Introduction to Modern Algebra I

Math 817 Fall 2024

November 10, 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 heavily based on notes by Mark Walker and Alexandra Seceleanu. Thanks to Gabriel Adams, Cal Heldt, and Reese White, who found typos in previous versions of the notes.

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

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

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 $x, y, z, a_1, \dots, a_n \in G$. 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) $(a_1 \dots a_n)^{-1} = a_n^{-1} \dots a_1^{-1}$.

(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. A group G is **finitely generated** if it is generated by finitely many elements.

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

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

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. $\square$

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 $(-1)^s$. 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.

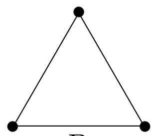
Example 1.46. The identity permutation is even. Every transposition is odd.

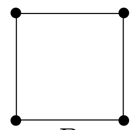
Example 1.47. The 3-cycle (123) can be rewritten as (12)(23), a product of 2 transpositions, so the sign of (123) is 1.

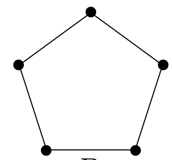
Exercise 8. Show that every permutation is a product adjacent transpositions, meaning transpositions of the form $(i \quad i+1)$.

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:


P_3


P_4


P_5

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:

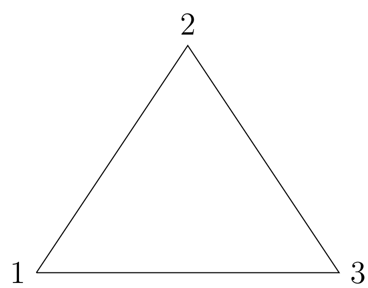
Lemma 1.51. *Every point on a regular polygon is completely determined, among all points on the polygon, by its distances to two adjacent vertices of the polygon.*

Exercise 9. Prove Lemma 1.51.

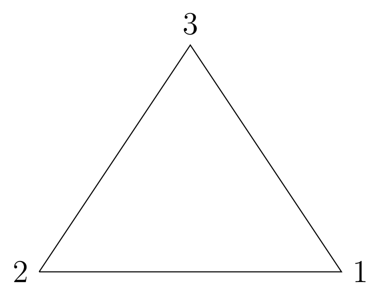
Definition 1.52 (Rotations in D_n)**.** Assume that the regular n-gon P_n is drawn in the plane with its center at the origin and one vertex on the x axis. Let r denote the rotation about the origin by $\frac{2\pi}{n}$ radians counterclockwise; this is an element of D_n. Its inverse is the clockwise 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.

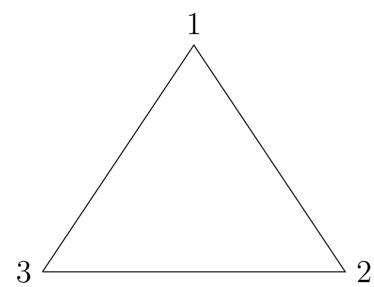
Example 1.53. Here are the rotations of D_3:



The identity



Rotation by $\frac{2\pi}{3}$

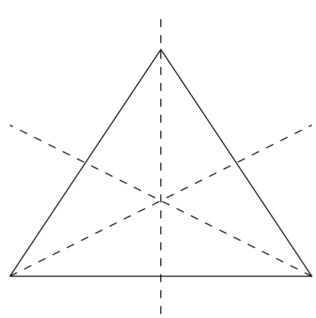


Rotation by $\frac{4\pi}{3}$

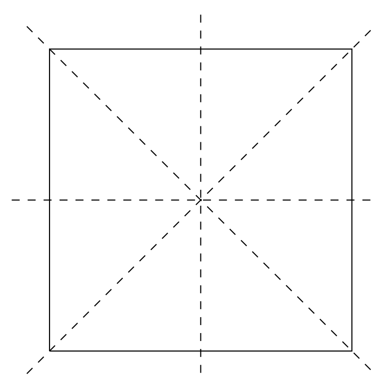
Definition 1.54 (Reflections in D_n)**.** For any line of symmetry of P_n, reflection about that line gives an element of D_n. When n is odd, the line connecting a vertex to the midpoint of the opposite side of P_n is a line of symmetry. When n is even, there are two types of reflections: the ones about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

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, $s^2 = \text{id}$.

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 $r^n = \text{id}$ and that the rotations $\text{id}, r, r^2, \ldots, r^{n-1}$ 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 $rsrs = (rs)^2 = \text{id}$ 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

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

Exercise 10. Show that $sr^i s^{-1} = r^{n-i}$ for all i.

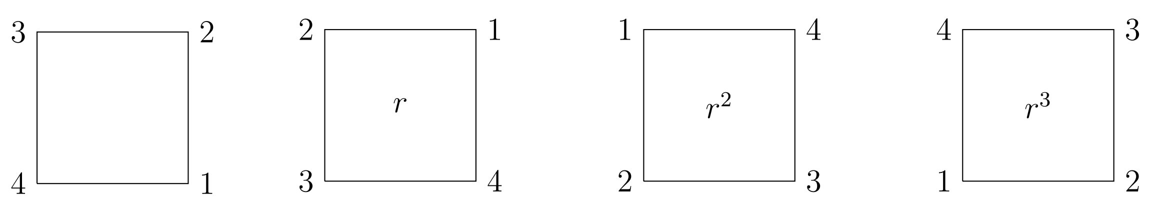
Theorem 1.63. *Every element in* D_n *can be written uniquely as* r^j *or* $r^j s$ *for* $0 \leqslant j \leqslant n-1$.

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 $r^{-j}\alpha = \text{id}$ 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. □

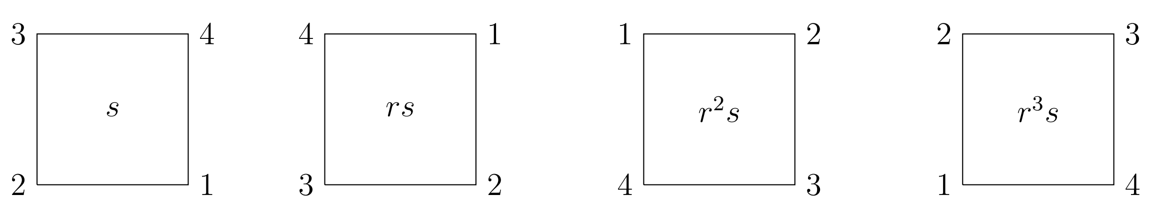
Remark 1.64. The elements $s, rs, \ldots, r^{n-1}$ are all reflections since they reverse orientation. Alternatively, we can check these are all reflections by checking they have order 2. As we noted before, the elements $\text{id}, r, \ldots, r^{n-1}$ are rotations, and preserve orientation.

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

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

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 $(xy)z = x(yz)$. $\square$

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 11. 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

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

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

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

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,

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

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 $f\colon G \to H$ 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 $f\colon G \longrightarrow H$ 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 $f\colon G \longrightarrow G$ is

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

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

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

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

Remark 1.77. Given any group homomorphism $f\colon G \longrightarrow G$, 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 $g = h$. $\square$

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. $\square$

Exercise 12. 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 12: 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

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

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

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

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

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

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

is a well-defined homomorphism of groups.

(2) Conversely, if $\rho : G \to \operatorname{Perm}(S)$ 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 $\operatorname{Orb}_G(s) = \operatorname{Orb}_G(t)$ or $\operatorname{Orb}_G(s) \cap \operatorname{Orb}_G(t) = \emptyset$.

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

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 $s_1, \dots, s_k$ be a complete set of orbit representatives — that is, assume each orbit contains exactly one member of the list $s_1, \dots, s_k$. Then*

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

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

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

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,

$$\begin{aligned} g \in \ker\rho \iff g \cdot x = x \text{ for all } x \in G \iff gxg^{-1} = x \text{ for all } x \in G \\ \iff gx = xg \text{ for all } x \in G \iff g \in \mathrm{Z}(G). \end{aligned}$$

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 $xy \in H$.

Remark 3.3. Let H be a subgroup of G. Since H itself is a group, it has an identity element e_H, and thus

$$e_H e_H = e_H$$

in H. But the product in H is just a restriction of the product of G, so this equality also holds in G. Multiplying by e_H^{-1}, we conclude that $e_H = e_G$.

In summary, if H is any subgroup of G, then we must have $e_G \in H$.

Example 3.4. 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 3.5. The group $\mathbb{Z}/2$ has no nontrivial subgroup.

Example 3.6. 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 3.7 (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. $\square$

Lemma 3.8 (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 $\mathrm{im}(f)$ must also be nonemtpy; for example, it contains $f(e_G) = e_H$. If $x, y \in \mathrm{im}(f)$, then $x = f(a)$ and $y = f(b)$ for some $a, b \in G$, and hence

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

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

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

Example 3.9. 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 3.8, this implies that $\mathrm{SL}_n(F)$ is indeed a subgroup of $\mathrm{GL}_n(F)$.

Definition 3.10. Let $f : G \to H$ 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 13. 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 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 3.11. 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 3.12. Note that by Lemma 3.8, $\langle X\rangle$ 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 3.13. 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 3.14. *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 $\langle X\rangle \subseteq S$. $\square$

Example 3.15. Lemma 3.14 implies that for an element x of a group G, $\langle x\rangle = \{x^j \mid j \in \mathbb{Z}\}$.

Example 3.16. 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 3.17. 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 3.18 (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 3.8, $\mathrm{im}(\rho)$ 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. $\square$

Remark 3.19. 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 3.20 (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.

Exercise 15. Let G be a finite group Suppose that A and B are subgroups of G such that $\gcd(|A|, |B|) = 1$. Show that $A \cap B = \{e\}$.

Example 3.21 (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 3.22 (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 3.27 below).

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

Example 3.23 (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 3.21.
- 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 3.22.
- 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 3.23.
- Every infinitely generated group has finitely generated subgroups.[1]
- Every subgroup of a cyclic group is cyclic; see Theorem 3.29.

