Introduction to Modern Algebra I

Math 817 Fall 2024

September 18, 2024

Warning!

Proceed with caution. These notes are under construction and are 100% guaranteed to contain typos. If you find any typos or errors, I will be most grateful to you for letting me know.

Acknowledgements

These notes are based on notes by Mark Walker and Alexandra Seceleanu. Thanks to Gabriel Adams who found a typo in a previous version of the notes.

Contents

I Groups **1**

1 Groups: an introduction **2**
1.1 Definitions and first examples 2
1.2 Permutation groups 6
1.3 Dihedral groups 12
1.4 The quaternions 17
1.5 Group homomorphisms 18

2 Group actions: a first look **23**
2.1 What is a group action? 23
2.2 Examples of group actions 26

3 Subgroups **27**
3.1 Definition and examples 27
3.2 Subgroups vs isomorphism invariants 31
3.3 Cyclic groups 33

4 Quotient groups **38**
4.1 Equivalence relations on a group and cosets 38

Index **41**

Part I

Groups

Chapter 1

Groups: an introduction

Many mathematical structures consist of a set with special properties. Groups are elementary algebraic structures that allow us to deal with many objects of interest, such as geometric shapes and polynomials.

1.1 Definitions and first examples

Definition 1.1. A **binary operation** on a set S is a function $S \times S \to S$. If the binary operation is denoted by $\cdot$, we write $x \cdot y$ for the image of (x, y) under the binary operation $\cdot$.

Remark 1.2. We often write xy instead of $x \cdot y$ if the operation is clear from context.

Remark 1.3. We say that that a set S is closed under the operation $\cdot$ when we want to emphasize that for any $x, y \in S$ the result xy of the operation is an element of S. But note that closure is really part of the definition of a binary operation on a set, and it is implicitly assumed whenever we consider such an operation.

Definition 1.4. A **group** is a set G equipped with a binary operation $\cdot$ on G called the **group multiplication**, satisfying the following properties:

- Associativity: For every $x, y, z \in G$, we have $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
- Identity element: There exists $e \in G$ such that $e \cdot x = x \cdot e = x$ for all $x \in G$.
- Inverses: For each $x \in G$, there is an element $y \in G$ such that $xy = e = yx$.

The element e is called the **identity element** or simply **identity** of the group. For each element $x \in G$, an element $y \in G$ such that $xy = e = yx$ is called an **inverse** of x. We may write that $(G, \cdot)$ is a group to mean that G is a group with the operation $\cdot$.

The **order** of the group G is the number of elements in the underlying set.

Remark 1.5. Although a group is the set *and* the operation, we will usually refer to the group by only naming the underlying set, G.

Remark 1.6. A set G equipped with a binary operation satisfying only the first two properties is known as a **monoid**. While *we will not be discussing monoids that are not groups in this class*, they can be useful and interesting objects. We will however include some fun facts about monoids in the remarks. In particular, there will be no monoids whatsoever in the qualifying exam.

Lemma 1.7. *For any group G, we have the following properties:*

(1) The identity is unique: there exists a unique $e \in G$ with $ex = x = xe$ for all $x \in G$.

(2) Inverses are unique: for each $x \in G$, there exists a unique $y \in G$ such that $xy = e = yx$.

Proof. Suppose e and e' are two identity elements; that is, assume e and e' satisfy $ex = x = xe$ and $e'x = x = xe'$ for all $x \in G$. Then

$$e = ee' = e'.$$

Now given $x \in G$, suppose y and z are two inverses for x, meaning that $yx = xy = e$ and $zx = xz = e$. Then

$$\begin{aligned} z &= ez && \text{since } e \text{ is the identity} \\ &= (yx)z && \text{since } y \text{ is an inverse for } x \\ &= y(xz) && \text{by associativity} \\ &= ye && \text{since } z \text{ is an inverse for } x \\ &= y && \text{since } e \text{ is the identity.} \end{aligned}$$

□

Remark 1.8. Note that our proof of Lemma 1.7 also applies to show that the identity element of a monoid is unique.

Given a group G, we can refer to *the* identity of G. Similarly, given an element $x \in G$, we can refer to *the* inverse of x.

Notation 1.9. Given an element x in a group G, we write x^{-1} to denote its unique inverse.

Remark 1.10. In a monoid G with identity e, an element x might have a **left inverse**, which is an element y satisfying $yx = e$. Similarly, x might have a **right inverse**, which is an element z satisfying $xz = e$. An element in a monoid might have several distinct right inverses, or several distinct left inverses, but if it has both a left and a right inverse, then it has a unique left inverse and a unique right inverse, and those elements coincide.

Exercise 1. Give an example of a monoid M and an element in M that has a left inverse but not a right inverse.

Definition 1.11. Let G be a group, $x \in G$, and $n \geqslant 1$ be an integer. We write x^n to denote the element obtained by multiplying x with itself n times:

$$x^n := \underbrace{x \cdots x}_{n \text{ times}}.$$

Exercise 2 (Properties of group elements)**.** Let G be a group and let $x, y, z, a_1, \ldots, a_n \in G$. Show that the following properties hold:

(1) If $xy = xz$, then $y = z$.

(2) If $yx = zx$, then $y = z$.

(3) $(x^{-1})^{-1} = x$.

(4) $(a_1 \ldots a_n)^{-1} = a_n^{-1} \ldots a_1^{-1}$.

(5) $(x^{-1}yx)^n = x^{-1}y^n x$ for any integer $n \geqslant 1$.

(6) $(x^{-1})^n = (x^n)^{-1}$.

Notation 1.12. Given a group G, an element $x \in G$, and a positive integer n, we write $x^{-n} := (x^n)^{-1}$.

Note that by Exercise 2, $x^{-n} = (x^{-1})^n$.

Exercise 3. Let G be a group and consider $x \in G$. Show that $x^a x^b = x^{a+b}$.

Definition 1.13. A group G is **abelian** if $\cdot$ is commutative, meaning that $x \cdot y = y \cdot x$ for all $x, y \in G$.

Often, but not always, the group operation for an abelian group is written as $+$ instead of $\cdot$. In this case, the identity element is usually written as 0 and the inverse of an element x is written as $-x$.

Example 1.14.

(1) The **trivial group** is the group with a single element $\{e\}$. This is an abelian group.

(2) The pairs $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are abelian groups.

(3) For any n, let $\mathbb{Z}/n$ denote the integers modulo n. Then $(\mathbb{Z}/n, +)$ is an abelian group where $+$ denotes addition modulo n.

(4) For any field F, such as $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{Z}/p$ for a prime p, the set $F^\times := F \setminus \{0\}$ is an abelian group under multiplication. We will later formally define what a field is, but these fields might already be familiar to you.

Example 1.15. Let F be any field. If you are not yet familiar with fields, the real or complex numbers are excellent examples. Consider a positive integer n, and let

$$\mathrm{GL}_n(F) := \{\text{invertible } n \times n \text{ matrices with entries in } F\}.$$

An invertible matrix is one that has a two-sided (multiplicative) inverse. It turns out that if an $n \times n$ matrix M has a left inverse N then that inverse N is automatically a right inverse too, and vice-versa; this is a consequence of a more general fact we mentioned in Remark 1.10.

It it not hard to see that $\mathrm{GL}_n(F)$ is a nonabelian group under matrix multiplication. Note that $(\mathrm{GL}_1(F), \cdot)$ is simply $(F^\times, \cdot)$.

Even if the group is not abelian, the set of elements that commute with every other element is particularly important.

Definition 1.16. Let G be a group. The **center** of G is the set

$$\mathrm{Z}(G) := \{x \in G \mid xy = yx \text{ for all } y \in G\}.$$

Remark 1.17. Note that the center of any group always includes the identity. Whenever $\mathrm{Z}(G) = \{e_G\}$, we say that the center of G is trivial.

Remark 1.18. Note that G is abelian if and only if $\mathrm{Z}(G) = G$.

One might describe a group by giving a presentation.

Informal definition 1.19. A **presentation** for a group is a way to specify a group in the following format:

$$G = \langle \text{ set of generators } \mid \text{ set of relations } \rangle.$$

A set S is said to **generate** or be a **set of generators** for G if every element of the group can be expressed in some way as a product of finitely many of the elements of S and their inverses (with repetitions allowed). A **relation** is an identity satisfied by some expressions involving the generators and their inverses. We usually record just enough relations so that every valid equation involving the generators is a consequence of those listed here and the axioms of a group.

Remark 1.20. We can only take products of finitely many of our generators and their inverses because we do not have a way to make sense of infinite products.

Note, however, that the set of generators and the set of relations are allowed to be infinite.

Example 1.21. The group $\mathbb{Z}$ has one generator, the element 1, which satisfies no relations.

Example 1.22. The following is a presentation for the group $\mathbb{Z}/n$ of integers modulo n:

$$\mathbb{Z}/n = \langle x \mid x^n = e \rangle.$$

Definition 1.23. A group G is called **cyclic** if it is generated by a single element.

Example 1.24. We saw above that $\mathbb{Z}$ and $\mathbb{Z}/n$ are cyclic groups.

Exercise 4. Prove that every cyclic group is abelian.

Exercise 5. Prove that $(\mathbb{Q}, +)$ and $\mathrm{GL}_2(\mathbb{Z}_2)$ are not cyclic groups.

In general, given a presentation, it is very difficult to prove certain expressions are not actually equal to each other. In fact,

> There is no algorithm that, given any group presentation as an input, can decide whether the group is actually the trivial group with just one element.

and perhaps more strikingly

> There exist a presentation with finitely many generators and finitely many relations such that whether or not the group is actually the trivial group with just one element is *independent of the standard axioms of mathematics*!

We will now dedicate the next few sections to some classes of examples are very important.

1.2 Permutation groups

Definition 1.25. For any set X, the **permutation group** on X is the set $\mathrm{Perm}(X)$ of all bijective functions from X to itself equipped with the binary operation given by composition of functions.

Notation 1.26. For an integer $n \geqslant 1$, we write $[n] := \{1, \ldots, n\}$ and $S_n := \mathrm{Perm}([n])$. An element of S_n is called a **permutation on n symbols**, sometimes also called a permutation on n letters or n elements.

We can write an element σ of S_n as a table of values:

i	1	2	3	$\cdots$	n
$\sigma(i)$	$\sigma(1)$	$\sigma(2)$	$\sigma(3)$	$\cdots$	$\sigma(n)$

We may also represent this using arrows, as follows:

$$\begin{aligned} 1 &\longmapsto \sigma(1) \\ 2 &\longmapsto \sigma(2) \\ &\vdots \\ n &\longmapsto \sigma(n). \end{aligned}$$

Remark 1.27. To count the elements $\sigma \in S_n$, note that

- there are n choices for $\sigma(1)$;
- once $\sigma(1)$ has been chosen, we have $n-1$ choices for $\sigma(2)$;

$$\vdots$$

- once $\sigma(1), \ldots, \sigma(n-1)$ have been chosen, there is a unique possible value for $\sigma(n)$, which is the only value left.

Thus the group S_n has $n!$ elements.

It is customary to use cycle notation for permutations.

Definition 1.28. If $i_1, \ldots, i_m$ are distinct integers between 1 and n, then $\sigma = (i_1\, i_2\, \ldots\, i_m)$ denotes the element of S_n determined by

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \quad \ldots, \quad \sigma(i_{m-1}) = i_m, \quad \text{and} \quad \sigma(i_m) = i_1,$$

and which fixes all elements of $[n] \setminus \{i_1, \ldots, i_m\}$, meaning that

$$\sigma(j) = j \quad \text{for all} \quad j \in [n] \text{ with } j \notin \{i_1, \ldots, i_m\}.$$

Such a permutation is called a **cycle** or an **m-cycle** when we want to emphasize its length. In particular, we say that σ has length m.

Remark 1.29. A 1-cycle is the identity permutation.

Notation 1.30. A 2-cycle is often called a **transposition**.

Remark 1.31. The cycles $(i_1 \dots i_m)$ and $(j_1 \dots j_m)$ represent the same cycle if and only if the two lists $i_1, \dots, i_m$ and $j_1, \dots, j_m$ are cyclical rearrangements of each other. For example, $(1\,2\,3) = (2\,3\,1)$ but $(1\,2\,3) \neq (2\,1\,3)$.

Remark 1.32. Consider the m-cycle $\sigma = (i_1 \dots i_m)$. Then for any integer k, we have

$$\sigma^k(i_j) = i_{j+k \pmod m}.$$

Here we interpret $j + k \pmod m$ to denote the unique integer $0 \leqslant s < m$ such that

$$s \equiv j + k \pmod m.$$

Notation 1.33. We denote the product (composition) of the cycles $(i_1 \dots i_s)$ and $(j_1 \dots j_t)$ by juxtaposition; more precisely, $(i_1 \dots i_s)(j_1 \dots j_t)$ denotes the composition of the two cycles, read from right to left.

