

Introduction to Groups

Tim Sullivan

August 16, 2006

Contents

1	Groups	1
1.1	Basic Definitions	1
1.2	Examples from Arithmetic	2
1.3	Isometry Groups	4
1.4	Matrix Groups	6
1.5	The Symmetric and Alternating Groups	6
1.6	Some Properties of Groups	8
2	Subgroups, Cosets, and Lagrange's Theorem	9
2.1	Subgroups	9
2.2	Generators	11
2.3	Cosets and Normal Subgroups	12
2.4	Lagrange's Theorem	13
3	Morphisms of Groups	14
3.1	Philosophy	14
3.2	Morphisms of Groups	15
3.3	Properties of Homomorphisms and Isomorphisms	17
4	Products of Groups	18
4.1	The Direct Product	19
5	The First Isomorphism Theorem	19
5.1	"The First Isomorphism Theorem for Sets"	19
5.2	The First Isomorphism Theorem for Groups	21

1 Groups

1.1 Basic Definitions

Definitions 1.1.1. A *group* is a non-empty set G together with a law of composition $*$: $G \times G \rightarrow G$ satisfying the following axioms:

- (i) *associativity*: for any three elements $g, h, k \in G$, $g * (h * k) = (g * h) * k$;

(ii) *identity*: there is a *neutral element* or *identity* $e \in G$ such that for all $g \in G$, $e * g = g * e = g$;

(iii) *inverses*: given any element $g \in G$, there is an element $g' \in G$ such that $g * g' = g' * g = e$.

The law of composition is often simply called the group *operation*.

The mantra is this: a group is a structure in which we can compose pairs of elements together to get new ones (law of composition $G \times G \rightarrow G$), parentheses don't matter (associativity), there's an element that does nothing (the identity), and we can undo the effect of any element (inverses).

Watch out! The idea that “parentheses don't matter” can lead one into the trap of believing that $g * h$ is the same thing as $h * g$. The order of composition is very much important. We have a special name for groups where the order of composition does not matter:

Definition 1.1.2. Let G be a group with operation $*$. If $g * h = h * g$ for all $g, h \in G$, we say that the group is *Abelian*¹ or *commutative*.

We have a simple definition for the “size” of a group:

Definition 1.1.3. Let G be a group with operation $*$. The *order* of G , written $|G|$, is defined to be the cardinality of the underlying set G — i.e., the number of elements.

Confusingly, there is another use of the word “order” in group theory:

Definition 1.1.4. Let G be a group with operation $*$. The *order* of an element $g \in G$, written $o(g)$ or $|g|$, is defined to be the smallest integer $n > 0$ such that

$$\underbrace{g * g * \cdots * g}_{n \text{ copies of } g} = e.$$

1.2 Examples from Arithmetic

Examples 1.2.1. The integers, \mathbb{Z} .

- (i) Consider the operation of addition, $+$: $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$. We know that addition is associative. The identity element is $0 \in \mathbb{Z}$. The inverse of $n \in \mathbb{Z}$ is $-n \in \mathbb{Z}$, where “ $-n$ ” means exactly what it has meant since primary school. So, \mathbb{Z} with $+$ is a group. In fact, addition is also commutative, so \mathbb{Z} with $+$ is an Abelian group.
- (ii) What about multiplication, \cdot : $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$? We know that multiplication is associative. The identity element is $1 \in \mathbb{Z}$. Unfortunately, not every integer has an integral inverse: the inverse of $2 \in \mathbb{Z}$ is $1/2 \notin \mathbb{Z}$. So, \mathbb{Z} with \cdot is *not* a group.

Examples 1.2.2. The rational numbers, \mathbb{Q} .

- (i) Consider the operation of addition, $+$: $\mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$. We know that addition is associative. The identity element is $0 \in \mathbb{Q}$. The inverse of $n \in \mathbb{Q}$ is $-n \in \mathbb{Q}$. So, \mathbb{Q} with $+$ is a group. In fact, addition is also commutative, so \mathbb{Q} with $+$ is an Abelian group.

¹Niels Henrik Abel (1802—1829) was a noted Norwegian mathematician.

- (ii) What about multiplication, $\cdot : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$? We know that multiplication is associative. The identity element is $1 \in \mathbb{Q}$. Unfortunately, not every rational has an inverse: $0 \in \mathbb{Q}$ has no inverse. So, \mathbb{Q} with \cdot is *not* a group. However, we can save the day: let \mathbb{Q}^* denote $\mathbb{Q} \setminus \{0\}$. We now have \mathbb{Q}^* with multiplication \cdot , a *bone fide* group. In fact, it's Abelian.

Exercises 1.2.3. The real numbers, \mathbb{R} .

- (i) Show that \mathbb{R} with $+$ is an Abelian group.
(ii) Show that \mathbb{R} with \cdot is not a group, but that $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$ with \cdot is an Abelian group.

Exercises 1.2.4. The complex numbers, \mathbb{C} .

- (i) Show that \mathbb{C} with $+$ is an Abelian group.
(ii) Show that \mathbb{C} with \cdot is not a group, but that $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$ with \cdot is an Abelian group.

Exercise 1.2.5. Let K be field a V a vector space over K . Show that V with vector addition is an Abelian group. (In fact, this can be taken as part of the definition of a vector space.)

Example 1.2.6. The integers modulo n , \mathbb{Z}_n . Consider the numbers $\mathbb{Z}_n := \{0, 1, \dots, n-1\}$. We can add these numbers “modulo n ” by the following rule:

$$a +_n b := \begin{cases} a + b & \text{if } a + b < n, \\ a + b - n & \text{if } a + b \geq n. \end{cases}$$

This new addition, $+_n$ on \mathbb{Z}_n , is associative (and commutative) because $+$ is associative (and commutative) on \mathbb{Z} . The identity element is again 0. Inverses are slightly different: the inverse of $a \in \mathbb{Z}_n$ is $n - a$, which we can calculate in \mathbb{Z} . So \mathbb{Z}_n with $+_n$ is an Abelian group. (We usually dispense with the extra subscript n and just write $+$ instead of $+_n$.) The order of \mathbb{Z}_n , $|\mathbb{Z}_n|$, is just n .

Example 1.2.7. The cyclic group of order n . Consider the set

$$C_n := \{1 = a^0, a = a^1, a^2, a^3, \dots, a^{n-1}\},$$

where we multiply elements of C_n according to the rule $a^i a^j = a^{i+j}$. The identity element is 1 and the inverse of a^i is a^{n-i} . C_n forms an Abelian group with respect to this multiplication for exactly the same reasons as \mathbb{Z}_n is an Abelian group with respect to addition. The two groups are essentially the same group written in two slightly different ways.

In order to save space, it is traditional in group theory to use “multiplicative notation” and write the group operation as juxtaposition (writing things next to one another) unless another more suitable notation is obvious (we wouldn't want to use anything other than $+$ to stand for addition in \mathbb{Z} , for example). In multiplicative notation the identity element of G is written as 1_G or simply 1. g^{-1} stands for the inverse of g , and

$$g^n := \begin{cases} \underbrace{gg \dots g}_{n \text{ copies}} & n > 0 \\ 1 & n = 0 \\ \underbrace{g^{-1}g^{-1} \dots g^{-1}}_{n \text{ copies}} & n < 0 \end{cases}$$

The cyclic group C_n is a perfect example of this multiplicative notation.

1.3 Isometry Groups

An important class of groups are those that represent the *isometries* or “rigid motions” of a space. In the course *Metric Spaces* you will learn a general definition of a metric, or “distance function”, and so will have a general idea of isometry. For the moment, however, it will be sufficient to consider the Euclidean case.