[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 3.24. 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 3.25. 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 3.26. 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 which you have proved in problem sets:

Lemma 3.27. *Every cyclic group is abelian.*

Lemma 3.28. *Let G be a group and $x \in G$. If $x^m = e$ then $|x|$ divides m.*

Now we can use these to say more about cyclic groups.

Theorem 3.29. *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

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

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

Proof. (a) By Lemma 3.14, 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 3.28. On the other hand, $x^{k|y|} = y^{|y|} = e$, so again by Lemma 3.28 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. $\square$

Corollary 3.30. *Let G be any finite group and consider $x \in G$. Then $|x|$ divides $|G|$.*

Proof. The subgroup $\langle x \rangle$ of G generated by x is a cyclic group, and since G is finite so is $\langle x \rangle$. By Theorem 3.29, $|x| = |\langle x \rangle|$, and by Lagrange's Theorem 3.20, the order of $\langle x \rangle$ divides the order of G. □

There is a sort of quasi-converse to Theorem 3.29:

Exercise 16. 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 3.29. 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 3.31. 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 3.32. 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 3.33. 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 $\operatorname{lcm}(a, b)$ and the infimum of a and b is $\gcd(a, b)$.

Example 3.34. 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 17. 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 3.35. *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 3.8 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 3.36. The isomorphism Ψ in Theorem 3.29 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 3.37 (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 $f\colon G \to H$ such that $f(x) = y$.

(2) If $|x| = \infty$, then for each $y \in H$, there exists a unique group homomorphism $f\colon G \to H$ 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 3.38. 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 3.28 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 3.39. 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

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

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

Remark 3.40. 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 3.41 (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 3.37, 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 3.37 gives us $g \circ f = \mathrm{id}_G$. Similarly, $f \circ g = \mathrm{id}_H$. We conclude that f and g are isomorphisms. $\square$

Example 3.42. 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

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

Exercise 18. Let $p > 0$ be a prime. Show that every group of order p is cyclic.

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

$$a \sim_H b \text{ if and only if } b = ha \text{ for some } h \in H.$$

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 H 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.

Lemma 4.7. *Let $H \leq G$. The following facts about left cosets are equivalent for $x, y \in G$:*

1. *The elements x and y belong to the same left coset of H in G.*
2. *$x = yh$ for some $h \in H$.*
3. *$y = xh$ for some $h \in H$.*
4. *$y^{-1}x \in H$.*
5. *$x^{-1}y \in H$.*
6. *$xH = yH$.*

Analogously, the following facts about right cosets are equivalent for all $x, y \in G$:

1. *The elements x and y belong to the same right coset of H in G.*
2. *There exists $h \in H$ such that $x = hy$.*
3. *There exists $h \in H$ such that $y = hx$.*
4. *We have $yx^{-1} \in H$.*
5. *We have $xy^{-1} \in H$.*
6. *We have $Hx = Hy$.*

Proof. We will only prove the statements about left cosets, since the statements about right cosets are analogous.

(1. $\Rightarrow$ 2.) Suppose that x and y belong to the same left coset gH of H in G. Then $x = ga$ and $y = gb$ for some $a, b \in H$, so $g = yb^{-1}$ and therefore $x = yb^{-1}h = ya$ where $h = b^{-1}a \in H$.

(2. $\Leftrightarrow$ 3.) We have $x = yh$ for some $h \in H$ if and only if $y = xh^{-1}$ and $h^{-1} \in H$.

(2. $\Leftrightarrow$ 4.) We have $x = yh$ for some $h \in H$ if and only if $y^{-1}x = h \in H$.

(4. $\Leftrightarrow$ 5.) Note that $y^{-1}x \in H \Leftrightarrow (y^{-1}x)^{-1} \in H \iff x^{-1}y \in H$.

(2. $\Rightarrow$ 6.) Suppose $x = ya$ for some $a \in H$. Then by 2. $\Rightarrow$ 3. we also have $y = xb$ for some $b \in H$. Note that for all $h \in H$, we also have $ah \in h$ and $bh \in H$. Then

$$xH = \{xh \mid h \in H\} = \{y\underbrace{(ah)}_{\in H} \mid h \in H\} \subseteq yH$$

and

$$yH = \{yh \mid h \in H\} = \{x\underbrace{(bh)}_{\in H} \mid h \in H\} \subseteq xH.$$

Therefore, $xH = yH$.

(6. $\Rightarrow$ 1.) Since $e_G = e_H \in H$, we have $x = xe_G \in xH$ and $y = ye_G \in yH$. If $xH = yH$ then, x and y belong to the same left coset. □

Remark 4.8. Note that Lemma 4.7 says in particular that $\sim_H$ is compatible with multiplication.

Lemma 4.9. *For $H \leq G$, the collection of left cosets of H in G form a partition of G, and similarly for the collection of right cosets:*

$$\bigcup_{x \in G} xH = G$$

and for all $x, y \in G$, either $xH = yH$ or $xH \cap yH = \emptyset$.

The analogous statement for right cosets also holds. Moreover, all left and right cosets have the same cardinality: for any $x \in G$,

$$|xH| = |Hx| = |H|.$$

Proof. Since the left (respectively, right) cosets are the equivalence classes for an equivalence relation, the first part of the statement is just a special case of a general fact about equivalence relation.

Let us nevertheless write a proof for the assertions for right cosets. Every element $g \in G$ belongs to at least one right coset, since $e \in H$ gives us $g \in Hg$. Thus

$$\bigcup_{x \in G} xH = G.$$

Now we need to show any two cosets are either identical or disjoint: if Hx and Hy share an element, then it follows from 1. $\Rightarrow$ 6. of Lemma 4.7 that $Hx = Hy$. This proves that the right cosets partition G.

To see that all right cosets have the same cardinality as H, consider the function

$$\rho\colon H \to Hg \quad \text{defined by} \quad \rho(h) = hg.$$

This function ρ is surjective by construction. Moreover, if $\rho(h) = \rho(h')$ then $hg = h'g$ and thus $h = h'$. Thus ρ is also injective, and therefore a bijection, so $|Hg| = |H|$. $\square$

Definition 4.10. The number of left cosets of a subgroup H in a finite group G is denoted by $[G : H]$ and called the **index** of H in G. Equivalently, the index $[G : H]$ is the number of right cosets of H.

We can now write a fancier version of Lagrange's Theorem 3.20; we leave the proof as an exercise.

Corollary 4.11 (Lagrange's Theorem revisited)**.** *If G is a finite group and $H \leq G$, then*

$$|G| = |H| \cdot [G : H].$$

In particular, $|H|$ is a divisor of $|G|$.

Another way to write this: if G is finite and H is any subgroup of G, then

$$[G : H] = \frac{|G|}{|H|}.$$

Example 4.12. For $G = D_n$ and $H = \langle s \rangle = \{e, s\}$, the left cosets gH of H in G are

$$\{e, s\}, \quad \{r, rs\}, \quad \{r^2, r^2 s\}, \cdots, \{r^{n-1}, r^{n-1}s\}$$

and the right cosets Hg are

$$\{e, s\}, \quad \{r, r^{-1}s\}, \quad \{r^2, r^{-2}s\}, \cdots, \{r^{n-1}, r^{-n+1}s\}.$$

Note that these lists are *not* the same, but they do have the same length. For example, r is in the left coset $\{r, rs\}$, while its right coset is $\{r, r^{-1}s\}$. We have $|G| = 2n$, $|H| = 2$ and $[G : H] = n$.

Keeping $G = D_n$ but now letting $K = \langle r \rangle$, the left cosets are K and

$$sK = \{s, sr, \ldots, sr^{n-1}\} = \{s, r^{n-1}s, r^{n-2}s, \ldots, rs\}$$

and the right cosets are K and

$$Ks = \{s, r^{n-1}s, r^{n-2}s, \ldots, rs\}.$$

In this case $sK = Ks$, and the left and right cosets are exactly the same. We have $|G| = 2n$, $|H| = n$ and $[G : H] = 2$.

4.2 Normal subgroups

Definition 4.13. A subgroup N of a group G is **normal** in G, written $N \trianglelefteq G$, if

$$gNg^{-1} = N \quad \text{for all } g \in G.$$

Example 4.14.

(1) The trivial subgroups $\{e\}$ and G of a group G are always normal.

(2) Any subgroup of an abelian group is normal.

(3) For any group G, $\mathrm{Z}(G) \trianglelefteq G$.

Remark 4.15. The relation of being a normal subgroup is not transitive. For example, for

$$V = \{e, (12)(34), (13)(24), (14)(23)\}$$

one can show that $V \trianglelefteq S_4$ (see Lemma 4.21 below), and since V is abelian (because you proved before that all groups with 4 elements are abelian!), the subgroup $H = \{e, (12)(34)\}$ is normal in V. But H is *not* normal in S_4, since for example

$$(13)[(12)(34)](13)^{-1} = (32)(14) \notin H.$$

Lemma 4.16. *Assume N is a subgroup of G. The following conditions are equivalent.*

(a) N is a normal subgroup of G, meaning that $gNg^{-1} = N$ for all $g \in G$.

(b) We have $gNg^{-1} \subseteq N$ for all $g \in G$, meaning that $gng^{-1} \in N$ for all $n \in N$ and $g \in G$.

(c) The right and left cosets of N agree. More precisely, $gN = Ng$ for all $g \in G$.

(d) We have $gN \subseteq Ng$ for all $g \in G$.

(e) We have $Ng \subseteq gN$ for all $g \in G$.

Proof. Note that $gNg^{-1} = N$ if and only if $gN = Ng$ and hence (1) $\iff$ (3).