Example 1.34. We claim that the permutation group $\mathrm{Perm}(X)$ is nonabelian whenever the set X has 3 or more elements. Indeed, given three distinct elements $x, y, z \in S$, consider the transpositions (xy) and (yz). Now consider the permutations $(yz)(xy)$ and $(yz)(xy)$, where the composition is read from right to left, such as function composition. Then

$$(yz)(xy): \quad \begin{array}{l} x \overset{(xy)}{\longmapsto} y \overset{(yz)}{\longmapsto} z \\ y \overset{(xy)}{\longmapsto} x \overset{(yz)}{\longmapsto} x \\ z \overset{(xy)}{\longmapsto} z \overset{(yz)}{\longmapsto} y \end{array} \qquad (xy)(yz): \quad \begin{array}{l} x \overset{(yz)}{\longmapsto} x \overset{(xy)}{\longmapsto} y \\ y \overset{(yz)}{\longmapsto} z \overset{(xy)}{\longmapsto} z \\ z \overset{(yz)}{\longmapsto} y \overset{(xy)}{\longmapsto} x \end{array}$$

Note that $(yz)(xy) \neq (xy)(yz)$, since for example the first one takes x to z while the second one takes x to y.

Lemma 1.35. *Disjoint cycles commute; that is, if*

$$\{i_1, i_2, \dots, i_m\} \cap \{j_1, j_2, \dots, j_k\} = \emptyset$$

then the cycles

$$\sigma_1 = (i_1\, i_2 \cdots i_m) \quad \textit{and} \quad \sigma_2 = (j_1\, j_2 \cdots j_k)$$

satisfy $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.

Proof. We need to show $\sigma_1(\sigma_2(l)) = \sigma_2(\sigma_1(l))$ for all $l \in [n]$. If $l \notin \{i_1, \dots, i_m, j_1, \dots, j_k\}$, Then $\sigma_1(l) = l = \sigma_2(l)$, so

$$\sigma_1(\sigma_2(l)) = \sigma_1(l) = l \qquad \text{and} \qquad \sigma_2(\sigma_1(l)) = \sigma_2(l) = l.$$

If $l \in \{j_1, \dots, j_k\}$, then $\sigma_2(l) \in \{j_1, \dots, j_k\}$ and hence, since the subsets are disjoint, l and $\sigma_2(l)$ are not in the set $\{i_1, i_2, \dots i_m\}$. It follows that σ_1 preserves l and $\sigma_2(l)$, and thus

$$\sigma_1(\sigma_2(l)) = \sigma_2(l) \quad \text{and} \quad \sigma_2(\sigma_1(l)) = \sigma_2(l).$$

The case when $l \in \{i_1, \dots, i_m\}$ is analogous. □

Theorem 1.36. *Each $\sigma \in S_n$ can be written as a product of disjoint cycles, and such a factorization is unique up to the order of the factors.*

Remark 1.37. For the uniqueness part of Theorem 1.36, one needs to establish a convention regarding 1-cycles: we need to decide whether the 1-cycles will be recorded. If we decide not to record 1-cycles, this gives the shorter version of our factorization into cycles. If all the 1-cycles are recorded, this gives a longer version of our factorization, but this option has the advantage that it makes it clear what the size n of our group S_n is. We will follow the first convention: we will write only m-cycles with $m \geqslant 2$. Under this convention, the identity element of S_n is the empty product of disjoint cycles. We will, however, sometimes denote the identity by (1) for convenience.

Proof. Fix a permutation σ. The key idea is to look at the *orbits* of σ: for each $x \in [n]$, its orbit by σ is the subset of $[n]$ of the form

$$O_x = \{\sigma(x), \sigma^2(x), \sigma^3(x), \ldots\} = \{\sigma^i(x) \mid i \geqslant 1\}.$$

Notice that the orbits of two elements x and y are either the same orbit, which happens precisely when $y \in O_x$, or disjoint. Since $[n]$ is a finite set, and σ is a bijection of σ, we will eventually have $\sigma^i(x) = \sigma^j(x)$ for some $j > i$, but then

$$\sigma^{j-i}(x) = \sigma^{i-i}(x) = \sigma^0(x) = x.$$

Thus we can find the smallest positive integer n_x such that $\sigma^{n_x}(x) = x$. Now for each $x \in [n]$, we consider the cycle

$$\tau_x = (\sigma(x)\ \sigma^2(x)\ \sigma^3(x)\ \cdots\ \sigma^{n_x}(x)).$$

Now let S be a set of indices for the distinct τ_x, where note that we are not including the τ_x that are 1-cycles. We claim that we can factor σ as

$$\sigma = \prod_{i \in S} \tau_i.$$

To show this, consider any $x \in [n]$. It must be of the form $\sigma^j(i)$ for some $i \in S$, given that our choice of S was exhaustive. On the right hand side, only τ_i moves x, and indeed by definition of τ_i we have

$$\tau_i(x) = \sigma^{j+1}(i) = \sigma(\sigma^j(i)) = \sigma(x).$$

This proves that

$$\sigma = \prod_{i \in S} \tau_i.$$

As for uniqueness, note that if $\sigma = \tau_1 \cdots \tau_s$ is a product of disjoint cycles, then each $x \in [n]$ is moved by at most one of the cycles τ_i, since the cycles are all disjoint. Fix i such that τ_i moves x. We claim that

$$\tau_x = (\sigma(x)\ \sigma^2(x)\ \sigma^3(x)\ \cdots\ \sigma^{n_x}(x)).$$

This will show that our product of disjoint cycles giving σ is the same (unique) product we constructed above. To do this, note that we do know that there is some integer s such that $\tau_x^s(x) = e$, and

$$\tau_x = (\tau_x(x)\ \tau_x^2(x)\ \tau_x^3(x)\ \cdots\ \tau_x^s(x)).$$

Thus we need only to prove that

$$\tau_x^k(x) = \sigma^k(x)$$

for all integers $k \geqslant 1$. Now by Lemma 1.35, disjoint cycles commute, and thus for each integer $k \geqslant 1$ we have

$$\sigma^k = \tau_1^k \cdots \tau_s^k.$$

But τ_j fixes x whenever $j \neq i$, so

$$\sigma^k = \tau_i^k(x).$$

We conclude that the integer n_x we defined before is the length of the cycle τ_i, and that

$$\tau_i = (x\, \tau_i(x)\, \tau_i^2(x) \cdots \tau_i^{n_x-1}(x)) = (x\, \sigma(x)\, \sigma^2(x) \cdots \sigma^{n_x-1}(x)).$$

Thus this decomposition of σ as a product of disjoint cycles is the same decomposition we described above. □

Example 1.38. Consider the permutation $\sigma \in S_5$ given by

$$\begin{aligned} 1 &\longmapsto 3 \\ 2 &\longmapsto 4 \\ 3 &\longmapsto 5 \\ 4 &\longmapsto 2 \\ 5 &\longmapsto 1. \end{aligned}$$

Its decomposition into a product of disjoint cycles is

$$(135)(24).$$

Definition 1.39. The **cycle type** of an element $\sigma \in S_n$ is the unordered list of lengths of cycles that occur in the unique decomposition of σ into a product of disjoint cycles.

Example 1.40. The element

$$(3\,4)(1\,5)(2\,6\,7)(9\,8\,11)(15\,16\,17\,105\,114)$$

of S_{156} has cycle type $2, 2, 3, 3, 5$. Note here that the n of S_n is not recorded, but is implicit.

It is also useful to write permutations as products of (not necessarily disjoint) transpositions. First, we need the following exercise:

Exercise 6. Show that

$$(i_1\, i_2\, \cdots\, i_p) = (i_1\, i_p)(i_1\, i_{p-2})(i_1\, i_3)(i_1\, i_2)$$

for any $p \geqslant 2$.

Corollary 1.41. *Every permutation is a product of transpositions, thus the group S_n is generated by transpositions.*

Proof. Given any permutation, we can decompose it as a product of cycles by Theorem 1.36. Thus it suffices to show that each cycle can be written as a product of permutations. For a cycle $(i_1\, i_2\, \cdots\, i_p)$, one can show that

$$(i_1\, i_2\, \cdots\, i_p) = (i_1\, i_2)(i_2\, i_3)\cdots(i_{p-2}\, i_{p-1})(i_{p-1}\, i_p),$$

which we leave as an exercise (see Exercise 6). □

Remark 1.42. Note however that when we write a permutation as a product of transpositions, such a product is no longer necessarily unique.

Example 1.43. If $n \geqslant 2$, the identity in S_n can be written as $(12)(12)$. In fact, any transposition is its own inverse, so we can write the identity as $(ij)(ij)$ for any $i \neq j$.

Exercise 7. Show that

$$(cd)(ab) = (ab)(cd) \qquad \text{and} \qquad (bc)(ab) = (ac)(bc)$$

for all distinct a, b, c, d in $[n]$.

Theorem 1.44. *Given a permutation $\sigma \in S_n$, the parity of the number of transpositions in any representation of σ as a product of transpositions depends only on σ.*

Proof. Suppose that σ is a permutation that can be written as a production of transpositions β_i and λ_j in two ways,

$$\sigma = \beta_1 \cdots \beta_s = \lambda_1 \cdots \lambda_t$$

where s is even and t is odd. As we noted in Example 1.43, every transposition is its own inverse, so we conclude that

$$e_{S_n} = \beta_1 \cdots \beta_s \lambda_t \cdots \lambda_1,$$

which is a product of $s+t$ transpositions. This is an odd number, so it suffices to show that it is not possible to write the identity as a product of an odd number of transpositions.

So suppose that the identity can be written as the product $(a_1 b_1)\cdots(a_k b_k)$, where each $a_i \neq b_i$. First, note that a single transposition *cannot* be the identity, and thus $k \neq 1$. So assume, for the sake of an argument by induction, that for a fixed k, we know that every product of fewer than k transpositions that equals the identity must use an even number of transpositions. We might as well have $k \geqslant 3$, since we 2 is even.

Now note that since $k > 1$, and our product is the identity, then some transposition $(a_i b_i)$ with $i > 1$ must move a_1; otherwise, b_1 would be sent to a_1, and our product would not be the identity.

Now notice that the two rules in Exercise 7 allow us to rewrite the overall product without changing the number of transpositions in such a way that the transposition $(a_2 b_2)$ moves a_1, meaning a_2 or b_2 is a_1. So let us assume that our product of transpositions has already been put in this form. Note also that $(a_i b_i) = (b_i a_i)$, so we might as well assume without loss of generality that $a_2 = a_1$. We will consider the cases when $b_2 = b_1$ and $b_2 \neq b_1$.

Case 1: When $b_1 = b_2$, our product is

$$(a_1b_1)(a_1b_1)(a_3b_3)\cdots(a_kb_k),$$

but $(a_1b_1)(a_1b_1)$ is the identity, so we can rewrite our product using only $k-2$ transpositions. By induction hypothesis, $k-2$ is even, and thus k is even.

Case 2: When $b_1 \neq b_2$, we can use Exercise 7 to write

$$(a_1b_1)(a_1b_2) = (a_1b_1)(b_2a_1) = (a_1b_2)(b_1b_2).$$

Notice here that it matters that a_1, b_1, and b_2 are all distinct, so that we can apply Exercise 7. So our product, which equals the identity, is

$$(a_1b_2)(b_1b_2)(a_3b_3)\cdots(a_kb_k).$$

The advantage of this shuffling is that while we have only changed the first two transpositions, we have decreased the number of transpositions that move a_1. We must now have some other transposition that moves a_1, and we can repeat the argument to keep decreasing the number of transpositions in our product that move a_1. Each time we do this, we cannot keep landing in case 2 indefinitely, as each time we lower the number of transpositions moving a_1. So eventually we will land in case 1, which allows us to lower the total number of transpositions, and using the induction hypothesis we will show that k must be even. □

Definition 1.45. Consider a permutation $\sigma \in S_n$. If $\sigma = \tau_1 \cdots \tau_s$ is a product of transpositions, the **sign** of σ is given by $(-1)^r$. Permutations with sign 1 are called **even** and those with sign -1 are called **odd**. This is also called the parity of the permutation.

Theorem 1.44 tells us that the sign of a permutation is well-defined.

