Elementary aspects of group theory

Abstract

Symmetries are codified mathematically in the subject of *group theory*. Naturally, the Part III Symmetries, Fields and Particles course will make a lot of use of this subject, so in this handout we will review some elementary aspects of the theory.

First, we review the basic definitions and notation used in group theory. We then give examples of some (hopefully familiar) finite groups, which are occasionally useful in practice. We proceed to develop the theory by describing how one can obtain new groups from old (by taking subgroups, quotient groups, and direct products), and maps between groups (including homomorphisms and isomorphisms). Finally, we describe a more advanced construction, namely the *semi-direct product* (which is useful in describing the structure of the *Poincaré group*, for example).

---

1 Groups: definitions and examples

For completeness, we begin by reminding ourselves of the definition of a group:

Definition 1.1: A *group* is a triple $(G, \cdot, e)$ consisting of a set G, a distinguished element $e \in G$, and a binary operation $\cdot : G \times G \to G$ such that the following axioms are obeyed:

(G1) Associativity. For all $g, h, k \in G$, we have $(g \cdot h) \cdot k = g \cdot (h \cdot k)$.

(G2) Identity. For all $g \in G$, we have $e \cdot g = g \cdot e = g$. We say that e is an *identity* for the group.

(G3) Inverses. For all $g \in G$, there exists an element $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$. We say that g^{-1} is an *inverse* for the group element g.

Taken together, the axioms imply the uniqueness of the identity and the inverses in the group.

The group axioms are sometimes stated with the additional axiom of *closure*:

(G0) Closure. For all $g, h \in G$, we have $g \cdot h \in G$.

This axiom is a little bit redundant, because the binary operation $\cdot : G \times G \to G$ is *defined* to have codomain G. However, it's sometimes useful to bear in mind as an axiom when we are checking that something is a group, since we do indeed need to check that the binary operation has the correct codomain G.

It is often the case that groups satisfy an additional axiom, *commutativity*, and hence we give these groups a special name:

Definition 1.2: A group $(G, \cdot, e)$ is called *Abelian* if it satisfies the additional axiom:

(G4) Commutativity. For all $g, h \in G$, we have $g \cdot h = h \cdot g$.

It's also worth noting that there is some standard notation used in group theory:

- Suppose that $(G, \cdot, e)$ is a group. If the identity is clear from context, we often abbreviate the group to $(G, \cdot)$. If both e and $\cdot$ are clear from context, we often simply abbreviate the group to G (hence it is common to refer to 'the group G').
- We often omit the $\cdot$ in group products i.e. $g \cdot h = gh$. This notation is almost universal, *except* for when the binary operation is an addition operation $+$ (e.g. addition of integers, vectors, etc.) - we then write $g \cdot h$ as $g + h$. Note that if the binary operation is written as $+$, we additionally write the identity as 0, and the inverse g^{-1} as $-g$.
- We very often use *power notation* for products of group elements (except for when the group operation is written $+$). The n-fold product of the group element g with itself, namely $g \cdot g \cdot ... \cdot g$, n times, is often abbreviated to g^n. The n-fold product of the inverse element g^{-1} with itself, namely $g^{-1} \cdot g^{-1} \cdot ... \cdot g^{-1}$, n times, is often abbreviated to g^{-n}. Finally, we define the zeroth power of a group element to be the identity, i.e. $g^0 := e$. With these definitions, we have the standard rules for manipulation of exponents:

$$g^n g^m = g^{n+m}, \qquad g^n g^{-m} = g^{n-m}, \qquad \text{etc.}$$

Examples of finite groups

With our definitions and notation fixed, let's see some examples of some familiar finite groups:

Example 1.3: The *cyclic group of order* n, written C_n, is defined to be the set:

$$C_n = \{e, r, r^2, ..., r^{n-1}\},$$

where elements are multiplied using the standard exponent rules described above, together with the rule $r^n = e$. Geometrically, C_n can be viewed as the set of all rotational symmetries of a regular planar n-gon; identifying r with an anticlockwise rotation by $2\pi/n$, we see that the rule $r^n = e$ tells us that an anticlockwise rotation by 2π takes us back to our initial position.

Example 1.4: The *dihedral group of the* n*-gon*, written D_n, is defined to be the set:

$$D_n = \{e, r, r^2, ..., r^{n-1}, s, sr, sr^2, ..., sr^{n-1}\},$$

where elements are multiplied using the standard exponent rules described above, together with the rules $r^n = e$, $s^2 = e$ and $rs = sr^{n-1}$. Geometrically, D_n can be viewed as the set of all rotational *and* reflectional symmetries of a regular planar n-gon. Identifying r with an anticlockwise rotation by $2\pi/n$, we see that the rule $r^n = e$ again tells us that an anticlockwise rotation by 2π returns us to our initial position. Identifying s with a fixed reflection through any axis of symmetry of the n-gon, we similarly see that the rule $s^2 = e$ tells us that reflecting twice in the same axis returns us to our initial position.

The equation $rs = sr^{n-1}$ is a little trickier to interpret geometrically. It tells us that a reflection followed by an *anti-clockwise* rotation by $2\pi/n$ is the same as a *clockwise* rotation by $2\pi(n-1)/n$ followed by a reflection.

Example 1.5: The *symmetric group on* n *symbols*, written S_n, is defined to be the set of all bijections:

$$\pi : \{1, ..., n\} \to \{1, ..., n\},$$

together with the operation of function composition.

Cayley tables

For groups of small order, it can be useful to visualise the group multiplication using *Cayley tables*, described as follows.

Definition 1.6: Let G be a finite group of order n, and let $(g_1, ..., g_n)$ be some ordering of its elements. The *Cayley table* of G (with respect to this ordering) is a matrix whose (i, j)th entry is the product $g_i g_j$.

An example of a Cayley table is given below.

Example 1.7: A Cayley table for D_3 is given by (appending an initial row and column to the matrix to help us keep track of which elements are being multiplied to produce the entries):

	e	r	r^2	s	sr	sr^2
e	e	r	r^2	s	sr	sr^2
r	r	r^2	e	sr^2	s	sr
r^2	r^2	e	r	sr	sr^2	s
s	s	sr	sr^2	e	r	r^2
sr	sr	sr^2	s	r^2	e	r
sr^2	sr^2	s	sr	r	r^2	e

One property of D_3 that is immediately clear from the Cayley table is that it is a *non-commutative* group. This follows immediately from the fact that the Cayley table is not symmetric about its leading diagonal.

