Chapter 3

Groups

1 Definition of a group and some examples

Definition 3.1. A **group** is a non-empty set G together with a binary operation $* : G \times G \to G$ (the image of (g, h) being denoted $g * h$ or simply gh) that satisfies the following properties:

1) $\forall g, h, k \in G, \quad (g * h) * k = g * (h * k)$ (associativity)

2) $\exists e \in G\, \forall g \in G, \quad g * e = g \wedge e * g = g$ (identity element)

3) $\forall g \in G\, \exists h \in G, \quad g * h = e \wedge h * g = e$ (inverses)

Remark. Since a group consists of a set G *and* an operation, a good notation would be $(G, *)$. However, it is common to suppress explicit mention of the operation and refer to the group simply as G.

Exercise 70. (a) Prove that the identity element is unique. That is, show that

$$(\forall g \in G, \quad g * e = g \wedge e * g = g) \wedge (\forall g \in G, \quad g * e' = g \wedge e' * g = g) \implies e = e'$$

(b) Show that the element h in the third axiom is uniquely determined by g. That is, for a given $g \in G$,

$$(g * h = e \wedge h * g = e) \wedge (g * h' = e \wedge h' * g = e) \implies h = h'$$

In light of this uniqueness, the element is denoted g^{-1} and called *the* inverse of g.

(c) Let $g, h \in G$. Show that $(g^{-1})^{-1} = g$ and $(g * h)^{-1} = h^{-1} * g^{-1}$.

Definition 3.2. A group G is called **abelian** if $\forall g, h \in G,\ gh = hg$. A group G is called **finite** if the underlying set G is finite.

Example 3.3. 1. $(\mathbb{Z}, +)$ is an infinite abelian group.

2. $(\mathbb{Z}, \times)$ is not a group.

3. $(\mathbb{Z}/2\mathbb{Z}, +)$ is a finite group. It has two elements.

4. If $(K, +, \times)$ is a field, then $(K, +)$ and $(K \setminus \{0\}, \times)$ are (different) abelian groups.

5. $(M_n(K), \times)$ is not a group.

6. $GL(n, K)$ is a (non-abelian) group.

7. Other matrix groups include:

$O(n)$	the group of all $n \times n$ orthogonal matrices (real matrices A such that $A^T A = I$)
$U(n)$	the group of all $n \times n$ unitary matrices (complex matrices U such that $U^* U = I$)
$SL(n, K)$	the group of all $n \times n$ matrices of determinant 1 with entries from the field K
$SO(n)$	the group of all $n \times n$ orthogonal matrices having determinant 1
$SU(n)$	the group of all $n \times n$ unitary matrices having determinant 1

Lemma 3.4

Let G be a group and $g, h, k \in G$. Then

1) $gh = gk \implies h = k$
2) $\exists!\, l \in G, \quad gl = h$
3) The map $L_g : G \to G$, $L_g(x) = gx$ is a bijection.
   The map $R_g : G \to G$, $R_g(x) = xg$ is also a bijection.

Exercise 71. Write out a proof of Lemma 3.4.

Example 3.5. Here are two groups of size 4. Let

$$V = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\} \subset GL(2, \mathbb{R})$$
$$C_4 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\} \subset GL(2, \mathbb{R})$$

with the operation in both cases defined to be matrix multiplication.
Notice that in V every element has square equal to the identity. That's not the case in C_4 where, for example, $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]^2 = \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right] \neq \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$.

1.1 Exercises

Exercise 72. Write down the multiplication tables for V and C_4.

Exercise 73. Show that the set of all rotations of the plane about a fixed centre P, together with the operation of composition, forms a group. What about all of the reflections for which the axis (or mirror) passes through P?

Exercise 74. Suppose that x and y are elements of a group. Show that there are elements w and z so that $wx = y$ and $xz = y$. Show that w and z are unique. Must w be equal to z?

Exercise 75. Set $X = \mathbb{R} \setminus \{0, 1\}$. Show the following set of functions $X \to X$, together with the operation of composition, forms a group.

$$\begin{array}{lll} f(x) = \frac{1}{1-x} & g(x) = \frac{x-1}{x} & h(x) = \frac{1}{x} \\ i(x) = x & j(x) = 1 - x & k(x) = \frac{x}{x-1} \end{array}$$

Exercise 76. If G is a group and $(gh)^2 = g^2h^2$ for all $g, h \in G$, prove that G is abelian.

2 The symmetric groups S_n

We investigate the permutations of a fixed set.

Definition 3.6. Let $n \in \mathbb{N}$. A **permutation** of the set $\{1, \ldots, n\}$ is a bijecion $\{1, \ldots, n\} \to \{1, \ldots, n\}$. The group of all permutations of the set $\{1, \ldots, n\}$ is denoted by S_n and called the **symmetric group** (on n letters). The operation is the usual composition of functions.

Remark. It is clear that $|S_n| = n!$.

2.1 Notations for permutations

Let $\sigma \in S_n$. One way of specifying σ is as two rows, with the image $\sigma(i)$ written directly below i. That is, as

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Example 3.7. There are six permutations of the set $\{1, 2, 3\}$. We can list the six elements of S_3 as follows:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 1 \end{pmatrix}, \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

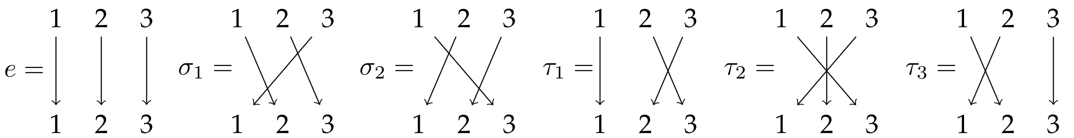
Since the operation is composition of functions we have, for example:

$$\tau_3\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \tau_1$$
$$\sigma_1\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau_2$$

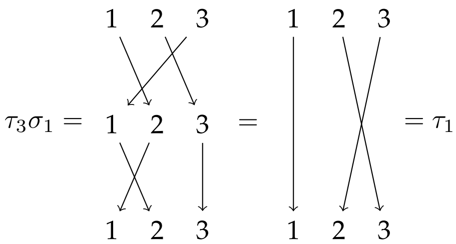
Notice that the group S_3 is not abelian since $\tau_3\sigma_1 \neq \sigma_1\tau_3$. The full multiplication table for S_3 is given on the right.