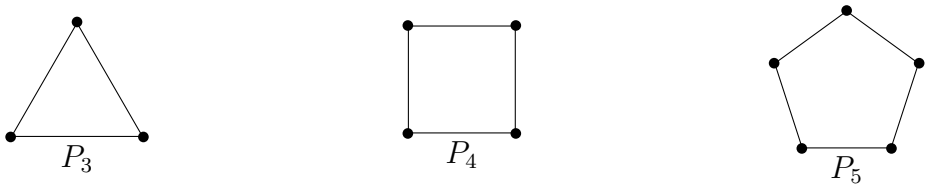
Example 1.46. The identity permutation is even. Every transposition is odd.

Example 1.47. The 3-cycle (123) can be rewritten as (12)(23), a product of 2 transpositions, so the sign of (123) is 1.

Exercise 8. Show that every permutation is a product adjacent transpositions, meaning transpositions of the form $(i \;\; i+1)$.

1.3 Dihedral groups

For any integer $n \geqslant 3$, let P_n denote a regular n-gon. For concreteness sake, let us imagine P_n is centered at the origin with one of its vertices located along the positive y-axis. Note that the size of the polygon will not matter. Here are some examples:



Definition 1.48. The **dihedral group** D_n is the set of symmetries of the regular n-gon P_n equipped with the binary operation given by composition.

Remark 1.49. There are competing notations for the group of symmetries of the n-gon. Some authors prefer to write it as D_{2n}, since, as we will show, that is the order of the group. Democracy has dictated that we will be denoting it by D_n, which indicates that we are talking about the symmetries of the n-gon. Some authors like to write $D_{2\times n}$, always keeping the 2, for example with $D_{2\times 3}$, to satisfy both camps.

Let us make this more precise. Let $d(-,-)$ denote the usual Euclidean distance between two points on the plane $\mathbb{R}^2$. An **isometry** of the plane is a function $f : \mathbb{R}^2 \to \mathbb{R}^2$ that is bijective and preserves the Euclidean distance, meaning that

$$d(f(A), f(B)) = d(A, B) \quad \text{for all } A, B \in \mathbb{R}^2.$$

Though not obvious, it is a fact that if f preserves the distance between every pair of points in the plane, then it must be a bijection.

A **symmetry** of P_n is an isometry of the plane that maps P_n to itself. By this I do not mean that f fixes each point of P_n, but rather that we have an equality of sets $f(P_n) = P_n$, meaning every point of P_n is mapped to a (possibly different) point of P_n and every point of P_n is the image of some point in P_n via f.

We are now ready to give the formal definition of the dihedral groups:

Remark 1.50. Let us informally verify that this really is a group. If f and g are in D_n, then $f \circ g$ is an isometry (since the composition of any two isometries is again an isometry) and

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

so that $f \circ g \in D_n$. This proves composition is a binary operation on D_n. Now note that associativity of composition is a general property of functions. The identity function on $\mathbb{R}^2$, denoted $\mathrm{id}_{\mathbb{R}^2}$, belongs to D_n and it is the identity element of D_n. Finally, the inverse function of an isometry is also an isometry. Using this, we see that every element of D_n has an inverse.

Later on we will need the following elementary fact, which we leave as an exercise:

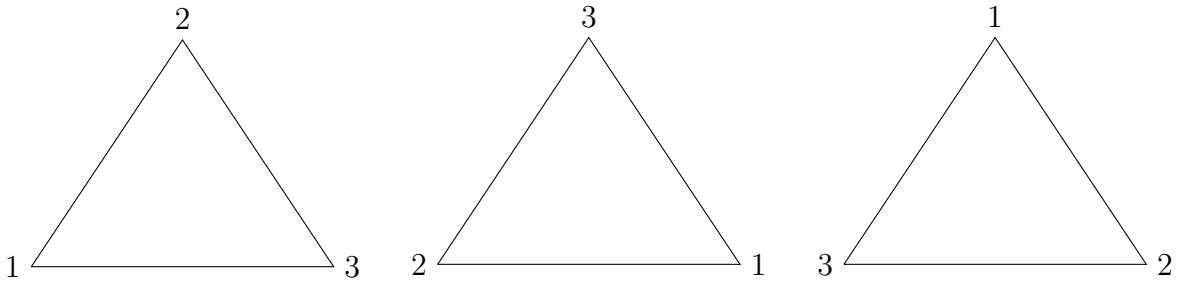
Lemma 1.51. *Every point on a regular polygon is completely determined, among all points on the polygon, by its distances to two adjacent vertices of the polygon.*

Exercise 9. Prove Lemma 1.51.

Definition 1.52 (Rotations in D_n)**.** Assume that the regular n-gon P_n is drawn in the plane with its center at the origin and one vertex on the x axis. Let r denote the rotation about the origin by $\frac{2\pi}{n}$ radians counterclockwise; this is an element of D_n. Its inverse is the clockwise rotation by $\frac{2\pi}{n}$. This gives us rotations r^i, where r^i is the counterclockwise rotation by $\frac{2\pi i}{n}$, for each $i = 1, \ldots, n$. Notice that when $i = n$ this is simply the identity map.

Each symmetry of P_n is completely determined by the images of the vertices. In particular, it is sometimes convenient to label the vertices of P_n with $1, 2, \ldots, n$, and to indicate each symmetry by indicating the images of the vertices, as in the following example.

Example 1.53. Here are the rotations of D_3:

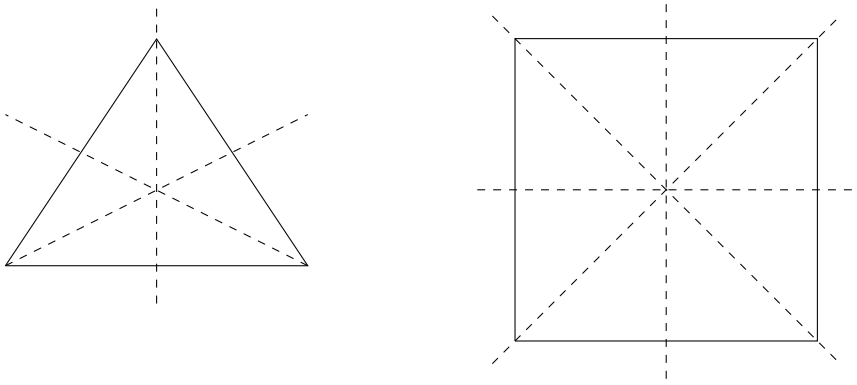


The identity | Rotation by $\frac{2\pi}{3}$ | Rotation by $\frac{4\pi}{3}$

Definition 1.54 (Reflections in D_n)**.** For any line of symmetry of P_n, reflection about that line gives an element of D_n. When n is odd, the line connecting a vertex to the midpoint of the opposite side of P_n is a line of symmetry. When n is even, there are two types of reflections: the ones about the line connecting tow opposite vertices, and the ones across the line connecting midpoints of opposite sides.

In both cases, these give us a total of n reflections.

Example 1.55.



The reflection lines in D_3 | The reflection lines in D_4

Let us summarize the content of this page:

Notation 1.56. Fix $n \geqslant 3$. We will consider two special elements of D_n:

- Let r denote the symmetry of P_n given by counterclockwise rotation by $\frac{2\pi}{n}$.
- Let s denote a reflection symmetry of P_n that fixes at least one of the vertices of P_n, as described in Definition 1.54. Let V_1 be a vertex of P_n that is fixed by s, and label the remaining vertices of P_n with $V_2, \ldots, V_n$ by going counterclockwise from V_1.

From now on, whenever we are talking about D_n, the letters r and s will refer only to these specific elements. Finally, we will sometimes denote the identity element of D_n by id, since it is the identity map.

Theorem 1.57. *The dihedral group D_n has $2n$ elements.*

Proof. First, we show that D_n has order at most $2n$. Any element $\sigma \in D_n$ takes the polygon P_n to itself, and must in particular send vertices to vertices and preserve adjacencies, meaning that any two adjacent vertices remain adjacent after applying σ. Fix two adjacent vertices A and B. By Lemma 1.51, the location of every other point P on the polygon after applying σ is completely determined by the locations of $\sigma(A)$ and $\sigma(B)$. There are n distinct possibilities for $\sigma(A)$, since it must be one of the n vertices of the polygon. But once $\sigma(A)$ is fixed, $\sigma(B)$ must be a vertex adjacent to $\sigma(B)$, so there are at most 2 possibilities for $\sigma(B)$. This gives us at most $2n$ elements in D_n.

Now we need only to present $2n$ distinct elements in D_n. We have described n reflections and n rotations for D_n; we need only to see that they are all distinct. First, note that the only rotation that fixes any vertices of P_n is the identity. Moreover, if we label the vertices of P_n in order with $1, 2, \ldots, n$, say by starting in a fixed vertex and going counterclockwise through each adjacent vertex, then the rotation by an angle of $\frac{2\pi i}{n}$ sends V_1 to V_{i+1} for each $i < n$, showing these n rotations are distinct. Now when n is odd, each of the n reflections fixes exactly one vertex, and so they are all distinct and disjoint from the rotations. Finally, when n is even, we have two kinds of reflections to consider. The reflections through a line connecting opposite vertices have exactly two fixed vertices, and are completely determined by which two vertices are fixed; since rotations have no fixed points, none of these matches any of the rotations we have already considered. The other reflections, the ones through the midpoint of two opposite sides, are completely determined by (one of) the two pairs of adjacent vertices that they switch. No rotation switches two adjacent vertices, and thus these give us brand new elements of D_n.

In both cases, we have a total of $2n$ distinct elements of D_n given by the n rotations and the n reflections. □

Remark 1.58. Given an element of D_n, we now know that it must be a rotation or a reflection. The rotations are the elements of D_n that preserve orientation, while the reflections are the elements of D_n that reverse orientation.

Remark 1.59. Any reflection is its own inverse. In particular, $s^2 = \mathrm{id}$.

Remark 1.60. Note that $r^j(V_1) = V_{1+j \pmod n}$ for any j. Thus if $r^j = r^i$ for some $1 \leqslant i, j \leqslant n$, then we must have $i = j$.

In fact, we have seen that $r^n = \mathrm{id}$ and that the rotations $\mathrm{id}, r, r^2, \ldots, r^{n-1}$ are all distinct, so $|r| = n$. In particular, the inverse of r is r^{n-1}.

Lemma 1.61. *Following Notation 1.56, we have* $srs^{-1} = r^{-1}$.

Proof. First, we claim that rs is a reflection. To see this, observe that $s(V_1) = V_1$, so

$$rs(V_1) = r(V_1) = V_2$$

and

$$rs(V_2) = r(V_n) = V_1.$$

This shows that rs must be a reflection, since it reverses orientation. Reflections have order 2, so $rsrs = (rs)^2 = \mathrm{id}$ and hence $srs = r^{-1}$. □

Remark 1.62. Given $|r| = n$ and $|s| = 2$, as noted in Remark 1.59 and Remark 1.60, we can rewrite Lemma 1.61 as

$$srs = r^{n-1}.$$

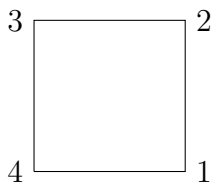
Theorem 1.63. *Every element in* D_n *can be written uniquely as* r^j *or* $r^j s$ *for* $0 \leqslant j \leqslant n-1$.

Proof. Let α be an arbitrary symmetry of P_n. Note α must fix the origin, since it is the center of mass of P_n, and it must send each vertex to a vertex because the vertices are the points on P_n at largest distance from the origin. Thus $\alpha(V_1) = V_j$ for some $1 \leqslant j \leqslant n$ and therefore the element $r^{-j}\alpha$ fixes V_1 and the origin. The only elements that fix V_1 are the identity and s. Hence either $r^{-j}\alpha = \mathrm{id}$ or $r^{-j}\alpha = s$. We conclude that $\alpha = r^j$ or $\alpha = r^j s$.

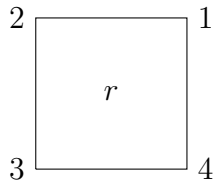
Notice that we have shown that D_n has exactly $2n$ elements, and that there are $2n$ distinct expressions of the form r^j or $r^j s$ for $0 \leqslant j \leqslant n-1$. Thus each element of D_n can be written in this form in a unique way. □

Remark 1.64. The elements $s, rs, \ldots, r^{n-1}$ are all reflections since they reverse orientation. Alternatively, we can check these are all reflections by checking they have order 2. As we noted before, the elements $\mathrm{id}, r, \ldots, r^{n-1}$ are rotations, and preserve orientation.