Definitions 1.3.1. Let \mathbb{R}^n be n -dimensional Euclidean space and $\|\cdot\| : \mathbb{R}^n \rightarrow \mathbb{R}_{\geq 0}$ the usual Euclidean norm: for a vector $x = (x^1, \dots, x^n) \in \mathbb{R}^n$,

$$\|x\| := \sqrt{\sum_{j=1}^n |x^j|^2}.$$

A map $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ is an *isometry* of Euclidean space if for all pairs $x, y \in \mathbb{R}^n$,

$$\|x - y\| = \|f(x) - f(y)\|.$$

Write $\mathcal{I}(\mathbb{R}^n)$ for the set of all isometries of \mathbb{R}^n . Similarly, if $X \subseteq \mathbb{R}^n$, define

$$\mathcal{I}(X) := \{f : X \rightarrow X \mid \forall x, y \in X, \|x - y\| = \|f(x) - f(y)\|\}.$$

$\mathcal{I}(X)$ is called the (*Euclidean*) *isometry group* of X and its elements are (*Euclidean*) *isometries* (of X).

An isometry is a map that preserves distances: however far apart x and y were in the beginning, they are the same distance apart after f has been applied. (“Isometry” = “iso” (Greek for “same”) + “metry” (Greek for “distance”).)

Exercises 1.3.2. Show that

- (i) an isometry of X is necessarily a bijection $X \rightarrow X$;
- (ii) $\mathcal{I}(X)$ is a group with respect to composition of functions.

Examples 1.3.3. (i) The interval $[-1, 1]$. As always, the identity map is an isometry of $[-1, 1]$ since it changes nothing. The only other isometry is the one that reflects the interval about 0, taking x to $-x$. Thus,

$$\mathcal{I}([-1, 1]) = \{\text{id} : x \mapsto x, r : x \mapsto -x\},$$

a group of order 2.

- (ii) The real line, \mathbb{R} . It’s clear that a translation of the real line, $T_z : x \mapsto z + x$ for some fixed $z \in \mathbb{R}$, is an isometry of \mathbb{R} . Slightly less immediate is the fact that reflections $R_z : x \mapsto z - x$ are also in $\mathcal{I}(\mathbb{R})$. So

$$\mathcal{I}(\mathbb{R}) = \{T_z : x \mapsto z + x \mid z \in \mathbb{R}\} \cup \{R_z : x \mapsto z - x \mid z \in \mathbb{R}\},$$

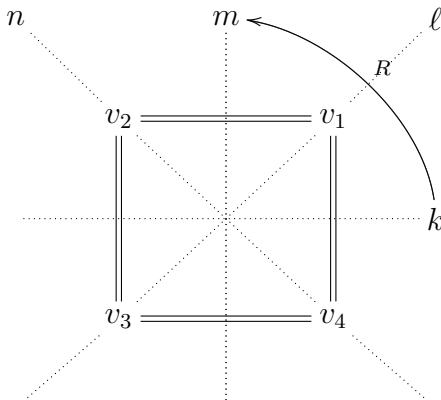
a group of infinite order. The identity map is the same as T_0 .

There is one example in particular that seems tailor-made for elementary courses in group theory: the group of isometries of a square.

Example 1.3.4. The isometries of a square. Let S denote the square

$$S := \{(x, y) \in \mathbb{R}^2 \mid -1 \leq x, y \leq 1\} = [-1, 1] \times [-1, 1] \subset \mathbb{R}^2.$$

What is the isometry group $\mathcal{I}(S)$?



To start with, as always, the identity map is in $\mathcal{I}(S)$. Then, rotation of the square by a right angle (in the anti-clockwise direction) is also an isometry — denote this map by R . Rotating by a right angle twice (i.e. rotating by $\pi = 180^\circ$) is also an isometry, $R^2 := R \circ R$. Similarly $R^3 := R \circ R \circ R = R^{-1}$, which is rotation by a right angle in the clockwise direction. $R^4 = \text{id}$, of course.

We can also reflect the square in four lines of symmetry, the lines labelled k , l , m and n above. Call these reflections r_k , r_l , r_m and r_n respectively. We now have all the isometries of the square:

$$\mathcal{I}(S) = \{\text{id}, R, R^2, R^3, r_k, r_l, r_m, r_n\},$$

a group of order 8. $\mathcal{I}(S)$ is not an Abelian group:

$$(R \circ r_k)(v_1) = v_1 \text{ but } (r_k \circ R)(v_1) = v_3 \neq v_1.$$

Example 1.3.5. The isometries of a regular n -gon. Let $n \geq 3$ and let P_n be a regular n -sided polygon: P_3 is an equilateral triangle, P_4 is a square, P_5 is a pentagon and so on. We can find $\mathcal{I}(P_n)$ just as before. $\mathcal{I}(P_n)$ contains the rotations by multiples of $2\pi/n$, and there are n of these including the identity, which is rotation by 0. There are also n reflections in n lines:

- (i) when n is odd, these are the n lines that join a vertex (corner) of P_n to the centre of the opposite edge (side);
- (ii) when n is even, these are the $n/2$ lines that join a vertex of P_n to the opposite vertex, and the $n/2$ lines that join the centre of an edge of P_n to the centre of the opposite edge.

So $\mathcal{I}(P_n)$ is a group of order $2n$. It is usually denoted D_{2n} (or sometimes D_n , for instance by chemists) and is called the *dihedral group* of order $2n$. In this notation, $\mathcal{I}(S) = D_8$, and that is the name that we shall use from now on.

1.4 Matrix Groups

Let $M_{m \times n}(K)$ denote the set of $m \times n$ matrices with entries from a given field K , for instance $K = \mathbb{R}$ or \mathbb{C} . As you know from previous courses on linear algebra, $M_{m \times n}(K)$ forms a vector space of dimension mn over the field K with the operations of matrix addition and scalar multiplication. Take $A = (\alpha_{ij})$, $B = (\beta_{ij})$, $C = (\gamma_{ij})$. If $C = A + B$ then

$$\gamma_{ij} = \alpha_{ij} + \beta_{ij}$$

and if $C = \lambda A$ for some $\lambda \in K$,

$$\gamma_{ij} = \lambda \alpha_{ij}.$$

Exercise 1.2.5 tells us that $M_{m \times n}(K)$ is a group with respect to matrix addition. The identity element is the zero matrix.

We can also have matrix groups with respect to matrix multiplication:

Definitions 1.4.1. Given a field K and an integer $n > 0$, we define the *general linear group* $\text{GL}(n, K)$ to be the set of all invertible $n \times n$ matrices with entries from the field K . The *special linear group* is defined to be

$$\text{SL}(n, K) := \{A \in \text{GL}(n, K) \mid \det A = 1\}$$

Exercise 1.4.2. Show that $\text{GL}(n, K)$ and $\text{SL}(n, K)$ are groups with respect to matrix multiplication.

Exercise 1.4.3. (Hard.) It should be fairly clear that $\text{GL}(n, K)$ is infinite when the field K is infinite, like $K = \mathbb{Q}$, \mathbb{R} , or \mathbb{C} . What about when K is a finite field? Try to find a formula for $|\text{GL}(n, K)|$ when $|K| = q \in \mathbb{N}$.

1.5 The Symmetric and Alternating Groups

Definition 1.5.1. Let Ω be a set. Let $\text{Sym}(\Omega)$ denote the set of all bijections $\sigma : \Omega \rightarrow \Omega$. Such functions are known as *permutations* of Ω . The operation will be composition of functions, \circ . $\text{Sym}(\Omega)$ is called the *symmetric group* on Ω .

From *Foundations*, composition of maps is always associative. There is an identity function

$$\begin{aligned} \text{id}_\Omega : \Omega &\rightarrow \Omega \\ a &\mapsto a \end{aligned}$$

which clearly satisfies $\sigma \circ \text{id}_\Omega = \sigma = \text{id}_\Omega \circ \sigma$ for all $\sigma \in \text{Sym}(\Omega)$. Given $\sigma \in \text{Sym}(\Omega)$, we can form the inverse function $\sigma^{-1} : \Omega \rightarrow \Omega$, which exists because σ is a bijection. Since σ is a bijection, so is σ^{-1} . As expected, $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \text{id}_\Omega$. So $\text{Sym}(\Omega)$ is indeed a group.

When Ω is a finite set with n elements, we conventionally identify it with the set $\{1, 2, \dots, n\}$. In this case we write $\text{Sym}(n)$ or simply S_n for the symmetric group on n elements. Since $\sigma \in S_n$ can take 1 to any one of n places, 2 to any of the $n - 1$ remaining places, and so on, $|S_n| = n!$.

