nb) = f(a)+f(b).$$

It is also injective, because $hcf(m,n) = 1$ means that $m, n$ generate $\mathbb{Z}$, which means that $mp + nq = 1$ for some integers $p, q$, and so if $a \in A$ with $(ma, na) = (0,0)$ then $a = (mp + nq)a = p(ma) + q(na) = 0$.

Finally, if $a \in A$ then $mna = 0$ by Lagrange's Theorem, since $|A| = mn$. If $p, q \in \mathbb{Z}$ with $mp + nq = 1$, then $f(mpa) = (m^2pa, mnpa) = (ma - mnqa, mnpa) = (ma, 0)$. Similarly, if $a' \in A$, then $f(nqa') = (0, na')$. But then an arbitrary element of $mA \times nA$ has the form $(ma, na') = f(mpa + nqa')$ for some $a, a' \in A$, and so $f$ is surjective.

Hence $f : A \to mA \times nA$ is an isomorphism. □

**Definition.** Let $p$ be a prime number. A *$p$-group* is a finite group whose order is a power of $p$.

**Lemma 26** *A finite abelian group $A$ is a $p$-group if and only if the order of each element $a \in A$ is a power of $p$.*

*Proof.* By Lagrange's Theorem, if $|A|$ is a power of $p$, then so is the order of each $a \in A$. We prove the converse by induction on $|A|$. The result is trivial if $|A| = 1$. If $|A| > 1$, choose $b \neq 0$ in $A$, and let $B = \langle b \rangle$. Then $|B|$ is a power of $p$ by hypothesis. Also, for any $a \in A$, the order of $a + B$ in $A/B$ divides the order of $a$ in $A$, and hence is a power of $p$. By inductive hypothesis, $|A/B|$ is a power of $p$, and hence so is $|A| = |B| \cdot |A/B|$. □

**Corollary 6** *Let $A$ be a finite abelian group, and let $p_1, \dots, p_k$ be the prime numbers that divide $|A|$. Then $A \cong A_1 \times \cdots \times A_k$, where for each $i = 1, \dots, k$ the group $A_i$ is a finite abelian $p_i$-group.*

*Proof.* Suppose that $|A| = mp_k^t$, where $p_k$ does not divide $m$. Then $A \cong mA \times nA$ where $n = p_k^t$. Note that $mA \cong A/p_k^t A$ is a group in which $p_k^t b = 0$ for each element $b$, and so the order of each element is a power of $p_k$, so $mA$ is a $p_k$-group.

By induction on $|A|$, we may assume that $nA$ is a direct product of $p_i$-groups for various primes $p_i$, and then the same is true for $A \cong mA \times nA$. The primes involved all divide the order of $A$, by Lagrange's Theorem. □

**Definition.** In the decomposition $A \cong A_1 \times \cdots \times A_k$ of $A$ as a direct product of $p_i$-groups for various primes $p_i$, the direct factors $A_i$ are called the *$p_i$-primary components* of $A$.

**Example.** The abelian group $\mathbb{Z}_{240}$ is isomorphic to $\mathbb{Z}_{16} \times \mathbb{Z}_3 \times \mathbb{Z}_5$ by the Chinese Remainder Theorem. Thus the 2-primary component of $\mathbb{Z}_{240}$ is $\mathbb{Z}_{16}$.

## 8.3 Finite Abelian $p$-groups

We are now reduced to the study of finite abelian $p$-groups. There are many examples of these - such as $\mathbb{Z}_p$, $\mathbb{Z}_{p^2}$, $\mathbb{Z}_p \times \mathbb{Z}_p$, etc.

Indeed, for any finite sequence $\sigma = (t_1, \dots, t_k)$ of positive integers, there is a finite abelian $p$-group

$$A_\sigma = \mathbb{Z}_{p^{t_1}} \times \cdots \times \mathbb{Z}_{p^{t_k}}.$$

Are these all different? Well, since $A \times B \cong B \times A$ (exercise), they can only be different up to reordering the factors, so we may assume (for example) that the sequence of positive integers $(t_1, \dots, t_k)$ is non-decreasing: $t_1 \leq \cdots \leq t_k$.

The groups $A_\sigma$ for different $\sigma$ are then non-isomorphic. To see this, one can easily check that the largest order of any element of $A_\sigma$ is $p^{t_k}$ where $t_k$ is the largest term of the sequence $\sigma$, and then argue by induction on the length $k$ of the sequence.

Finally, we show that the groups $A_\sigma$ just defined are the only finite abelian $p$-groups, up to isomorphism. Let $A = \mathbb{Z}^n/K$ be a finite abelian $p$-group, where $n$ is chosen to be as small as possible, and $K$ is a rank $n$ subgroup of $\mathbb{Z}^n$. The proof of Lemma 23 shows that we may choose a presentation matrix $M$ for $A$ which is upper triangular. The order of $A$ is then the absolute value of the determinant of $M$, which is the product of the diagonal elements. Thus each diagonal element of $M$ is a power of $p$.

We have already seen how to manipulate $M$ using the elementary row operations: (i) interchange two rows; and (ii) subtract a multiple of one row from another row.

We can also use the corresponding elementary column operations: (i)' interchange two columns; and (ii)' subtract a multiple of one column from another column. These represent a change of basis in $\mathbb{Z}^n$, so do not change the isomorphism type of the corresponding quotient group $\mathbb{Z}^n/K$.

Using elementary row and column operations, we may change $M$ in such a way that the top left hand entry is the highest common factor of *all* the entries in the matrix, and such that moreover all the other entries in the first row and in the first column are zero.