S_3	e	σ_1	σ_2	τ_1	τ_2	τ_3
e	e	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	e	τ_3	τ_1	τ_2
σ_2	σ_2	e	σ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	e	σ_1	σ_2
τ_2	τ_2	τ_3	τ_1	σ_2	e	σ_1
τ_3	τ_3	τ_1	τ_2	σ_1	σ_2	e

Another notation used for elements of S_n is to write the set $\{1, \ldots, n\}$ twice and then join i to $\sigma(i)$ by a directed edge. To illustrate, we list the elements of S_3 in this notation:



To multiply elements in this notation, we simply place one diagram on top of the other and amalgamate the directed edges. For example:



Cycle notation

A third more compact notation is known as **cycle notation**. In this notation each element $\sigma \in S_n$ is represented by a collection tuples ('cycles') in which each element $i \in \{1, \ldots, n\}$ appears exactly once as in followed immediately by $\sigma(i)$ (with the last element of a tuple being 'followed' by the first). Some examples will make this clear. We list the elements of S_3 in cycle notation:

$$e = (1)(2)(3) \quad \sigma_1 = (1, 2, 3) \quad \sigma_2 = (1, 3, 2) \quad \tau_1 = (1)(2, 3) \quad \tau_2 = (1, 3)(2) \quad \tau_3 = (1, 2)(3)$$

It is common to adopt the further conventions that singletons are omitted and commas are dropped (unless the notation would be made ambiguous). With these conventions we have:

$$\sigma_1 = (123) \quad \sigma_2 = (132) \quad \tau_1 = (23) \quad \tau_2 = (13) \quad \tau_3 = (12)$$

The identity element will be denoted as (1) or simply as e.

We will generally use cyclic notation and give here an example of multiplication written in cycle notation.

Example 3.8. Consider $\sigma, \tau \in S_7$ given by $\sigma = (1234)(567)$, $\tau = (143)(267)$. Then

$$\sigma\tau = (1234)(567)(143)(267) = (1)(273)(4)(56) = (273)(56)$$
$$\tau\sigma = (143)(267)(1234)(567) = (162)(3)(4)(57) = (162)(57)$$

Remark. Cycle notation for a permutation is *not* unique, for example $(123) = (231) = (312)$ as they all represent the permutation mapping $1 \mapsto 2$, $2 \mapsto 3$ and $3 \mapsto 1$. Also, $(123)(45) = (45)(123)$.

Exercise 77. Find the product of the following permutations:

(a) $(123)(456) * (134)(25)(6)$ (b) $(12345) * (1234567)$ (c) $(123456) * (123) * (123) * (1)$

3 Subgroups

Definition 3.9. Let G be a group. A **subgroup** of G is a subset $H \subset G$ which, when equipped with the operation from G (restricted to H), itself forms a group. We will use the notation $H \leqslant G$.

Remark. It is clear from the definition that $\{e\} \leqslant G$. It is called the **trivial subgroup**.

Example 3.10. Some examples of groups G and a subgroup $H \leqslant G$.

1. $G = (\mathbb{Z}/4\mathbb{Z}, +)$, $H = \{[0], [2]\}$
2. $G = S_3$, $H = \{e, (123), (132)\}$
3. $G = S_3$, $H = \{e, (13)\}$
4. $G = (\mathbb{Z}, +)$, $H = 2\mathbb{Z}$
5. $G = GL(n, K)$, $H = SL(n, K)$
6. $G = GL(n, K)$, $H = \{\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right], \left[\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right], \left[\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right], \left[\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right]\}$

Example 3.11. $\{e, (12), (23)\} \subset S_3$ is *not* a subgroup of S_3.

Lemma 3.12

Let G be a group and $H \subseteq G$ a non-empty subset. Then the following are equivalent:

1) H is a subgroup of G
2) $\forall x, y \in H,\ (xy \in H) \wedge (x^{-1} \in H)$
3) $\forall x, y \in H,\ xy^{-1} \in H$

Proof. That the first implies the second is immediate from the definition of a subgroup.
Assume the the second holds. Let $x, y \in H$. Then $y^{-1} \in H$ and therefore $xy^{-1} \in H$. Therefore the second implies the third.
Assume that the third condition holds. We will show that H is a subgroup. Note first that H is non-empty by hypothesis. Let $h \in H$. Then $e = hh^{-1} \in H$ by (3).

$$\begin{aligned} k \in H &\implies ek^{-1} \in H && \text{(by (3))} \\ &\implies k^{-1} \in H \end{aligned}$$

and therefore

$$\begin{aligned} h, k \in H &\implies h, k^{-1} \in H \\ &\implies h(k^{-1})^{-1} \in H && \text{(by (3))} \\ &\implies hk \in H && ((k^{-1})^{-1} = k) \end{aligned}$$

Therefore the group operation $G \times G \to G$ restricts to an operation $H \times H \to H$. We need to show that the axioms of a group are satisfied by H equipped with this operation. Let $h, k, l \in H$. Then we have

$$\begin{aligned} h(kl) &= (hk)l && \text{(since this holds for the original, unrestricted, operation)} \\ eh &= he = h && \text{(and } e \in H \text{ as noted above)} \\ hh^{-1} &= h^{-1}h = e && \text{(and } h^{-1} \in H \text{ as noted above)} \end{aligned}$$

□

Exercise 78. Let G be a group and $\{H_i \leqslant G \mid i \in I\}$ a set of subgroups of G. Show that $\cap_{i \in I} H_i$ is a subgroup of G.

Definition 3.13. Let G be a group and let $S \subseteq G$ be a subset of G. The **subgroup generated** by S is denoted by $\langle S \rangle$ and defined to be the subgroup given by theintersection of all subgroups that contain S. That is,

$$\langle S \rangle = \bigcap_{\substack{H \leqslant G \\ S \subseteq H}} H$$

Remark. It follows from the definition that $\langle \emptyset \rangle = \langle \{e\} \rangle = \{e\}$.

Example 3.14. We give some examples of subsets S of a group G and the generated generated.

G	$S \subset G$	$\langle S \rangle \leqslant G$
S_3	$\{(123)\}$	$\{e, (123), (132)\}$
S_3	$\{(12), (23)\}$	S_3
$(\mathbb{C} \setminus \{0\}, \times)$	{i}	{ 1,i,-1,i}
$\mathrm{GL}(2, \mathbb{R})$	$\{\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]\}$	$SL(2, \mathbb{Z})$

G	$S \subset G$	$\langle S \rangle \leqslant G$
$(\mathbb{Z}, +)$	$\{0\}$	$\{0\}$
$(\mathbb{Z}, +)$	$\{1\}$	$\mathbb{Z}$
$(\mathbb{Z}, +)$	$\{-1\}$	$\mathbb{Z}$
$(\mathbb{Z}, +)$	$\{2, 9\}$	$\mathbb{Z}$
$(\mathbb{Z}, +)$	$\{6, 9\}$	$3\mathbb{Z}$

The following result reflects the fact that the subgroup generated by S is the smallest subgroup of G that contains S.