We can write elements $\sigma \in S_n$ in many ways. There is the “brute force” method of listing each number $1, \dots, n$ and their images $\sigma(1), \dots, \sigma(n)$. For example:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix} \in S_6$$

This means that $\sigma(1) = 2$, $\sigma(2) = 1$, etc.

There is another notation that is far more compact: *disjoint cycle notation*. In disjoint cycle notation, we pick a number i , then write down $\sigma(i)$, then $\sigma^2(i) = \sigma(\sigma(i))$ etc. until we come back on ourselves in a cycle, finishing where we started, at i . We then do this to any element left over, and so on until we have covered all the numbers $1 \leq i \leq n$. So, in the above example:

$$\sigma = (1, 2)(3)(4, 5, 6)$$

It is conventional to omit cycles of length 1 (containing only one number), so the above σ would be written as $(1, 2)(4, 5, 6)$.

Remember that objects such as $(1, 2)$ are functions:

$$(1, 2)(i) = \begin{cases} 2 & i = 1 \\ 1 & i = 2 \\ i & \text{otherwise.} \end{cases}$$

Exercise 1.5.2. Write down some more elements of S_6 (or S_n for any reasonably small n) in the “brute force” notation and then convert them to disjoint cycle notation. Do the reverse, too: write down some products of cycles and convert them to “brute force” notation.

Definition 1.5.3. A cycle of length 2, i.e. a permutation $(i, j) \in S_n$ for some $1 \leq i \neq j \leq n$, is called a *transposition*.

Proposition 1.5.4. Any $\sigma \in S_n$ can be written as a product of transpositions.

Proof. We can convert any permutation into disjoint cycle notation, so we need only check that cycles can be written as products of transpositions. This is indeed true:

$$(a_1, a_2, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \dots (a_1, a_3)(a_1, a_2).$$

Thus, we are done. □

Definitions 1.5.5. $\sigma \in S_n$ is called *even* if it is a product of an even number of transpositions; it is called *odd* if it is the the product of an even number of transpositions.

Examples 1.5.6. (i) $(1, 2) \in S_3$ is odd.

(ii) $(1, 2, 3) = (1, 3)(1, 2) \in S_3$ is even.

(iii) $(1, 2, 3) = (1, 3)(1, 2)(4, 5)(4, 5) \in S_5$ is even.

(iv) $(1, 2, 3)(4, 5) = (1, 3)(1, 2)(4, 5) \in S_5$ is odd.

It is a fact (you might like to try and prove it) that no permutation can be both even and odd.

Definition 1.5.7. Given a set Ω , the *alternating group* on Ω is

$$\text{Alt}(\Omega) := \{\sigma \in \text{Sym}(\Omega) \mid \sigma \text{ is even}\}.$$

We also write $\text{Alt}(n)$ or A_n for the alternating group on n objects.

Exercise 1.5.8. Show that A_n is a group of order $n!/2$.

The symmetric group is, in some sense, “the mother of all groups”:

Theorem 1.5.9. (Cayley’s Theorem.) *Every group is isomorphic to a subgroup of $\text{Sym}(\Omega)$ for some set Ω .*

(The notions of subgroup and isomorphism will be introduced later.)

Exercise 1.5.10. Consider how D_8 permutes the vertices v_1, v_2, v_3 and v_4 of the square. The rotation R acts like this:

$$R : v_1 \mapsto v_2 \mapsto v_3 \mapsto v_4 \mapsto v_1,$$

so R “is” the permutation $(1, 2, 3, 4)$. The reflection r_k acts as

$$r_k : \begin{cases} v_1 \mapsto v_4 \mapsto v_1 \\ v_2 \mapsto v_3 \mapsto v_2 \end{cases}$$

so r_k “is” the permutation $(1, 4)(2, 3)$. Write down the permutations corresponding to the other elements of D_8 .

Exercise 1.5.11. Label the edges of the square and, as in the previous exercise, work out how D_8 permutes them. Do the same for the action of D_8 on the lines k, ℓ, m and n . Warning: you will not get the same permutations as before.

1.6 Some Properties of Groups

We shall now quickly establish some properties of groups that will prove useful later on:

Proposition 1.6.1. *Let G be a group. Then*

- (i) *there is only one identity element in G ;*
- (ii) *given $g \in G$, g has only one inverse.*

Proof. (i) Suppose that e and e' are two identity elements for G . Then

$$\begin{aligned} e &= ee' \text{ since } e' \text{ is an identity} \\ &= e' \text{ since } e \text{ is an identity.} \end{aligned}$$

So $e = e'$ and there is only one identity element.

(ii) Suppose that h and k are both inverses for $g \in G$. Then

$$gh = gk = e.$$

Now multiply on the left by one of the inverses, h , say:

$$hgh = h g k = h e,$$

so, since h is an inverse for g , and e is the neutral element,

$$h = k = h.$$

So any two inverses for g are equal. □

Exercises 1.6.2. (i) Prove the Cancellation Law: if g, h, k are elements of a group G , then

$$gh = gk \Rightarrow h = k.$$

(ii) For any group G , prove that for $g \in G$, $o(g) = 1 \Leftrightarrow g = 1_G$, and $o(g) = 2 \Rightarrow g = g^{-1}$. Why is it false that $g = g^{-1} \Rightarrow o(g) = 2$?

2 Subgroups, Cosets, and Lagrange's Theorem

2.1 Subgroups

Definitions 2.1.1. Let G be a group. A non-empty subset $H \subseteq G$ is called a *subgroup* of G if it is also a group under the same operation as G . When H is a subgroup of G , we shall write $H \leq G$.

Before giving any examples, we shall first prove a diagnostic test that makes hunting for subgroups a lot easier.

Proposition 2.1.2. *A non-empty subset H of a group G is a subgroup if and only if for all $g, h \in H$, $gh \in H$ and $g \in H$, i.e. H is closed under products and taking inverses.²*

Proof. If $H \leq G$ then the required properties clearly hold.

Conversely, suppose that $H \neq \emptyset$ is closed under products and taking inverses. The law of multiplication must be associative on H since it is associative on G . Because H is closed under products, the law really is a map $H \times H \rightarrow H$. Since $H \neq \emptyset$, there is an element $h \in H$. But since H is closed under taking inverses, $h^{-1} \in H$ as well, and so $1 = hh^{-1} \in H$. So $H \leq G$. □

Example 2.1.3. Any group G always has two very uninteresting subgroups: $\{1_G\}$ and G itself.

Examples 2.1.4. (i) $\mathbb{Z} \leq \mathbb{Q}$ since the sum of two integers is an integer, and the negative of an integer is also an integer.

(ii) $\mathbb{Q} \leq \mathbb{R}$ since the sum of two rational numbers is a rational number, and the negative of a rational is also rational.

(iii) $\mathbb{R} \leq \mathbb{C}$ since the sum of two real numbers is a real, and the negative of a real number is also real.

²This can be shortened to checking that $g, h \in H \Rightarrow gh^{-1} \in H$.

Examples 2.1.5. (i) $\mathbb{Q}^* \leq \mathbb{R}^*$ since the product of two rational numbers is a rational number, and the inverse of a non-zero rational number is also rational.

(ii) $\mathbb{R}^* \leq \mathbb{C}^*$ since the product of two real numbers is a real, and the inverse of a non-zero real number is also real.

Exercises 2.1.6. (i) Show that $\mathbb{Q}_{>0} := \{x \in \mathbb{Q} | x > 0\}$ is a subgroup of the multiplicative group \mathbb{Q}^* .

(ii) Show that $\mathbb{R}_{>0} := \{x \in \mathbb{R} | x > 0\}$ is a subgroup of the multiplicative group \mathbb{R}^* .

(iii) Why doesn't it make sense to talk about $\mathbb{C}_{>0}$?

Exercise 2.1.7. The unit circle. Let $S^1 := \{z \in \mathbb{C} | |z| = 1\} \subset \mathbb{C}^*$ denote the unit circle of complex numbers of unit length. Show that $S^1 \leq \mathbb{C}^*$. Hint: use the formula that for $z, w \in \mathbb{C}$, $|zw| = |z||w|$.