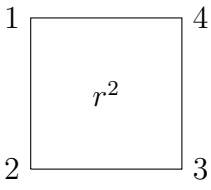
Example 1.65. The 8 elements of D_4, the group of symmetries of the square, are



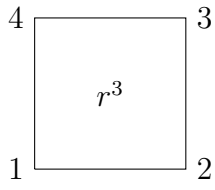
The identity



Rotation by $\frac{2\pi}{4} = \frac{\pi}{2}$

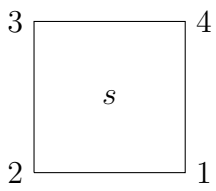


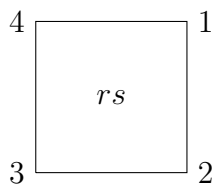
Rotation by $\frac{4\pi}{4} = \pi$

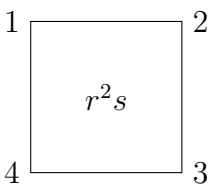


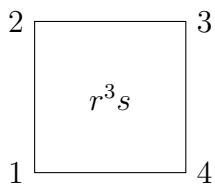
Rotation by $\frac{6\pi}{4} = \frac{3\pi}{2}$

and the reflections









Let us now give a presentation for D_n.

Theorem 1.66. *Let $r : \mathbb{R}^2 \to \mathbb{R}^2$ denote counterclockwise rotation around the origin by $\frac{2\pi}{n}$ radians and let $s : \mathbb{R}^2 \to \mathbb{R}^2$ denote reflection about the x-axis respectively. Set*

$$X_{2n} = \langle r, s \mid r^n = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle.$$

Then $D_n = X_{2n}$, that is,

$$D_n = \langle r, s \mid r^n = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle.$$

Proof. Theorem 1.63 shows that $\{r, s\}$ is a set of generators for D_n. Moreover, we also know that the relations listed above $r^n = 1, s^2 = 1, srs^{-1} = r^{-1}$ hold; the first two are easy to check, and the last one is Lemma 1.61. The only concern we need to deal with is that we may not have discovered all the relations of D_n; or rather, we need to check that we have found enough relations so that any other valid relation follows as a consequence of the ones listed.

Let

$$X_{2n} = \langle r, s \mid r^n = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle.$$

Assume that D_n has more relations than X_{2n} does. Then D_n would be a group of cardinality strictly smaller than X_{2n}, meaning that $|D_n| < |X_{2n}|$. [1] We will show below that in fact $|X_{2n}| \leqslant 2n = |D_n|$, thus obtaining a contradiction.

Now we show that X_{2n} has at most $2n$ elements using just the information contained in the presentation. By definition, since r and s generated X_{2n} then every element $x \in X_{2n}$ can be written as

$$x = r^{m_1} s^{n_1} r^{m_2} s^{n_2} \cdots r^{m_j} s^{n_j}$$

for some j and (possibly negative) integers $m_1, \ldots, m_j, n_1, \ldots, m_j$.[2] As a consequence of the last relation, we have

$$sr = r^{-1} s,$$

and its not hard to see that this implies

$$sr^m = r^{-m} s$$

for all m. Thus, we can slide an s past a power of r, at the cost of changing the sign of the power. Doing this repeatedly gives that we can rewrite x as

$$x = r^M s^N.$$

By the first relation, $r^n = 1$, from which it follows that $r^a = r^b$ if a and b are congruent modulo n. Thus we may assume $0 \leqslant M \leqslant n-1$. Likewise, we may assume $0 \leqslant N \leqslant 1$. This gives a total of at most $2n$ elements, and we conclude that X_{2n} must in fact be D_n. □

Note that we have *not* shown that

$$X_{2n} = \langle r, s \mid r^n, s^2, srs^{-1} = r^{-1} \rangle$$

has at least $2n$ elements using just the presentation. But for this particular example, since we know the group presented is the same as D_n, we know from Theorem 1.63 that it has exactly $2n$ elements.

[1] This will become more clear once we properly define presentations.

[2] Note that, m_1 could be 0, so that expressions beginning with a power of s are included in this list.

1.4 The quaternions

For our last big example we mention the group of quaternions, written Q_8.

Definition 1.67. The **quaternion group** Q_8 is a group with 8 elements

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

satisfying the following relations: 1 is the identity element, and

$$i^2 = -1, \quad j^2 = -1, \quad k^2 = -1, \quad ij = k, \quad jk = i, \quad ki = j,$$

$$(-1)i = -i, \quad (-1)j = -j, \quad (-1)k = -k, \quad (-1)(-1) = 1.$$

To verify that this really is a group is rather tedious, since the associative property takes forever to check. Here is a better way: in the group $\mathrm{GL}_2(\mathbb{C})$, define elements

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad A = \begin{bmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{bmatrix}$$

where $\sqrt{-1}$ denotes the complex number whose square is -1, to avoid confusion with the symbol $i \in Q_8$. Let $-I, -A, -B, -C$ be the negatives of these matrices.

Then we can define an injective map $f : Q_8 \to \mathrm{GL}_2(\mathbb{C})$ by assigning

$$\begin{aligned} 1 &\mapsto I, & -1 &\mapsto -I \\ i &\mapsto A, & -i &\mapsto -A \\ j &\mapsto B, & -j &\mapsto -B \\ k &\mapsto C, & -k &\mapsto -C. \end{aligned}$$

It can be checked directly that this map has the nice property (called being a *group homomorphism*) that

$$f(xy) = f(x)f(y) \text{ for any elements } x, y \in \mathbb{Q}_8.$$

Let us now prove associativity for Q_8 using this information:

Claim: For any $x, y, z \in Q_8$, we have $(xy)z = x(yz)$.

Proof. By using the property $f(xy) = f(x)f(y)$ as well as associativity of multiplication in $\mathrm{GL}_2(\mathbb{C})$ (marked by $*$) we obtain

$$f((xy)z) = f(xy)f(z) = (f(x)f(y))\, f(z) \overset{*}{=} f(x)\, (f(y)f(z)) = f(x)f(yz) = f(x(yz)).$$

Since f is injective and $f((xy)z) = f(x(yz))$, we deduce $(xy)z = x(yz)$. □

The subset $\{\pm I, \pm A, \pm B, \pm C\}$ of $\mathrm{GL}_2(\mathbb{C})$ is a *subgroup* (a term we define carefully later), meaning that it is closed under multiplication and taking inverses. (For example, $AB = C$ and $C^{-1} = -C$.) This proves it really is a group and one can check it satisfies an analogous list of identities as the one satisfied by Q_8.

This is an excellent motivation to talk about group homomorphisms.

1.5 Group homomorphisms

A group homomorphism is a function between groups that preserves the group structure.

Definition 1.68. Let $(G, \cdot_G)$ and $(H, \cdot_H)$ be groups. A (group) **homomorphism** from G is H is a function $f : G \to H$ such that

$$f(x \cdot_G y) = f(x) \cdot_H f(y).$$

Note that a group homomorphism does not necessarily need to be injective nor surjective, it can be any function as long as it preserves the product.

Definition 1.69. Let G and H be groups A homomorphism $f\colon G \to H$ is an **isomorphism** if there exists a homomorphism $g : H \to G$ such that

$$f \circ g = \mathrm{id}_H \text{ and } g \circ f = \mathrm{id}_G .$$

If $f : G \to H$ is an isomorphism, G and H are called **isomorphic**, and we denote this by writing $G \cong H$. An isomorphism $G \longrightarrow G$ is called an **automorphism** of G. We de denote the set of all automorphisms of G by $\mathrm{Aut}(G)$.

Remark 1.70. Two groups G and H are isomorphic if we can obtain H from G by renaming all the elements, without changing the group structure. One should think of an isomorphism $f : G \xrightarrow{\cong} H$ of groups as saying that the multiplication tables of G and H are the same up to renaming the elements. The multiplication rule $\cdot_G$ for G can be visualized as a table with both rows and columns labeled by elements of G, and with $x \cdot_G y$ placed in row x and column y. The isomorphism f sends x to $f(x)$, y to $f(y)$, and the table entry $x \cdot_G y$ to the table entry $f(x) \cdot_H f(y)$. The inverse map f^{-1} does the opposite.

Remark 1.71. Suppose that $f\colon G \to H$ is an isomorphism. As a function, f has an inverse, and thus it must necessarily be a bijective function. Our definition, however, requires more: the inverse must in fact also be a group homomorphism. Note that many books define group homomorphism by simply requiring it to be a homomorphism that is bijective: and we will soon show that this is in fact equivalent to the definition we gave. There are however good reasons to define it as we did: in many contexts, such as sets, groups, rings, fields, or topological spaces, the correct meaning of the word "isomorphism" in "a morphism that has a two-sided inverse". This explains our choice of definition.

Exercise 10. Let G be a group. Show that $\mathrm{Aut}(G)$ is a group under composition.

Example 1.72.

(a) For any group G, the identity map $\mathrm{id}_G\colon G \to G$ is a group isomorphism.

(b) For all groups G and H, the constant map $f\colon G \to H$ with $f(g) = e_H$ for all $g \in G$ is a homomorphism, which we sometimes refer to as the **trivial homomorphism**.

(c) The exponential map and the logarithm map

$$\begin{array}{ccc} \exp\colon (\mathbb{R},+) \longrightarrow (\mathbb{R}\setminus\{0\},\cdot) & & \ln\colon (\mathbb{R}_{>0},\cdot) \longrightarrow (\mathbb{R},+) \\ x \longmapsto e^x & & y \longmapsto \ln y \end{array}$$

are both isomorphisms, so $(\mathbb{R},+) \cong (\mathbb{R}_{>0},\cdot)$. In fact, these maps are inverse to each other.

(d) The function $f\colon \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = 2x$ is a group homomorphism that is injective but not surjective.

(e) For any positive integer n and any field F, the determinant map

$$\begin{array}{c} \det\colon \mathrm{GL}_n(F) \longrightarrow (F\setminus\{0\},\cdot) \\ A \longmapsto \det(A) \end{array}$$

is a group homomorphism. For $n \geqslant 2$, the determinant map is not injective (you should check this!) and so it cannot be an isomorphism. It is however surjective: for each $c \in F\setminus\{0\}$, the diagonal matrix

$$\begin{pmatrix} c & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

has determinant c.

(f) Fix an integer $n > 1$, and consider the function $f\colon (\mathbb{Z},+) \to (\mathbb{C}^*,\cdot)$ given by $f(n) = e^{\frac{2\pi i}{n}}$. This is a group homomorphism, but it is neither surjective nor injective. It is not surjective because the image only contains complex number x with $|x| = 1$, and it is not injective because $f(0) = f(n)$.

Group homomorphisms preserve the group structure. In particular, group homomorphisms preserve the identity and all inverses.

Lemma 1.73 (Properties of homomorphisms)**.** *If $f : G \to H$ is a homomorphism of groups, then*

$$f(e_G) = e_H.$$

Moreover, for any $x \in G$ we have

$$f(x^{-1}) = f(x)^{-1}.$$

Proof. By definition,

$$f(e_G)f(e_G) = f(e_G e_G) = f(e_G).$$

Multiplying both sides by $f(e_G)^{-1}$, we get

$$f(e_G) = e_H.$$

Now given any $x \in G$, we have

$$f(x^{-1})f(x) = f(x^{-1}x) = f(e) = e,$$

and thus $f(x^{-1}) = f(x)^{-1}$. □

Remark 1.74. Let G be a cyclic group generated by the element g. Then any homomorphism $f: G \to H$ is completely determined by $f(g)$, since any other element $h \in G$ can be written as $h = g^n$ for some integer n, and

$$f(g^n) = f(g)^n.$$

More generally, given a group G a set S of generators for G, any homomorphism $f: G \longrightarrow H$ is completely determined by the images of the generators in S: the element $g = s_1 \cdots s_m$, where s_i is either in S or the inverse of an element of S, has image

$$f(g) = f(s_1 \cdots s_m) = f(s_1) \cdots f(s_m).$$

Note, however, that not all choices of images for the generators might actually give rise to a homomorphism; we need to check that the map determined by the given images of the generators is well-defined.

Definition 1.75. The **image** of a group homomorphism $f: G \longrightarrow G$ is

$$\operatorname{im}(f) := \{f(g) \mid g \in G\}.$$

Notice that $f: G \to H$ is surjective if and only if $\operatorname{im}(f) = H$.

Definition 1.76. The **kernel** of a group homomorphism $f: G \longrightarrow G$ is

$$\ker(f) := \{g \in G \mid f(g) = e_H\}.$$

Remark 1.77. Given any group homomorphism $f: G \longrightarrow G$, we must have $e_G \in \ker f$ by Lemma 1.73.

When the kernel of f is as small as possible, meaning $\ker(f) = \{e\}$, we say that f the kernel of f is trivial. A homomorphism is injective if and only if it has a trivial kernel.

Lemma 1.78. *A group homomorphism $f: G \to H$ is injective if and only if* $\ker(f) = \{e_G\}$.