The implication $(a) \Rightarrow (b)$ is immediate. Conversely, if $gNg^{-1} \subseteq N$ for all g, then

$$N = g^{-1}(gNg^{-1})g \subseteq g^{-1}Ng.$$

Thus (b) implies (a).

Finally, (b), (d), and (e) are all equivalent since

$$gNg^{-1} \subseteq N \iff gN \subseteq Ng$$

and

$$g^{-1}Ng \subseteq N \iff Ng \subseteq gN.$$

□

Exercise 19. Kernels of group homomorphisms are normal.

We will see later that, conversely, all normal subgroups are kernels of group homomorphisms.

Exercise 20. Any subgroup of index two is normal.

Exercise 21. Preimages of normal subgroups are normal, that is, if $f : G \to H$ is a group homomorphism and $K \trianglelefteq H$, then $f^{-1}(K) \trianglelefteq G$.

Remark 4.17. Let $A \leq B$ be subgroups of a group G. If A is a normal subgroup of G, then in particular for all $b \in B$ we have

$$bab^{-1} \in A,$$

since $b \in B \subseteq G$. Therefore, A is a normal subgroup of B.

Example 4.18. Let us go back to Example 4.12, where we considered the group $G = D_n$ and the subgroups

$$H = \langle s \rangle = \{e, s\} \quad \text{and} \quad K = \langle r \rangle.$$

We showed that the left and right cosets of H are not the same, and thus H is not a normal subgroup of G. We also showed that the left and right cosets of K are in fact the same, which proves that K is a normal subgroup of G. Note that H is nevertheless a very nice group – it is cyclic and thus abelian – despite not being a normal subgroup of G. This indicates that whether a subgroup H is a normal subgroup of G has a lot more to do about the relationship between H and G than the properties of H as a group on its own.

Definition 4.19. The **alternating group** A_n is the subgroup of S_n generated by all products of two transpositions.

Remark 4.20. Recall that we proved in Theorem 1.44 that the sign of a permutation is well-defined. Notice also that the inverse of an even permutation must also be even, and the product of any two even permutations is even, and thus A_n can also be described as the set of all even permutations.

Lemma 4.21. *For all $n \geqslant 2$, $A_n \trianglelefteq S_n$.*

Proof. Consider the sign map $\operatorname{sign}\colon S_n \to \mathbb{Z}/2$ that takes each permutation to its sign, meaning

$$\operatorname{sign}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

This a group homomorphism (exercise!), and by construction the kernel of sign is A_n. By Exercise 19, we conclude that A_n must be a normal subgroup of S_n.

Alternatively, we can prove Lemma 4.21 by showing that A_n is a subgroup of S_n of index 2, and using Exercise 20. $\square$

The last condition in Lemma 4.16 implies that for all $g \in G$ and $n \in N$, we have $gn = n'g$ for some $n' \in N$, which is precisely what was needed to make the group law on $G/\sim_H$ well-defined. Recall that

$$a \sim_H b \text{ if and only if } b = ha \text{ for some } h \in H.$$

Lemma 4.22. *Let G be a group. An equivalence relation $\sim$ on G is compatible with multiplication if and only if $\sim = \sim_N$ for some normal subgroup $N \trianglelefteq G$.*

Proof. ($\Rightarrow$) Suppose $\sim$ is compatible with multiplication, and set $N := \{g \in G \mid g \sim e\}$. Then we claim that $N \trianglelefteq G$ and $\sim = \sim_N$.

To see that $N \trianglelefteq G$, let $n \in N$ and $g \in G$. Since $n \in N$, then $n \sim e$, and thus since $\sim$ is compatible with multiplication we conclude that for all $g \in G$ we have

$$gng^{-1} \sim geg^{-1} = e \in N.$$

This shows that $gng^{-1} \subseteq N$ for any $n \in N$ and any $g \in G$, and thus N is a normal subgroup of G by Lemma 4.16.

It remains to check that $\sim = \sim_N$. Given any $a, b \in G$, since $\sim$ is compatible with multiplication then

$$a \sim b \implies ab^{-1} \sim bb^{-1} = e \implies ab^{-1} \in H.$$

Thus there exists some $h \in H$ such that

$$ab^{-1} = h \implies a = hb. \iff a \sim_H b.$$

($\Leftarrow$) If $\sim = \sim_N$, then in particular $\sim$ is compatible with multiplication. Let $x, y, z \in G$ such that $x \sim_N y$. Then $y = nx$ for some $n \in N$, so $yz = nxz$ and

$$zy = znx = zn(z^{-1}z)x = (znz^{-1})zx = n'zx$$

for some $n' \in N$, where the last equality uses the normal subgroup property. We deduce that $yz \sim_N xz$ and $zy \sim_N zx$. $\square$

4.3 Quotient groups

Definition 4.23. Let N be a normal subgroup of a group G. The **quotient group** G/N is the group $G/\sim_N$, where $\sim_N$ is the equivalence relation induced by the left action of N on G. Thus G/N is the set of left cosets of N in G, and the multiplication is given by

$$xN \cdot yN := (xy)N.$$

The identity elements is $e_G N = N$ and for each $g \in G$, the inverse of gN is $(gN)^{-1} = g^{-1}N$.

Remark 4.24. Note that, by Lemma 4.9, G/N is also the set of right cosets of N in G with multiplication given by

$$Nx \cdot Ny := N(xy).$$

In order to prove statements about a quotient G/N, it is often useful to rewrite those statements in terms of elements in the original group G, but one needs to be careful when translating.

Remark 4.25. Given a group G and a normal subgroup N, equality in the quotient does not mean that the representatives are equal. By Lemma 4.7,

$$gN = hN \iff gh^{-1} \in N.$$

In particular, $gN = N$ if and only if $g \in N$.

Remark 4.26. Note that $|G/N| = [G : N]$. By Lagrange's Theorem, if G is finite then

$$|G/N| = \frac{|G|}{|N|}.$$

Example 4.27. We saw in Example 4.18 that the subgroup $N = \langle r \rangle$ of D_n is normal. The quotient D_n/N has just two elements, N and sN, and hence it must be cyclic of order 2, since that is the only one group of order 2. In fact, note that $|N| = n$ and $|D_n| = 2n$, so by Lagrange's Theorem

$$|D_n/N| = \frac{2n}{n} = 2.$$

Example 4.28. The **infinite dihedral group** D_∞ is the set

$$D_\infty = \{r^i, r^i s \mid i \in \mathbb{Z}\}$$

together with the multiplication operation defined by

$$r^i \cdot r^j = r^{i+j}, \quad r^i \cdot (r^j s) = r^{i+j} s, \quad (r^i s) \cdot r^j = r^{i-j} s, \quad \text{and} \quad (r^i s)(r^j s) = r^{i-j}.$$

One can show that D_∞ is the group with presentation

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

Then $\langle r^n \rangle \trianglelefteq D_\infty$ and $D_\infty/\langle r^n \rangle \cong D_n$ via the map $r\langle r^n \rangle \mapsto r$ and $s\langle r^n \rangle \mapsto s$.

Remark 4.29. In Example 4.28 above, both groups D_∞ and $\langle r^n \rangle$ are infinite, but

$$[D_\infty : \langle r^n \rangle] = |D_\infty / \langle r^n \rangle| = |D_n| = 2n.$$

This shows that the quotient of an infinite group by an infinite subgroup can be a finite group.

The quotient of an infinite group by an infinite subgroup can also be infinite. In contrast, a quotient of any finite group must necessarily be finite.

Lemma 4.30. *Let G be a group and consider a normal subgroup N of G. Then the map*

$$\begin{aligned} G &\xrightarrow{\ \pi\ } G/N \\ g &\longmapsto \pi(g) = gN \end{aligned}$$

is a surjective group homomorphism with $\ker(\pi) = N$.

Proof. Surjectivity is immediate from the definition. Now we claim that π is a group homomorphism:

$$\begin{aligned} \pi(gg') &= (gg')N && \text{by definition of } \pi \\ &= gN \cdot g'N && \text{by definition of the multiplication on } G/N \\ &= \pi(g)\pi(g') && \text{by definition of } \pi. \end{aligned}$$

Finally, by Lemma 4.7, we have

$$\ker(\pi) = \{g \in G \mid gN = e_G N\} = N. \qquad \square$$

Definition 4.31. Let G be any group and N be a normal subgroup of G. The group homomorphism

$$\begin{aligned} G &\xrightarrow{\ \pi\ } G/N \\ g &\longmapsto \pi(g) = gN \end{aligned}$$

is called the **canonical (quotient) map**, the **canonical surjection**, or the **canonical projection** of G onto G/N.

The canonical projection is a surjective homomorphism. We might indicate that in our notation by writing $\pi\colon G \twoheadrightarrow G/N$. More generally

Notation 4.32. If $f\colon A \to B$ is a surjective function, we might write $f\colon A \twoheadrightarrow B$ to denote that surjectivity.

Normal subgroups are precisely those that can be realized as kernels of a group homomorphism.

Corollary 4.33. *A subgroup N of a group G is normal in G if and only if N is the kernel of a homomorphism with domain G.*

Proof. By Exercise 19, the kernel of any group homomorphism is a normal subgroup; we have just shown in Lemma 4.30 that every normal subgroup can be realized as the kernel of a group homomorphism. $\square$

Definition 4.34. Let G be any group. For $x, y \in G$, the **commutator** of x and y is the element

$$[x, y] := xyx^{-1}y^{-1}.$$

The **commutator subgroup** or **derived subgroup** of G, denoted by G' or $[G, G]$, is the subgroup generated by all commutators of elements in G. More precisely,

$$[G, G] := \langle [x, y] \mid x, y \in G \rangle.$$

Remark 4.35. Note that $[x, y] = e$ if and only if $xy = yx$. More generally, $[G, G] = \{e_G\}$ if and only if G is abelian.

The commutator subgroup measures how far G is from being abelian: if the commutator is as small as possible, then G is abelian, so a larger commutator indicates the group is somehow further from being abelian.