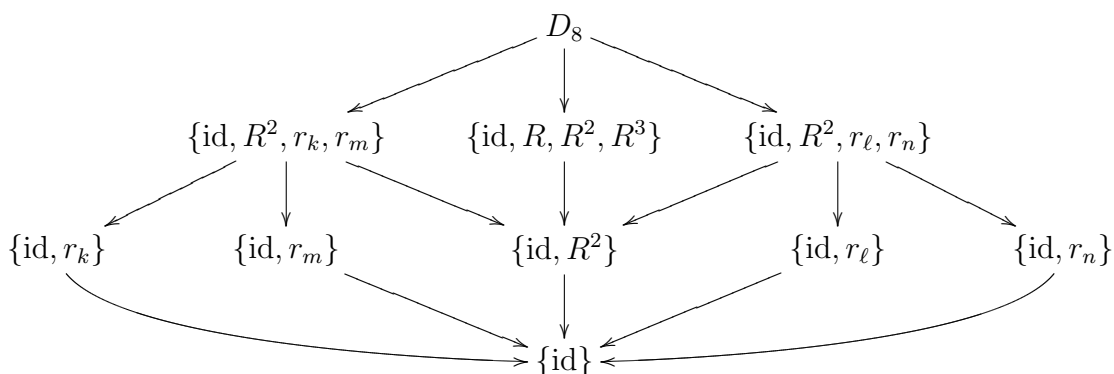
Example 2.1.8. We have already met the alternating group $A_n \leq S_n$.

Exercise 2.1.9. Show that $SL(n, K) \leq GL(n, K)$.

Example 2.1.10. The isometry group of the square,

$$D_8 = \{\text{id}, R, R^2, R^3, r_k, r_\ell, r_m, r_n\}$$

has quite a lot of subgroups. We'll draw them in a kind of "tree diagram", with an arrow pointing from a group to a subgroup (of course, a subgroup of a subgroup of G is also a subgroup of G):



As an exercise, show that these subsets are indeed subgroups. As a harder exercise, try showing that they are the only ones. Also, notice that the order of each subgroup divides 8, the order of D_8 .

Definition 2.1.11. For a group G define the *centre* of G by

$$Z(G) := \{g \in G | \forall h \in G, gh = hg\}.$$

That is, the centre of the group is the set of all elements that commute with everything.

Exercises 2.1.12. (i) Show that $Z(G) \leq G$ for any group G .

(ii) Show that G is Abelian if and only if $Z(G) = G$.

(iii) Find $Z(G)$ for some of the groups that have been introduced so far.

2.2 Generators

It is not always necessary to specify all the elements of a group or subgroup to know what it looks like. Instead, we can specify a few basic elements and build up the rest of the (sub)group from there.

Definition 2.2.1. Let G be a group and $S \subseteq G$ a subset. The *subgroup generated by S* is

$$\langle S \rangle := \{s_1^{\pm 1} s_2^{\pm 1} \dots s_r^{\pm 1} \mid s_i \in S\}.$$

That is, $\langle S \rangle$ consists of all the elements of G that we can make up as finite combinations of the elements of S and their inverses.

Definition 2.2.2. If $G = \langle S \rangle$ we say that S *generates* G and call the elements of S *generators*. If there is an element $g \in G$ such that $G = \langle g \rangle$ then we say that G is *cyclic*.

Examples 2.2.3. (i) In D_8 , $\langle R \rangle = \{\text{id}, R, R^2, R^3\}$.

(ii) $D_8 = \langle R, r_k \rangle$. In fact, D_8 is generated by R (or R^3) and any reflection.

(iii) \mathbb{Z}_n is cyclic. It is always generated by 1, and there may be other generators.

(iv) In \mathbb{Z} , $\langle n \rangle = n\mathbb{Z}$, the integer multiples of n .

(v) \mathbb{Z} is cyclic. It is generated by $+1$; it is also generated by -1 .

Exercises 2.2.4. (i) Show that every cyclic group is Abelian.

(ii) Show that every group of prime order is cyclic.

(iii) Give an example of an Abelian group that is not cyclic. (Hint: consider vector spaces.)

We can also specify a group by defining it to be the group generated by some elements that interact in certain ways. For example, we could define \mathbb{Z}_n to be the group generated by an element a such that a^n is the identity. We would write this as

$$C_n = \langle a \mid a^n = 1 \rangle.$$

This is called a *group presentation*: the $\langle a \mid$ part contains *generators*, and the $\mid a^n = 1 \rangle$ parts contains the *relations* that the generators must satisfy. It requires quite a bit of work to show that this method really does specify a group, and only one group. Fortunately, the idea can be used quite naively:

Examples 2.2.5. (i) $C_n = \langle a \mid a^n = 1 \rangle$.

(ii) $\mathbb{Z} = \langle a \mid \rangle$ — this is called the *free group* generated by a .

(iii) $D_8 = \langle a, b \mid a^4 = 1, b^2 = 1, bab = a^{-1} \rangle$. Here a is rotation by $\pi/2$, which we called R before, and b is any one of the reflections r_k, r_ℓ, r_m or r_n .

(iv) $D_{2n} = \langle a, b \mid a^n = 1, b^2 = 1, bab = a^{-1} \rangle$.

2.3 Cosets and Normal Subgroups

Definitions 2.3.1. Let G be a group and $S \subseteq G$. The *right coset* of S by g is

$$Sg := \{sg | s \in S\} \subseteq G.$$

Similarly, the *left coset* of $S \subseteq G$ by g is

$$gS := \{gs | s \in S\} \subseteq G.$$

The group element g is often called a *representative* of the coset gS (or Sg).

It can help to think of S as being a “blob” in the group, and that g moves this blob around: try drawing the cosets $x + [0, 1]$ in the additive group \mathbb{R} for a few values of $x \in \mathbb{R}$.

Now, since a coset can have many representatives, it would be nice to know when two apparently different cosets are in fact the same:

Lemma 2.3.2. *Suppose that $K \leq G$. Then*

$$gK = hK \Leftrightarrow g \in hK \Leftrightarrow g = hk \text{ for some } k \in K \Leftrightarrow h^{-1}g \in K,$$

and the same for right cosets.

Proposition 2.3.3. *For a subgroup N of a group G , the following are equivalent:*

(i) *for all $g \in G$, $gN = Ng$;*

(ii) *for all $g \in G$ and $n \in N$, $gng^{-1} \in N$.*

Definitions 2.3.4. If either (and hence both) of these conditions is true then we say that N is *normal* in G and write $N \trianglelefteq G$. When $N \trianglelefteq G$ we denote by $\frac{G}{N}$ the set of right (or, equivalently) left cosets of N in G :

$$\frac{G}{N} := \{gN | g \in G\} = \{Ng | g \in G\}.$$

Example 2.3.5. Any group G always has two normal subgroups: $\{1_G\}$ and G itself.

Proposition 2.3.6. *If G is an Abelian group then every subgroup of G is normal in G .*

Proof. Let $H \leq G$ and let $g \in G$, $h \in H$ be arbitrary. Then

$$ghg^{-1} = gg^{-1}h = h \in H,$$

so $H \trianglelefteq G$. □

This result gives us a large family of normal subgroups for the example groups that we have met so far:

Examples 2.3.7. (i) $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ for any $n \in \mathbb{Z}$.

(ii) $\mathbb{Z} \trianglelefteq \mathbb{Q} \trianglelefteq \mathbb{R} \trianglelefteq \mathbb{C}$.

- (iii) If V is a vector space and U a subspace of V , then $U \trianglelefteq V$.
- (iv) $\mathbb{Q}^* \trianglelefteq \mathbb{R}^* \trianglelefteq \mathbb{C}^*$.
- (v) $S^1 \trianglelefteq \mathbb{C}^*$.
- (vi) $\{\text{id}, R^2\} \trianglelefteq \{\text{id}, R, R^2, R^3\}$ in D_8 .