2 New groups from old

In mathematics, there are three fundamental constructions which can be used to construct new sets from old ones:

- We can take *subsets* $S' \subseteq S$.
- Given some *equivalence relation* $\sim$ on the set S, we can construct the *quotient set* $S/\sim$, which consists of all equivalence classes in S under the equivalence relation $\sim$.
- Given two sets S_1, S_2, we can construct their *Cartesian product*, $S_1 \times S_2$.

When we define additional mathematical structure on a set, we often ask the natural question: how can we take subsets, quotients and products of instances of that structure, such that the resulting spaces inherit the same structure? In this section, we carry out this analysis in the case of groups.

Subgroups

Let's begin with the simplest set construction: taking subsets. We declare a *subgroup* to be a subset of a group which is a group in its own right, with respect to the same binary operation as the ambient group:

Definition 2.1: Suppose that a subset H of a group G constitutes a group in its own right, with respect to the binary operation of G. We say that H is a *subgroup* of G, and we write $H \leq G$.

Every group possesses at least two subgroups: the *improper subgroup* is the whole group, $G \leq G$, and the *trivial subgroup* is the subgroup containing only the identity $\{e\} \leq G$. We define a *proper subgroup* of G to be a subgroup of G which is not improper, i.e. not G. We write $H < G$ to mean that H is a proper subgroup of G. Similarly, we define a *non-trivial subgroup* of G to be a subgroup of G which is not trivial, i.e. not $\{e\}$.

Checking all of the group axioms is tedious, so it would be very nice if we had some general criteria under which $H \subseteq G$ implies $H \leq G$. Let's begin by noting that for *any* subset H, we will have associativity, i.e. for all $g, h, k \in H$, $(gh)k = g(hk)$, since this must be inherited from the group G. Furthermore, since the identity and inverses of a given binary operation on a group are unique, given a subset $H \subseteq G$ we have $H \leq G$ if and only if:

(i) the identity is in H, $e \in H$;

(ii) H is closed under the group multiplication, i.e. for all $g, h \in H$ we have $gh \in H$;

(iii) the inverse of any element $g \in H$ is also contained in H, $g^{-1} \in H$.

The three conditions above can be further repackaged as the *subgroup test*, which we state and prove as follows.

Proposition 2.2: (**The subgroup test**) Let $H \subseteq G$ be a subset of the group G. We have $H \leq G$ if and only if:

(i) H is non-empty, $H \neq \emptyset$;

(ii) for all $g, h \in H$, we have $gh^{-1} \in H$.

Proof: Suppose $H \leq G$. Then $e \in H$, so H is non-empty. For any $h \in H$, we have $h^{-1} \in H$ since H is closed is taking under inverses. Then by closure of the subgroup H, for all $g, h \in H$ we have $gh^{-1} \in H$.

Conversely, suppose (i) and (ii). Since H is non-empty, there exists some $g \in H$, and hence by (ii) we have $gg^{-1} = e \in H$. Thus H contains the identity. Now applying (ii) to the identity and a generic element $g \in H$, we have $eg^{-1} = g^{-1} \in H$, so H is closed under taking inverses. Finally, suppose that $g, h \in H$ are any two elements in H. Then $h^{-1} \in H$, since H is closed under taking inverses; it follows by (ii) that $g(h^{-1})^{-1} = gh \in H$. Thus H is closed. □

The extra group structure that subgroups afford us (as opposed to considering generic subsets of a group) allows us to start proving some interesting results. One of the most important ideas associated with subgroups is that they can be 'transported' around the group using the group multiplication:

Definition 2.3: Let G be a group. Given a subgroup $H \leq G$ and an element $g \in G$, we define the *left coset* gH to be the set $gH := \{gh : h \in H\}$, i.e. we apply g to all elements of H (on the left). There is an obvious analogous definition of a *right coset*, Hg. The set of all left cosets is called the *left coset space*, and is written G/H.

This indeed captures the notion of 'transporting' subgroups around the group; for example, if $h \in H$, then by multiplying through by $g \in G$, we 'transport' this element to $gh \in gH$. Hence, under multiplication by g, the subgroup H is 'transported' to the left coset gH instead.

Similarly, we can transport left cosets to other left cosets. For example, given any element $g_1 h \in g_1 H$, under multiplication by $g_2 g_1^{-1}$, we have $g_2 g_1^{-1} g_1 h = g_2 h \in g_2 H$, so the coset $g_1 H$ is 'transported' into the left coset $g_2 H$.

There are some natural questions that this notion of transportation raises:

(i) Is the transportation *surjective*? We have seen that transporting $g_1 H \to g_2 H$ via multiplication by $g_2 g_1^{-1}$ certainly maps $g_1 H$ *into* the coset $g_2 H$, but do we hit *all* elements of $g_2 H$?

(ii) Is there any overlap between the left cosets? That is, could $g_1 H$ and $g_2 H$ be distinct left cosets which overlap in some region? In that case, our transportation would be much more disappointing - we might hope to map $g_1 H \to g_2 H$, but some elements might just stay in the original set!

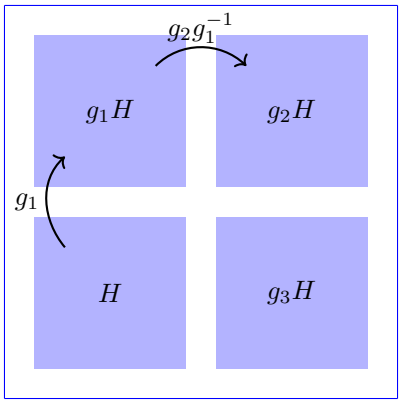

Figure 1: *Using the group multiplication we can transport left cosets to other left cosets.*

Fortunately both of these questions have straightforward answers: *yes*, the transportation is surjective, and *no*, there is no overlap between distinct left cosets. This statement is precisely *Lagrange's* celebrated theorem:

Theorem 2.4: (Lagrange's Theorem) Let G be a group, and let $H \leq G$ be a subgroup. The left cosets of H obey the following:

(i) There exists a bijection between any two left cosets of H.

(ii) The left cosets of H partition G.