Lemma 3.15

Let G be a group, $H \leqslant G$ a subgroup of G and $S \subseteq G$ a subset. Then

1) $S \subseteq \langle S \rangle$
2) $S \subseteq H \implies \langle S \rangle \leqslant H$

Proof. Both are almost immediate from the definition. □

3.1 Exercises

Exercise 79. List all of the subgroups of $\mathbb{Z}/12\mathbb{Z}$.

Exercise 80. Decide whether or not the following are subgroups:

(a) the positive integers in the additive group of the integers;

(b) the set of all rotations in the group of symmetries of a plane tesselation;

(c) the set of all permutations in S_n which fix 1.

Exercise 81. Show that the set of complex numbers z which are nth roots of unity for some (variable) natural number n, together with multiplication of complex numbers, forms a group. That is, show that the set $\{z \in \mathbb{C} \mid \exists n \in \mathbb{N},\ z^n = 1\}$ forms a subgroup of $\mathbb{C}^\times$.

Exercise 82. If H is a subgroup of a group G and if $g \in G$, show that $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ is a subgroup of G.

4 Cyclic groups

Lemma 3.16

Let $g \in G$. Then $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

Proof. Let $H = \{g^n \mid n \in \mathbb{Z}\}$. Note first that H is a subgroup of G, since $H \neq \emptyset$ and

$$\begin{aligned} h, k \in H &\implies h = g^m, k = g^n \quad \text{for some } m, n \in \mathbb{Z} \\ &\implies hk^{-1} = g^{m-n} \\ &\implies hk^{-1} \in H \end{aligned}$$

Therefore H is a subgroup of G and $g \in H$. Now suppose that K is a subgroup of G such that $g \in K$. For all $n \in \mathbb{Z}$ we have $g^n \in H$, because H is a subgroup. It follows that $K \leqslant H$ and hence $\langle g \rangle = H$.

□

Example 3.17. Let $g = (123) \in S_3$. Then $\langle g \rangle = \{e, (123), (132)\}$.

Definition 3.18. A group G is called **cyclic** if there exists $g \in G$ such that $\langle g \rangle = G$. Such an element g is called a **generator** for the cyclic group G.

Remark. It is clear from the definition that cyclic groups are abelian. The converse is false. The group V of Example 3.5 is abelian, but not cyclic.

Example 3.19.
1. $\mathbb{Z}$ is cyclic
2. $3\mathbb{Z}$ is a cyclic subgroup of $\mathbb{Z}$
3. $\langle 6, 9 \rangle \leqslant \mathbb{Z}$ is a cyclic subgroup
4. $\mathbb{Z}/6\mathbb{Z}$ is cyclic
5. S_3 is not cyclic
6. $\{\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right], \left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]\} \leqslant GL(2, \mathbb{R})$ is not a cyclic subgroup. (But it is abelian.)

Lemma 3.20

Every subgroup of a cyclic group is itself cyclic.

Proof. Let G be a cyclic group and $g \in G$ such that $G = \langle g \rangle$. Let H be a subgroup of G. If $H = \{e\}$, then H is cyclic. So assume that H is non-trivial. Let $d = \min\{m \in \mathbb{N} \mid g^n \in H\}$. We will show that $\langle g^d \rangle = H$. Let $h \in H$. Then, since $h \in G$, we have that $h = g^a$ for some $a \in \mathbb{Z}$. We need to show that $d \mid a$. Let $q, r \in \mathbb{Z}$ be such that $a = qd + r$ and $0 \leqslant r < d$. Then $h = (g^d)^q g^r$, which implies that $g^r \in H$. From the minimality of d we conclude that $r = 0$. □

5 Order of an element

Definition 3.21. Let G be a group and $g \in G$. Let $S\{n \in \mathbb{N} \mid g^n = e\}$. If $S = \emptyset$, we say that g has **infinite order**. If $S \neq \emptyset$ we say that g has **finite order** and define the **order** of g to be the minimal element of S. The order of g is denoted $o(g)$ or $|g|$.

Remark. The order of an element is equal to the size of the subgroup generated by g, i.e., $|g| = |\langle g \rangle|$.

Example 3.22.
1. The orders of the elements of S_3 are: $|e| = 1$, $|(123)| = 3$, $|(132)| = 3$, $|(12)| = 2$, $|(13) = 2$, $|(23)| = 2$.
2. $(12)(34) \in S_4$ has order 2
3. $(123)(45) \in S_5$ has order 6

Lemma 3.23

Let $g \in G$ and $n \in \mathbb{N}$. If $g^n = e$ then g has finite order and $|g|$ divides n.

Proof. That g has finite order is clear from the definition of order. Let $d = |g|$ and write $n = qd + r$ with $q, r \in \mathbb{Z}$ and $0 \leqslant r < d$. Then note that $g^n = g^{(qd+r)} = (g^d)^q g^r = e^q g^r = eg^r = g^r$. Therefore $g^r = e$ and $r < |g|$. Therefore $r = 0$ and hence $d \mid n$. □

Exercise 83. Let G be a group and $g \in G$.

(a) Suppose that g has infinite order. Show that $\forall m, n \in \mathbb{Z},\ g^m = g^n \implies m = n$.

(b) Suppose that g has finite order. Show that $\forall m, n \in \mathbb{Z},\ g^m = g^n \implies m \equiv n \pmod{|g|}$.

Lemma 3.24

Let G be a group and $g \in G$. Let $h \in \langle g \rangle \setminus \{e\}$.

1) If g has infinite order, then h has infinite order.

2) If g has finite order, then h has finite order and $|h| \mid |g|$.

Proof. Let $n \in \mathbb{Z} \setminus \{0\}$ be such that $h = g^n$. For that first part, we have the following.

$$\begin{aligned} h \text{ has finite order} &\implies \exists m \in \mathbb{N},\ h^m = e \\ &\implies (g^n)^m = e \\ &\implies g^{|mn|} = e \qquad\qquad \text{(note that } mn \neq 0) \\ &\implies g \text{ has finite order} \end{aligned}$$

Now suppose that g has finite order. Note that $h^{|g|} = (g^n)^{|g|} = (g^{|g|})^n = e^n = e$, and therefore, by Lemma 3.23, we have that $|h| \mid |g|$. □

Example 3.25. We list the elements of $\langle g \rangle$ together with their orders for $g = (1243) \in S_4$.