Exercises 2.3.8. Show that

- (i) $A_n \trianglelefteq S_n$. Hint: if $\sigma \in A_n$ can be written using $2k$ transpositions, and $\tau \in S_n$ using ℓ transpositions, how many transpositions are there in $\tau\sigma\tau^{-1}$?
- (ii) $Z(G) \trianglelefteq G$ for any group G ;
- (iii) $\text{SL}(n, K) \trianglelefteq \text{GL}(n, K)$;
- (iv) $\{\text{id}, R, R^2, R^3\} \trianglelefteq D_8$;
- (v) $\{\text{id}, R, r_k, r_m\}$ and $\{\text{id}, R, r_\ell, r_n\} \trianglelefteq D_8$;
- (vi) $\{\text{id}, r_k\}$ is not normal in D_8 , but $\{\text{id}, r_k\} \trianglelefteq \{\text{id}, R^2, r_k, r_\ell\}$;

Exercise 2.3.9. *Important exercise.* Find a counterexample (i.e. a group G with subgroups H and K) to disprove the following claim:

$$H \trianglelefteq K \trianglelefteq G \Rightarrow H \trianglelefteq G.$$

2.4 Lagrange's Theorem

The aim of this subsection is to prove that the order of a subgroup of a group must divide the order of the group. To do this we need a few preliminary results. Although we will work with left cosets, we could equally well work with right cosets and get the same results.

Lemma 2.4.1. *Let $H \leq G$.*

- (i) Define a relation \sim on G by $g \sim h \Leftrightarrow gh^{-1} \in H$. Then \sim is an equivalence relation on G .
- (ii) The left cosets of H in G partition G , i.e. they are disjoint and their union is G .
- (iii) The left cosets of H in G all have $|H|$ elements.

Proof. This is an exercise. (i) is routine. To show (ii), show that the cosets of H in G are the equivalence classes of H in G . To show (iii), consider the coset $1_G H$. \square

Theorem 2.4.2. (Lagrange's Theorem.) *Let G be a finite group and let H be a subgroup of G . Then the order of H divides the order of G .*

Proof. The left cosets of H in G partition G and all have $|H|$ elements. Since G is finite, there are only finitely many cosets in such a partition, say

$$g_1 H, \dots, g_r H.$$

Then $r|H| = |G|$, so $|H|$ divides $|G|$. \square

Definition 2.4.3. The number of left (or right) cosets of H in G is called the *index* of H in G and is denoted $|G : H|$.

Exercise 2.4.4. Show that if G is any group, $H \leq G$, and $|G : H| = 2$, then $H \trianglelefteq G$.

Corollary 2.4.5. Let G be a finite group and $g \in G$. Then $o(g) \mid |G|$.

Proof. g generates a cyclic subgroup $\langle g \rangle \leq G$ of order $o(g)$. □

It is not true that a group G has a subgroup of every order that divides $|G|$. What is true is the following result, which is outside the scope of this course, but is included for interest:

Theorem 2.4.6. Let G be a group and p a prime number. Then for every prime power p^r , $r \geq 0$, with $p^r \mid |G|$, G has a subgroup of order p^r .

3 Morphisms of Groups

3.1 Philosophy

When are two groups really the same? If we take a group G and re-name all its elements, but keep the same law of composition, we have not really changed the group. On the other hand, the groups \mathbb{Z}_6 and S_3 have the same size, and we could re-label the elements of \mathbb{Z}_6 as elements of S_3 , but that wouldn't be right — the two groups somehow “aren't the same”. How can we make this notion of “sameness” precise?

One of the major themes of mathematics is that of sets with structure. For instance, a group is a set with the structure of multiplication (composition). A field is a set with two structures: addition and multiplication. A vector space has even more structure: vector addition and scalar multiplication, and the structure of the underlying field of scalars.

Once we have sets with structure, it's natural to talk about maps of those sets that “preserve” the structures that we are interested in. You have met such maps before: in the case of vector spaces, they are the linear maps that you encountered in *Linear Algebra*. There is an area of mathematics, called *category theory*, that studies this idea in its most general setting. Very loosely, a “category” is a collection of “objects” (sets with “structure”) and “morphisms” (maps from objects to other objects that “preserve structure”).

Objects	Morphisms
Sets	Functions $f : X \rightarrow Y$ of sets
Groups	Homomorphisms $\phi : G \rightarrow H$ of groups
Vector spaces	Linear maps $T : V \rightarrow W$ of vector spaces
Rings	Homomorphisms $\phi : R \rightarrow S$ of rings
Modules over a ring R	R -homomorphisms $\phi : M \rightarrow N$ of R -modules

This entire subsection has been a philosophical remark that you need not understand fully — or at all. It is rather unfair to expect you to understand it before you know what a group homomorphism is, or have even heard of rings and modules. Nonetheless, I hope that it will light the way upon further reflection and later readings.

3.2 Morphisms of Groups

Definitions 3.2.1. Let G and H be groups. A *homomorphism* from G to H is a function $\phi : G \rightarrow H$ such that $\phi(gh) = \phi(g)\phi(h)$ for all $g, h \in G$. The set of all homomorphisms from G to H is denoted $\text{Hom}(G, H)$.

It is important to note that the group operation is different on the two sides of the above equality: if G has operation $*$ and H has operation \bowtie , say, then the homomorphism condition demands that for all $g, h \in G$,

$$\phi(g * h) = \phi(g) \bowtie \phi(h).$$

In other words, it does not matter if we first multiply g and h in G using $*$ and then apply ϕ , or apply ϕ to g and h separately and then multiply them together in H using \bowtie . We sometimes say that ϕ “preserves the group operation”.

Definitions 3.2.2. A homomorphism of groups $\phi : G \rightarrow H$ is called an *isomorphism* if it is also a bijection.³ If there is an isomorphism $\phi : G \rightarrow H$ we say that G and H are *isomorphic* and write $G \cong H$.

The notion of isomorphism is exactly the idea of “sameness” that was mentioned earlier.

Exercise 3.2.3. Show that \cong behaves like an equivalence relation on the class⁴ of all groups. That is,

- (i) for any group G , $G \cong G$;
- (ii) for any two groups G and H , $G \cong H \Rightarrow H \cong G$;
- (iii) for any three groups G, H, K , $G \cong H \cong K \Rightarrow G \cong K$.

Definitions 3.2.4. (i) A *monomorphism* is an injective homomorphism $G \rightarrow H$.

(ii) An *epimorphism* is a surjective homomorphism $G \rightarrow H$.

(iii) An *isomorphism* is a bijective homomorphism $G \rightarrow H$.

(iv) An *endomorphism* of G is a homomorphism $G \rightarrow G$; the set of endomorphisms of G is denoted $\text{End}(G)$.

(v) An *automorphism* of G is an isomorphism $G \rightarrow G$; the set of automorphisms of G is denoted $\text{Aut}(G)$.

Proposition 3.2.5. For any group G , $\text{Aut}(G)$ is also a group under the operation of composition of functions.

³Technical point: we should really demand that ϕ^{-1} be a homomorphism from H to G as well. It's possible, but boring, to prove that $\phi^{-1} \in \text{Hom}(H, G) \Leftrightarrow \phi \in \text{Hom}(G, H)$ is a bijection, so the two competing definitions are in fact the same.

⁴This is a *really* technical point: there's no such thing as the set of all groups, just a class.

Proof. Composition of functions is always associative. If $\phi, \psi \in \text{Aut}(G)$, then $\psi \circ \phi$ is a bijection and

$$(\psi \circ \phi)(gh) = \psi(\phi(gh)) = \psi(\phi(g)\phi(h)) = \psi(\phi(g))\psi(\phi(h)) = (\psi \circ \phi)(g)(\psi \circ \phi)(h)$$

for all $g, h \in G$. So $\psi \circ \phi \in \text{Aut}(G)$. The identity function $\text{id}_G : G \rightarrow G$ is the identity of $\text{Aut}(G)$, and the inverse to $\phi \in \text{Aut}(G)$ is $\phi^{-1} \in \text{Aut}(G)$. \square

Exercise 3.2.6. What part of this proof fails if we try to use it to prove that $\text{End}(G)$ is a group?