Remark 4.36 (The commutator is a normal subgroup)**.** A typical element of $[G, G]$ has the form

$$[x_1, y_1] \cdots [x_k, y_k] \qquad \text{for } k \geqslant 1 \text{ and } x_1, \ldots, x_k, y_1, \ldots, y_k \in G.$$

We do not need to explicitly include inverses since

$$[x, y]^{-1} = yxy^{-1}x^{-1} = [y, x].$$

Exercise 22. Show that $[G, G]$ is a normal subgroup of G.

Definition 4.37. Let G be a group and $[G, G]$ be its commutator subgroup. The associated quotient group

$$G^{\text{ab}} := G/[G, G]$$

is called the **abelianization** of G.

Remark 4.38. In this remark we will write G' instead of $[G, G]$ for convenience. The abelianization G/G' of any group G is an abelian, since

$$[xG', yG'] = [x, y]G' = G' = e_{G/G'}$$

for all $x, y \in G$.

Exercise 23. Let G be any group. The abelianization of G is the *largest* quotient of G that is abelian, in the sense that if G/N is abelian for some normal subgroup N, then $N \subseteq [G, G]$.

It is now time to prove the famous (and very useful!) Isomorphism Theorems.

4.4 The Isomorphism Theorems for groups

Theorem 4.39 (Universal Mapping Property (UMP) of a Quotient Group)**.** *Let G be a group and N a normal subgroup. Given any group homomorphism $f : G \to H$ with $N \subseteq \ker(f)$, there exists a unique group homomorphism*

$$\overline{f} : G/N \to H$$

such that the triangle

$$\begin{tikzcd} & G \arrow[dl, two heads, "\pi"'] \arrow[dr, "f"] & \\ G/N \arrow[rr, dashed, "\overline{f}"'] & & H \end{tikzcd}$$

commutes, meaning that $\overline{f} \circ \pi = f$.

Moreover, $\mathrm{im}(f) = \mathrm{im}(\overline{f})$*. In particular, if f is surjective, then $\overline{f}$ is also surjective. Finally,*

$$\ker(\overline{f}) = \ker(f)/N := \{gN \mid f(g) = e_H\}.$$

Proof. Suppose that such a homomorphism $\overline{f}$ exists. Since $f = \pi \circ \overline{f}$, then $\overline{f}$ has to be given by

$$\overline{f}(gN) = \overline{f}(\pi(g)) = f(g).$$

In particular, $\overline{f}$ is necessarily unique. To show existence, we just need to show that this formula determines a well-defined homomorphism. Given $xN = yN$, we have

$$y^{-1}x \in N \subseteq \ker(f)$$

and so

$$f(y)^{-1}f(x) = f(y^{-1}x) = e \implies f(y) = f(x).$$

This shows that $\overline{f}$ is well-defined. Moreover, for any $x, y \in G$, we have

$$\overline{f}((xN)(yN)) = \overline{f}((xy)N) = f(xy) = f(x)f(y) = \overline{f}(xN)\overline{f}(yN).$$

Thus $\overline{f}$ is a group homomorphism.

The fact that $\mathrm{im}\, f = \mathrm{im}\, \overline{f}$ is immediate from the formula for $\overline{f}$ given above, and hence f is surjective if and only if $\overline{f}$ is surjective.

Finally, we have

$$xN \in \ker(\overline{f}) \iff \overline{f}(xN) = e_H \iff f(x) = e_H \iff x \in \ker(f).$$

Therefore, if $xN \in \ker(\overline{f})$ then $xN \in \ker(f)/N$. On the other hand, if $xN \in \ker(f)/N$ for some $x \in G$, then $xN = yN$ for some $y \in \ker(f)$ and hence $x = yz$ for some $z \in N$. Since $N \subseteq \ker(f)$, then $x, y \in \ker(f)$, and thus we conclude that $x = yz \in \ker(f)$. $\square$

In short, the UMP of quotient groups says that to give a homomorphism from a quotient G/N is the same as to give a homomorphism from G with kernel containing N.

Corollary 4.40. *Let G be any group and let A be an abelian group. Any group homomorphism $f : G \to A$ must factor uniquely through the abelianization G^{ab} of G: there exists a unique homomorphism $\overline{f}$ such that f factors as the composition*

$$f\colon G \xrightarrow{\pi} G/[G,G] \xrightarrow{\overline{f}} A.$$

Proof. Let $\pi\colon G \to G^{\mathrm{ab}} = G/[G,G]$ be the canonical projection. Since A is abelian, then

$$f([x,y]) = [f(x), f(y)] = e$$

for all $x, y \in G$, and thus $[G,G] \subseteq \ker(f)$. By Theorem 4.39, the homomorphism f must uniquely factor as

$$f\colon G \xrightarrow{\pi} G/[G,G] \xrightarrow{\overline{f}} A. \qquad \square$$

The slogan for the previous result is that any homomorphism from a group G to any abelian group factors uniquely through the abelianization $G/[G,G]$ of G.

We are now ready for the First (and most important) Isomorphism Theorem.

Theorem 4.41 (First Isomorphism Theorem)**.** *If $f\colon G \to H$ is a homomorphism of groups, then $\ker(f) \trianglelefteq G$ and the map $\overline{f}$ defined by*

$$\begin{aligned} G/\ker(f) &\xrightarrow{\overline{f}} H \\ g \cdot ker(f) &\longmapsto f(g) \end{aligned}$$

induces an isomorphism

$$\overline{f}\colon G/\ker(f) \xrightarrow{\cong} \operatorname{im}(f).$$

In particular, if f is surjective, then f induces an isomorphism $\overline{f}\colon G/\ker(f) \xrightarrow{\cong} H$.

Proof. The fact that the kernel is a normal subgroup is Exercise 19. Let us first restrict the target of f to $\operatorname{im}(f)$, so that we can assume without loss of generality that f is surjective. By Theorem 4.39, there exists a (unique) homomorphism $\overline{f}$ such that $\overline{f} \circ \pi = f$, where $\pi : G \to G/\ker(f)$ is the canonical projection. Moreover, the kernel $\ker(f)/\ker(f)$ of $\overline{f}$ consists of just one element, the coset $\ker(f)$ of the identity, and so $\overline{f}$ it injective. Moreover, Theorem 4.39 also says that the image of $\overline{f}$ equals the image of f. We conclude that $\overline{f}$ is an isomorphism. $\square$

Example 4.42. Let F be a field and consider $G = \mathrm{GL}_n(F)$ for some integer $n \geqslant 1$. We claim that $H = \mathrm{SL}_n(F)$, the square matrices with determinant 1, is a normal subgroup of $G = \mathrm{GL}_n(F)$. Indeed, given $A \in \mathrm{GL}_n(F)$ and $B \in \mathrm{SL}_n(F)$, then

$$\det(ABA^{-1}) = \det(A)\underbrace{\det(B)}_{1}\det(A)^{-1} = \det(A)\det(A)^{-1} = 1,$$

so $ABA^{-1} \in H$. The map

$$\det\colon \mathrm{GL}_n(F) \to (F^\times, \cdot)$$

is a surjective group homomorphism whose kernel is by definition of $\mathrm{SL}_n(F)$. By the First Isomorphism Theorem,

$$\mathrm{GL}_n(F)/\,\mathrm{SL}_n(F) \cong (F^\times, \cdot).$$

Example 4.43. Note that $N = (\{\pm 1\}, \cdot)$ is a subgroup of $G = (\mathbb{R} \setminus \{0\}, \cdot)$, and N is normal in G since G is abelian. We claim that G/N is isomorphic to $(\mathbb{R}_{>0}, \cdot)$. To prove this, define

$$f \colon \mathbb{R}^\times \to \mathbb{R}_{>0}$$

to be the absolute value function, so that $f(r) = |r|$. Then f is a surjective homomorphism and its kernel is N. The First Isomorphism Theorem gives

$$G/N \cong (\mathbb{R}_{>0}, \cdot).$$

Example 4.44. We showed in Example 4.27 that $D_n/ < r >$ is isomorphic to the cyclic group of order 2. Let us now reprove that fact using the First Isomorphism Theorem.

Recall that $(\{\pm 1\}, \cdot)$ is a group with $\cdot$ the usual multiplication. Define $f \colon D_n \longrightarrow \{\pm 1\}$ by

$$f(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ preserves orientation} \\ -1 & \text{if } \alpha \text{ reverses orientation} \end{cases} = \begin{cases} 1 & \text{if } \alpha \text{ is a rotation} \\ -1 & \text{if } \alpha \text{ is a reflection.} \end{cases}$$

One can show (exercise!) that this is a surjective homomorphism with kernel $\ker f = \langle r \rangle$, and hence by the First Isomorphism Theorem

$$D_n/\langle r \rangle \cong (\{\pm 1\}, \cdot).$$

To set up the Second Isomorphism Theorem, we need some more background first.

Definition 4.45. Given subgroups H and K of a group G, we define the subset HK of G by

$$HK := \{hk \mid h \in H, k \in K\}.$$

Note that HK is in general only a subset of G, not a subgroup.

Remark 4.46. Given subgroups H and K of a group G, note that H and K are both subgroups of HK. For example, any element $h \in H$ is in HK because $e \in K$ and $h = he \in HK$.

Exercise 24. Let H and K be subgroups of G.

(1) The subset HK is a subgroup of G if and only if $HK = KH$.

(2) If at least one of H or K is a normal subgroup of G, then

$$HK \leq G \quad \text{and} \quad HK = KH = \langle H \cup K \rangle.$$

Warning! The identity $HK = KH$ does not mean that every pair of elements from H and K must commute, as the example below will show; this is only an equality of sets.