$g^0 = e$	$g^1 = (1243)$	$g^2 = (14)(23)$	$g^3 = (1432)$
$\lvert g^0 \rvert = 1$	$\lvert g \rvert = 4$	$\lvert g^2 \rvert = 2$	$\lvert g^3 \rvert = 4$

5.1 Exercises

Exercise 84. Find the orders of the following elements:

(a) $(123)(4567)(89)$ in S_{10}

(b) $(14)(23567)$ in S_7

(c) a reflection in the plane

(d) a translation in the group of all symmetries of a plane pattern

(e) the elements $[6]_{20}, [12]_{20}, [11]_{20}, [14]_{20}$ in the additive group of $\mathbb{Z}/20\mathbb{Z}$

(f) the elements $[2]_{13}, [12]_{13}, [8]_{13}$ in the multiplicative group of non-zero elements of $\mathbb{Z}/13\mathbb{Z}$

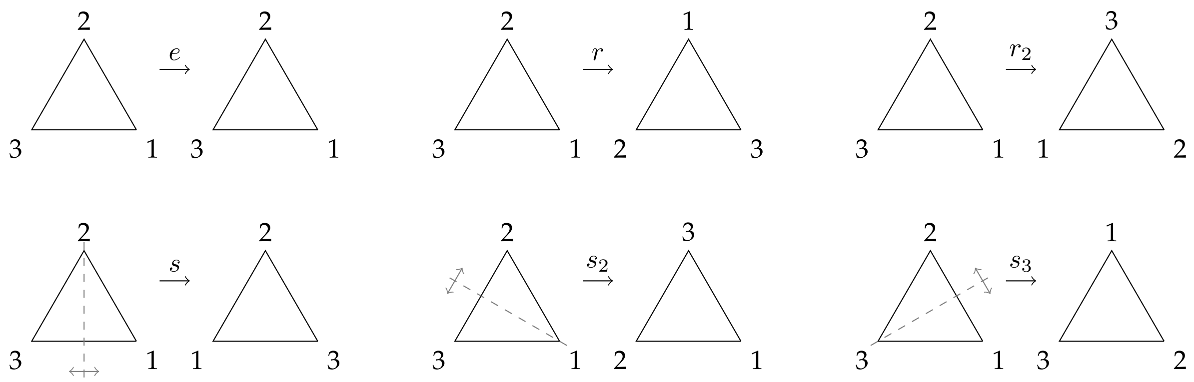
Exercise 85. If g is an element of a group G, prove that the orders of g and g^{-1} are equal.

Exercise 86. Show that, in an abelian group, the product of two elements of finite order again has finite order.

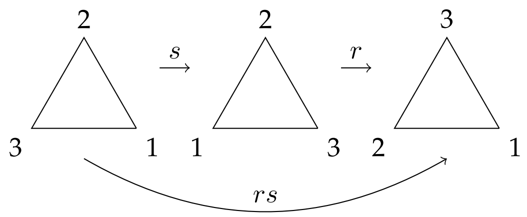
Exercise 87. Let $A, B \in GL(2, \mathbb{R})$ be given by $A = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Show that A has order 3, that B has order 4, and that AB has infinite order.

6 The dihedral groups D_n

The dihedral groups are another important family of non-abelian finite groups. We start by describing the group D_3. Consider the ways in which two copies of an equilateral triangle can by placed one on top of the other. There are a total of six possibilities: three rotations (including the identity) and three reflections.



Two such maps can by combined. Denote by r the map given by rotating the triangle through $2\pi/3$ and by s the map given by reflection across the line indicated above. The product rs is the map given by first applying s and then applying r. The product rs is equal to s_2.



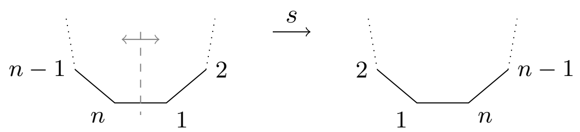
Similarly, we can show that $r^2 s = sr = s_3$ and $r^2 = r_2$. Notice that $rs \neq sr$. Equipped with this operation the given set of six symmetries forms a (non-abelian, finite) group, which is denoted D_3. Given our calculations so far, we have $D_3 = \{e, r, r^2, s, rs, r^2 s\}$. The multiplication table for this group is given on the right.

D_3	e	r	r^2	s	rs	r^2s
e	e	r	r^2	s	rs	r^2s
r	r	r^2	e	rs	r^2s	s
r^2	r^2	e	r	r^2s	s	rs
s	s	r^2s	rs	e	r^2	r
rs	rs	s	r^2s	r	e	r^2
r^2s	r^2s	rs	s	r^2	r	e

We can generalise from an equilateral triangle to a regular n-gon.

Definition 3.26. Let $n \in \mathbb{N}$ with $n \geqslant 3$. The **dihedral group D_n** is the group of symmetries of the regular n-gon. The group operation is composition.

For a fixed $n \geqslant 3$, we denote by $r \in D_n$ the element given by rotation through $2\pi/n$ and by $s \in D_n$ the element given by reflection across the perpendicular bisector of a fixed edge.



Proposition 3.27

The group D_n is a non-abelian group and has $2n$ elements. The elements r and s satisfy $r^n = e$, $s^2 = e$, $sr = r^{n-1}s$. The elements of D_n can be listed as

$$D_n = \{e, r, r^2, \dots, r^{n-1}, s, rs, r^2 s, \dots r^{n-1}s\}$$

Proof. An element of D_n is uniquely determined by the image an edge. There are n choices for the image of the vertex labelled 1. Given a choice for the image of the vertex labelled 1, there are then two choices for the image of vertex labelled n. Hence $|D_n| = 2n$. It is obvious from the way in which they are defined that $r^n = e$ and $s^2 = e$. We now show that $sr = r^{n-1}s$. Given that an element of D_n is determined by the images of the vertices labelled 1 and n, it is enough to show that $sr(1) = r^{n-1}s(1)$ and $sr(n) = r^{n-1}s(n)$. We calculate

$$sr(1) = s(2) = n-1 \qquad r^{n-1}s(1) = r^{n-1}(n) = r^{-1}(n) = n-1$$
$$sr(n) = s(1) = n \qquad r^{n-1}s(n) = r^{n-1}(1) = r^{-1}(1) = n$$

Exercise 88. Finish the proof by showing that no two of the listed elements are equal.