Proof. First, note that $e_G \in \ker f$ by Lemma 1.73. If f is injective, then e_G must be the only element that f sends to e_H, and thus $\ker(f) = \{e_G\}$.

Now suppose $\ker(f) = \{e_G\}$. If $f(g) = f(h)$ for some $g, h \in G$, then

$$f(h^{-1}g) = f(h^{-1})f(g) = f(h)^{-1}f(g) = e_H.$$

But then $h^{-1}g \in \ker(f)$, so we conclude that $h^{-1}g = e_G$, and thus $g = h$. □

Example 1.79. First, number the vertices of P_n from 1 to n in any manner you like. Now define a function $f: D_n \to S_n$ as follows: given any symmetry $\alpha \in D_n$, set $f(\alpha)$ to be the permutation of $[n]$ that records how α permutes the vertices of P_n according to your labelling. So $f(\alpha) = \sigma$ where σ is the permutation that for all $1 \leqslant i \leqslant n$, if α sends the ith vertex to the jth one in the list, then $\sigma(i) = j$. This map f is a group homomorphism.

Now suppose $f(\alpha) = \mathrm{id}_{S_n}$. Then α must fix all the vertices of P_n, and thus α must be the identity element of D_n. We have thus shown that the kernel of f is trivial. By Lemma 1.78, this proves f is injective.

We defined isomorphisms to be homomorphisms that have an inverse that is also a homomorphism. We are now ready to show that this can simplified: an isomorphism is a bijective group homomorphism.

Lemma 1.80. *Suppose $f : G \to H$ is a group homomorphism. Then f an isomorphism if and only if f is bijective.*

Proof. ($\Rightarrow$) A function $f : X \to Y$ between two sets is bijective if and only if it has an inverse, meaning that there is a function $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$. Our definition of group isomorphism implies that this must hold for any isomorphism (and more!), as we noted in Remark 1.71.

($\Leftarrow$) If f is bijective homomorphism, then as a function is has a *set-theoretic* two-sided inverse g, as remarked in Remark 1.71. But we need to show that this inverse g is actually a homomorphism. For any $x, y \in H$, we have

$$\begin{aligned} f(g(xy)) &= xy && \text{since } fg = \mathrm{id}_G \\ &= f(g(x))f(g(y)) && \text{since } fg = \mathrm{id}_G \\ &= f(g(x)g(y)) && \text{since } f \text{ is a group homomorphism.} \end{aligned}$$

Since f is injective, we must have $g(xy) = g(x)g(y)$. Thus g is a homomorphism, and f is an isomorphism. □

Exercise 11. Let $f : G \to H$ be an isomorphism. Show that for all $x \in G$, we have $|f(x)| = |x|$.

In other words, isomorphisms preserve the order of an element. This is an example of an isomorphism invariant.

Definition 1.81. An **isomorphism invariant** (of a group) is a property P (of groups) such that whenever G and H are isomorphic groups and G has the property P, then H also has the property P.

Theorem 1.82. *The following are isomorphism invariants:*

(a) the order of the group,

(b) the set of all the orders of elements in the group,

(c) the property of being abelian,

(d) the order of the center of the group,

(e) being finitely generated.

Recall that by definition two sets have the same cardinality if and only if they are in bijection with each other.

Proof. Let $f : G \to H$ be any a group isomorphism.

(a) Since f is a bijection by Remark 1.71, we conclude that $|G| = |H|$.

(b) We wish to show that $\{|x| \mid x \in G\} = \{|y| \mid y \in H\}$.

($\subseteq$) follows from Exercise 11: given any $x \in G$, we have $|x| = |f(x)|$, which is the order of an element in H.

($\supseteq$) follows from the previous statement applied to the group isomorphism f^{-1}: given any $y \in H$, we have $f^{-1}(y) \in G$ and $|y| = |f^{-1}(y)|$ is the order of an element of G.

(c) For any $y_1, y_2 \in H$ there exist some $x_1, x_2 \in G$ such that $f(x_i) = y_i$. Then we have

$$y_1 y_2 = f(x_1)f(x_2) = f(x_1 x_2) \overset{*}{=} f(x_2 x_1) = f(x_2)f(x_1) = y_2 y_1,$$

where $*$ indicates the place where we used that G is abelian.

(d) Exercise. The idea is to show f induces an isomorphism $Z(G) \cong Z(H)$.

(e) Exercise. Show that if S generates G then $f(S) = \{f(s) \mid s \in S\}$ generates H. □

The easiest way to show that two groups are not isomorphic is to find an isomorphism invariant that they do not share.

Remark 1.83. Let G and H be two groups. If P is an isomorphism invariant, and G has P while H does not have P, then G is not isomorphic to H.

Example 1.84.

(1) We have $S_n \cong S_m$ if and only if $n = m$, since $|S_n| = n!$ and $|S_m| = m!$ and the order of a group is an isomorphism invariant.

(2) Since $\mathbb{Z}/6$ is abelian and S_3 is not abelian, we conclude that $\mathbb{Z}/6 \ncong S_3$.

(3) You will show in Problem Set 2 that $|Z(D_{24})| = 2$, while S_n has trivial center. We conclude that $D_{24} \ncong S_4$.

Chapter 2

Group actions: a first look

We come to one of the central concepts in group theory: the action of a group on a set. Some would say this is the main reason one would study groups, so we want to introduce it early both as motivation for studying group theory but also because the language of group actions will be very helpful to us.

2.1 What is a group action?

Definition 2.1. For a group $(G, \cdot)$ and set S, an **action** of G on S is a function

$$G \times S \to S,$$

typically written as $(g, s) \mapsto g \cdot s$, such that

(1) $g \cdot (h \cdot s) = (gh) \cdot s$ for all $g, h \in G$ and $s \in S$.

(2) $e_G \cdot s = s$ for all $s \in S$.

Remark 2.2. To make the first axiom clearer, we will write $\cdot$ for the action of G on S and no symbol (concatenation) for the multiplication of two elements in the group G.

A group action is the same thing as a group homomorphism.

Lemma 2.3 (Permutation representation)**.** *Consider a group G and a set S.*

(1) Suppose $\cdot$ is an action of G on S. For each $g \in G$, let $\mu_g \colon S \longrightarrow S$ denote the function given by $\mu_g(s) = g \cdot s$. Then the function

$$\begin{aligned} \rho \colon G &\longrightarrow \mathrm{Perm}(S) \\ g &\longmapsto \mu_g \end{aligned}$$

is a well-defined homomorphism of groups.

(2) Conversely, if $\rho : G \to \mathrm{Perm}(S)$ is a group homomorphism, then the rule

$$g \cdot s := (\rho(g))(s)$$

defines an action of G on S.

Proof. (1) Assume we are given an action of G on S. We first need to check that for all g, μ_g really is a permutation of S. We will show this by proving that μ_g has a two-sided inverse; in fact, that inverse is $\mu_{g^{-1}}$. Indeed, we have

$$\begin{aligned}
(\mu_g \circ \mu_{g^{-1}})(s) &= \mu_g(\mu_{g^{-1}}(s)) && \text{by the definition of composition} \\
&= g \cdot (g^{-1} \cdot s) && \text{by the definitinion for } \mu_g \text{ and } \mu_{g^{-1}} \\
&= (gg^{-1}) \cdot s && \text{by the definition of a group action} \\
&= e_G \cdot s && \text{by the definition of a group} \\
&= s && \text{by the definition of a group action}
\end{aligned}$$

thus $\mu_g \circ \mu_{g^{-1}} = \mathrm{id}_S$, and a similar argument shows that $\mu_{g^{-1}} \circ \mu_g = \mathrm{id}_S$ (exercise!). This shows that μ_g has an inverse, and thus it is bijective; it must then be a permutation of S.

Finally, we wish to show that ρ is a homomorphism of groups, so we need to check that $\rho(gh) = \rho(g) \circ \rho(h)$. Equivalently, we need to prove that $\mu_{gh} = \mu_g \circ \mu_h$. Now for all s, we have

$$\begin{aligned}
\mu_{gh}(s) &= (gh) \cdot s && \text{by definition of } \mu \\
&= g \cdot (h \cdot s) && \text{by definition of a group action} \\
&= \mu_g\left(\mu_h(s)\right) && \text{by definition of } \mu_g \text{ and } \mu_h \\
&= (\mu_g \circ \mu_h)(s).
\end{aligned}$$

This proves that ρ is a homomorphism.

(2) On the other hand, given a homomorphism ρ, the function

$$\begin{aligned}
G \times S &\longrightarrow S \\
(g, s) &\longmapsto g \cdot s = \rho(g)(s)
\end{aligned}$$

is an action, because

$$\begin{aligned}
h \cdot (g \cdot s) &= \rho(h)(\rho(g)(s)) && \text{by definition of } \rho \\
&= (\rho(h) \circ \rho(g))(s) \\
&= \rho(gh)(s) && \text{since } \rho \text{ is a homomorphism} \\
&= (gh) \cdot s && \text{by definition of } \rho,
\end{aligned}$$

and

$$e_G s = \rho(e_G)(s) = \mathrm{id}(s) = s. \qquad \square$$

Definition 2.4. Given a group G acting on a set S, the group homomorphism ρ associated to the action as defined in Lemma 2.3 is called the **permutation representation** of the action.

Definition 2.5. Let G be a group acting on a set S. The equivalence relation on S induced by the action of G, written $\sim_G$, is defined by $s \sim_G t$ if and only if there is a $g \in G$ such that $t = g \cdot s$. The equivalence classes of $\sim_G$ are called **orbits**: the equivalence class

$$\mathrm{Orb}_G(s) := \{g \cdot s \mid g \in G\}$$

is the orbit of s. The set of equivalence classes with respect to $\sim_G$ is written S/G.

Lemma 2.6. *Let G be a group acting on a set S. Then*

(a) The relation $\sim_G$ really is an equivalence relation.

(b) For any $s, t \in S$ either $\mathrm{Orb}_G(s) = \mathrm{Orb}_G(t)$ or $\mathrm{Orb}_G(s) \cap \mathrm{Orb}_G(t) = \emptyset$.

(c) The orbits of the action of G form a partition of S: $S = \bigcup_{s \in S} \mathrm{Orb}_G(s)$.

Proof. Assume G acts on S.

(a) We really need to prove three things: that $\sim_G$ is reflexive, symmetric, and transitive.

(Reflexive): We have $x \sim_G x$ for all $x \in S$ since $x = e_G \cdot x$.

(Symmetric): If $x \sim_G y$, then $y = g \cdot x$ for some $g \in G$, and thus

$$g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x,$$

which shows that $y \sim_G x$.

(Transitive): If $x \sim_G y$ and $y \sim_G z$, then $y = g \cdot x$ and $z = h \cdot y$ for some $g, h \in G$ and hence $z = h \cdot (g \cdot x) = (hg) \cdot x$, which gives $x \sim_G z$.

Parts (b) and (c) are formal properties of the equivalence classes for any equivalence relation. □

Corollary 2.7. *Suppose a group G acts on a finite set S. Let $s_1, \ldots, s_k$ be a complete set of orbit representatives — that is, assume each orbit contains exactly one member of the list $s_1, \ldots, s_k$. Then*

$$|S| = \sum_{i=1}^{k} |\,\mathrm{Orb}_G(s_i)|.$$

Proof. This is an immediate corollary of the fact that the orbits form a partition of S. □

Remark 2.8. Let G be a group acting on S. The associated group homomorphism ρ is injective if and only if it has trivial kernel, by Lemma 1.78. This is equivalent to the statement $\mu_g = \mathrm{id}_S \implies g = e_G$. The later can be written in terms of elements of S: for each $g \in G$,

$$g \cdot s = s \quad \text{for all } s \in S \implies g = e_G.$$

Definition 2.9. Let G be a group acting on a set S. The action is **faithful** if the associated group homomorphism is injective. Equivalently, the action is faithful if and only if

$$g \cdot s = s \quad \text{for all } s \in S \implies g = e_G.$$

The action is **transitive** if for all $p, q \in S$ there is $g \in G$ such that $q = g \cdot p$. Equivalently, the action is transitive if there is only one orbit, meaning that

$$\mathrm{Orb}_G(p) = S \text{ for all } p \in S.$$

2.2 Examples of group actions

Example 2.10 (Trivial action)**.** For any group G and any set S, $g \cdot s := s$ defines an action, the **trivial action**. The associated group homomorphism is the map

$$\begin{aligned} G &\longrightarrow \mathrm{Perm}(S) \\ g &\longmapsto \mathrm{id}_S\,. \end{aligned}$$

A trivial action is not faithful unless the group G is trivial; in fact, the corresponding group homomorphism is trivial.