Example 3.2.7. Consider the complex numbers \mathbb{C} under addition, and the map $\phi : \mathbb{C} \rightarrow \mathbb{C}$ given by $\phi(z) := \bar{z}$, the complex conjugate of z :

$$\overline{x + iy} := x - iy.$$

Geometrically, conjugation is just reflection in the real axis. Conjugation is a homomorphism:

$$\begin{aligned} \overline{(x + iy) + (x' + iy')} &= \overline{(x + x') + i(y + y')} \\ &= (x + x') - i(y + y') \\ &= (x - iy) + (x' - iy') \\ &= \overline{(x + iy)} + \overline{(x' + iy')} \end{aligned}$$

Conjugation is also an isomorphism, because it is its own inverse. So $z \mapsto \bar{z}$ is an automorphism of the complex numbers \mathbb{C} .

Exercise 3.2.8. Show that conjugation is also an automorphism of the multiplicative group \mathbb{C}^* . This shows that conjugation is a *field automorphism* of the field \mathbb{C} — field automorphisms are very important in an area of mathematics called Galois theory.

Exercise 3.2.9. Show that $\det : \text{GL}(n, K) \rightarrow \mathbb{R}^*$ is an epimorphism.

Example 3.2.10. Consider the integers \mathbb{Z} and the subgroup of even numbers $2\mathbb{Z} \leq \mathbb{Z}$. Define a map $\phi : \mathbb{Z} \rightarrow 2\mathbb{Z}$ by $\phi(n) := 2n$. This ϕ is a homomorphism:

$$\phi(m + n) = 2(m + n) = 2m + 2n = \phi(m) + \phi(n).$$

ϕ is also an isomorphism: consider the map $\psi : 2\mathbb{Z} \rightarrow \mathbb{Z}$ defined by $\psi(n) := n/2$ — this is valid, because every element of $2\mathbb{Z}$ is indeed divisible by 2. Then $\phi \circ \psi = \text{id}_{2\mathbb{Z}} : 2\mathbb{Z} \rightarrow 2\mathbb{Z}$ and $\psi \circ \phi = \text{id}_{\mathbb{Z}} : \mathbb{Z} \rightarrow \mathbb{Z}$, so $\psi = \phi^{-1}$. Thus ϕ is an isomorphism and $\mathbb{Z} \cong 2\mathbb{Z}$. Similarly, $\mathbb{Z} \cong n\mathbb{Z}$ for any integer $n \neq 0$.

At first sight it may seem completely ridiculous that a group could be isomorphic to a proper subgroup of itself. This is the price that we pay for allowing groups to be infinite in size.

Example 3.2.11. The exponential map. Define the *exponential map* $\exp : \mathbb{R} \rightarrow \mathbb{R}_{>0}$ by $\exp(x) := e^x$. \exp is a homomorphism:

$$\exp(x + y) = e^{x+y} = e^x e^y = \exp(x) \exp(y)$$

\exp is also a bijection, because the natural logarithm $\log : \mathbb{R}_{>0} \rightarrow \mathbb{R}$ is its inverse. So \exp is an isomorphism and $\mathbb{R} \cong \mathbb{R}_{>0}$. Notice that we have changed operation: \mathbb{R} is an additive group, whereas $\mathbb{R}_{>0}$ is a multiplicative group.

Example 3.2.12. Consider the *sign map* $\text{sgn} : S_n \rightarrow \{\pm 1\}$ defined by

$$\text{sgn}(\sigma) := \begin{cases} +1 & \sigma \text{ is an even permutation,} \\ -1 & \sigma \text{ is an odd permutation.} \end{cases}$$

The set $\{\pm 1\}$ has a group structure with the operation of multiplication. (Quick exercise: show that $\{\pm 1\} \cong \mathbb{Z}_2 \cong C_2 \cong S_2$.) The map sgn is a group homomorphism since

- (i) the product of two even permutations is even;
- (ii) the product of two odd permutations is even;
- (iii) the product of an odd and an even permutation is odd.

sgn is a monomorphism if and only if $n \leq 2$, and an epimorphism if and only if $n \geq 2$, and so is an isomorphism only for $\text{sgn} : S_2 \rightarrow \{\pm 1\}$.

Exercise 3.2.13. Show that $\mathbb{Z}_n \cong C_n$.

Exercise 3.2.14. Let G be any group and H a subgroup of G . Let $i : H \rightarrow G$ be the inclusion, so $i(h) := h$ for all $h \in H$. Show that i is a monomorphism (an injective homomorphism).

Exercise 3.2.15. Pick your favourite $n > 0$, choose some elements of S_n , and calculate their sign.

Example 3.2.16. Let D_8 denote the isometry group of the square, as usual. Then the homomorphism $\phi : \mathbb{Z}_4 \rightarrow D_8$ defined by $\phi(n) := R^n$ can be restricted to $\phi : \mathbb{Z}_4 \rightarrow \{\text{id}, R, R^2, R^3\}$, and is then an isomorphism. To see this, simply observe that the inverse is $\psi : R^n \mapsto n$.

Exercise 3.2.17. Let D_6 denote the isometry group of an equilateral triangle in the plane. Show that $D_6 \cong S_3$.

3.3 Properties of Homomorphisms and Isomorphisms

Proposition 3.3.1. *Let $\phi : G \rightarrow H$ be a homomorphism of groups. Then*

- (i) $\phi(1_G) = 1_H$;
- (ii) for all $g \in G$, $\phi(g)^{-1} = \phi(g^{-1})$.

Proof. Do this as an exercise. You will need to use Proposition 1.6.1. □

Exercise 3.3.2. Let $\phi : G \rightarrow H$ be an isomorphism of groups. Then

- (i) $|G| = |H|$;
- (ii) for all $g \in G$, $o(\phi(g)) = o(g)$;
- (iii) If G and H are two groups, G is Abelian, and $G \cong H$, then H is also Abelian.

Definitions 3.3.3. Let $\phi : G \rightarrow H$ be a homomorphism of groups. Define the *kernel*

$$\ker \phi := \{g \in G \mid \phi(g) = 1_H \in H\}.$$

and the *image*

$$\phi(G) := \{\phi(g) \in H \mid g \in G\}.$$

Proposition 3.3.4. Let $\phi : G \rightarrow H$ be a homomorphism of groups. Then $\ker \phi \trianglelefteq G$ and $\phi(G) \leq H$.

Proof. $\ker \phi$ forms a subgroup of G : for if $g, h \in \ker \phi$,

$$\phi(gh^{-1}) = \phi(g)\phi(h^{-1}) = 1_H 1_H^{-1} = 1_H,$$

so $gh^{-1} \in \ker \phi$. $\ker \phi$ is normal: if $g \in G$ and $k \in \ker \phi$,

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)1_H\phi(g)^{-1} = 1_H,$$

so $gkg^{-1} \in \ker \phi$.

Let $h, h' \in \phi(G)$. Then there exist elements $g, g' \in G$ with $\phi(g) = h$, $\phi(g') = h'$. Since ϕ is a homomorphism,

$$\phi(gg') = \phi(g)\phi(g') = hh',$$

and $gg' \in G$. So $hh' \in \phi(G)$. Similarly, $\phi(g^{-1}) = \phi(g)^{-1} = h^{-1} \in \phi(G)$. □

Example 3.3.5. Consider the sign map $\text{sgn} : S_n \rightarrow \{\pm 1\}$. The kernel $\ker \text{sgn}$ is precisely the alternating group A_n , and we already know that $A_n \trianglelefteq S_n$.

Proposition 3.3.6. Let $\phi : G \rightarrow H$ be a homomorphism of groups. Then $\ker \phi = \{1_G\}$ if and only if ϕ is injective.

Proof. We always have $1_G \in \ker \phi$. If ϕ is injective then no element of G other than 1_G can go to 1_H , so $\ker \phi = \{1_G\}$.

On the other hand, suppose that $\ker \phi = \{1_G\}$. Suppose that $g, g' \in G$ are such that $\phi(g) = \phi(g')$; we want $g = g'$.

$$\begin{aligned} \phi(g) = \phi(g') &\Rightarrow \phi(g)^{-1}\phi(g') = 1_H \\ &\Rightarrow \phi(g^{-1}g') = 1_H \\ &\Rightarrow g^{-1}g' \in \ker \phi \\ &\Rightarrow g^{-1}g' = 1_G \\ &\Rightarrow g = g' \end{aligned}$$

as required. □

4 Products of Groups

There are basically two ways of making a new group from two given groups G and H , called the *direct product* and *semidirect product*. The first is easy, and will be covered here; the second is more complicated, and we'll miss it out.