□

Exercise 89. Determine the possible orders of elements in the dihedral group D_n.

7 Group homomorphisms

Definition 3.28. Let G and H be groups. A **homomorphism** from G to H is a function $\varphi : G \to H$ with the property that: $\forall x, y \in G,\ \varphi(xy) = \varphi(x)\varphi(y)$.

Example 3.29.
1. $\varphi : \mathbb{Z} \to \mathbb{Z}$, $\varphi(n) = 4n$
2. $\varphi : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$, $\varphi(n) = [n]_6$
3. $\varphi : GL(n, \mathbb{R}) \to \mathbb{R}^\times$, $\varphi(A) = \det(A)$
4. $\varphi : S_3 \to GL(3, K)$, $(\varphi(\sigma))_{ij} = \delta_{i,\sigma(j)}$

Lemma 3.30

Let $\varphi : G \to H$ be a homomorphism. Then

a) $\varphi(e_G) = e_H$

b) $\forall g \in G, \varphi(g^{-1}) = \varphi(g)^{-1}$

c) If $g \in G$ has finite order, then so does $\varphi(g)$ and $|\varphi(g)| \mid |g|$

d) If φ is a bijection, then the inverse function $\varphi^{-1} : H \to G$ is a homomorphism.

Proof. For part (a) we have:

$$\begin{aligned}
\varphi(e_G) &= \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G) \\
\implies \varphi(e_G)^{-1}\varphi(e_G) &= \varphi(e_G)^{-1}\varphi(e_G)\varphi(e_G) \\
\implies e_H &= e_H\varphi(e_G) \\
\implies e_H &= \varphi(e_G)
\end{aligned}$$

Part (b) is left as an exercise.

For part (c), let $n = |g|$. We have $\varphi(g)^n = \varphi(g^n) = e_H$, which implies that $|\varphi(g)| \mid n$ by Lemma 3.23.

For part (d) we need to show that $\forall\, h_1, h_2 \in H$ we have $\varphi^{-1}(h_1h_2) = \varphi^{-1}(h_1)\varphi^{-1}(h_2)$. Note that

$$\begin{aligned}
h_1h_2 &= \varphi(\varphi^{-1}(h_1))\varphi(\varphi^{-1}(h_2)) \\
&= \varphi(\varphi^{-1}(h_1)\varphi^{-1}(h_2)) \\
\implies \varphi^{-1}(h_1h_2) &= \varphi^{-1}(h_1)\varphi^{-1}(h_2)
\end{aligned}$$

□

Example 3.31. The map $\varphi : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$, $\varphi([n]_4) = [3m]_6$ is a homomorphism. Note that $|\varphi([1]_4)| = |[3]_6| = 2$ and $|[1]_4| = 4$.

Example 3.32. Let $m \in \mathbb{N}$. There is only one homomorphism $\varphi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}$. To see this, note that every element $g \in \mathbb{Z}/m\mathbb{Z}$ has finite order. Therefore, $\varphi(g) = 0$ as this is the only element of $\mathbb{Z}$ that has finite order. The only homomorpism is therefore $\varphi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}$, $\varphi(g) = 0$.

Definition 3.33. A bijective homomorphism is called an **isomorphism**. Two groups G and H are said to be **isomorphic** (denoted $G \cong H$) if there exists an isomorphism $G \to H$.

Remark. If two groups are isomorphic, then they are essentially the 'same' group. More precisely, any algebraic property satisfied by one will also be satisfied by the other. For example, if $G \cong H$ and G is abelian, then H is abelian.

Example 3.34.

1. $(\mathbb{Z}/4\mathbb{Z}, +) \cong (\{1, i, -1, -i\}, \times)$
2. $D_3 \cong S_3$
3. $(\mathbb{R}, +) \cong (\mathbb{R}^+, \times)$
4. $(\mathbb{Z}/4\mathbb{Z}, +) \ncong (\mathbb{Z}/3\mathbb{Z}, +)$
5. $(\mathbb{Z}/4\mathbb{Z}, +) \ncong V$

Exercise 90. Suppose that $\varphi : G \to H$ is an isomorphism. Show that

(a) $\varphi^{-1} : H \to G$ is an isomorphism

(b) $\forall\, g \in G,\ |\varphi(g)| = |g|$

Proposition 3.35

Let G be a cyclic group. If G is infinite, then $G \cong \mathbb{Z}$. If G is finite, then $G \cong \mathbb{Z}/m\mathbb{Z}$ where $m = |G|$.

Proof. Let $g \in G$ be such that $\langle g \rangle = G$.

Suppose first that g has infinite order. Define $\varphi : \mathbb{Z} \to G$ by $\varphi(m) = g^m$. Note that φ is a homomorphism since:

$$\varphi(m+n) = g^{m+n} = g^m g^n = \varphi(m)\varphi(n)$$

That φ is surjective follows from Lemma 3.16. It is also injective since

$$\varphi(m) = \varphi(n) \implies g^m = g^n \implies g^{m-n} = e \implies m - n = 0$$

Now suppose that g has finite order and let $m = |g|$. Define $\psi : \mathbb{Z}/m\mathbb{Z} \to G$ by $\psi([a]_m) = g^a$. Note that this map is well-defined because

$$[a]_m = [b]_m \implies m \mid (a-b) \implies a - b = mk \quad \text{(for some } k \in \mathbb{Z}) \implies g^{a-b} = g^{mk} = e^k = e \implies g^a = g^b$$

It is clear that ψ is surjective (Lemma 3.16). For injectivity we have

$$\psi([a]_m) = \psi([b]_m) \implies g^a = g^b \implies g^{a-b} = e \implies m \mid (a-b) \implies [a]_m = [b]_m$$

□

7.1 Exercises

Exercise 91. Show that the matrix group $SO(2)$ is isomorphic to the group $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ of complex numbers having modulus 1 (and operation given by multiplication of complex numbers).

Exercise 92. Show that if m divides n, then D_m is isomorphic to a subgroup of D_n.

Exercise 93. Show that:

(a) $(\mathbb{R}, +)$ and $(\mathbb{R} \setminus \{0\}, \times)$ are not isomorphic

(b) $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are not isomorphic

(c) The additive group of rational numbers $(\mathbb{Q}, +)$ is not isomorphic to the multiplicative group of positive rationals $(\mathbb{Q}^+, \times)$.