Example 2.11. The group D_n acts on the vertices of P_n, which we will label with $V_1, \ldots, V_n$ in a counterclockwise fashion, with V_1 on the positive x-axis, as in Notation 1.56. Note that D_n acts on $\{V_1, \ldots, V_n\}$: for each $g \in D_n$ and each integer $1 \leqslant j \leqslant n$, we set

$$g \cdot V_j = V_i \quad \text{if and only if} \quad g(V_j) = V_i.$$

This satisfies the two axioms of a group action (check!).

Let $\rho\colon D_n \to \mathrm{Perm}\left(\{V_1, \ldots, V_n\}\right) \cong S_n$ be the associated group homomorphism. Note that ρ is injective, because if an element of D_n fixes all n vertices of a polygon, then it must be the identity map. More generally, if an isometry of $\mathbb{R}^2$ fixes any three noncolinear points, then it is the identity. To see this, note that given three noncolinear points, every point in the plane is uniquely determined by its distance from these three points (exercise!).

The action of D_n on the n vertices of P_n is faithful; in fact, we saw before that each $\sigma \in D_n$ is completely determined by what it does to any two adjacent vertices.

Example 2.12 (group acting on itself by left multiplication)**.** Let G be any group and define an action $\cdot$ of G on G (regarded as just a set) by the rule

$$g \cdot x := gx.$$

This is an action, since multiplication is associative and $e_G \cdot x = x$ for all x; it is know as the **left regular action** of G on itself.

The left regular action of G on itself is faithful, since if $g \cdot x = x$ for all x (or even for just one x), then $g = e$. It follows that the associated homomorphism is injective. This action is also transitive: given any $g \in G$, $g = g \cdot e$, and thus $\mathrm{Orb}_G(e) = G$.

Example 2.13 (conjugation)**.** Let G be any group and fix an element $g \in G$. Define the **c**onjugation action of G on itself by setting

$$g \cdot x := gxg^{-1} \text{ for any } g, x \in G.$$

The action of G on itself by conjugation is not necessarily faithful. In fact, we claim that the kernel of the permutation representation $\rho\colon G \to \mathrm{Perm}(G)$ for the conjugation action is the center $\mathrm{Z}(G)$. Indeed,

$$g \in \ker\rho \iff g \cdot x = x \text{ for all } x \in G \iff gxg^{-1} = x \text{ for all } x \in G$$

$$\iff gx = xg \text{ for all } x \in G \iff g \in \mathbb{Z}(G).$$

If G is nontrivial, this action is *never* transitive unless G is trivial: note that $\mathrm{Orb}_G(e) = \{e\}$.

Chapter 3

Subgroups

Every time we define a new abstract structure consisting of a set S with some extra structure, we then want to consider subsets of S that inherit that special structure. It is now time to discuss subgroups.

3.1 Definition and examples

Definition 3.1. A nonempty subset H of a group G is a **subgroup** of G if H is a group under the multiplication law of G. If H is a subgroup of G, we write $H \leq G$, or $H < G$ if we want to indicate that H is a subgroup of G but $H \neq G$.

Remark 3.2. Note that if H is a subgroup of G, then necessarily H must be closed for the product in G, meaning that for any $x, y \in H$ we must have $xy \in H$.

Example 3.3. Any group G has two **trivial subgroups**: G itself, and $\{e_G\}$.

Any subgroup H of G that is neither G nor $\{e_G\}$ is a **nontrivial subgroup**. A group might not have any nontrivial subroups.

Example 3.4. The group $\mathbb{Z}/2$ has no nontrivial subgroup.

Example 3.5. The following are strings of subgroups with the obvious group structure:

$$\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C} \quad \text{and} \quad \mathbb{Z}^\times < \mathbb{Q}^\times < \mathbb{R}^\times < \mathbb{C}^\times.$$

To prove that a certain subset H of G forms a subgroup, it is very inefficient to prove directly that H forms a group under the same operation as G. Instead, we use one of the following two tests:

Lemma 3.6 (Subgroup tests)**.** *Let G be a subset of a group G.*

- *Two-step test: If H is nonempty and closed under multiplication and taking inverses, then H is a subgroup of G. More precisely, if for all $x, y \in H$, we have $xy \in H$ and $x^{-1} \in H$, then H is a subgroup of G.*
- *One-step test: If H is nonempty and $xy^{-1} \in H$ for all $x, y \in H$, then H is a subgroup of G.*

Proof. We prove the One-step test first. Assume H is nonempty and for all $x, y \in H$ we have $xy^{-1} \in H$. Since H is nonempty, there is some $h \in H$, and hence $e_G = hh^{-1} \in H$. Since $e_G x = x = x e_G$ for any $x \in G$, and hence for any $x \in H$, then e_G is an identity element for H. For any $h \in H$, we that $h^{-1} = eh^{-1} \in H$, and since in G we have $h^{-1}h = e = hh^{-1} \in H$ and this calculation does not change when we restrict to H, we can conclude that every element of H has an inverse inside H. For every $x, y \in H$ we must have $y^{-1} \in H$ and thus

$$xy = x(y^{-1})^{-1} \in H$$

so H is closed under the multiplication operation. This means that the restriction of the group operation of G to H is a well-defined group operation. This operation is associative by the axioms for the group G. The axioms of a group have now been established for $(H, \cdot)$.

Now we prove the Two-Step test. Assume H is nonempty and closed under multiplication and taking inverses. Then for all $x, y \in H$ we must have $y^{-1} \in H$ and thus $xy^{-1} \in H$. Since the hypothesis of the One-step test is satisfied, we conclude that H is a subgroup of G. □

Lemma 3.7 (Examples of subgroups)**.** *Let G be a group.*

(a) If H is a subgroup of G and K is a subgroup of H, then K is a subgroup of G.

(b) Let J be any (index) set. If H_α is a subgroup of G for all $\alpha \in J$, then $H = \bigcap_{\alpha \in J} H_\alpha$ is a subgroup of G.

(c) If $f : G \to H$ is a homomorphism of groups, then $\operatorname{im}(f)$ *is a subgroup of H.*

(d) If $f : G \to H$ is a homomorphism of groups, and K is a subgroup of G, then

$$f(K) := \{f(g) \mid g \in K\}$$

is a subgroup of H.

(e) If $f : G \to H$ is a homomorphism of groups, then $\ker(f)$ *is a subgroup of G.*

(f) The center $\mathrm{Z}(G)$ *is a subgroup of G.*

Proof.

(a) By definition, K is a group under the multiplication in H, and the multiplication in H is the same as that in G, so K is a subgroup of G.

(b) First, note that H is nonempty since $e_G \in H_\alpha$ for all $\alpha \in J$. Moreover, given $x, y \in H$, for each α we have $x, y \in H_\alpha$ and hence $xy^{-1} \in H_\alpha$. It follows that $xy^{-1} \in H$. By the Two-Step test, H is a subgroup of G.

(c) Since G is nonempty, then $\operatorname{im}(f)$ must also be nonemtpy; for example, it contains $f(e_G) = e_H$. If $x, y \in \operatorname{im}(f)$, then $x = f(a)$ and $y = f(b)$ for some $a, b \in G$, and hence

$$xy^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in \operatorname{im}(f).$$

By the Two-Step Test, $\operatorname{im}(f)$ is a subgroup of H.

(d) The restriction $g \colon K \to H$ of f to K is still a group homomorphism, and thus $f(K) = \operatorname{im} g$ is a subgroup of H.

(e) Using the One-step test, note that if $x, y \in \ker(f)$, meaning $f(x) = f(y) = e_G$, then

$$f(xy^{-1}) = f(x)f(y)^{-1} = e_G.$$

This shows that if $x, y \in \ker(f)$ then $xy^{-1} \in \ker(f)$, so $\ker(f)$ is closed for taking inverses. By the Two-Step test, $\ker(f)$ is a subgroup of G.

(f) The center $\mathrm{Z}(G)$ is the kernel of the permutation representation $G \to \mathrm{Perm}(G)$ for the conjugation action, so $\mathrm{Z}(G)$ is a subgroup of G since the kernel of a homomorphism is a subgroup. □

Example 3.8. For any field F, the **special linear group**

$$\mathrm{SL}_n(F) := \{A \mid A = n \times n \text{ matrix with entries in } F, \det(A) = 1_F\}$$

is a subgroup of the general linear group $\mathrm{GL}_n(F)$. To prove this, note that $\mathrm{SL}_n(F)$ is the kernel of the determinant map $\det\colon \mathrm{GL}_n(F) \to F^\times$, which is one of the homomorphisms in Example 1.72. By Lemma 3.7, this implies that $\mathrm{SL}_n(F)$ is indeed a subgroup of $\mathrm{GL}_n(F)$.

Definition 3.9. Let $f\colon G \to H$ be a group homomorphism and $K \leq H$. The **preimage** of K if given by

$$f^{-1}(K) := \{g \in G \mid f(g) \in K\}$$

Exercise 12. Prove that if $f : G \to H$ is a group homomorphism and $K \leq H$, then the preimage of K is a subgroup of G.

Exercise 13. Let G be a group and $a \in G$. Let

$$C_G(a) := \{x \in G \mid xa = ax\}.$$

Prove that $C_G(a)$, called the **centralizer** of a in G, is a subgroup of G.

Exercise 14. The set of rotational symmetries $\{r^i \mid i \in \mathbb{Z}\} = \{\mathrm{id}, r, r^2, \ldots, r^{n-1}\}$ of P_n is a subgroup of D_n.

In fact, this is the subgroup generated by r.

Definition 3.10. Given a group G and a subset X of G, the **subgroup of G generated by X** is

$$\langle X \rangle := \bigcap_{\substack{H \leq G \\ H \supseteq X}} H.$$

If $X = \{x\}$ is a set with one element, then we write $\langle X \rangle = \langle x \rangle$ and we refer to this as the **cyclic subgroup generated by** x. More generally, when $X = \{x_1, \ldots, x_n\}$ is finite, we may write $\langle x_1, \ldots, x_n \rangle$ instead of $\langle X \rangle$. Finally, given two subsets X and Y of G, we may sometimes write $\langle X, Y \rangle$ instead of $\langle X \cup Y \rangle$.

Remark 3.11. Note that by Lemma 3.7, $\langle X \rangle$ really is a subgroup of G. By definition, the subgroup generated by X is the smallest (with respect to containment) subgroup of G that contains X, meaning that $\langle X \rangle$ is contained in any subgroup that contains X.

Remark 3.12. Do not confuse this notation with giving generators and relations for a group; here we are forgoing the relations and focusing only on writing a list of generators. Another key difference is that we have picked elements in a given group G, but the subgroup they generate might not be G itself, but rather some other subgroup of G.

Lemma 3.13. *For a subset X of G, the elements of $\langle X \rangle$ can be described as:*

$$\langle X \rangle = \left\{ x_1^{j_1} \cdots x_m^{j_m} \mid m \geqslant 0, j_1, \ldots, j_m \in \mathbb{Z} \text{ and } x_1, \ldots, x_m \in X \right\}.$$

Note that the product of no elements is by definition the identity.

Proof. Let

$$S = \left\{ x_1^{j_1} \cdots x_m^{j_m} \mid m \geqslant 0, j_1, \ldots, j_m \in \mathbb{Z} \text{ and } x_1, \ldots, x_m \in X \right\}.$$

Since $\langle X \rangle$ is a subgroup that contains X, it is closed under products and inverses, and thus must contain all elements of S. Thus $X \supseteq S$.

To show $X \subseteq S$, we will prove that the set S is a subgroup of G using the One-step test:

- $S \neq \emptyset$ since we allow $m = 0$ and declare the empty product to be e_G.
- Let a and b be elements of S, so that they can be written as $a = x_1^{j_1} \cdots x_m^{j_m}$ and $b = y_1^{i_1} \cdots y_n^{i_n}$. Then

$$ab^{-1} = x_1^{j_1} \cdots x_m^{j_m} (y_1^{i_1} \cdots y_n^{i_m})^{-1} = x_1^{j_1} \cdots x_m^{j_m} y_n^{-i_n} \cdots y_1^{-i_1} \in S.$$

Therefore, $S \leq G$ and $X \subseteq S$ (by taking $m = 1$ and $j_1 = 1$) and by the minimality of $\langle X \rangle$ we conclude that $\langle X \rangle \subseteq S$. □

Example 3.14. Lemma 3.13 implies that for an element x of a group G, $\langle x \rangle = \{x^j \mid j \in \mathbb{Z}\}$.