We may then repeat this procedure on the matrix $M$ with the first row and column removed, and so on. In this way, we can replace $M$ by a diagonal matrix. Let $m_1, \dots, m_n$ be the diagonal entries of this amended matrix $M$. Writing the standard basis elements $(1,0,\dots,0), (0,1,0,\dots,0)$, etc. as $e_1, e_2, \dots$, we see that the rows of $M$ are $m_1e_1, \dots, m_ne_n$, so

$$A = \frac{\mathbb{Z}^n}{K} = \frac{\mathbb{Z} \times \cdots \times \mathbb{Z}}{m_1\mathbb{Z} \times \cdots \times m_n\mathbb{Z}} \cong \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{m_n\mathbb{Z}}.$$

## 8.4 Conclusion

We have proved the following result, which almost classifies finitely generated abelian groups.

**Theorem 10** *Any finitely generated abelian group is a direct product of cyclic groups.*

This is only an 'almost' classification, since the representation of finite abelian groups as direct products of cyclics is not unique. Indeed the Chinese Remainder Theorem explicitly tells us how to further decompose cyclic groups as direct products of cyclic groups. On the other hand, one can obtain a 'canonical' decomposition as follows. Firstly, decompose as a direct product of $\mathbb{Z}^r$ and a finite abelian group. Secondly, decompose the finite part into its primary components, each of which has a unique expression as a direct product of cyclic groups. Finally, collect together the largest cyclic direct factor for each prime number involved, and express their direct product as a cyclic group using the Chinese Remainder Theorem; repeat with the second-largest factor for each prime, and so on.

The result is as follows:

**Theorem 11** *Let $A$ be a finitely generated abelian group. Then there is a unique non-negative integer $r$ and a unique sequence $m_1, m_2, \dots, m_k$ of positive integers, such that $m_i$ divides $m_{i+1}$ for $1 \leq i \leq k-1$ and*

$$A \cong \mathbb{Z}^r \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}.$$

The direct product decomposition of a finitely generated group $A$ given in this Theorem is called *canonical.*

**Example.** To find the canonical decomposition of $A = \mathbb{Z}_{36} \times \mathbb{Z}_{40} \times \mathbb{Z}_{175}$, we first find the $p$-primary component for each prime $p$ dividing the order of $A$:

$$|A| = 36 \cdot 40 \cdot 175 = (2^2 \cdot 3^2) \cdot (2^3 \cdot 5) \cdot (5^2 \cdot 7).$$

The primes concerned are $2, 3, 5, 7$. The $p$-primary components are

$$A_2 = \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_2, \quad A_3 = \mathbb{Z}_9, \quad A_5 = \mathbb{Z}_5 \times \mathbb{Z}_{25}, \quad A_7 = \mathbb{Z}_7.$$

For each prime, take the largest of the factors, ie $\mathbb{Z}_8$, $\mathbb{Z}_9$, $\mathbb{Z}_{25}$ and $\mathbb{Z}_7$, and combine then using the Chinese Remainder Theorem:

$$\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_{25} \times \mathbb{Z}_7 \cong \mathbb{Z}_{12600}.$$

For the primes $3, 7$ there is only one factor; for $2, 5$ the second largest factor is $\mathbb{Z}_4, \mathbb{Z}_5$ respectively. Combining these gives

$$\mathbb{Z}_4 \times \mathbb{Z}_5 \cong \mathbb{Z}_{20}.$$

For the prime 5, that is all; while for the prime 2 there is one more factor $\mathbb{Z}_2$. Thus the canonical decomposition of $A$ is

$$A \cong \mathbb{Z}_2 \times \mathbb{Z}_{20} \times \mathbb{Z}_{12600}.$$

## 8.5 Exercises

1. Find the rank of each of the following $m \times n$ matrices $M$. Hence find the torsion free rank $d$ of the abelian group $A \cong \mathbb{Z}^n/K \cong A_0 \times \mathbb{Z}^d$, where $K$ is the subgroup of $\mathbb{Z}^n$ generated by the rows of $M$, and $A_0$ is a finite group.

   (a) $\begin{pmatrix} 1 & 1 \end{pmatrix}$;

   (b) $\begin{pmatrix} 1 & 2 & 5 \\ 3 & 6 & 10 \end{pmatrix}$;

   (c) $\begin{pmatrix} 0 & 2 & -2 \\ 3 & -4 & 4 \\ -6 & 26 & -26 \end{pmatrix}$.

2. Find the 2-primary component of each of the following finite abelian groups:

   (a) $\mathbb{Z}_{100}$;

   (b) $\mathbb{Z}_8 \times \mathbb{Z}_6$;

   (c) $\mathbb{Z}_{24} \times \mathbb{Z}_{33} \times \mathbb{Z}_{46}$;

   (d) $\mathbb{Z}_{99} \times \mathbb{Z}_3 \times \mathbb{Z}_{277}$.

3. If positive integers $m, n$ are coprime (that is, their highest common factor is 1), show that there is a surjective homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_m \times \mathbb{Z}_n$, and deduce that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

4. Let $K$ be the subgroup of $\mathbb{Z}^3$ generated by the rows of the matrix $M = \begin{pmatrix} 0 & 2 & 4 \\ 3 & 1 & 1 \\ 6 & 0 & 2 \end{pmatrix}$.
   By calculating the determinant of $M$, show that the group $A = \mathbb{Z}^3/K$ is finite, and determine its order.
   Use integer row and column operations to diagonalise $M$, and hence express $A$ as a direct product of cyclic groups.

5. Express each of the groups in question 2 as

   (a) the direct product of cyclic groups of prime-power orders
   (NB. 23 and 277 are prime numbers);

   (b) a direct product of cyclic groups in canonical form $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, where $n_{i+1}$ is a multiple of $n_i$ for $i = 1, \ldots, k-1$.