Proof: (i) Let g_1H, g_2H be two left cosets of G. Then $f : g_1H \to g_2H$ given by $f(x) = g_2g_1^{-1}x$ certainly maps g_1H into g_2H. Next, observe that if $f(x) = f(y)$, we have $g_2g_1^{-1}x = g_2g_1^{-1}y$. Multiplying on the left by $g_1g_2^{-1}$, we see $x = y$ and hence f is injective. Finally, note that for any $g_2h \in g_2H$, we have $g_1h \in g_1H$ and $f(g_1h) = g_2g_1^{-1}g_1h = g_2h$, so f is surjective. Thus g_1H, g_2H are in bijection. □

(ii) For any $g \in G$, we have $g = ge \in gH$ since $e \in H$, so all elements of the group are in some left coset. Next, suppose that two left cosets g_1H, g_2H intersect non-trivially (they 'overlap' in the above motivation); if $g \in g_1H \cap g_2H$, then we have $g = g_1h_1 = g_2h_2$ for some $h_1, h_2 \in H$. In particular, this implies that $g_1 = g_2h_2h_1^{-1}$. Now let $x = g_1h \in g_1H$ be any element of the left coset g_1H. Then $x = g_1h = g_2h_2h_1^{-1}h \in g_2H$, and it follows that $g_1H \subseteq g_2H$. The argument can clearly be run the other way to obtain $g_2H \subseteq g_1H$. It follows that the left cosets g_1H, g_2H are either distinct or equal, and thus they must partition the group G. □

This has an immediate consequence for finite groups, also called Lagrange's theorem:

Corollary 2.5: (Lagrange's Theorem for finite groups) Let G be a finite group, and let $H \leq G$ be a subgroup. Then:

$$|G| = |H||G/H|,$$

so in particular the order of H divides the order of G.

Proof: This follows immediately from the more general form of Lagrange's theorem. Since the left cosets of H partition G, we have:

$$|G| = \sum |gH|$$

where the sum is over all *distinct* left cosets. But all left cosets are in bijection so have the same size; since $eH = H$ is itself a left coset, it follows that $|gH| = |H|$ in all cases. There are $|G/H|$ left cosets in total, and hence $|G| = |H||G/H|$ as required. □

As a final note about subgroups, observe that since Lagrange's theorem gives us a natural partition of the group for any given subgroup H, we can construct an associated *equivalence relation* induced by the partition:

Definition 2.6: Given a subgroup $H \leq G$ of a group G, we define the *subgroup equivalence relation* $\sim_H$ on G by declaring $g_1 \sim_H g_2$ if and only if g_1, g_2 are in the same left coset of H. The equivalence classes are precisely the left cosets of H in G.

We can formulate this definition in a useful equivalent form:

Proposition 2.7: Let $H \leq G$ be a subgroup of a group G, and let $\sim_H$ be the subgroup equivalence relation. Then $g_1 \sim_H g_2$ if and only if $g_2^{-1}g_1 \in H$.

Proof: Suppose that $g_1, g_2 \in gH$ are in the same left coset. Then $g_1 = gh_1, g_2 = gh_2$ for some $h_1, h_2 \in H$, which implies $g_2g_1^{-1} = (gh_1)^{-1}(gh_1) = h_2^{-1}g^{-1}gh_1 = h_2^{-1}h_1 \in H$.

Conversely, if $g_2^{-1}g_1 \in H$, we have $g_2^{-1}g_1 = h$ for some $h \in H$, so $g_1 = g_2h \in g_2H$. It follows that g_1 is in g_2H, and clearly $g_2 = g_2e \in g_2H$, so the two elements are in the same left coset. □

The subgroup equivalence relation will be immediately useful for our next construction, *quotient groups*.

Quotient groups

Let's consider the next set construction, namely *quotients* of sets by equivalence relations. Given an equivalence relation $\sim$ on a group G, we would like to establish under what conditions the set $G/\sim$ has a *natural* group structure, given by the natural multiplication:

$$[a] \cdot [b] = [ab],$$

where $[a]$ denotes the equivalence class containing the element $a \in G$. Indeed, we can quickly establish conditions under which this is true:

Proposition 2.8: Let $\sim$ be an equivalence relation on the group G. The quotient space $G/\sim$ is a group under the operation $[a] \cdot [b] = [ab]$ if and only if the equivalence relation is a subgroup equivalence relation, $\sim_H$, for some subgroup H obeying $gHg^{-1} \subseteq H$ for all $g \in G$ (a subgroup obeying this special condition is called a *normal subgroup*).

Proof: Suppose that $G/\sim$ is a group under the given operation, and write $H = [e]$ for the equivalence class containing the identity e. This equivalence class must be the identity for the quotient space $G/\sim$, since $[e] \cdot [g] = [eg] = [g]$ for all $g \in G$. In particular, we can deduce that inverses in the quotient group are given by $[g]^{-1} = [g^{-1}]$.

We claim that $H = [e]$ is a subgroup. Note first that $e \in H$, and hence it is non-empty. Now for any $a, b \in H$, we have $[a] = [b] = [e]$, and hence $[ab^{-1}] = [a] \cdot [b]^{-1} = [e] \cdot [e]^{-1} = [e]$. Thus $ab^{-1} \in H$, and H is a subgroup by the subgroup test. Furthermore, H is a *normal subgroup*, for suppose that $g \in G$ and $h \in H$. Then $[ghg^{-1}] = [g] \cdot [h] \cdot [g]^{-1} = [g] \cdot [e] \cdot [g]^{-1} = [e]$, and hence $ghg^{-1} \in H$.

Next, we claim that $\sim$ is the subgroup equivalence relation for H. We note that if $a \sim b$, then we must have $[b^{-1}a] = [b]^{-1} \cdot [a] = [e]$, and so $b^{-1}a \in H$. Conversely, if $b^{-1}a \in H$, then $[b] = [b] \cdot [e] = [b] \cdot [b^{-1}a] = [a]$. Thus we have $a \sim b$. It follows that $\sim$ is indeed the subgroup equivalence relation for H.

It remains to prove the converse; we must show that if $H \leq G$ is a normal subgroup of G, then under the subgroup equivalence relation $\sim_H$ we have that $G/\sim_H$ is a group with the operation $[a] \cdot [b] = [ab]$. First, we should show that this operation is well-defined. Suppose that $a_1 \sim_H a_2$ and $b_1 \sim_H b_2$, so that $a_2^{-1}a_1 = h_a$ and $b_2^{-1}b_1 = h_b$ for some $h_a, h_b \in H$. Then:

$$(a_2b_2)^{-1}(a_1b_1) = b_2^{-1}a_2^{-1}a_1b_1 = b_2^{-1}h_ab_1 = b_2^{-1}h_ab_2h_b \in H,$$

since H is a normal subgroup, so $b_2^{-1}h_ab_2 \in H$. It follows that $a_1b_1 \sim_H a_2b_2$, and hence $[a_1] \cdot [b_1] = [a_2] \cdot [b_2]$. Thus the group operation is well-defined.