Example 3.15. We showed in Theorem 1.63 that $D_n = \langle r, s \rangle$, so D_n is the subgroup of D_n generated by $\{r, s\}$. But do not mistake this for a presentation with no relations! In fact, these generators satisfy lots of relations, such as $srs = r^{-1}$, which we proved in Lemma 1.61.

Example 3.16. For any $n \geqslant 1$, we proved in Problem Set 2 that S_n is generated by the collection of adjacent transpositions $(i \quad i+1)$.

Theorem 3.17 (Cayley's Theorem)**.** *Every finite group is isomorphic to a subgroup of S_n.*

Proof. Suppose G is a finite group of order n and label the group elements of G from 1 to n in any way you like. The left regular action of G on itself determines a permutation representation $\rho \colon G \to \mathrm{Perm}(G)$, which is injective. Note that since G has n elements, $\mathrm{Perm}(G)$ is the group of permutations on n elements, and thus $\mathrm{Perm}(G) \cong S_n$. By Lemma 3.7, $\mathrm{im}(\rho)$ is a subgroup of S_n. If we restrict ρ to its image, we get an isomorphism $\rho \colon G \to \mathrm{im}(\rho)$. Hence $G \cong \mathrm{im}(\rho)$, which is a subgroup of S_n. □

Remark 3.18. From a practical perspective, this is a nearly useless theorem. It is, however, a beautiful fact.

3.2 Subgroups vs isomorphism invariants

Some properties of a group G pass onto all its subgroups, but not all. In this section, we collect some facts examples illustrating some of the most important properties.

Theorem 3.19 (Lagrange's Theorem)**.** *If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.*

You will prove Lagrange's Theorem in the next problem set.

Example 3.20 (Infinite group with finite subgroup)**.** The group $\mathrm{SL}_2(\mathbb{R})$ is infinite, but the matrix

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

has order 2 and it generates the subgroup $\langle A \rangle = \{A, I\}$ with two elements.

Example 3.21 (Nonabelian group with abelian subgroup)**.** The dihedral group D_n, with $n \geqslant 3$, is nonabelian, while the subgroup of rotations (see Exercise 14) is abelian (for example, because it is cyclic; see Lemma 3.26 below).

To give an example of a finitely generated group with an infinitely generated group, we have to work a bit harder.

Example 3.22 (Finitely generated group with infinitely generated subgroup)**.** Consider the subgroup G of $\mathrm{GL}_2(\mathbb{Q})$ generated by

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

Let H be the subgroup of $\mathrm{GL}_2(\mathbb{Q})$ given by

$$H = \left\{ \begin{pmatrix} 1 & \frac{n}{2^m} \\ 0 & 1 \end{pmatrix} \in G \mid n, m \in \mathbb{Z} \right\}.$$

We leave it as an exercise to check that this is indeed a subgroup of $\mathrm{GL}_2(\mathbb{Q})$. Note that for all integers n and m we have

$$A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad B^m = \begin{pmatrix} 2^m & 0 \\ 0 & 1 \end{pmatrix},$$

and

$$B^{-m} A^n B^m = \begin{pmatrix} 1 & \frac{n}{2^m} \\ 0 & 1 \end{pmatrix} \in H.$$

Therefore, H is a subgroup of G, and in fact

$$H = \langle B^{-m} A^n B^m \mid n, m \in \mathbb{Z} \rangle.$$

While $G = \langle A, B \rangle$ is finitely generated by construction, we claim that H is not. The issue is that

$$\begin{pmatrix} 1 & \frac{a}{2^b} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \frac{c}{2^d} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{a}{2^b} + \frac{c}{2^d} \\ 0 & 1 \end{pmatrix},$$

so the subgroup generated by any finite set of matrices in H, say

$$\left\langle \begin{pmatrix} 1 & \frac{n_1}{2^{m_1}} \\ 0 & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & \frac{n_t}{2^{m_t}} \\ 0 & 1 \end{pmatrix} \right\rangle$$

does not contain

$$\begin{pmatrix} 1 & \frac{1}{2^N} \\ 0 & 1 \end{pmatrix} \in H$$

with $N = \max_i\{|m_i|\} + 1$. Thus H is infinitely generated.

In the previous example, we constructed a group with two generators that has an infinitely generated subgroup. We will see in the next section that we couldn't have done this with less generators; in fact, the subgroups of a cyclic group are all cyclic.

Below we collect some important facts about the relationship between finite groups and their subgroups, including some explained by the examples above and others which we leave as an exercise.

Order of the group:

- Every subgroup of a finite group is finite.
- There exist infinite groups with finite subgroups; see Example 3.20.
- Lagrange's Theorem: If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Orders of elements:

- If $H \subseteq G$, then the set of orders of elements of H is a subset of the set of orders of elements of G.

Abelianity:

- Every subgroup of an abelian group is abelian.
- There exist nonabelian groups with abelian subgroups; see Example 3.21.
- Every cyclic (sub)group is abelian.

Generators:

- There exist a finitely generated group G and a subgroup H of G such that H is not finitely generated; see Example 3.22.
- Every infinitely generated group has finitely generated subgroups.[1]
- Every subgroup of a cyclic group is cyclic; see Theorem 3.28.

[1]This one is a triviality: we are just noting that even if the group is infinitely generated, we can always consider the subgroup generated by our favorite element, which is, by definition, finitely generated.

3.3 Cyclic groups

Recall the definition of a cyclic group.

Definition 3.23. If G is a group a generated by a single element, meaning that there exists $x \in G$ such that $G = \langle x \rangle$, then G is a **cyclic group**.

Remark 3.24. Given a cyclic group G, we may be able to pick different generators for G. For example, $\mathbb{Z}$ is a cyclic group, and both 1 or -1 are a generator. More generally, for any element x in a group G

$$\langle x \rangle = \langle x^{-1} \rangle.$$

Example 3.25. The main examples of cyclic groups, in additive notation, are the following:

- The group $(\mathbb{Z}, +)$ is cyclic with generator 1 or -1.
- The group $(\mathbb{Z}/n, +)$ of congruences modulo n is cyclic, since it is for example generated by [1]. Below we will find all the choices of generators for this group.

In fact, we will later prove that up to isomorphism these are the *only* examples of cyclic groups.

Let us record some facts important facts about cyclic groups.

Lemma 3.26. *Every cyclic group is abelian.*

Lemma 3.27. *Let G be a group and $x \in G$. If $x^m = e$ then $|x|$ divides m.*

Theorem 3.28. *Let $G = \langle x \rangle$, where x has finite order n. Then*

(a) $|G| = |x| = n$ *and* $G = \{e, x, \ldots, x^{n-1}\}$.

(b) For any integer k, then $|x^k| = \frac{n}{\gcd(k,n)}$. *In particular,*

$$\langle x^k \rangle = G \iff \gcd(n, k) = 1.$$

(c) There is a bijection

$$\begin{array}{ccc} \{\text{divisors of } |G|\} & \longleftrightarrow & \{\text{subgroups of } G\} \\ d & \xmapsto{\Psi} & \langle x^{\frac{|G|}{d}} \rangle \\ |H| & \xleftarrow[\Phi]{} & H \end{array}$$

Thus all subgroups of G are cyclic, and there is a unique subgroup of each order.

Proof. (a) By Lemma 3.13, we know $G = \{x^i \mid i \in \mathbb{Z}\}$. Now we claim that the elements

$$e = x^0, x^1, \ldots, x^{n-1}$$

are all distinct. Indeed, if $x^i = x^j$ for some $0 \leqslant i < j < n$, then $x^{j-i} = e$ and $1 \leqslant j - i < n$, contradicting the minimality of the order n of x. In particular, this shows that $|G| \geqslant n$.

Now take any $m \in \mathbb{Z}$. By the Division Algorithm, we can write $m = qn + r$ for some integers q, r with $0 < r \leqslant n$. Then

$$x^m = x^{nq+r} = (x^n)^q x^r = x^r.$$

This shows that every element in G can be written in the form x^r with $0 \leqslant r < n$, so

$$G = \{x^0, x^1, \ldots, x^{n-1}\} \qquad \text{and} \qquad |G| = n.$$

(b) Let k be any integer. Set $y := x^k$ and $d := \gcd(n, k)$, and note that $n = da, k = db$ for some $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$. We have

$$y^a = x^{ka} = x^{dba} = (x^n)^b = e,$$

so $|y|$ divides a by Lemma 3.27. On the other hand, $x^{k|y|} = y^{|y|} = e$, so again by Lemma 3.27 we have n divides $k|y|$. Now

$$da = n \text{ divides } k|y| = db|y|$$

and thus

$$a \text{ divides } b|y|.$$

But $\gcd(a, b) = 1$, so we conclude that a divides $|y|$. Since $|y|$ also divides a and both a and $|y|$ are positive, we conclude that

$$|y| = a = \frac{n}{\gcd(k, n)}.$$

(c) Consider any subgroup H of G with $H \neq \{e\}$, and set

$$k := \min\{i \in \mathbb{Z} \mid i > 0 \text{ and } g^i \in H\}.$$

On the one hand, $H \supseteq \langle g^k \rangle$, since $H \ni g^k$ and H is closed for products. Moreover, given any other positive integer i, we can again write $i = kq + r$ for some integers q, r with $0 \leqslant r < k$, and

$$g^r = g^{i-kq} = g^i (g^k)^q \in H,$$

so by minimality of r we conclude that $r = 0$. Therefore, $k|r$, and thus we conclude that

$$H = \langle g^k \rangle.$$

Now to show that Ψ is a bijection, we only need to prove that Φ is a well-defined function and a two-sided inverse for Ψ, and this we leave as an exercise. □

There is a sort of quasi-converse to Theorem 3.28:

Exercise 15. Show that if G is a finite group G has a unique subgroup of order d for each positive divisor d of $|G|$, then G must be cyclic.

We can say a little more about the bijection in Theorem 3.28. Notice how smaller subgroups (with respect to containment) correspond to smaller divisors of G. We can make this observation rigorous by talking about partially ordered sets.

Definition 3.29. An **order relation** on a set S is a binary relation $\leq$ that satisfies the following properties:

- Reflexive: $s \leq s$ for all $s \in S$.
- Antisymmetric: if $a \leq b$ and $b \leq a$, then $a = b$.
- Transitive: if $a \leq b$ and $b \leq c$, then $a \leq c$.

A **partially ordered set** or **poset** consists of a set S endowed with an order relation $\leq$, which we might indicate by saying that the pair $(S, \leq)$ is a partially ordered set.

Given a poset $(S, \leq)$ and a subset $T \subseteq S$, an **upper bound** for T is an element $s \in S$ such that $t \leq s$ for all $t \in T$, while a **lower bound** is an element $s \in S$ such that $s \leq t$ for all $t \in T$. An upper bound s for T is called a **supremum** if $s \leq u$ for all upper bounds u of T, while a lower bound t for T is an **infimum** if $l \leq t$ for all lower bounds t for T. A **lattice** is a poset in which every two elements have a unique supremum and a unique infimum.

Remark 3.30. Note that the word *unique* can be removed from the definition of lattice. In fact, if a subset $T \subseteq S$ has a supremum, then that supremum is necessarily unique. Indeed, given two suprema s and t, then by definition $s \leq t$, since s is a supremum and t is an upper bound for T, but also $t \leq s$ since t is a supremum and s is an upper bound for T. By antisymmetry, we conclude that $s = t$.

Example 3.31. The set of all positive integers is a poset with respect to divisibility, setting $a \leq b$ whenever $a|b$. In fact, this is a lattice: the supremum of a and b is $\text{lcm}(a, b)$ and the infimum of a and b is $\gcd(a, b)$.

Example 3.32. Given a set S, the **power set** of S, meaning the set of all subsets of S, is a poset with respect to containment, where the order is defined by $A \leq B$ whenever $A \subseteq B$. In fact, this is a lattice: the supremum of A and B is $A \cup B$ and the infimum of A and B is $A \cap B$.

Exercise 16. Show that the set of all subgroups of a group G is a poset with respect to containment, setting $A \leq B$ if $A \subseteq B$.

Lemma 3.33. *The set of all subgroups of a group G is a lattice with respect to containment.*

Proof. Let A and B be subgroups of G. We need to prove that A and B have an infimum and a supremum. We claim that $A \cap B$ is the infimum and $\langle A, B \rangle$ is the supremum. First, these are both subgroups of G, by Lemma 3.7 in the case $A \cap B$ and by definition for the other. Moreover, $A \cap B$ is a lower bound for A and B and $\langle A, B \rangle$ is an upper bound by definition. Finally, if $H \leq A$ and $H \leq B$, then every element of h is in both A and B, and thus it must be in $A \cap B$, so $H \leq A \cap B$. Similarly, if $A \leq H$ and $B \leq H$, then $\langle A, B \rangle \subseteq H$. $\square$

Remark 3.34. The isomorphism Ψ in Theorem 3.28 satisfies the following property: if $d_1 \mid d_2$ then $\Psi(d_1) \subseteq \Psi(d_2)$. In other words, Ψ preserves the poset structure. This means that Ψ is a **lattice isomorphism** between the lattice of divisors of $|G|$ and the lattice of subgroups of G. Of course the inverse map $\Phi = \Psi^{-1}$ is also a lattice isomorphism.

