Introduction to Modern Algebra I

Math 817 Fall 2024

August 30, 2024

Contents

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 $(F^\times, \cdot)$.

Informal definition 1.16. 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 1.17. 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 1.18. The group $\mathbb{Z}$ has one generator, the element 1, which satisfies no relations.

Example 1.19. 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 1.20. A group G is called **cyclic** if it is generated by a single element.

Example 1.21. 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 1.22. 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 1.23. 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 1.24. 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 1.25. 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 1.26. A 1-cycle is the identity permutation.

Notation 1.27. A 2-cycle is often called a **transposition**.

Remark 1.28. 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 1.29. Consider the m-cycle $\sigma = (i_1 \dots i_m)$. Then for any k, we have

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

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 1.30. 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 1.31. 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

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

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 1.32. *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 1.33. *Each $\sigma \in S_n$ can be written as a product of disjoint cycles, and such a factorization is unique up to the ordering of the factors.*

Remark 1.34. For the uniqueness part of Theorem 1.33, 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 1.32, 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 1.35. 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 1.36. 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 1.37. 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:

Corollary 1.38. *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 1.33. 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. □

Remark 1.39. Note however that when we write a permutation as a product of transpositions, such a product is no longer necessarily unique.

Exercise 6. Show that

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

Example 1.40. 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 1.41. *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 1.40, 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 1.42. 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 1.41 tells us that the sign of a permutation is well-defined.

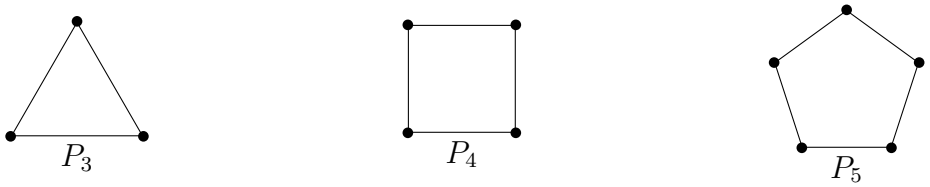
Example 1.43. The identity permutation is even. Every transposition is odd.

Example 1.44. 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 1.45. The **dihedral group** D_{2n} is the group of symmetries of P_n.

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:

Definition 1.46. The **dihedral group** D_{2n} is the set of symmetries of the regular n-gon P_n equipped with the binary operation given by composition.

Remark 1.47. Let us informally verify that this really is a group. If f and g are in D_{2n}, then $f \circ g$ is an isometry (since the composition of any two isometries is again an isometry) and

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

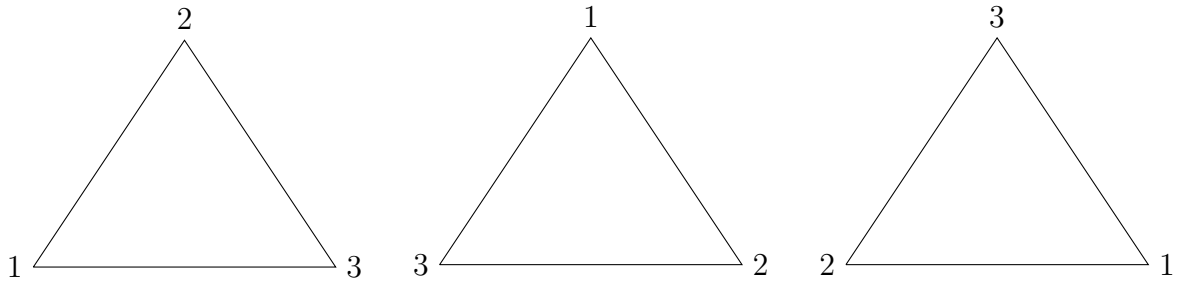
so that $f \circ g \in D_{2n}$. This proves composition is a binary operation on D_{2n}. Now note that associativity of composition is a general property of functions. The identity function on $\mathbb{R}^2$, denoted $\mathrm{id}_{\mathbb{R}^2}$, belongs to D_{2n} and it is the identity element of D_{2n}.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

We will see very soon that the index $2n$ in D_{2n} corresponds to the number of elements of this group (symmetries of P_n). First, we introduce the elements of the dihedral group:

Definition 1.48 (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. If r denotes rotation about the origin by $\frac{2\pi}{n}$ radians counterclockwise, then $r \in D_{2n}$. Its inverse is the clockwise rotation by $\frac{2\pi}{n}$. This gives us rotations r^i, where r^i is the clockwise rotation by $\frac{2\pi i}{n}$, for each $i = 1, \ldots, n$. Notice that when $i = n$ this is simply the identity map.

As we will soon see, 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 1.49. Here are the rotations of D_3:

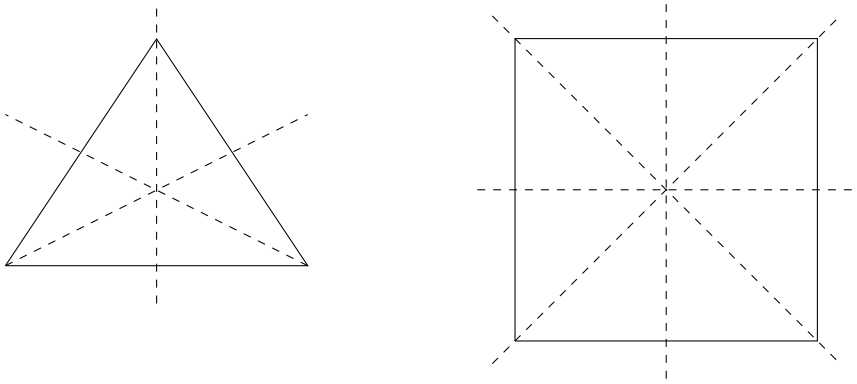


The identity | Rotation by $\frac{2\pi}{3}$ | Rotation by $\frac{4\pi}{3}$

Definition 1.50 (Reflections in D_n)**.** For any line of symmetry of P_n, reflection about that line gives an element of D_{2n}. 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 1.51.