Example 4.47. In D_n, consider the subgroups $H = \langle s \rangle$ and $K = \langle r \rangle$. The work we did in Example 4.12 shows that

$$HK = KH = D_2,$$

but r and s do not commute. The fact that $HK = KH$ can also be justified by observing that $K \trianglelefteq D_n$ (see Example 4.18) and using Exercise 24.

Theorem 4.48 (Second Isomorphism Theorem)**.** *Let G be a group, $H \leq G$, and $N \trianglelefteq G$. Then*

$$HN \leq G, \quad N \cap H \trianglelefteq H, \quad N \trianglelefteq HN$$

and there is an isomorphism

$$\frac{H}{N \cap H} \xrightarrow{\cong} \frac{HN}{N}$$

given by

$$h \cdot (N \cap H) \mapsto hN.$$

Proof. We leave the facts that $HN \leq G$ and $N \cap H \trianglelefteq H$ as exercises. Since $N \trianglelefteq G$, then $N \trianglelefteq HN$. Let $\pi \colon HN \to \frac{HN}{N}$ be the canonical projection. Define

$$\begin{aligned} H &\xrightarrow{\ f\ } \tfrac{HN}{N} \\ h &\longrightarrow f(h) = hN. \end{aligned}$$

This is a homomorphism, since it is the composition of homomorphisms

$$f \colon H \subseteq HN \xrightarrow{\pi} \frac{HN}{N},$$

where the first map is just the inclusion. Moreover, f is surjective since

$$hnN = hN = f(h)$$

for all $h \in H$ and $n \in N$. The kernel of f is

$$\ker(f) = \{h \in H \mid hN = N\} = H \cap N.$$

The result now follows from the First Isomorphism Theorem applied to f. □

Corollary 4.49. *If H and N are finite subgroups of G and $N \trianglelefteq G$, then*

$$|HN| = \frac{|H| \cdot |N|}{|H \cap N|}.$$

Proof. By Theorem 4.48,

$$\frac{H}{N \cap H} \cong \frac{HN}{N}.$$

The result now follows from Remark 4.26, which is really just an application of Lagrange's Theorem:

$$\frac{|H|}{|N \cap H|} = \frac{|HN|}{|N|}. \qquad \square$$

In fact, the corollary is also true without requiring that N is normal.

Example 4.50. Fix a field F and an integer $n \geqslant 1$. Let $G = \mathrm{GL}_n(F)$ and $N = \mathrm{SL}_n(F)$, and recall that we showed in Example 4.42 that N is a normal subgroup of G. Let H be the set of diagonal invertible matrices, which one can show is also a subgroup of G. One can show that every invertible matrix A can be written as a product of a diagonal matrix and a matrix of determinant 1, and thus $HN = G$. By the Second Isomorphism Theorem,

$$H/(N \cap H) \cong G/N$$

and since we showed in Example 4.42 that

$$G/N \cong (F^\times, \cdot),$$

where $F^\times = F \setminus \{0\}$, we get

$$H/(N \cap H) \cong (F^\times, \cdot).$$

Before we prove what is known as the Third Isomorphism Theorem, we need to get a better understanding of the subgroups of a quotient group. That is the content of what is known as the Lattice Isomorphism Theorem, sometimes (rarely?) called the Fourth Isomorphism Theorem.

Theorem 4.51 (The Lattice Isomorhism Theorem)**.** *Let G be a group and N a normal subgroup of G, and let $\pi : G \twoheadrightarrow G/N$ be the quotient map. There is an order-preserving bijection of posets (a lattice isomorphism)*

$$\begin{array}{rcl}
\{\textit{subgroups of } G \textit{ that contain } N\} & \underset{\Phi}{\overset{\Psi}{\rightleftarrows}} & \{\textit{subgroups of } G/N\} \\
H & \longmapsto & \Psi(H) = H/N \\
\Phi(A) = \pi^{-1}(A) = \{x \in G \mid \pi(x) \in A\} & \longleftarrow\!\shortmid & A
\end{array}$$

Then this bijection enjoys the following properties:

(1) Subgroups correspond to subgroups:

$$H \leq G \iff H/N \leq G/N.$$

(2) Normal subgroups correspond to normal subgroups:

$$H \trianglelefteq G \iff H/N \trianglelefteq G/N.$$

(3) Indices are preserved:

$$[G : H] = [G/N : H/N].$$

(4) Intersections and unions are preserved:

$$N/N \cap K/N = (H \cap K)/N \quad \textit{and} \quad \langle H/N \cup K/N \rangle = \langle H \cup K \rangle /N.$$

Proof. We showed in Lemma 4.30 that the quotient map $\pi\colon G \to G/N$ is a surjective group homomorphism. It will be useful to rewrite the maps in the statement of the theorem in terms of π. Notice that $\Psi(H) = H/N = \{hN \mid h \in H\} = \pi(H)$. Note that Ψ does indeed land in the correct codomain, since by Lemma 3.8 images of subgroups through group homomorphisms are subgroups, and thus $\pi(H) \leq G/N$ for each $H \leq G$. Thus Ψ is well-defined. We claim Φ also lands in the correct codomain. Indeed, by Exercise 13 preimages of subgroups through group homomorphisms are subgroups, and thus in particular for each $A \leq G$ we have $\pi^{-1}(A) \leq G$. Moreover, for any $A \leq G$ we have $\{e_G N\} \subseteq A$, hence

$$N = \ker(\pi) = \pi^{-1}(\{e_G N\}) \subseteq \pi^{-1}(A) = \Phi(A).$$

Thus Ψ is well-defined.

To show that Ψ is bijective, we will show that Φ and Ψ are mutual inverses. First, note that since π is surjective, then $\pi(\pi^{-1}(A)) = A$ for all subgroups A of G/N, and thus

$$(\Psi \circ \Phi)(A) = \pi(\pi^{-1}(A)) = A.$$

Moreover,

$$\begin{aligned} x \in \pi^{-1}(H/N) &\iff \pi(x) \in H/N \\ &\iff xN = hN && \text{for some } h \in H \\ &\iff x \in hN && \text{for some } h \in H \\ &\iff x \in H && \text{since } N \subseteq H. \end{aligned}$$

Thus

$$(\Phi \circ \Psi)(H) = \pi^{-1}(\pi(H)) = \pi^{-1}(H/N) = H.$$

Thus, Ψ and Φ are well-defined and inverse to each other. Since π and π^{-1} both preserve containments, each of Ψ, Ψ^{-1} preserves containments as well.

Again by Lemma 3.8 and Exercise 13, images and preimages of subgroups by group homomorphisms are subgroups, which proves (1). Moreover, if $N \leq H \leq G$ and $H \trianglelefteq G$, then $ghg^{-1} \in H$ for all $g \in G$ and all $h \in G$, and thus

$$(gN)(hN)(gN)^{-1} = (ghg^{-1})N \in H/N.$$

Therefore, if $N \leq H \trianglelefteq G$, then $H/N \trianglelefteq G/N$. Finally, by Exercise 21, the preimage of a normal subgroup is normal. We have now shown (2).

We leave (3) as an exercise, and (4) is a consequence of the more general fact that lattice isomorphisms preserve suprema and infima. $\square$

We record here what is left to do.

Exercise 25. Let G be a group and N a normal subgroup of G. For all subgroups H of G with $N \leq H$, show that

$$[G : H] = [G/N : H/N] \quad \text{and} \quad [G : \pi^{-1}(A)] = [G/N : A].$$

Theorem 4.52 (Third Isomorphism Theorem)**.** *Let G be a group, $M \leq N \leq G$, $M \trianglelefteq G$ and $N \trianglelefteq G$. Then*

$$M \trianglelefteq N, \qquad N/M \trianglelefteq G/M,$$

and there is an isomorphism

$$\begin{aligned} \tfrac{(G/M)}{(N/M)} &\xrightarrow{\cong} G/N \\ gM &\longmapsto gN. \end{aligned}$$

Proof. By Remark 4.17, since M is a normal subgroup of G, then it is also a normal subgroup of N. Similarly, the fact that N is normal in G implies that it is normal in G/M, by Theorem 4.51.

The kernel of the canonical map $\pi : G \twoheadrightarrow G/N$ contains M, and so by Theorem 4.39 we get an induced homomorphism

$$\phi\colon G/M \to G/N$$

with $\phi(gM) = \pi(g) = gN$. Moreover, we know

$$\ker(\phi) = \ker(\pi)/M = N/M.$$

Finally, apply the First Isomorphism Theorem to ϕ. □

We can now prove the statement about indices in the Lattice Isomorphism Theorem in the case of normal subgroups.

Corollary 4.53. *Let G be a group and N a normal subgroup of G. For all normal subgroups H of G with $N \leq H$,*

$$[G : H] = [G/N : H/N] \quad \textit{and} \quad [G : \pi^{-1}(A)] = [G/N : A].$$

Proof. By the Third Isomorphism Theorem,

$$G/H \cong \frac{(G/N)}{(H/N)}$$

and thus their orders are the same; in particular,

$$[G : H] = |G/H| = \left| \frac{(G/N)}{(H/N)} \right| = [G/N : H/N] = [G/N : H/N].$$ □

4.5 Presentations as quotient groups

We can finally define group presentations in a completely rigorous manner.

Definition 4.54. Let A be a set. Consider the new set of symbols

$$A^{-1} = \{a^{-1} \mid a \in A\}.$$

Consider the set of all finite words written using symbols in $A \cup A^{-1}$, including the empty word. If a word w contains consecutive symbols aa^{-1} or $a^{-1}a$, we can simplify w by erasing those two consecutive symbols, and we obtain a word that is equivalent to w. If a word cannot be simplified any further, we say that it is **reduced**. Given any $a \in A$, a^1 denotes a, to distinguish it from a^{-1}.

The **free group** on A, denoted $F(A)$, is the set of all reduced words in $A \cup A^{-1}$. In symbols,

$$F(A) = \{a_1^{i_1} a_2^{i_2} \cdots a_m^{i_m} \mid m \geqslant 0, a_j \in A, i_j \in \{-1, 1\}\}.$$

The set $F(A)$ is a group with the operation in which any two words are multiplied by concatenation.