Lemma 3.35 (Universal Mapping Property of a Cyclic Group)**.** *Let $G = \langle x \rangle$ be a cyclic group and let H be any other group.*

(1) If $|x| = n < \infty$, then for each $y \in H$ such that $y^n = e$, there exists a unique group homomorphism $f : G \to H$ such that $f(x) = y$.

(2) If $|x| = \infty$, then for each $y \in H$, there exists a unique group homomorphism $f : G \to H$ such that $f(x) = y$.

In both cases this unique group homomorphism is given by $f(x^i) = y^i$ for any $i \in \mathbb{Z}$.

Remark 3.36. We will later discuss a universal mapping property of any presentation. This is a particular case of that universal mapping property of a presentation, since a cyclic group is either presented by $\langle x \mid x^n = e \rangle$ or $\langle x \mid - \rangle$.

Proof. Recall that either $G = \{e, x, x^2, \ldots, x^{n-1}\}$ has exactly n elements if $|x| = n$ or $G = \{x^i \mid i \in \mathbb{Z}\}$ with no repetitions if $|x| = \infty$.

Uniqueness: We have already noted that any homomorphism is uniquely determined by the images of the generators of the domain in Remark 1.74, and that f must then be given by $f(x^i) = f(x)^i = y^i$.

Existence: In either case, define $f(x^i) = y^i$. We must show this function is a well-defined group homomorphism. To see that f is well-defined, suppose $x^i = x^j$ for some $i, j \in \mathbb{Z}$. Then, since $x^{i-j} = e_G$, using Lemma 3.27 we have

$$\begin{cases} n \mid i-j & \text{if } |x| = n \\ i - j = 0 & \text{if } |x| = \infty \end{cases} \implies \begin{cases} y^{i-j} = y^{nk} & \text{if } |x| = n \\ y^{i-j} = y^0 & \text{if } |x| = \infty \end{cases} \implies y^{i-j} = e_H \implies y^i = y^j.$$

Thus, if $x^i = x^j$ then $f(x^i) = y^i = y^j = f(x^j)$. In particular, if $x^k = e$, then $f(x^k) = e$, and f is well-defined.

The fact that f is a homomorphism is immediate:

$$f(x^i x^j) = f(x^{i+j}) = y^{i+j} = y^i y^j = f(x^i) f(x^j). \qquad \square$$

Definition 3.37. The **infinite cyclic group** is the group

$$C_\infty := \{a^i | i \in \mathbb{Z}\}$$

with multiplication $a^i a^j = a^{i+j}$.

For any natural number n, the **cyclic group of order** n is the group

$$C_n := \{a^i | i \in \{0, \ldots, n-1\}\}$$

with multiplication $a^i a^j = a^{i+j \pmod n}$.

Remark 3.38. The presentations for these groups are

$$C_\infty = \langle a \mid - \rangle \qquad \text{and} \qquad C_n = \langle a \mid a^n = e \rangle.$$

Theorem 3.39 (Classification Theorem for Cyclic Groups)**.** *Every infinite cyclic group is isomorphic to C_∞. Every cyclic group of order n is isomorphic to C_n.*

Proof. Suppose $G = \langle x \rangle$ with $|x| = n$ or $|x| = \infty$, and set

$$H = \begin{cases} C_n & \text{if } |x| = n \\ C_\infty & \text{if } |x| = \infty. \end{cases}$$

By Lemma 3.35, there are homomorphisms $f : G \to H$ and $g : G \to H$ such that $f(x) = a$ and $g(a) = x$. Now $g \circ f$ is an endomorphisms of G mapping x to x. But the identity map also has this property, and so the uniqueness clause in Lemma 3.35 gives us $g \circ f = \mathrm{id}_G$. Similarly, $f \circ g = \mathrm{id}_H$. We conclude that f and g are isomorphisms. □

Example 3.40. For a fixed $n \geqslant 1$,

$$\mu_n := \{z \in \mathbb{C} \mid z^n = 1\}$$

is a subgroup of $(\mathbb{C} \setminus \{0\}, \cdot)$. Since $\|z^n\| = \|z\|^n = 1$ for any $z \in \mu_n$, then we can write $z = e^{ri}$ for some real number r. Moreover, the equality $1 = z^n = e^{nri}$ implies that nr is an integer multiple of 2π. It follows that

$$\mu_n = \{1, e^{2\pi i/n}, e^{4\pi i/n}, \cdots, e^{(n-1)2\pi i/n}\}$$

and that $e^{2\pi i/n}$ generates μ_n. Thus μ_n is cyclic of order n. This group is therefore isomorphic to C_n, via the map

$$\begin{array}{ccc} C_n & \longrightarrow & \mu_n \\ a^j & \longmapsto & {}^{2j\pi i/n}. \end{array}$$

Chapter 4

Quotient groups

Recall from your undergraduate algebra course the construction for the integers modulo n: one starts with an equivalence relation $\sim$ on $\mathbb{Z}$, considers the set $\mathbb{Z}/n$ of all equivalence classes with respect to this equivalence relation, and verifies that the operations on $\mathbb{Z}$ give rise to well defined binary operations on the set of equivalence classes.

This idea still works if we replace $\mathbb{Z}$ by an arbitrary group, but one has to be somewhat careful about what equivalence relation is used.

4.1 Equivalence relations on a group and cosets

Let G be a group and consider an equivalence relation $\sim$ on G. Let $G/\sim$ denote the set of equivalence classes for $\sim$ and write $[g]$ for the equivalence class that the element $g \in G$ belongs to, that is

$$[x] := \{g \in G \mid g \sim x\}.$$

When does $G/\sim$ acquire the structure of a group under the operation

$$[x] \cdot [y] := [xy] \ ?$$

Right away, we should be worried about whether this operation is well-defined, meaning that it is independent of our choice of representatives for each class. That is, if $[x] = [x']$ and $[y] = [y']$ then must $[xy] = [x'y']$? In other words, if $x \sim x'$ and $y \sim y'$, must $xy \sim x'y'$?

Definition 4.1. We say an equivalence relation $\sim$ on a group G is **compatible with multiplication** if $x \sim y$ implies $xz \sim yz$ and $zx \sim zy$ for all $x, y, z \in G$.

Lemma 4.2. *For a group G and equivalence relation $\sim$, the rule $[x]\cdot[y] = [xy]$ is well-defined and makes $G/\sim$ into a group if and only if $\sim$ is compatible with multiplication.*

Proof. To say that the rule $[x] \cdot [y] = [xy]$ is well-defined is to say that for all $x, x', y, y' \in G$ we have

$$[x] = [x'] \text{ and } [y] = [y'] \implies [x][y] = [x'][y'].$$

So $[xy] = [x'y']$ if and only if whenever $x \sim x'$ and $y \sim y'$, then $xy \sim x'y'$.

Assume $\sim$ is compatible with multiplication. Then $x \sim x'$ implies $xy \sim x'y$ and $y \sim y'$ implies $x'y \sim x'y'$, hence by transitivity $xy \sim x'y'$. Thus $[x] \cdot [y] = [xy]$ is well-defined.

Conversely, assume the rule $[x] \cdot [y] = [xy]$ is well-defined, so that

$$[x] = [x'] \text{ and } [y] = [y'] \implies [x][y] = [x'][y'].$$

Setting $y = y'$ gives us

$$x \sim x' \implies xy \sim x'y.$$

Setting $x = x'$ gives us

$$y \sim y' \implies xy \sim xy'.$$

Hence $\sim$ is compatible with multiplication.

So now assume that the multiplication rule is well-defined, which we have now proved is equivalent to saying that $\sim$ is compatible with the multiplication in G. We need to prove that $G/\sim$ really is a group. Indeed, since G itself is a group then given any $x, y, z \in G$ we have

$$[x] \cdot ([y] \cdot [z]) = [x] \cdot [yz] = [x(yz)] = [(xy)z] = [xy][z] = ([x][y])[z]$$

Moreover, for all $x \in G$ we have

$$[e_G][x] = [e_G x] = [x] \qquad \text{and} \qquad [x][e_G] = [xe_G] = [x],$$

so that $[e_G]$ is an identity for $G/\sim$. Finally,

$$[x][x^{-1}] = [e_G] = e_{G/\sim},$$

so that every element in $G/\sim$ has an inverse; in fact, this shows that $[x]^{-1} = [x^{-1}]$. □

Definition 4.3. Let G be a group and let $\sim$ be an equivalence relation on G that is compatible with multiplication. The **quotient group** is the set $G/\sim$ of equivalence classes, with group multiplication $[x] \cdot [y] = [xy]$.

Example 4.4. Let $G = \mathbb{Z}$ and fix an integer $n \geqslant 1$. Let $\sim$ be the equivalence relation given by congruence modulo n, so $\sim = \equiv \pmod{n}$. Then

$$(\mathbb{Z}, +)/\sim = (\mathbb{Z}/n, +).$$

But how do we come up with equivalence relations that are compatible with the group law?

Definition 4.5. Let H be a subgroup of a group G. The **left action of H on G** is given by

$$h \cdot g = hg \quad \text{for} h \in H, g \in G.$$

The equivalence relation $\sim_H$ on G induced by the left action of H is given by

$$g \sim_H g' \text{ if and only if } g' = hg \text{ for some } n \in H.$$

The equivalence class of $g \in G$, also called the orbit of g, and also called the **right coset** of H in G containing g is

$$Hg := \{hg \mid h \in H\}.$$

There is also a **left coset** of N in G containing g, defined by

$$gH := \{gh \mid h \in H\}.$$

Example 4.6. Let $G = \mathbb{Z}$ and $H = \langle n \rangle = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$. Then

$$x \sim_{n\mathbb{Z}} y \iff x = y + nk \text{ for some } k \in \mathbb{Z} \iff x \equiv y \pmod{n}.$$

Therefore the equivalence relation $\sim_{n\mathbb{Z}}$ is the same as congruence modulo n and the right and left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are the congruence classes of integers modulo n.

Index

$C_G(a)$, 29
C_∞, 36
C_n, 36
D_n, 12
$G/\sim$, 39
$H \leq G$, 27
$H < G$, 27
Q_8, 17
$[n]$, 6
$\mathrm{Aut}(G)$, 18
$\mathrm{Orb}_G(s)$, 24
$\ker(f)$, 20
$\sim_H$, 39
f^{-1} (for a homomorphism f), 29
m-cycle, 6

abelian group, 4
action, 23
action by conjugation, 26
action of a group on a set, 23
automorphism, 18

binary operation, 2

c, 26
Cayley's Theorem, 30
center of a group, 5
centralizer, 29
compatible with multiplication (for an equivalence relation), 38
conjugation action, 26
cycle, 6
cycle type, 9
cyclic group, 5, 33
cyclic group of order n, 36
cyclic subgroup generated by an element, 29

dihedral group, 12

even permutation, 11

faithful action, 25

generators for a group, 5
group, 2
group homomorphism, 18
group isomorphism, 18

homomorphism (of groups), 18

identity, 2
identity element, 2
image, 20
infimum, 35
infinite cyclic group, 36
inverse, 2
isometry, 12
isomorphic groups, 18
isomorphism, 18
isomorphism (of groups), 18
isomorphism invariant, 21

kernel, 20
kernel of a group homomorphism, 20

Lagrange's Theorem, 31
lattice, 35
lattice isomorphism, 36
left action of a subgroup, 39
left coset, 39
left inverse, 3
left regular action, 26
length of a cycle, 6
lower bound, 35

monoid, 3

nontrivial subgroup, 27

orbit (of an action), 24
order of a group, 2
order relation, 35

parity of a permutation, 11
partially ordered set, 35
permutation group of a set X, 6
permutation on n symbols, 6
permutation representation, 24
poset, 35
power set, 35
preimage of a homomorphism, 29
presentation of a group, 5

quaternion group, 17
quotient group, 39

reflections of D_n, 13
relations for a group, 5
right coset, 39
right inverse, 3
rotations of D_n, 13

special linear group, 29
subgroup, 27
subgroup generated by a set, 29
supremum, 35
symmetry, 12

transitive action, 25
transposition, 7
trivial action, 26
trivial center, 5
trivial group, 4
trivial homomorphism, 18
trivial subgroups, 27

upper bound, 35