8 Direct product

Definition 3.36. Let G and H be groups. The **direct product** of G and H is the group with underlying set the cartesian product

$$G \times H = \{(g, h) \mid g \in G, h \in H\}$$

and operation given by

$$(g_1, h_1) * (g_2, h_2) = (g_1 g_2, h_1 h_2)$$

Exercise 94. (a) Show that $(G \times H, *)$ forms a group and that $e_{G\times H} = (e_G, e_H)$.

(b) Show that if G and H are both abelian, then $G \times H$ is abelian

Example 3.37. 1. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is a (non-cyclic) group of size 4

2. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z}$ are all abelian groups of size 8. No two are isomorphic.

9 Cosets and Lagrange's theorem

Definition 3.38. Let G be a group and $H \leqslant G$ a subgroup. The set $gH = \{gh \mid h \in H\}$ is called a **left coset** of H in G. The set $Hg = \{hg \mid h \in H\}$ is called a **right coset** of H in G.

Remark. 1. H itself is both a left and right coset: $eH = He = H$.

2. If $g \notin H$, then gH is not a subgroup of G. Similarly, Hg is not a subgroup.

Example 3.39. 1. If $G = \mathbb{Z}$ and $H = 3\mathbb{Z}$, there are three (left) cosets: $0 + H = [0]_3, 1 + H = [1]_3, 2 + H = [2]_3$.

2. Let $G = S_3$ and $H = \{e, (123), (132)\}$. There are two left cosets:

$$eH = (123)H = (132)H = H \quad \text{and} \quad (12)H = (13)H = (23)H = \{(12), (13), (23)\}$$

There are two right cosets:

$$He = H(123) = H(132) = H \quad \text{and} \quad (12)H = H(13) = H(23) = \{(12), (13), (23)\}$$

3. Let $G = S_3$ and $H = \{e, (12)\}$. There are three left cosets:

$$eH = (12)H = H \quad \text{and} \quad (123)H = (13)H = \{(123), (13)\} \quad \text{and} \quad (132)H = (23)H = \{(132), (23)\}$$

There are three right cosets:

$$He = H(12) = H \quad \text{and} \quad H(123) = H(23) = \{(123), (23)\} \quad \text{and} \quad H(132) = H(13) = \{(132), (13)\}$$

Note that, in this example, the left and right cosets are not the same.

Lemma 3.40

Let G be a group and $H \leqslant G$ a subgroup. Let $a, b \in G$.

a) (i) $aH = bH \iff a^{-1}b \in H$ (ii) $Ha = Hb \iff ab^{-1} \in H$

b) (i) The left cosets partition G. (ii) The right cosets partition G.

c) (i) The map $aH \to bH$, $ah \mapsto bh$ is a bijection. (ii) The map $Ha \to Hb$, $ha \mapsto hb$ is a bijection.

Proof. We prove the statements for left cosets, and leave the right coset versions as an exercise.

$$\begin{aligned} aH = bH &\implies b \in aH \\ &\implies b = ah && \text{(for some } b \in H) \\ &\implies a^{-1}b = h \in H \end{aligned}$$

Conversely, suppose that $a^{-1}b \in H$. Then

$$x \in aH \implies x = ah \quad \text{(for some } h \in H) \implies x = b(a^{-1}b)^{-1}h \implies x \in bH \quad \text{(since } (a^{-1}b)^{-1} \in H)$$
$$x \in bH \implies x = bh \quad \text{(for some } h \in H) \implies x = a(a^{-1}b)h \implies x \in aH \quad \text{(since } (a^{-1}b) \in H)$$

Therefore (a) holds.

For (b) we need to show that every element of G is contained in exactly one coset. Let $g \in G$. There is at least one coset that contains g since $g \in gH$. Suppose now that $g \in kH$. Our aim is to show that $kH = gH$. Using part (a) we have

$$g \in kH \implies g = kh \quad \text{(for some } h \in H) \implies k^{-1}g \in H \implies kH = gH$$

For part (c), let $f : aH \to bH$ be the map $f(ah) = bh$. We have

$$f(ah_1) = f(ah_2) \implies bh_1 = bh_2 \implies h_1 = h_2 \implies ah_1 = ah_2$$
$$x \in bH \implies x = bh \quad \text{(for some } h \in H) \implies x = f(ah)$$

□

Remark. 1. It follows from part (c) that $\forall\, g \in G,\ |gH| = |Hg| = |H|$. That is, all cosets (left and right) have the same size as H.

2. It follows from the lemma that the number of left cosets is equal to the number of right cosets.

Definition 3.41. Let G be a group and $H \leqslant G$ a subgroup. The number of cosets of H in G is called the **index** of H in G and is denoted by $[G : H]$. That is,

$$[G : H] = |\{gH \mid g \in G\}|$$

Example 3.42. (cf. Example 3.39)

1. $[\mathbb{Z} : 3\mathbb{Z}] = 3$
2. $[S_3 : \langle(123)\rangle] = 2$
3. $[S_3 : \langle(12)\rangle] = 3$

That the cosets partition G and all have the same size leads directly to the following fundamental and useful result.

Theorem 3.43: Lagrange's Theorem

Let G be a finite group and $H \leqslant G$ a subgroup. Then $|G| = [G : H]|H|$.

Proof. We saw in Lemma 3.40 that the left cosets partition G and all have size equal to $|H|$. Let $k = [G : H]$ and $g_1, \dots, g_k \in G$ be such that the (distinct) cosets are $g_1H, \dots, g_kH$. Then

$$\begin{aligned} |G| &= |g_1H| + \cdots + |g_kH| && \text{(cosets are disjoint)} \\ &= k|H| && (|g_iH| = |H|) \\ &= [G : H]|H| \end{aligned}$$

□

Example 3.44.

1. $|S_3| = 6 = 2 \times 3 = [S_3 : \langle(123)\rangle]\,|\langle(123)\rangle|$
2. $|S_3| = 6 = 3 \times 2 = [S_3 : \langle(12)\rangle]\,|\langle(12)\rangle|$

Example 3.45. Since $|S_4| = 24$ and $|\langle(12),(34)\rangle| = 4$, we deduce that $[S_4 : \langle(12),(34)\rangle] = 6$.

Corollary 3.46

Let G be a finite group and $g \in G$. Then $g^{|G|} = e$ and $|g| \mid |G|$.