Finally, we must show that this operation indeed makes $G/\sim_H$ into a group. Closure is obvious, and associativity is inherited from G. Clearly we have an identity, $[e]$, and finally the inverse of $[g]$ is given by $[g^{-1}]$. So we're done. □

We should emphasise that the fact $G/\sim$ is a well-defined group if and only if $\sim$ is the subgroup equivalence relation of a normal subgroup is an *accident* of group theory.

Indeed, for some other mathematical structures, there are no restrictions on when quotient spaces inherit the same mathematical structure (e.g. topological spaces), whilst in others the ability to construct a quotient space doesn't depend on some substructure of the same type but on something entirely different (e.g. in *ring* theory the notion of 'quotienting by a normal subring' makes no sense - instead, quotient rings are only well-defined if we have a different substructure called an *ideal*).

Now we have decided when we can give a group structure to the quotient space, we bake these ideas into some definitions:

Definition 2.9: A *normal* (or *invariant*) subgroup is a subgroup $H \leq G$ such that $gHg^{-1} \subseteq H$ for all $g \in G$. This is denoted $H \trianglelefteq G$.

Given a normal subgroup $H \trianglelefteq G$, we define the *quotient group* G/H to be the quotient space $G/\sim_H$, together with the group operation $[g]\cdot[h] = [gh]$ (note that G/H is precisely the left coset space when $\sim$ is the subgroup equivalence relation, so the notation matches up with what we had before). That this is a well-defined group is a consequence of the above work.

Some useful examples of normal subgroups and quotient groups include:

Example 2.10: For any group G, we always have $\{e\} \trianglelefteq G$ and $G \trianglelefteq G$. One can easily verify that the corresponding quotient groups are given by $G/\{e\} \cong G$ and $G/G \cong \{e\}$.

Example 2.11: If G is an Abelian group, then all subgroups $H \leq G$ are normal. To check this, simply note that if $g \in G$ and $h \in H$, we have $ghg^{-1} = hgg^{-1} = h \in H$, since all elements commute.

In particular, given any subgroup $H \trianglelefteq G$ of an Abelian group G, we can form the quotient group G/H.

Example 2.12: The *centre* of the group G, written $Z(G)$, is the set:

$$Z(G) = \{g \in G : hg = gh \text{ for all } h \in H\}.$$

In other words, $Z(G)$ is the collection of elements of G which commute with all other elements of G. It is an Abelian, normal subgroup; you will check this in the exercises at the end of the handout.

Since $Z(G) \trianglelefteq G$, we can form the quotient group $G/Z(G)$. You will show in the exercises at the end of this handout that this is isomorphic to a special group of maps associated to the group, called the *inner automorphisms* of the group.

We have seen that whenever we can identify a normal subgroup of a group, we can reduce the study of the group to a smaller quotient group instead. Iterating this process, we arrive at the most 'fundamental' groups, which have *no* (proper, non-trivial) normal subgroups. These groups are of particular interest in group theory (especially finite group theory), and they have a special name:

Definition 2.13: A group G is called *simple* if it has no proper, non-trivial normal subgroups.

Direct products

The final set construction is the *direct product*. Given two groups G, H, we would like to produce a natural group structure on their Cartesian product $G \times H$. There are numerous ways of achieving this (in Section 4 we shall see a vast generalisation of the construction presented here), but the easiest is to simply use *component-wise* multiplication of group elements:

Definition 2.14: Let G, H be groups. We define the *direct product* of G, H to be the set $G \times H$ together with the binary operation:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2),$$

for all $(g_1, h_1), (g_2, h_2) \in G \times H$.

We can straightforwardly show that the direct product $G \times H$ forms a group as follows:

Proposition 2.15: The direct product $G \times H$ of the groups G, H is itself a group.

Proof: Certainly $G \times H$ is closed under the multiplication; this follows immediately from the definition of the operation and the closure of G, H separately. Similarly, the operation is associative because of the associativity of G, H separately; for all $(g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \times H$, we have:

$$\begin{aligned}(g_1, h_1) \cdot \big((g_2, h_2) \cdot (g_3, h_3)\big) &= (g_1, h_1) \cdot (g_2 g_3, h_2 h_3) \\ &= (g_1(g_2 g_3), h_1(h_2 h_3)) \\ &= ((g_1 g_2) g_3, (h_1 h_2) h_3) \\ &= (g_1 g_2, h_1 h_2) \cdot (g_3, h_3) \\ &= \big((g_1, h_1) \cdot (g_2, h_2)\big) \cdot (g_3, h_3).\end{aligned}$$

An identity for the operation is given by $(e_G, e_H) \in G \times H$, where $e_G \in G$ is the identity in G, and $e_H \in H$ is the identity in H. This is an identity since for all $(g, h) \in G \times H$, we have:

$$(e_G, e_H) \cdot (g, h) = (e_G g, e_H h) = (g, h) = (g e_G, h e_H) = (g, h) \cdot (e_G, e_H),$$

using the fact that e_G is an identity for G, and e_H is an identity for H. Finally, we note that $(g, h) \in G \times H$ has inverse $(g, h)^{-1} = (g^{-1}, h^{-1}) \in G \times H$, since:

$$(g, h) \cdot (g, h)^{-1} = (g, h) \cdot (g^{-1}, h^{-1}) = (g g^{-1}, h h^{-1}) = (e_G, e_H),$$

and similarly

$$(g, h)^{-1} \cdot (g, h) = (g^{-1}, h^{-1}) \cdot (g, h) = (g^{-1} g, h^{-1} h) = (e_G, e_H).$$

Thus all axioms are satisfied, and $G \times H$ is indeed a group under component-wise multiplication. □

3 Maps between groups

Aside from producing new natural instances of a mathematical structure from existing instances using the three standard set constructions, another interesting question we can ask when we introduce a new mathematical structure is: what are the natural structure-preserving maps between instances of our new mathematical structure? In the case of group theory, there is little additional structure on top of our set - we just add in a *binary operation*. Therefore, we might say that a map $\theta : G \to H$ respects the structure of the groups G, H if it simply respects the operations on the groups:

$$\theta(g_1 g_2) = \theta(g_1)\theta(g_2),$$

for all $g_1, g_2 \in G$. That is, θ is a map such that it doesn't matter whether we perform multiplication of group elements in the domain first then apply the map, or apply the map first then perform multiplication of group elements in the codomain.

In this section, we begin by studying this type of structure-preserving map, which we call a *homomorphism* between groups. We then specialise to homomorphisms which are *bijective*, called *isomorphisms*. We conclude with some important *isomorphism theorems* which can help us prove various relations between groups.