Example 4.55. The free group on a singleton set $A = x$ is the infinite cyclic group C_∞.

Theorem 4.56 (Universal mapping property for free groups)**.** *Let A be a set, let $F(A)$ be the free group on A, and let H be any group. Given a function $g\colon A \to H$, there is a unique group homomorphism $f\colon F(A) \to H$ satisfying $f(a) = g(a)$ for all $a \in A$.*

Proof. Let $f\colon F(A) \to H$ be given by

$$f(a_1^{i_1} a_2^{i_2} \cdots a_m^{i_m}) = g(a_1)^{i_1} g(a_2)^{i_2} \cdots g(a_m)^{a_m}$$

for any $m \geqslant 0$, $a_j \in A$, and $i_j \in \{-1, 1\}$. To check that this is a well-defined function, note that

$$f(a_1^{i_1} a_2^{i_2} \cdots aa^{-1} \cdots a_m^{i_m}) = g(a_1)^{i_1} g(a_2)^{i_2} \cdots g(a)g(a)^{-1} \cdots g(a_m)^{a_m} = f(a_1^{i_1} a_2^{i_2} \cdots a_m^{i_m})$$

for any $a \in G$ and similarly for inserting $a^{-1}a$. The fact that f is a group homomorphism and its uniqueness are left as an exercise. $\square$

Definition 4.57. Let G be a group and let $R \subseteq G$ be a set. The *normal subgroup of G generated by R*, denoted $\langle R \rangle^N$, is the set of all products of conjugates of elements of R and inverses of elements of R. In symbols,

$$\langle R \rangle^N = \{g_1 r_1^{i_1} g_1^{-1} \ldots g_m r_m^{i_m} g_m^{-1} \mid m \geqslant 0, i_j \in \{1, -1\}, r_j \in R, g_j \in G\}.$$

Definition 4.58. Let A be a set and let R be a subset of the free group $F(A)$. The group with **presentation**

$$\langle A \mid R \rangle = \langle A | \{r = e \mid r \in R\} \rangle$$

is defined to be the quotient group $F(A)/\langle R \rangle^N$.

Example 4.59. Let $A = \{x\}$ and consider $R = \{x^n\}$. Then the group with presentation $\langle A \mid R\rangle$ is the cyclic group of order n:

$$C_n = \langle x \mid x^n = e\rangle = \frac{F(\{x\})}{\langle x^n\rangle^N} = C_\infty/\langle x^n\rangle.$$

Example 4.60. Taking $A = \{r, s\}$ and $R = \{s^2, r^n, srsr\}$, $\langle A \mid R\rangle$ is the usual presentation for D_n:

$$D_n = \langle r, s \mid s^2 = e, r^n = e, srsr = e\rangle = \frac{F(\{r, s\})}{\{s^2, r^n, srsr\}^N}.$$

Theorem 4.61 (Universal mapping property of a presentation)**.** *Let A be a set, let $F(A)$ be the free group on A, let R be a subset of $F(A)$, and let H be a group. Let $g\colon A \to H$ be a function satisfying the property that whenever $r = a_1^{i1} \cdots a_m^{i_m} \in R$, with each $a_j \in A, g_j \in G$ and $i_j \in \{1, -1\}$, then*

$$(g(a_1))^{i_1} \cdots (g(a_m))^{i_m} = e_H.$$

Then there is a unique homomorphism $\overline{f}\colon \langle A|R\rangle \to H$ satisfying

$$\overline{f}(a\langle R\rangle^N) = g(a) \quad \textit{for all } a \in A.$$

Proof. By Theorem 4.56, there is a unique group homomorphism $\tilde{f} : F(A) \to H$ such that $f(a) = g(a)$ for all $a \in A$. Then for

$$r = a_1^{i1} \cdots a_m^{i_m} \in R$$

we have

$$f(r) = (g(a_1))^{i_1} \cdots (g(a_m))^{i_m} = e_H,$$

showing that $R \subseteq \ker(f)$. Since $\ker(f) \trianglelefteq F(A)$ and $\langle R\rangle^N$ is the smallest normal subgroup containing R, it follows that $\langle R\rangle^N \subseteq \ker(f)$. By Theorem 4.39, f induces a group homomorphism $\overline{f} : G/\langle R\rangle^N \to H$. Moreover, for each $a \in A$ we have

$$g(a) = f(a) = \overline{f}(a\langle R\rangle^N).$$

□

Remark 4.62. The universal property of a presentation in Theorem 4.61 says that to give a group homomorphism from a group G with a given presentation to a group H is the same as picking images for each of the generators that satisfy the same relations in H as those given in the presentation.

Example 4.63. To find a groups homomorphism $D_n \to \mathrm{GL}_2(\mathbb{R})$, it suffices to pick images for r and s, say $r \mapsto R, s \mapsto S$, and to verify that

$$S^2 = I_2, \quad R^n = I_2, \quad SRSR = I_2.$$

One can check that this does hold for the matrices

$$S = \begin{pmatrix} \cos 2\pi n & -\sin 2\pi n \\ \sin 2\pi n & \cos 2\pi n \end{pmatrix} \quad \text{and} \quad R = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

By the UMP of the presentation there is a unique group homomorphism $D_n \to \mathrm{GL}_2(\mathbb{R})$ that sends r to R and s to S.

Presentations of groups are remarkably complex mathematical constructions. What makes them so complicated is that $\langle R \rangle^N$ is very hard to calculate in general. The following theorem is a negative answer to what is know as the Word Problem, and illustrates how complicated the story can become:

Theorem 4.64 (Boone-Novikov)**.** *There exists a finite set A and a finite subset R of $F(A)$ such that there exists no algorithm that determines whether a given element of $\langle A \mid R \rangle$ is equal to the trivial element.*

Chapter 5

Group actions... in action

It is time for some more group actions. We will start with some general facts about group actions, and then we will focus on some specific actions and use them to prove results about the structure of finite groups.

5.1 Orbits and Stabilizers

Let G be a group acting on a set S. Let us recall some notation and facts about group actions. The **orbit** of an element $s \in S$ is

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

A **permutation representation** of a group G is a group homomorphism $\rho\colon G \to \mathrm{Perm}(S)$ for some set S. By Lemma 2.3, to give an action of G on a set S is equivalent to giving a permutation representation $\rho\colon G \to \mathrm{Perm}(S)$, which is induced by the action via

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

An action is **faithful** if the only element $g \in G$ such that $g \cdot s = s$ for all $s \in S$ is $g = e_G$. Equivalently an action is faithful if $\ker(\rho) = \{e_G\}$. An action is **transitive** if for all $p, q \in S$ there is a $g \in G$ such that $q = g \cdot p$. Equivalently, an action is transitive if $\mathrm{Orb}_G(p) = S$ for any $p \in S$.

Definition 5.1. Let G be a group acting on a set S. The **stabilizer** of an element s in S is the set of group elements that fix s under the action:

$$\mathrm{Stab}_G(s) = \{g \in G \mid g \cdot s = s\}.$$

Definition 5.2. Let G be a group acting on a set S. An element $s \in S$ is a **fixed point** of the action if $g \cdot s = s$ for all $g \in G$.

Remark 5.3. Let G be a group acting on a set S. An element $s \in S$ is a fixed point if and only if $\mathrm{Orb}_G(s) = \{s\}$. Moreover, s is a fixed point if and only if $\mathrm{Stab}_G(s) = G$.

The stabilizer of any element is always a subgroup of G.

Lemma 5.4. *Let G be a group acting on a set S, and let $s \in S$. The stabilizer* $\operatorname{Stab}_G(s)$ *of s is a subgroup of G.*

Proof. By definition of group action, $e \cdot s = s$, so $e \in \operatorname{Stab}_G(e)$. If $x, y \in \operatorname{Stab}_G(s)$, then $(xy)s = x(ys) = xs = s$ and thus $xy \in \operatorname{Stab}_G(s)$. If $x \in \operatorname{Stab}_G(s)$, then

$$xs = s \Rightarrow s = x^{-1}xs = x^{-1}s \Rightarrow x^{-1} \in \operatorname{Stab}_G(s). \qquad \square$$

The following theorem can easily be remembered by the mnemonic LOIS, which stands for

LOIS = The Length of the Orbit is the Index of the Stabilizer.