Corollary 3.47

Let G be a finite group. If $|G|$ is prime, then $G \cong \mathbb{Z}/p\mathbb{Z}$, where $p = |G|$.

9.1 Exercises

Exercise 95. If H and K are subgroups of a group G and if $|H| = 7$ and $|K| = 29$, show that $H \cap K = \{e_G\}$.

Exercise 96. Let G be the subgroup of $GL(2,\mathbb{R})$ of the form

$$G = \left\{ \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} \mid x, y \in \mathbb{R}, x > 0 \right\}$$

Let H be the subgroup of G defined by

$$H = \left\{ \begin{bmatrix} z & 0 \\ 0 & 1 \end{bmatrix} \mid z \in \mathbb{R}, z > 0 \right\}$$

Each element of G can be identified with a point (x, y) of the (x, y)-plane. Use this to describe the right cosets of H in G geometrically. Do the same for the left cosets of H in G.

Exercise 97. Consider the set of linear equations of the form $AX = B$, where X and B are column matrices, X is the matrix of unknowns and A the matrix of coefficients. Let W be the subspace (and so additive subgroup) of $\mathbb{R}^n$ which is the set of solutions of the homogeneous equations $AX = 0$. Show that the set of solutions of $AX = B$ is either empty or is a coset of W in the group $(\mathbb{R}^n, +)$.

Exercise 98.

(a) Let H be a subgroup of index 2 in a group G. Show that if $a, b \in G \setminus H$, then $ab \in H$.

(b) Let H be a subgroup of a group G with the property that if $a, b \in G \setminus H$, then $ab \in H$. Show that H has index 2 in G.

Exercise 99. Determine all subgroups of the dihedral group D_5.

Exercise 100. Determine all subgroups of the dihedral group D_4 as follows:

(a) List the elements of D_4 and hence find all of the cyclic subgroups.

(b) Find two non-cylic subgroups of order 4 in D_4.

(c) Explain why any non-cylic subgroup of D_4, other than D_4 itself, must be of order 4 and, in fact, must be one of the two subgroups you have listed in the previous part.

Exercise 101. Let G denote the group of rotational symmetries of a regular tetrahedron. Note that $|G| = 12$.

(a) Show that G has subgroups of order 1,2,3,4 and 12.

(b) Show that G has no subgroup of order 6.

Exercise 102. Let G be a group of order 841 (which is $(29)^2$). If G is not cyclic, show that every element g of G satisfies $g^{29} = 1$.

10 Normal subgroups and quotient groups

Given a group G and a subgroup $H \leqslant G$, we would like to define a group G/H in a way that mimics the construction of $(\mathbb{Z}/m\mathbb{Z}, +)$. The set will be the set of all (left) cosets, but what should the operation be? The natural choice to make is to define $aH * bH = (ab)H$. However, this is not always well-defined.

For example, consider $G = S_3$ and $H = \{e, (12)\}$. The left cosets are $C_1 = \{e, (12)\}$, $C_2 = \{(23), (132)\}$, $C_3 = \{(13), (123)\}$. What should $C_1 * C_2$ be? The coset $(ab)H$ depends on the choice of a and b:

$$C_1 * C_2 = eH * (23)H = (e(23))H = (23)H = C_2$$

but, also

$$C_1 * C_2 = (12)H * (23)H = ((12)(23))H = (123)H = C_3$$

The solution is to put a condition on the subgroup H.

Definition 3.48. A subgroup $H \leqslant G$ is called a **normal subgroup** if $\forall g \in G$, $gH = Hg$. This will be denoted $H \lhd G$.

Remark. It is immediate from the definition that $\{e\} \lhd G$ and $G \lhd G$.

Exercise 103. Let H be a subgroup of a group G. Show that H is normal if and only if $\forall g \in G \, \forall h \in H$, $ghg^{-1} \in H$.

Remark. If G is abelian, then all subgroups of G are normal.

Example 3.49.

1. $3\mathbb{Z} \lhd \mathbb{Z}$
2. $\langle (123) \rangle \lhd S_3$
3. $SL(n, K) \lhd GL(n, K)$
4. $\langle (12) \rangle \ntriangleleft S_3$
5. $\langle (123) \rangle \ntriangleleft S_4$

Exercise 104. Let $G = S_4$ and $H = \{e, (12)(34), (13)(24), (14)(23)\}$. Show that $H \lhd G$.

Exercise 105. Let G be a group and $H \leqslant G$ a subgroup. Show that if $[G : H] = 2$, then $H \lhd G$.

Definition 3.50. Let G be a group and $H \lhd G$ a normal subgroup. The **quotient group** G/H is the group whose elements are the (left) cosets $G/H = \{gH \mid g \in G\}$ and whose operation is given by $(g_1H) * (g_2H) = (g_1g_2)H$.

Exercise 106. Check that the above operation is well-defined and that G/H is a group and $e_{G/H} = e_G H$.

Remark.

1. If G is finite, from Lagrange's Theorem we have $|G/H| = |G|/|H|$.
2. If $G = \mathbb{Z}$ and $H = m\mathbb{Z}$, the notation G/H agrees with for our existing notation for $\mathbb{Z}/m\mathbb{Z}$.

Example 3.51. Let $G = D_4$ and $r, s \in D_4$ as in Definition 3.26. Then $H = \{e, r^2\}$ is a normal subgroup of G. The multiplication table for $D_4/\langle r^2 \rangle$ is

	eH	rH	sH	rsH
eH	eH	rH	sH	rsH
rH	rH	eH	rsH	sH
sH	sH	srH	eH	rH
rsH	rsH	sH	rH	eH

In fact, $D_4/\langle r^2 \rangle \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ (see Example 3.57).

10.1 Exercises

Exercise 107. Show that the set of matrices

$$H = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : ad \neq 0 \right\}$$

forms a subgroup of $GL(2, \mathbb{R})$. Show that the set of matrices

$$K = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in \mathbb{R} \right\}$$

forms a normal subgroup of H.

Exercise 108. Show that if K and L are normal subgroups of a group G, then $K \cap L$ is a normal subgroup of G.

Exercise 109. Let G be a group and $n \in \mathbb{N}$. If H is the only subgroup of G which has order n, show that H is a normal subgroup of G.

Exercise 110. Find all of the normal subgroups of D_4. (See Exercise 100.)