Homomorphisms

Motivated by the above, we define a *homomorphism* as follows:

Definition 3.1: Let G, H be groups, and let $\theta : G \to H$ be a function satisfying:

$$\theta(g_1 g_2) = \theta(g_1)\theta(g_2)$$

for all $g_1, g_2 \in G$. We say that θ is a *homomorphism* from the group G to the group H. In the special case $G = H$, we call a homomorphism $\theta : G \to G$ an *endomorphism*.

As anticipated, homomorphisms preserve various pieces of structure in the groups that we have previously defined:

Proposition 3.2: Let $\theta : G \to H$ be a homomorphism between the groups G, H. Then:

(i) (**Identities**) Let $e_G \in G$ be the identity of G. Then $\theta(e_G) \in H$ is the identity of H.

(ii) (**Inverses**) Let $g \in G$ have inverse $g^{-1} \in G$. Then the inverse of $\theta(g) \in H$ is given by $\theta(g)^{-1} = \theta(g^{-1}) \in H$.

(iii) (**Subgroups**) Let $K \leq G$ be a subgroup of G. Then the image $\theta(K) \leq H$ is a subgroup of H, and further, every subgroup of H is the image of some subgroup of G under θ.

Proof: (i) Note $\theta(e_G)^2 = \theta(e_G^2) = \theta(e_G)$. Multiplying on the left by $\theta(e_G)^{-1}$, we have $\theta(e_G) = e_H$, where $e_H \in H$ is the identity in H.

(ii) We have $\theta(g)\theta(g^{-1}) = \theta(gg^{-1}) = \theta(e_G) = \theta(g^{-1}g) = \theta(g^{-1})\theta(g)$, so $\theta(g)^{-1} = \theta(g^{-1})$ as required.

(iii) Let $K \leq G$ be a subgroup of G. Then $e_G \in K$, so $\theta(e_G) \in \theta(K)$, and hence $\theta(K)$ is non-empty. Furthermore, given $\theta(k_1), \theta(k_2) \in \theta(K)$, we have $\theta(k_1)\theta(k_2)^{-1} = \theta(k_1)\theta(k_2^{-1}) = \theta(k_1 k_2^{-1}) \in \theta(K)$. Thus $\theta(K) \leq H$ is a subgroup of H, by the subgroup test.

On the other hand, suppose that $L \leq H$ is a subgroup of H. Then $\theta(e_G) = e_H \in L$, so $e_G \in \theta^{-1}(L)$; thus the preimage $\theta^{-1}(L)$ is non-empty. Now suppose that $k_1, k_2 \in \theta^{-1}(L)$. Then $\theta(k_1), \theta(k_2) \in L$ so $\theta(k_1 k_2^{-1}) = \theta(k_1)\theta(k_2^{-1}) = \theta(k_1)\theta(k_2)^{-1} \in L$ since $L \leq H$. Hence $k_1 k_2^{-1} \in \theta^{-1}(L)$, and it follows that $\theta^{-1}(L) \leq G$ is a subgroup of G, by the subgroup test. □

Some special cases of (iii) in the above proposition have names, which will be useful shortly:

Definition 3.3: Let $\theta : G \to H$ be a group homomorphism. We define:

- The *image* of θ is the subgroup $\mathrm{im}(\theta) := \theta(G) = \{\theta(g) : g \in G\} \leq H$.
- The *kernel* of θ is the subgroup $\ker(\theta) := \theta^{-1}(\{e_H\}) = \{g \in G : \theta(g) = e_H\} \leq G$.

The kernel is particularly important, because it is a *normal subgroup* of G; this will allow us to construct the quotient group $G/\ker(\theta)$ shortly.

Proposition 3.4: Let $\theta : G \to H$. Then $\ker(\theta)$ is a normal subgroup of G.

Proof: We have already seen that $\ker(\theta) \leq G$ is a subgroup of G. Now note that given any $g \in G$ and $k \in \ker(\theta)$, we have:

$$\theta(gkg^{-1}) = \theta(g)\theta(k)\theta(g)^{-1} = \theta(g)e_H\theta(g)^{-1} = \theta(g)\theta(g)^{-1} = e_H.$$

Hence $gkg^{-1} \in \ker(\theta)$, so it follows that $g\ker(\theta)g^{-1} \subseteq \ker(\theta)$. Hence $\ker(\theta)$ is normal, as required. □

Isomorphisms

An important special case of a homomorphism is an *isomorphism* between groups:

Definition 3.5: A bijective homomorphism $\theta : G \to H$ between groups is called an *isomorphism*. In the special case $G = H$, we call an isomorphism $\theta : G \to G$ an *automorphism*.

If there is an isomorphism between two groups G, H, then we say that G, H are *isomorphic*. We write this as $G \cong H$.

If two groups G, H are isomorphic, then we cannot tell them apart using only their group structure; from the point of view of group theory, the two groups are identical, we have merely labelled their elements in different ways.

As an example of two isomorphic groups, consider the following:

Example 3.6: The set of integers modulo n, $\mathbb{Z}_n = \{0, 1, ..., n-1\}$, forms a group under addition modulo n. Closure is clear; associativity comes from the associativity of standard integer addition; the identity is $0 \in \mathbb{Z}_n$; the inverse of $m \in \mathbb{Z}_n$ is $-m \pmod n \in \mathbb{Z}_n$.

We claim that $\mathbb{Z}_n \cong C_n$. An isomorphism is given by $\phi : \mathbb{Z}_n \to C_n$, with $\phi(i) = r^i$. This is clearly a bijection; furthermore, it is a homomorphism since for all $i, j \in \mathbb{Z}_n$ we have:

$$\phi(i + j \pmod n) = r^{i+j \pmod n} = r^{i+j} = r^i r^j = \phi(i)\phi(j).$$

where in the second equality we recall that $r^n = e$, so the exponent can always be taken modulo n.