Theorem 5.5 (LOIS)**.** *Let G be a group that acts on a set S. For any $s \in S$ we have*

$$|\operatorname{Orb}_G(s)| = [G : \operatorname{Stab}_G(s)].$$

Proof. Let $\mathcal{L}$ be the collection of left cosets of $\operatorname{Stab}_G(s)$ in G. Let $\alpha : \mathcal{L} \to \operatorname{Orb}_G(s)$ be given by

$$\alpha(x \operatorname{Stab}_G(s)) = x \cdot s.$$

This function is well-defined and injective:

$$x \operatorname{Stab}_G(s) = y \operatorname{Stab}_G(s) \iff x^{-1}y \in \operatorname{Stab}_G(s) \iff x^{-1}y \cdot s = s \iff y \cdot s = x \cdot s.$$

The function α is surjective by definition of $\operatorname{Orb}_G(s)$, and thus it is a bijection. Finally, we can now conclude that

$$[G : \operatorname{Stab}_G(s)] = |\mathcal{L}| = |\operatorname{Orb}_G(s)|. \qquad \square$$

Corollary 5.6 (Orbit-Stabilizer Theorem)**.** *Let G be a finite group acting on a set S. For any $s \in S$ we have*

$$|G| = |\operatorname{Orb}_G(s)| \cdot |\operatorname{Stab}_G(s)].$$

Proof. This is a direct consequence of LOIS, since by Lagrange's Theorem

$$[G : \operatorname{Stab}_G(s)] = |G| / |\operatorname{Stab}_G(s)|. \qquad \square$$

Remark 5.7. Let G be a group acting on a finite set S. The orbits of the action form a partition of S. The one-element orbits correspond to the fixed points of the action. Pick one element $s_1, \ldots, s_m$ in each of the other orbits. This gives us the

$$\text{The Orbit Formula:} \quad |S| = (\text{the number of fixed points}) + \sum_{i=1}^{m} |\operatorname{Orb}_G(s_i)|.$$

By LOIS, we can rewrite this as

$$\text{The Stabilizer Formula:} \quad |S| = (\text{the number of fixed points}) + \sum_{i=1}^{m} [G : \operatorname{Stab}_G(s_i)].$$

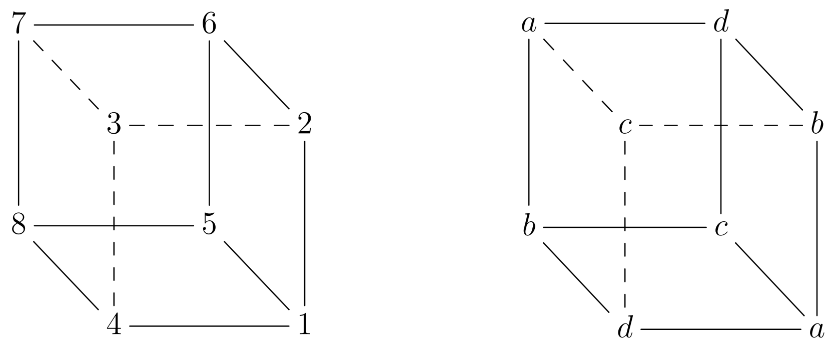
We will later see that these are very useful formulas.

We can now use these simple facts to do some explicit calculations with groups.

Example 5.8. Let G be the group of rotational (orientation-preserving) symmetries of the cube. To count the number of elements of G, think about an isometry as picking up a cube lying on a table, moving it, and placing it back in the same location. To do this, one must pick a face to place on the table. This can be chosen in 6 ways. Once that face is chosen, one needs to decide on where each vertex of that face goes and this can be done in 4 ways. Thus $|G| = 24$.

We can restrict the action of G to the four lines that join opposite vertices of the cube; the group of permutations of the four lines is S_4, so the corresponding permutation representation associated to this action is a group homomorphism $\rho\colon G \to S_4$.

We claim that this homomorphism ρ is actually an isomorphism from G to S_4. To see this, first label each vertex of the cube 1 through 8. Let a, b, c, and d denote each of the four lines, and let us also label the vertices of the cube a, b, c, or d according to which of the diagonal lines goes through that vertex.



Now note that each face corresponds to a unique order on a, b, c, d, read counterclockwise from the outside of the cube:

The face 1234	corresponds to	*adcb*
The face 1256	corresponds to	*abdc*
The face 1458	corresponds to	*adbc*
The face 5678	corresponds to	*abcd*
The face 2367	corresponds to	*adbc*
The face 3478	corresponds to	*acdb*.

So suppose that $g \in G$ fixes all of the four lines a, b, c, d. Then the face at the bottom must be *abcb*, which corresponds to 1234, and thus all the vertices of the cube in the bottom face must be fixed. We conclude that g must fix the entire cube, and thus g must be the identity.

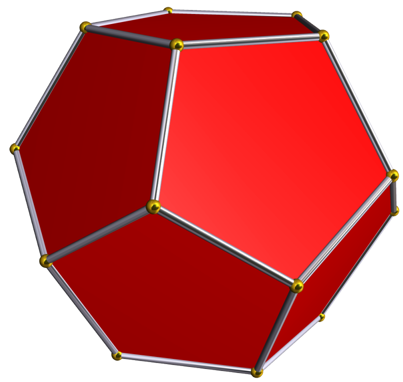
Thus the action is faithful, and hence the permutation representation $\rho : G \to S_4$ is injective. Moreover, we showed above that $|G| = 24 = |S_4|$, and thus ρ is an injective function between two finite sets of the same size. We conclude that ρ must actually be a bijection, and thus an isomorphism.

The same group G also acts on the six faces of the cube. This action is transitive, since we can always pick up the cube and put it back on the table with any face on the top. Thus the one and only orbit for the action of G on the six faces of the cube has length 6. By LOIS, it follows that for any face f of the cube, its stabilizer has index 6 and, since we already know that $|G| = 24$, the Orbit-Stabilizer Theorem gives us

$$|\operatorname{Stab}_G(f)| = \frac{|G|}{|\operatorname{Orb}_G(s)|} = \frac{24}{6} = 4.$$

Thus, there are four symmetries that map f to itself. Indeed, they are the 4 rotations by 0, $\frac{\pi}{2}$, π or $\frac{3\pi}{2}$ about the line of symmetry passing through the midpoint of f and the midpoint of the opposite face.

Example 5.9. Let X be a regular dodecahedron, with 12 faces, centered at the origin in $\mathbb{R}^3$.



A picture of a Dodecahedron from Wikipedia

Let G be the group of isometries of the cube that preserve orientation:

$$G := \{\alpha : \mathbb{R}^3 \to \mathbb{R}^3 \mid \alpha \text{ is an isometry, } \alpha \text{ preserves orientation, and } \alpha(X) = X\}.$$

This is a subgroup of the group of all bijections from $\mathbb{R}^3$ to $\mathbb{R}^3$. Though not obvious, every element of G is given as rotation about a line of symmetry. There are three kinds of such lines: those joining midpoints of opposite face, those joining midpoints of opposite edges, and those joining opposite vertices. To count the number of elements of G informally, think about an isometry as picking up a dodecaedron that was lying on a table and replacing it in the same location. To do this, one must first pick one of the twelve faces to place on the table, and, for each possible face, there are five ways to orient it. Thus

$$|G| = 12 \cdot 5 = 60.$$

Let us use LOIS to do this more formally. Note that G act on the collection S of the 12 faces of X. This action is transitive since it is possibly to move one face to any other via an appropriate rotation. So, the one and only orbit has length 12. Letting F be any one of the faces, the orientation preserving isometries of X that map F to itself are just the orientation-preserving elements of D_{10}, of which there are 5. Indeed, these correspond to the five rotations of X by $\frac{2\pi nj}{5}$ radians for $j = 0, 1, 2, 4$ about the axis of symmetry passing through the midpoint of F and the midpoint of the opposite face. Applying the Orbit-Stabilizer Theorem gives

$$|G| = |\operatorname{Orb}_G(F)| \cdot |\operatorname{Stab}_G(F)] = 12 \cdot 5 = 60.$$

5.2 The class equation

The main goal of this subsection is to apply the Orbit-Stabilizer Formula to the action of G on itself by conjugation. Let G be a group. As we saw before, G acts on $S = G$ by conjugation: the action is defined by $g \cdot x = gxg^{-1}$.

Definition 5.10. Let G be a group. Two elements $g, g' \in G$ are **conjugate** if there exists $h \in G$ such that

$$g' = hgh^{-1}.$$

Equivalently, g and g' are conjugate if they are in the same orbit of the conjugation action. The **conjugacy class** of an element $g \in G$ is

$$[g]_c := \{hgh^{-1} \mid h \in G\}.$$

Equivalently, the conjugacy class of g is the orbit of g under the conjugation action.

Remark 5.11. Let G be any group. Then $geg^{-1} = e$ for all $g \in G$, and thus $[e]_c = e = \{e\}$.

Let us study the conjugacy classes of S_n. You proved in a problem set that two cycles in S_n are conjugate if and only if they have the same length:

Lemma 5.12. *For any $\sigma \in S_n$ and distinct integers $i_1, \ldots, i_p$, we have*

$$\sigma(i_1\, i_2\, \cdots\, i_p)\sigma^{-1} = (\sigma(i_1)\ \cdots\ \sigma(i_p)).$$

Note that the right-hand cycle is a cycle since σ is injective. This generalizes to the following:

Theorem 5.13. *Two elements of S_n are conjugate if and only if they have the same cycle type.*

Proof. Consider two conjugate elements of S_n, say α and $\beta = \sigma\alpha\sigma^{-1}$. By Theorem 1.36, we may write α as a product of disjoint cycles $\alpha = \alpha_1 \cdots \alpha_m$. Then

$$\beta = \sigma\alpha\sigma^{-1} = (\sigma\alpha_1\sigma^{-1}) \cdots (\sigma\alpha_m\sigma^{-1}).$$

Since $\alpha_1, \ldots, \alpha_m$ are disjoint cycles, then by Lemma 5.12 the elements $(\sigma\alpha_1\sigma^{-1}), \cdots, (\sigma\alpha_m\sigma^{-1})$ are also disjoint cycles, and $\sigma\alpha_i\sigma^{-1}$ has the same length as α_i. We conclude that α and β must have the same cycle type.

Conversely, consider two elements α and β with the same cycle type. More precisely, assume $\alpha = \alpha_1 \cdots \alpha_k$ and $\beta = \beta_1 \cdots \beta_k$ are decompositions into disjoint cycles and that α_i, β_i both have length $p_i \geqslant 2$ for each i. We need to prove that α and β are conjugate. Let us start with the case $k = 1$. Given two cycles of the same length,

$$\alpha = (i_1\ \ldots\ i_p) \quad \text{and} \quad \beta = (j_1\ \ldots\ j_p).$$

By Lemma 5.12, any permutation σ such that $\sigma(i_m) = j_m$ for all $1 \leqslant m \leqslant p$ must satisfy $\sigma\alpha\sigma^{-1} = \beta$.