Exercise 111. The *quaternion* group Q_8 is the subgroup of $GL(2, \mathbb{C})$ consisting of the matrices $\{\pm U, \pm I, \pm J, \pm K\}$ where

$$U = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \quad J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad K = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

(a) Verify that
$$I^2 = J^2 = K^2 = -U, \quad IJ = K, JK = I, KI = J$$
and so that these 8 elements do give a subgroup of $GL(2, \mathbb{C})$.

(b) Find all of the cyclic subgroups of Q_8.

(c) Show that every subgroup of Q_8, except Q_8 itself, is cyclic.

(d) Show that all subgroups of Q_8 are normal. (Even though Q_8 is not abelian.)

(e) Are Q_8 and D_4 isomorphic?

Exercise 112. (a) Show that if G is an abelian group, then every quotient G/N is abelian.

(b) Show that if G is a cyclic group, then every quotient G/N is cyclic.

Exercise 113. Let $\mathbb{R}$ denote the group of real numbers with the operation of addition and let $\mathbb{Q}$ and $\mathbb{Z}$ denote the subgroups of rational numbers and integers, respectively. Show that it is possible to regard $\mathbb{Q}/\mathbb{Z}$ as a subgroup of $\mathbb{R}/\mathbb{Z}$ and show that this subgroup consists exactly of the elements of finite order in $\mathbb{R}/\mathbb{Z}$.

Exercise 114. Let H denote the subgroup of D_8 generated by r^4 (where, as in Definition 3.26, r is rotation by $\pi/4$).

(a) Show that H is normal.

(b) Write out the multiplication table of D_8/H.

11 The first isomorphism theorem

Definition 3.52. Let $\varphi : G \to H$ be a homomorphism. The **kernel** of φ is defined to be

$$\ker(\varphi) = \{g \in G \mid \varphi(g) = e_H\}$$

The **image** of φ is defined to be

$$\mathrm{im}(\varphi) = \{\varphi(g) \mid g \in G\}$$

Example 3.53.

1. $\varphi : \mathbb{Z} \to \mathbb{Z}$, $\varphi(m) = 4m$. Then $\ker(\varphi) = \{0\}$ and $\mathrm{im}(\varphi) = 4\mathbb{Z}$.
2. $\varphi : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$, $\varphi(m) = [4m]_6$. Then $\ker(\varphi) = 3\mathbb{Z}$ and $\mathrm{im}(\varphi) = \{[0]_6, [2]_6, [4]_6\}$.
3. $\varphi : GL(n, \mathbb{R}) \to \mathbb{R}^\times$, $\varphi(A) = \det(A)$. Then $\ker(\varphi) = SL(n, \mathbb{R})$ and $\mathrm{im}(\varphi) = \mathbb{R}^\times$.

Exercise 115. Show that $\ker(\varphi)$ is a subgroup of G and that $\mathrm{im}(\varphi)$ is a subgroup of H.

Lemma 3.54

Let $\varphi : G \to H$ be a homomorphism.

1. $\ker(\varphi) \lhd G$
2. φ is injective if and only if $\ker(\varphi) = \{e\}$

Proof. The $\ker(\varphi)$ is a subgroup of G is shown in Exercise 115. To see that it is normal, let $g \in G$ and $k \in \ker(\varphi)$. Then $\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g)^{-1} = \varphi(g)\varphi(h)\varphi(g)^{-1} = e_H$. Therefore $gkg^{-1} \in \ker(\varphi)$ and hence $\ker(\varphi)$ is normal by 103.

If φ is injective, then $k \in \ker(\varphi) \implies \varphi(k) = \varphi(e_G) \implies k = e_G$, and therefore $\ker(\varphi) = \{e_G\}$.

Now suppose that $\ker(\varphi) = \{e_G\}$. For $g_1, g_2 \in G$ we have

$$\varphi(g_1) = \varphi(g_2) \implies \varphi(g_1)\varphi(g_2)^{-1} = e_H \implies \varphi(g_1 g_2^{-1}) = e_H \implies g_1 g_2^{-1} \in \ker(\varphi) \implies g_1 g_2^{-1} = e_G \implies g_1 = g_2$$

Therefore, if $\ker(\varphi) = \{e_G\}$ then φ is injective. □

Not only is the kernel of a homomorphism normal, every normal subgroup is the kernel of some homomorphism.

Lemma 3.55

Let G be a group and $H \triangleleft G$ a normal subgroup. Then the map $\varphi : G \to G/H$, $\varphi(g) = gH$ is a surjective homomorphism and $\ker(\varphi) = H$.

Remark. The above map $G \to G/H$ is often called the **projection map**.

Proof. That the map is a surjective homomorphism is clear from the definition of the quotient group G/H. Further, $k \in \ker(\varphi) \iff \varphi(k) = e_{G/H} \iff kH = H \iff k \in H$. □

Theorem 3.56: First isomorphism theorem

Let $\varphi : G \to H$ be a homomorphism and let $K = \ker(\varphi)$. Then the map $\overline{\varphi} : G/K \to H$ given by $\overline{\varphi}(gK) = \varphi(g)$ is an injective homomorphism. It follows that $G/\ker(\varphi) \cong \operatorname{im}(\varphi)$.

Proof. First we verify that the given map is well-defined:

$$g_1K = g_2K \implies g_1^{-1}(g_2) \in K \implies \varphi(g_1^{-1}g_2) = e_H \implies \varphi(g_1)^{-1}\varphi(g_2) = e_H \implies \varphi(g_1) = \varphi(g_2)$$

Now that $\overline{\varphi}$ is a homomorphism:

$$\overline{\varphi}((g_1K)(g_2K)) = \overline{\varphi}((g_1g_2)K) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}(g_1K)\overline{\varphi}(g_2K)$$

It is injective:

$$\overline{\varphi}(gK) = e_H \implies \varphi(g) = e_H \implies g \in K \implies gK = K \implies gK = e_{G/K}$$

□

Example 3.57. (cf. Example 3.51) Let $\varphi : D_4 \to (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ be given by

$$\varphi(e) = e, \varphi(r) = (1,0), \varphi(r^2) = (0,0), \varphi(r^3) = (1,0), \varphi(s) = (0,1), \varphi(rs) = (1,1), \varphi(r^2s) = (0,1), \varphi(r^3s) = (1,1)$$

Then φ is a surjective homomorphism and $\ker(\varphi) = \{e, r^2\}$. Therefore $D_4/\langle r^2\rangle \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Exercise 116. Let $\varphi : \mathbb{Z}/8\mathbb{Z} \to H$ be a homomorphism. Show that $\operatorname{im}(\varphi)$ is isomorphic to one of: $\{e\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$.