Isomorphism theorems

Proving that two groups are isomorphic can be made a little easier with the help of the following two theorems. The first constructs an isomorphism from a given homomorphism:

Theorem 3.7: (**The first isomorphism theorem**) Let $\theta : G \to H$ be a homomorphism. Then:

$$\frac{G}{\ker(\theta)} \cong \mathrm{im}(\theta).$$

Proof: Define $\phi : G/\ker(\theta) \to \mathrm{im}(\theta)$ by $\phi(g\ker(\theta)) = \theta(g)$. Then:

- The map ϕ is well-defined. To see this, let g_1, g_2 be two representatives of the same left coset of $\ker(\theta)$. Then $g_2^{-1}g_1 \in \ker(\theta)$, so we have $\theta(g_2^{-1}g_1) = e$, which implies $\theta(g_1) = \theta(g_2)$ using the properties of homomorphisms. Thus $\phi(g_1\ker(\theta)) = \phi(g_2\ker(\theta))$. Furthermore, the map certainly has the correct codomain, $\mathrm{im}(\theta)$.
- The map is injective, since $\theta(g_1) = \theta(g_2)$ implies $\theta(g_2^{-1}g_1) = e$, so that $g_2^{-1}g_1 \in \ker(\theta)$. Thus g_1, g_2 are in the same left coset of $\ker(\theta)$, i.e. $g_1\ker(\theta) = g_2\ker(\theta)$.
- The map is surjective, since given $h \in \mathrm{im}(\theta)$, there exists $g \in G$ with $\theta(g) = h$. Then $\phi(g\ker(\theta)) = \theta(g) = h$.
- The map is a homomorphism. To see this, note:

$$\phi(g_1\ker(\theta) \cdot g_2\ker(\theta)) = \phi(g_1g_2\ker(\theta)) = \theta(g_1g_2) = \theta(g_1)\theta(g_2) = \phi(g_1\ker(\theta))\phi(g_2\ker(\theta)).$$

Hence ϕ is a well-defined bijective homomorphism from $G/\ker(\theta)$ to $\mathrm{im}(\theta)$. The result follows. □

The second theorem we shall prove constructs an isomorphism between a group and the direct product of two of its subgroups (under some special conditions):

Theorem 3.8: (**The direct product theorem**) Let $H, K \leq G$ be subgroups of the group G. Suppose that:

(i) For all $h \in H, k \in K$, we have $hk = kh$.

(ii) Given any $g \in G$, there exists $h \in H$ and $k \in K$ such that $g = hk$.

(iii) The two subgroups H, K have trivial intersection, $H \cap K = \{e\}$.

Then $G \cong H \times K$; that is, G is isomorphic to the direct product $H \times K$.

Proof: Define a map $\phi : H \times K \to G$ given by $\phi(h, k) = hk$. We shall show that this map is an isomorphism. First, we note that it is a homomorphism, since:

$$\phi((h, k) \cdot (h', k')) = \phi(hh', kk') = hh'kk' = hkh'k' = \phi(h, k)\phi(h', k'),$$

using the commutativity of elements drawn from H and drawn from K (assumption (i)).

Next, we show that the map is injective; suppose that $\phi(h, k) = \phi(h', k')$. Then $hk = h'k'$, which implies $k(k')^{-1} = h^{-1}h'$. The left hand side is an element of K whilst the right hand side is an element of H. By (iii), these two subgroups are trivially intersecting, and hence $k(k')^{-1} = e$ and $h^{-1}h' = e$, from which it follows that $k = k'$ and $h = h'$.

Finally, the map is clearly a surjection, since assumption (ii) tells us that any $g \in G$ can be written as $g = hk$ for some $h \in H$ and some $k \in K$. It follows that $g = \phi(h, k)$, and we're done. □

4 Semi-direct products

In Section 2, we introduced a group structure on the Cartesian product $G \times H$ of two groups using component-wise multiplication, which we called the *direct product* of the groups. In general, we can obtain more interesting group structures on $G \times H$, and it is the goal of this section to introduce such a structure.

It is of course possible to impose arbitrarily silly group structures on $G \times H$. This wouldn't be very useful, however - we will restrict the types of group structures which we shall endow $G \times H$ with by imposing the following natural conditions:

(1) G, H **arise naturally as subgroups of** $G \times H$**.** We should have subgroups $G \times \{e\} \leq G \times H$ and $\{e\} \times H \leq G \times H$, which are isomorphic to G and H respectively; that is, the group multiplication should obey:

$$(g_1, e) \cdot (g_2, e) = (g_1 g_2, e), \qquad (e, h_1) \cdot (e, h_2) = (e, h_1 h_2)$$

for all $g_1, g_2 \in G$ and $h_1, h_2 \in H$.

(2) **Elements of** $G \times H$ **can be naturally factored.** Multiplying an element '$g \in G$', represented in the direct product by $(g, e) \in G \times \{e\}$, by an element '$h \in H$', represented in the direct product by $(e, h) \in \{e\} \times H$, we would like to get the element 'gh', which should be interpreted as the element $(g, h) \in G \times H$. Thus we impose the equation:

$$(g, e) \cdot (e, h) = (g, h)$$

for all $g \in G, h \in H$. In this way, elements of $G \times H$ can be 'factored' into a product of an element from G and an element from H. Note that this doesn't work the other way around; multiplying $(e, h) \cdot (g, e)$ should give us the element 'hg', which only has a natural corresponding element in $H \times G$.

These assumptions are enough to force the group multiplication to be of a very specific form, determined completely by two maps $\alpha : H \times G \to G$ and $\beta : H \times G \to H$; we can see this as follows. Note that to evaluate the generic product of group elements, $(g_1, h_1), (g_2, h_2) \in G \times H$ we first 'factor' both terms using the second assumption:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1, e) \cdot (e, h_1) \cdot (g_2, e) \cdot (e, h_2).$$

Now since we want $G \times H$ to be a group, for closure we require $(e, h_1) \cdot (g_2, e) = (\alpha(h_1, g_2), \beta(h_1, g_2))$ for some $\alpha(h_1, g_2) \in G$ and some $\beta(h_1, g_2) \in H$. This defines some functions $\alpha : H \times G \to G$ and $\beta : H \times G \to H$. We can now evaluate the product in terms of the functions α, β using our two basic assumptions:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1, e) \cdot (\alpha(h_1, g_2), \beta(h_1, g_2)) \cdot (e, h_2) = (g_1, e) \cdot (\alpha(h_1, g_2), e) \cdot (e, \beta(h_1, g_2)) \cdot (e, h_2)$$

$$= (g_1 \alpha(h_1, g_2), e) \cdot (e, \beta(h_1, g_2) h_2) = (g_1 \alpha(h_1, g_2), \beta(h_1, g_2) h_2).$$

This shows that the group operation must be of the form:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \alpha(h_1, g_2), \beta(h_1, g_2) h_2)$$

for some functions $\alpha : H \times G \to G$ and $\beta : H \times G \to H$.

So far we have shown that the group operation is *necessarily* of this form. It is also possible to derive some *sufficient* conditions on the functions α, β for the multiplication defined above to yield a group,[1] but in practice two special cases suffice:

- The *direct product* corresponds to the special case $\alpha(h_1, g_2) = g_2, \beta(h_1, g_2) = h_1$. The group operation simplifies to component-wise multiplication:
$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2).$$
We already introduced this structure in Section 2.

[1] The general structure is called the *external Zappa-Szép product* via α, β.