4.1 The Direct Product

Definition 4.1.1. Let G and H be groups. We define the *direct product* of G and H to be

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

with multiplication law

$$(g, h)(g', h') := (gg', hh').$$

Exercises 4.1.2. (i) Prove that $G \times H$ is a group, and that if both G and H are finite, $|G \times H| = |G||H|$.

(ii) Prove that $G \times H$ is Abelian if and only if both G and H are Abelian.

Exercise 4.1.3. Show that $C_m \times C_n \cong C_{mn}$ if and only if $\text{hcf}(m, n) = 1$.

In particular, $C_2 \times C_2$ is not the same as C_4 . $C_2 \times C_2$ forms the *Klein four group*, sometimes denoted V_4 (“V” for *Viergruppe* = German “four-group”). Incidentally, we now have

Theorem 4.1.4. (Classification of Small Groups.) *Let G be any group with $|G| < 8$. Then G is isomorphic to one, and only one, of the following:*

$ G $	$G \cong$
1	$\{1\}$
2	C_2
3	C_3
4	C_4 or $V_4 \cong C_2 \times C_2$
5	C_5
6	C_6 or $D_6 \cong S_3$
7	C_7

Proof. Do this as an exercise. A good place to start is by proving the fact that a group of prime order p is isomorphic to C_p . If you’re feeling adventurous, try classifying the groups of order 8. Hint: there are five of them. □

5 The First Isomorphism Theorem

The First Isomorphism Theorem for groups is probably the single most confusing thing that mathematics undergraduates meet during their first year at Warwick. Having (for the most part) mastered convergence, continuity and other nasties, all the talk of cosets and quotient groups seems to be the straw that breaks the camel’s back. This is a great pity, since the First Isomorphism Theorem is actually a very natural statement, be it couched in the language of groups, rings, modules, vector spaces, algebras or whatever. So, let’s try to clear these somewhat muddy waters.

5.1 “The First Isomorphism Theorem for Sets”

We’ll begin with a silly but accessible example, leading into the natural statement of “the First Isomorphism Theorem for sets”. Those readers who quite liked the idea of objects and

morphisms might like to read this section with those ideas in mind.

Suppose that you have a (finite) set C of cows. Cows, of course, exist to be sent to market; let M be the set of markets to which you might send your cows. When you decide to sell off your herd, there's a natural function

$$\begin{aligned} \phi : C &\rightarrow M \\ \text{cow} &\mapsto \text{intended market for that cow.} \end{aligned}$$

Now, when it comes to actually packing the cows off to market, you could go through them one at a time: consider each cow $c \in C$, and send it to its destination $\phi(c) \in M$. However, this is clearly quite inefficient: why not first group the cows together according to destination, and then send them in batches? So, create a set of pens \mathcal{P} ; for each market $m_i \in M$, put in pen $P_i \in \mathcal{P}$ all the cows that go to market m_i . In symbols,

$$P_i := \{c \in C \mid \phi(c) = m_i\}.$$

Of course, the P_i are subsets of C ; \mathcal{P} is a collection of subsets of C . In fact, \mathcal{P} is a *partition* of C : the P_i are pairwise disjoint and their union is C .

There's a natural "penning function" π ,

$$\begin{aligned} \pi : C &\rightarrow \mathcal{P} \\ \text{cow} &\mapsto \text{pen corresponding to intended market for that cow.} \end{aligned}$$

Consider the markets that actually receive some cows, i.e. the image $\phi(C) \subseteq M$. Now, here's the obvious statement that is "the First Isomorphism Theorem for sets": *the set of "used" markets, $\phi(C)$, and the set of pens, \mathcal{P} , are in bijection.*

$$\begin{array}{ccc} C & \xrightarrow{\phi} & M \\ \pi \downarrow & & \uparrow i \\ \mathcal{P} & \xrightarrow{\bar{\phi}} & \phi(C) \end{array}$$

Here,

- $\pi : C \rightarrow \mathcal{P}$ is the "penning function", which is *surjective*;
- $i : \phi(C) \rightarrow M$ denotes the natural inclusion map, given by $i(m) := m$ for $m \in \phi(C)$, and which is *injective*;
- and $\bar{\phi} : \mathcal{P} \rightarrow \phi(C)$ is *bijective*.

What is this mysterious $\bar{\phi} : \mathcal{P} \rightarrow \phi(C)$? Simply this: $\bar{\phi}(P) := \phi(c)$ for any $c \in P$ — and this is a perfectly valid definition, since we already know that all the cows $c \in P$ go to the same market in $\phi(C) \subseteq M$.

Why is $\bar{\phi}$ a bijection? Well, it's injective because if P, P' are distinct pens, their member cows must go to different markets, otherwise they'd be in the same pen. In symbols: let $P, P' \in \mathcal{P}$ be distinct, $c \in P, c' \in P'$. Then

$$P \neq P' \Rightarrow \pi(c) \neq \pi(c') \Rightarrow \phi(c) \neq \phi(c') \Rightarrow \bar{\phi}(P) \neq \bar{\phi}(P').$$

As for surjectivity, this is obvious: by definition, every market in $\phi(C)$ receives at least one cow, and so is $\bar{\phi}(P)$ for at least one pen P .

There's another way of writing \mathcal{P} : as C modulo an equivalence relation. We have a natural equivalence relation on cows: two cows are equivalent if they go to the same market. In symbols, $c \sim c' \Leftrightarrow \phi(c) = \phi(c')$. The *equivalence class* of $c \in C$ is simply all the cows it's equivalent to:

$$[c] := \{c' \in C \mid c \sim c'\}.$$

We write $\frac{C}{\sim}$ for the set of equivalence classes of \sim in C . But $\frac{C}{\sim}$ is just the same as \mathcal{P} : the pens $P \in \mathcal{P}$ are the equivalence classes $[c] \in \frac{C}{\sim}$. As before, π is the function that assigns to each cow its pen / equivalence class: $\pi(c) := [c]$.

Let's tidy all this up in one statement, and then move on:

Theorem 5.1.1. (The First Isomorphism Theorem for Sets.) *Let X, Y be sets and $\phi : X \rightarrow Y$ any function. Let \sim on X be the relation $x \sim y \Leftrightarrow \phi(x) = \phi(y)$. Then there is a bijection $\bar{\phi} : \frac{X}{\sim} \rightarrow \phi(X) \subseteq Y$, i.e.*

$$\begin{array}{ccc} X & \xrightarrow{\phi} & Y \\ \pi \downarrow & & \uparrow i \\ \frac{X}{\sim} & \xrightarrow{\bar{\phi}} & \phi(X) \end{array}$$

with $\pi : X \rightarrow \frac{X}{\sim}$ the surjective projection map and $i : \phi(X) \rightarrow Y$ the injective inclusion map. Moreover, $\bar{\phi}([x]) = \phi(x)$.

5.2 The First Isomorphism Theorem for Groups

Suppose we have a homomorphism of groups $\phi : G \rightarrow H$. Theorem 5.1.1 tells us that there's a bijection $\bar{\phi}$ between $\frac{G}{\sim}$ and $\phi(G) \subseteq H$ as sets — but the First Isomorphism Theorem for groups tells us even more: *that these two objects are isomorphic as groups*. This is essentially because the homomorphism property forces the equivalence classes $[g]$ have a very special form: they are the cosets of $\ker \phi$ in G .

Remember that $\ker \phi$ is a normal subgroup of G whose elements are precisely the $g \in G$ that go to the identity in H : in the old language, $\ker \phi = [1_G]$. Also, $\ker \phi$ is just the coset $1_G \ker \phi$.