The reflection lines in D_3 | The reflection lines in D_4

Notation 1.52. Fix $n \geqslant 3$. We will consider two special elements of D_n:

- Let r denote the symmetry of P_n given by clockwise 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 1.50. 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 clockwise from V_1.

From now on, whenever we are talking about D_{2n}, the letters r and s will refer only to these specific elements.

Finally, to show that D_n has exactly $2n$ elements, we will need the following elementary fact, which we leave as an exercise:

Lemma 1.53. *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 1.53.

Theorem 1.54. *The dihedral group D_{2n} has $2n$ elements.*

Proof. First, we show that D_{2n} has order at most $2n$. Any element $\sigma \in D_{2n}$ 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 1.53, 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_{2n}.

Now we need only to present $2n$ distinct elements in D_{2n}. We have described n reflections and n rotations for D_{2n}; 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 clockwise through each adjacent vertex, then the rotation by an angle of $\frac{2\pi i}{n}$ sends 1 to $i+1$ for each $i < n$. 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. □

Lemma 1.55. *Following Notation 1.52, 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. It follows that rs fixes the point $P = \frac{V_1+V_2}{2}$, which is the midpoint of the line segment joining V_1 to V_2. Since rs also fixes the center of P_n, then rs must be either the identity or a reflection across the line joining the origin and P. It cannot be the identity since it sends V_1 to V_2. Since rs is a reflection, we have $rsrs = (rs)^2 = e$ and hence $srs = r^{-1}$. □

Theorem 1.56. *Every element in D_{2n} can be written uniquely as r^j or $r^j s$ for $0 \leqslant j \leqslant n-1$.*

Notice that we have shown that D_{2n} has exactly $2n$ elements, and that there are $2n$ such expressions, and thus the uniqueness portion of the statement follows immediately once we show existence.

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. Hence either $r^{-j}\alpha = \mathrm{id}$ or $r^{-j}\alpha = s$. We conclude that $\alpha = r^j$ or $\alpha = r^j s$, proving the first assertion. □

Remark 1.57. First, 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 $i = j$.

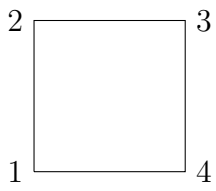
Remark 1.58. The elements $e, r, \ldots, r^{n-1}$ are rotations, and thus preserve orientation, while the elements $s, rs, \ldots, r^{n-1}$ are reflections since they reverse orientation.

Let us prove that the group described abstractly by the presentation

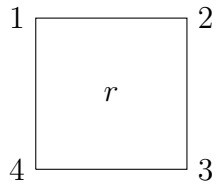
$$\langle r, s \mid r^n = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle$$

is D_{2n}. Here $1 = 1_{\mathbb{R}^2}$ is the identity map on $\mathbb{R}^2$.

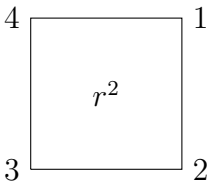
Example 1.59. The 8 elements of $D_{2\times 4}$, the group of symmetries of the square, are



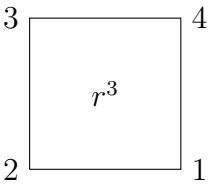
The identity



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

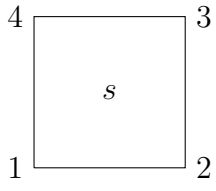


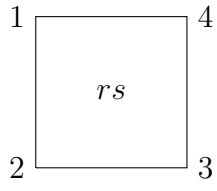
Rotation by $\frac{4\pi}{4} = \pi$

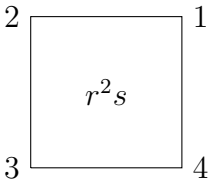


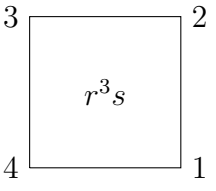
Rotation by $\frac{6\pi}{4} = \frac{3\pi}{2}$

and









Theorem 1.60. *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 $D_{2n} = X_{2n}$, that is,

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

Proof. Theorem 1.56 shows that $\{r, s\}$ is a set of generators for D_{2n}. 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 1.55. The only concern we need to deal with is that we

may not have discovered all the relations of D_{2n}; 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_{2n} has more relations than X_{2n} does. Then D_{2n} would be a group of cardinality strictly smaller than X_{2n}, meaning that $|D_{2n}| < |X_{2n}|$. [1] We will show below that in fact $|X_{2n}| \leqslant 2n = |D_{2n}|$, 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_{2n}. □

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_{2n}, we know from Theorem 1.56 that it has exactly $2n$ elements.

1.4 The quaternions

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

[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.

Definition 1.61. 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.

Index