- The *semi-direct product* corresponds to the special case $\beta(h_1, g_2) = h_1$ (and with α obeying some extra sufficient conditions which we shall describe below). In particular, this generalises the direct product construction described in the previous bullet point. The group operation simplifies to:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1\alpha(h_1, g_2), h_1h_2).$$

We have already seen that the first choice leads to a group structure on $G \times H$; we shall now determine the conditions on α in the second choice which lead to a group structure on $G \times H$.

Proposition 4.1: Given groups G, H and a map $\alpha : H \times G \to G$, consider the Cartesian product $G \times H$ together with the binary operation:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1\alpha(h_1, g_2), h_1h_2).$$

The set $G \times H$ forms a group under this operation, with the multiplication obeying $(g_1, e) \cdot (g_2, e) = (g_1g_2, e)$ for all $g_1, g_2 \in G$, and $(e, h_1) \cdot (e, h_2) = (e, h_1h_2)$ for all $h_1, h_2 \in H$, if and only if α satisfies the following additional properties:

(i) $\alpha(h, -) : G \to G$ is an automorphism for all $h \in H$;

(ii) $\alpha(h_1h_2, g) = \alpha(h_1, \alpha(h_2, g))$ for all $g \in G$ and $h_1, h_2 \in H$.

Proof: First, let's suppose that $G \times H$ is a group under the given operation, and that the operation obeys the given condition. We begin by showing that $\alpha(h, -)$ is an automorphism for fixed $h \in H$. Suppose that $\alpha(h, g_1) = \alpha(h, g_2)$ for $g_1, g_2 \in G$. By definition of the operation, we have:

$$(e, h) \cdot (g_1, e) = (\alpha(h, g_1), h) = (\alpha(h, g_2), h) = (e, h) \cdot (g_2, e).$$

Since we assume that $G \times H$ is a group under the given operation, inverses exists, and hence we can multiply on the left by $(e, h)^{-1}$. We conclude that $g_1 = g_2$, so $\alpha(h, -)$ is an injection.

Next, note that given any $g \in G$, we have by the assumptions:

$$(\alpha(h, \alpha(h^{-1}, g)), h) = (e, h) \cdot (\alpha(h^{-1}, g), e) = (e, h) \cdot (e, h^{-1}) \cdot (g, h) = (g, h).$$

Hence $\alpha(h, \alpha(h^{-1}, g)) = g$, so $\alpha(h, -)$ is a surjection. It follows that $\alpha(h, -)$ is a bijection.

To finish showing (i), it remains to show that $\alpha(h, -)$ is a homomorphism. We use associativity together with the assumed condition:

$$(\alpha(h, g_1g_2), h) = (e, h) \cdot (g_1g_2, e) = (e, h) \cdot (g_1, e) \cdot (g_2, e) = (\alpha(h, g_1), h) \cdot (g_2, e) = (\alpha(h, g_1)\alpha(h, g_2), h),$$

so $\alpha(h, g_1g_2) = \alpha(h, g_1)\alpha(h, g_2)$. It follows that $\alpha(h, -)$ is a homomorphism. All in all, we have that $\alpha(h, -)$ is an automorphism for each $h \in H$.

Finally, we can demonstrate property (ii) using associativity and the assumed condition:

$$\begin{aligned}(\alpha(h_1h_2, g), h_1h_2) &= (e, h_1h_2) \cdot (g, e) = (e, h_1) \cdot (e, h_2) \cdot (g, e) = (e, h_1) \cdot (\alpha(h_2, g), h_2) \\ &= (\alpha(h_1, \alpha(h_2, g)), h_1h_2).\end{aligned}$$

It follows that $\alpha(h_1h_2, g) = \alpha(h_1, \alpha(h_2, g))$ as required.

Now we prove the converse: assuming (i) and (ii), the given operation endows $G \times H$ with a group structure, where the multiplication obeys the given condition. We trivially have closure since $g_1\alpha(h_1, g_2) \in G$, $h_1h_2 \in H$ for all $g_1, g_2 \in G, h_1, h_2 \in H$, by the closure of G, H.

Next, note that we have associativity; we evaluate the product $(g_1, h_1) \cdot (g_2, h_2) \cdot (g_3, h_3)$ in the following two ways:

$$\big((g_1, h_1) \cdot (g_2, h_2)\big) \cdot (g_3, h_3) = (g_1\alpha(h_1, g_2), h_1h_2) \cdot (g_3, h_3) = (g_1\alpha(h_1, g_2)\alpha(h_1h_2, g_3), h_1h_2h_3),$$

and:

$$(g_1, h_1) \cdot \big((g_2, h_2) \cdot (g_3, h_3)\big) = (g_1, h_1) \cdot (g_2\alpha(h_2, g_3), h_2h_3) = (g_1\alpha(h_1, g_2\alpha(h_2, g_3)), h_1h_2h_3).$$

These agree since $\alpha(h_1, g_2\alpha(h_2, g_3)) = \alpha(h_1, g_2)\alpha(h_1, \alpha(h_2, g_3))$ since, assuming (i), $\alpha(h_1, -)$ is a homomorphism for each $h_1 \in H$, and $\alpha(h_1, g_2)\alpha(h_1, \alpha(h_2, g_3)) = \alpha(h_1, g_2)\alpha(h_1h_2, g_3)$ using (ii).

We now claim that the identity is (e, e). We note that:

$$(e, e) \cdot (g, h) = (\alpha(e, g), h).$$

Now $\alpha(e, g) = \alpha(e^2, g) = \alpha(e, \alpha(e, g))$ by property (ii), and by property (i) injectivity of $\alpha(e, -)$ then implies $\alpha(e, g) = g$. Thus $(e, e) \cdot (g, h) = (g, h)$. On the other hand, we have:

$$(g, h) \cdot (e, e) = (g\alpha(h, e), h) = (g, h),$$

since by property (i), $\alpha(h, -)$ is a homomorphism so maps the identity to the identity.

Finally, we show that inverses exist. We have:

$$(g_1, g_2) \cdot (\alpha(g_2^{-1}, g_1^{-1}), g_2^{-1}) = (g_1\alpha(g_2, \alpha(g_2^{-1}, g_1^{-1})), e).$$

Now by property (ii), we have $\alpha(g_2, \alpha(g_2^{-1}, g_1^{-1})) = \alpha(e, g_1^{-1})$, then by the above discussion we have $\alpha(e, g_1^{-1}) = g_1^{-1}$. It follows that we have produced the right inverse of (g_1, g_2). We also see that this is a left inverse for (g_1, g_2):

$$(\alpha(g_2^{-1}, g_1^{-1}), g_2^{-1}) \cdot (g_1, g_2) = (\alpha(g_2^{-1}, g_1^{-1})\alpha(g_2^{-1}, g_1), e).$$

Using property (i), $\alpha(g_2^{-1}, -)$ is a homomorphism, so we have: $\alpha(g_2^{-1}, g_1^{-1})\alpha(g_2^{-1}, g_1) = \alpha(g_2^{-1}, e) = e$ as required.