Now suppose that K is the kernel, $K := \ker \phi$. Then

$$g \in hK \Leftrightarrow h^{-1}g \in K \Leftrightarrow \phi(h^{-1}g) = 1_H \Leftrightarrow \phi(g) = \phi(h).$$

In other words: *the cosets of $\ker \phi$ in G are precisely the equivalence classes of \sim in G , where $g \sim h \Leftrightarrow \phi(g) = \phi(h)$, i.e.*

$$\frac{G}{\sim} = \frac{G}{\ker \phi}$$

As before, there's a natural function

$$\begin{aligned} \pi : G &\rightarrow G/K \\ g &\mapsto gK \end{aligned}$$

called the *quotient map*.

Now, we know how to multiply elements of G because G is a group. Can we multiply cosets, elements of $\frac{G}{K}$? If not, then there's no sense in which we can have a group homomorphism with $\frac{G}{K}$ as its domain or target. Fortunately, the answer is yes, like this:

$$(gK)(hK) := (gh)K = g(hK)$$

The fact that $K \trianglelefteq G$ is exactly what we need to make sure that this definition works:

Lemma 5.2.1. *The above operation on $\frac{G}{K}$ is well-defined in the sense that*

$$gK = g'K \text{ and } hK = h'K \Rightarrow (gK)(hK) = (g'K)(h'K).$$

precisely when $K \trianglelefteq G$.

Definition 5.2.2. $\frac{G}{K}$ with this law of multiplication is called the *quotient group* of G by K .

Exercise 5.2.3. Check that the quotient map is an epimorphism (a surjective homomorphism).

We now state and prove the First Isomorphism Theorem for groups:

Theorem 5.2.4. (The First Isomorphism Theorem for Groups.) *Let G, H be groups and $\phi : G \rightarrow H$ a homomorphism of groups with kernel $K := \ker \phi$. Then there is an isomorphism $\bar{\phi} : \frac{G}{K} \rightarrow \phi(G) \subseteq H$, i.e.*

$$\begin{array}{ccc} G & \xrightarrow{\phi} & H \\ \pi \downarrow & & \uparrow i \\ \frac{G}{K} & \xrightarrow{\bar{\phi}} & \phi(G) \end{array}$$

with $\pi : G \rightarrow \frac{G}{K}$ the surjective quotient homomorphism and $i : \phi(G) \rightarrow H$ the injective inclusion homomorphism. Moreover, $\bar{\phi}(gK) = \phi(g)$.

Proof. We already know that $\ker \phi \trianglelefteq G$, and so the group operation on $\frac{G}{K}$ is well-defined. Also $\phi(G)$ is a subgroup of H . It's also easy to see that $\bar{\phi}$ is both injective and surjective, and a homomorphism.

We're not done, though. Logically, this bit comes first: we have to check that $\bar{\phi}$ is actually well-defined! Remember that the same coset can have different representatives, so we need to be sure that if we give $\bar{\phi}$ the same coset by two different names it will still give us the same answer. This is quick to check, though, and is rather like checking injectivity (the \Rightarrow direction is the well-defined-ness check; the \Leftarrow direction is the injectivity check):

$$\begin{aligned} gK = hK &\Leftrightarrow h^{-1}g \in K \\ &\Leftrightarrow \phi(h^{-1}g) = 1_H \\ &\Leftrightarrow \phi(h)^{-1}\phi(g) = 1_H \\ &\Leftrightarrow \phi(g) = \phi(h) \\ &\Leftrightarrow \bar{\phi}(gK) = \bar{\phi}(hK). \end{aligned}$$

□

We'll end with a couple of examples.

Example 5.2.5. Time. Consider time in hours as integers in \mathbb{Z} . Hour 0 can be whatever you like — if you're a fan of UNIX, you'll probably want to choose midnight, January 1, 1970. \mathbb{Z} , as you know, is an Abelian group under usual addition $+$. However, we don't usually give time this way: we give it in the range 1 o'clock to 12 o'clock. We implicitly make all 12 o'clocks the same: midnight tonight is a 12 o'clock just like mid-day tomorrow will be a 12 o'clock. $12\mathbb{Z}$, the collection of all the 12 o'clocks, is a normal subgroup of \mathbb{Z} . Its cosets are

$$12\mathbb{Z} = 0 + 12\mathbb{Z}, 1 + 12\mathbb{Z}, 2 + 12\mathbb{Z}, \dots, 10 + 12\mathbb{Z}, 11 + 12\mathbb{Z}.$$

Two cosets $n + 12\mathbb{Z}$ and $m + 12\mathbb{Z}$ are equal exactly when $n - m$ is a multiple of 12, i.e. $(n - m) \in 12\mathbb{Z}$. We can add these cosets in the natural way:

$$(n + 12\mathbb{Z}) + (m + 12\mathbb{Z}) := (n + m) + 12\mathbb{Z}.$$

When we think of time as going from 0 to 11, we add hours modulo 12: 3 hours after 11 o'clock is 2 o'clock, not 14 o'clock. This is suspiciously like adding the cosets of $12\mathbb{Z}$. In fact, if we write \mathbb{Z}_{12} for the integers $\{0, 1, \dots, 11\}$ with this addition modulo 12, the First Isomorphism Theorem tells us that

$$\frac{\mathbb{Z}}{12\mathbb{Z}} \cong \mathbb{Z}_{12}.$$

How can we realise this isomorphism? Well, let $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_{12}$ be the function (check that it's a homomorphism) that assigns to every integer its remainder on division by 12. Then $\phi(\mathbb{Z}) = \mathbb{Z}_{12}$, $\ker \phi = 12\mathbb{Z}$, and

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\phi} & \mathbb{Z}_{12} \\ \pi \downarrow & & \uparrow \text{id} \\ \frac{\mathbb{Z}}{12\mathbb{Z}} & \xrightarrow{\bar{\phi}} & \mathbb{Z}_{12} \end{array}$$

with $\bar{\phi}(n + 12\mathbb{Z}) = \phi(n)$.

(By the way, if you feel cheated by this example, as if it has said absolutely nothing — then GOOD!)

Example 5.2.6. A string of pearls. Consider the cyclic Abelian group \mathbb{Z}_8 : draw it as an octagon, or as the eight 8th roots of unity in \mathbb{C} . Similarly, consider \mathbb{Z}_4 , which you might like to think of as (isomorphic to) $\{1, i, -1, -i\} \subset \mathbb{C}$. Now let $\phi : \mathbb{Z}_8 \rightarrow \mathbb{Z}_4$ be the group homomorphism defined by

$$\begin{aligned} \phi(0) = \phi(4) &:= 0 & \phi(1) = \phi(5) &:= 1 \\ \phi(2) = \phi(6) &:= 2 & \phi(3) = \phi(7) &:= 3 \end{aligned}$$

The reason that I titled this example “a string of pearls” is that you can visualize this homomorphism ϕ as tightening the loop \mathbb{Z}_8 so that two “pearls” (elements of \mathbb{Z}_8) lie above one another, turning the necklace (\mathbb{Z}_8) into a two-layered choker, which looks like \mathbb{Z}_4 when viewed from above. The kernel of ϕ is $K := \{0, 4\}$, and so $\frac{G}{K} = \{K, 1 + K, 2 + K, 3 + K\}$. By now, the isomorphism $\frac{\mathbb{Z}_8}{K} \cong \mathbb{Z}_4$ should be obvious.

Exercises 5.2.7. Using the First Isomorphism Theorem, prove the following:

(i) Let K be a field and $n \in \mathbb{N}$. Then

$$\frac{\mathrm{GL}(n, K)}{\mathrm{SL}(n, K)} \cong K^* := K \setminus \{0\}.$$

(Hint: determinant.)

(ii) $\mathbb{C}^*/S^1 \cong \mathbb{R}_{>0}$; $\mathbb{C}^*/\mathbb{R}_{>0} \cong S^1$. (Hint: absolute value, argument.) Hence show that $\mathbb{C}^* \cong \mathbb{R}_{>0} \times S^1$.

(iii) $S_n/A_n \cong C_2$.

(iv) Using Theorem 4.1.4, identify every subgroup $H \leq D_8$ and identify D_8/N for each $N \trianglelefteq D_8$. (“Identify” means find one of the standard groups C_n , V_4 etc. that each H (or G/N) is isomorphic to.)