All that remains is to show that the group multiplication obeys $(g_1, e) \cdot (h_1, e) = (g_1h_1, e)$ and $(e, g_2) \cdot (e, h_2) = (e, g_2h_2)$ for all $g_1, h_1 \in G_1$ and $g_2, h_2 \in G_2$. We simply note:

$$(g_1, e) \cdot (h_1, e) = (g_1\alpha(e, h_1), e) = (g_1h_1, e),$$

using the property we derived above, and similarly using property (i) that $\alpha(h_1, -)$ is a homomorphism we have:

$$(e, h_1) \cdot (e, h_2) = (\alpha(h_1, e), h_1h_2) = (e, h_1h_2).$$

Hence $G_1 \times G_2$ is indeed a group under this operation, and the given condition on the multiplication holds. □

Now we have proved that this more general operation endows $G \times H$ with a group structure, provided we have conditions (i) and (ii) in the above proposition, we can bake things into a definition. Before doing so, it is convenient to observe that condition (ii) in the above, namely:

$$\alpha(h_1 h_2, g) = \alpha(h_1, \alpha(h_2, g))$$

can be interpreted as saying that the map $\phi : H \to \mathrm{Aut}(G)$ from H into the set $\mathrm{Aut}(G)$ of all automorphisms of G, given by $\phi(h) = \alpha(h, -)$, is a *homomorphism*. In order for this to be the case, we require the set of all automorphisms to be a group under composition of automorphisms; you will check this in the exercises at the end of this handout:

Proposition 4.2: Let G be a group, and let $\mathrm{Aut}(G)$ be the set of all automorphisms of G. Then $\mathrm{Aut}(G)$ is a group under composition.

Proof: Left as an exercise to the reader, at the end of the handout. □

This observation allows us to conveniently write the definition of the semi-direct product as follows:

Definition 4.3: Let G, H be groups, let $\phi : H \to \mathrm{Aut}(G)$ be a homomorphism, and write ϕ_h for the image of $h \in H$ under ϕ (so that $\phi_h := \phi(h)$ here). The set $G \times H$ together with the binary operation:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \phi_{h_1}(g_2), h_1 h_2)$$

forms a group called the *semi-direct product of G, H with respect to ϕ*. We use the notation $G \rtimes_\phi H$ to mean the set $G \times H$ endowed with this binary operation.

A non-trivial example of semi-direct product is the following:

Example 4.4: The dihedral groups can be written as the semi-direct products of cyclic groups, $D_n \cong \mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2$, where $\phi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_n)$ is given by $\phi_0(x) = x, \phi_1(x) = -x$.

To see this, define $\theta : \mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2 \to D_n$ by $\theta(a, b) = r^a s^b$. This is clearly surjective and injective (e.g. note $r^a s^b = r^a$ for $b = 0$, and $r^a s^b = s r^{-a} = s r^{n-a}$ for $b = 1$); it remains to show that it is a homomorphism. We have:

$$\theta((a, b) \cdot (a', b')) = \theta(a \phi_b(a'), bb') = r^{a \phi_b(a')} s^{bb'} = r^a r^{\phi_b(a')} s^b s^{b'}.$$

Now if $b = 0$, we have $r^{\phi_b(a')} s^b = r^{a'} = s^b r^{a'}$. On the other hand if $b = 1$, we have $r^{\phi_b(a')} s^b = r^{-a'} s = s r^{a'} = s^b r^{a'}$. Thus in all cases we have $\theta((a, b) \cdot (a', b')) = r^a s^b r^{a'} s^{b'} = \theta(a, b)\theta(a', b')$.

✎ Exercises

Examples of groups

1. Consider the set $\mathbb{R}^2$ consisting of pairs of real numbers. For $(x, y) \in \mathbb{R}^2$, find which of the following operations make $\mathbb{R}^2$ into a group (and if not, find why not):
   (a) $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$
   (b) $(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2)$
   (c) $(x_1, y_1) \circ (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)$.
2. Let G be a set of $n \times n$ matrices.
   (a) Prove that if G is a group under matrix multiplication and if one of the elements of G is a non-singular matrix then all of the elements of G must be non-singular matrices. Conclude that the elements of G are either all non-singular matrices or all singular matrices.
   (b) Consider the set of 2×2 singular matrices G of the form:

$$\begin{pmatrix} x & x \\ x & x \end{pmatrix} \qquad (*)$$

   where $x \in \mathbb{R}$ and $x \neq 0$. Prove that G is a group with respect to matrix multiplication. Determine the matrix corresponding to the identity element of G. Determine the inverse element of $(*)$.

New groups from old

3. Write down the Cayley table for the dihedral group D_4. Enumerate the subgroups and the normal subgroups. Can D_4 be written as the non-trivial direct product of some of its subgroups?
4. Let $Z(G)$ be the centre of the group G.
   (a) Show that $Z(G)$ is an Abelian subgroup of G.
   (b) Show that $Z(G)$ is a normal subgroup of G.
   (c) Find the centre of D_4 and construct the group $D_4/Z(D_4)$. Determine whether the isomorphism

$$D_4 \cong [D_4/Z(D_4)] \times Z(D_4)$$

   is valid.

Maps between groups

5. Identify a well known mathematical object that is isomorphic to $\mathbb{R}^2 \backslash \{(0, 0)\}$ under the operation $\circ$, as defined in Question 1(c). Similarly, identify a well known group that is isomorphic to the group defined in Question 2(b).
6. Recall that an automorphism is an isomorphism from a group G to itself.
   (a) Show that for any $g \in G$, the mapping $T_g(x) = gxg^{-1}$ is an automorphism (called an *inner automorphism*), where $x \in G$.
   (b) Show that the set of all inner automorphisms of G, denoted by $\mathcal{I}(G)$, is a group.
   (c) Show that $\mathcal{I}(G) \cong G/Z(G)$, where $Z(G)$ is the centre of G.
   (d) Show that the set of all automorphisms of G, denoted by $\mathcal{A}(G)$, is a group and that $\mathcal{I}(G)$ is a normal subgroup of $\mathcal{A}(G)$. The quotient group $\mathcal{A}(G)/\mathcal{I}(G)$ is called the group of *outer automorphisms* of G.