Note that such σ has no restrictions on what it does to the set $\{1, \ldots, n\} \setminus \{i_1\ \ldots\ i_p\}$: it can map $\{1, \ldots, n\} \setminus \{i_1\ \ldots\ i_p\}$ bijectively to $\{1, \ldots, \} \setminus \{j_1\ \ldots\ j_p\}$ in any way possible. From this observation, the general case follows: since the cycles are disjoint, we can find a single permutation σ such that $\sigma\alpha_i\sigma^{-1} = \beta_i$ for all i. □

We can now classify all the conjugacy classes in S_n based on their cycle type.

Example 5.14. Given Theorem 5.13, we can now write a complete list of the conjugacy classes of S_4:

(1) The conjugacy class of the identity $\{e\}$.
(2) The conjugacy class of (12), which is the set of all two cycles and has $\binom{4}{2} = 6$ elements.
(3) The conjugacy class of (123), which is the set of all three cycles and has $4 \cdot 2 = 8$ elements.
(4) The conjugacy class of (1234), which is the set of all four cycles and has $3! = 6$ elements.
(5) The conjugacy class of (12)(34), which is the set of all products of two disjoint 2-cycles and has 3 elements.

We can check our work by recalling that the conjugacy classes partition S_4, and indeed we counted 24 elements.

Example 5.15. Given Theorem 5.13, we can now write a complete list of the conjugacy classes of S_5:

(1) The conjugacy class of the identity $\{e\}$.
(2) The conjugacy class of (12), which is the set of all 2-cycles and has $\binom{5}{2} = 10$ elements.
(3) The conjugacy class of (123), containing all 3-cycles, of size $2! \cdot \binom{5}{3} = 20$ elements.
(4) The conjugacy class of (1234), containing all 4-cycles, of size $5 \cdot 3! = 30$ elements.
(5) The conjugacy class of (12345), which is the set of all 5-cycles, and has $4! = 24$ elements.
(6) The conjugacy class of (12)(34), which is the set of all products of two disjoint 2-cycles and has $5 \cdot 3 = 15$ elements.
(7) The conjugacy class of (12)(345), which is the set of all products of a 2-cycle by a 3-cycle, and has $\binom{5}{2} \cdot 2! = 20$ elements.

We can check our work by noting that indeed

$$1 + 10 + 20 + 30 + 24 + 15 + 20 = 120 = 5!.$$

Remark 5.16. For any nontrivial group G, since $[e]_c = \{e\}$ and the conjugacy classes partition G, then $[g]_c \neq G$ for all $g \in G$.

Definition 5.17. Let G be a group and $a \in G$. The **centralizer** of a is the set of elements of G that commute with a:

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

More generally, given a subset $S \subseteq G$, the **centralizer** of S is the set

$$C_G(S) := \{x \in G \mid xs = sx \text{ for all } s \in S\}$$

Definition 5.18. Let G be a group and consider a subset $S \subseteq G$. The **normalizer** of S is the set

$$N_G(S) := \{g \in G \mid gSg^{-1} = S\}.$$

Exercise 26. Let G be a group and $S \subseteq G$. Prove that the centralizer and the normalizer of S are subgroups of G.

Lemma 5.19. *Let $S \subseteq G$ be any subset of a group G. Then $C_G(S) \subseteq N_G(S)$.*

Proof. Let G be a group and $S \subseteq G$. If $x \in C_G(S)$, then for all $s \in S$ we have

$$xs = sx \implies xsx^{-1} = s \in S \text{ and } x^{-1}sx = s.$$

Thus $xSx^{-1} \subseteq S$ and $x^{-1}Sx \subseteq S$. Now for any $s \in S$ we have $x^{-1}sx \in S$ and s can be written as

$$s = x(x^{-1}sx)x^{-1} \in xSx^{-1}.$$

This shows that $S \subseteq xSx^{-1}$. Thus $xSx^{-1} = S$, and therefore $x \in N_G(S)$. $\square$

Remark 5.20. If G is an abelian group, then for any $a \in G$ we have $C_G(a) = G = N_G(a)$.

Exercise 27. Let H be a subgroup of a group G, and S a subset of H. Then

$$C_H(S) = C_G(S) \cap H \quad \text{and} \quad N_H(S) = N_G(S) \cap H.$$

Exercise 28. Let G be a group and let H be a subgroup of G. Show that $N_G(H)/C_G(H)$ is isomorphic to a subgroup of the automorphism group $\operatorname{Aut}(H)$ of H.

Exercise 29. Let G be a group and H a subgroup of G. Prove that if H is normal in G, then so is $C_G(H)$, and that $G/C_G(H)$ is isomorphic to a subgroup of the automorphism group of H.

Lemma 5.21. *Let G be a group. Consider the action of G on G by conjugation, where $g \cdot h = ghg^{-1}$. For all $g \in G$,*

$$\operatorname{Orb}_G(g) = [g]_c \quad \text{and} \quad \operatorname{Stab}_G(g) = C_G(g) \quad \text{and} \quad |[g]_c| = [G : C_G(g)].$$

Proof. The first statement is the definition of the conjugacy class of g: $\operatorname{Orb}_G(g) = [g]_c$. Moreover, by simply following the definitions we see that

$$h \in \operatorname{Stab}_G(g) \iff h \cdot g = g \iff hgh^{-1} = g \iff hg = gh \iff h \in C_G(G).$$

Thus, $\operatorname{Stab}_G(g) = C_G(G)$, and by the Orbit-Stabilizer Theorem,

$$|[g]_c| = |\operatorname{Orb}_G(g)| = [G : C_G(g)].$$ $\square$

Exercise 30. Let G be a group. Consider the action of G on the power set

$$P(G) = \{S \mid S \subseteq G\}$$

of G by conjugation, meaning $g \cdot S = gSg^{-1}$. For all $S \in P(G)$,

$$\operatorname{Stab}_G(S) = N_G(S) \quad \text{and} \quad |\operatorname{Orb}_G(S)| = [G : N_G(S)].$$

Corollary 5.22. *For a finite group G, the size of any conjugacy class divides $|G|$.*

Proof. Let $g \in G$. By Lemma 5.21, the order of the conjugacy class of g is the index of the centralizer:

$$|[g]_c| = [G : C_G(g)]$$

By Lagrange's Theorem, the index of any subgroup must divide $|G|$, and thus in particular $|[g]_c|$ divides $|G|$. □

We will take the Orbit Equation and apply it to the special case of the conjugation action. In order to do that, all that remains is to identify the fixed points of the action.

Lemma 5.23. *Let G be a group acting on itself by conjugation. An element $g \in G$ is a fixed point of the conjugation action if and only $g \in \mathrm{Z}(G)$.*

Proof. ($\Leftarrow$) Suppose that $g \in \mathrm{Z}(G)$. Then for all $h \in G$, g commutes with h, and thus

$$hgh^{-1} = (hg)h^{-1} = g(hh^{-1}) = g.$$

Thus g is conjugate to only itself, meaning it is a fixed point for the conjugation action.

($\Rightarrow$) Conversely, suppose that g is a fixed point for the conjugation action. Then for all $h \in G$,

$$hgh^{-1} = h \cdot g = g \implies hg = gh.$$

Thus $g \in \mathrm{Z}(G)$. □

We can now write the Orbit Equation for the conjugation action; this turns out to be a very useful formula.

Theorem 5.24 (The Class Equation)**.** *Let G be a finite group. For each conjugacy class of sizer greater than 1, pick a unique representative, and let $g_1, \ldots g_r \in G$ be the list of all the chosen representatives. Then*

$$|G| = |\,\mathrm{Z}(G)| + \sum_{i}^{r} |G : C_G(g_i)|.$$

Proof. By Lemma 5.23, the elements of $\mathrm{Z}(G)$ are precisely the fixed points of the conjugation action. In particular, $|\,\mathrm{Z}(G)|$ counts the number of orbits that have only one element. Because the orbits of the conjugation action partition G, and the conjugacy classes are the orbits, then as noted in Remark 5.7

$$|G| = |\,\mathrm{Z}(G)| + \sum_{i}^{r} [g_i]_c.$$

By LOIS, the index of the stabilizer is the order of the conjugacy class. Thus for each g_i as in the statement we have

$$[g_i]_c = [G : C_G(g_i)].$$

The class equation follows from substituting this into the equation above:

$$|G| = |\,\mathrm{Z}(G)| + \sum_{i}^{r} |G : C_G(g_i)|.$$ □

Remark 5.25. The class equation is not very interesting if G is abelian, since there is only one term on the right hand side: $|\operatorname{Z}(G)|$.

But when G is nonabelian, the class equation can lead us to discover some very interesting facts, despite its simplicity.

Exercise 31. Prove that if G is a nonabelian group of order 21, then there is only one possible class equation for G, meaning that the numbers appearing in the class equation are uniquely determined up to permutation.

Corollary 5.26. *If p is a prime number and G is a finite group of order p^m for some $m > 0$, then $\operatorname{Z}(G)$ is not the trivial group.*

Proof. Let $g_1, \dots g_r \in G$ be a list of unique representatives of all of the conjugacy classes of G of size greater than 1, as in the Class Equation. By construction, each g_i is not a fixed point of the action, and thus $\operatorname{Stab}_G(g_i) \neq G$. By Lemma 5.21, $C_G(g_i) = \operatorname{Stab}_G(g_i)$, so $C_G(g_i) \neq G$. In particular, $[G : C_G(g_i)] \neq 1$. Since $1 \neq [G : C_G(g_i)]$ and $[G : C_G(g_i)]$ divides $|G| = p^m$, we conclude that p divides $[G : C_G(g_i)]$ for each i. From the Class Equation, we can now conclude that p divides $|\operatorname{Z}(G)|$, and in particular $|\operatorname{Z}(G)| \neq 1$. □

Exercise 32. Let p be prime and let G be a group of order p^m for some $m \geqslant 1$. Show that if N is a nontrivial normal subgroup of G, then $N \cap Z(G) \neq \{e\}$. In fact, show that $|N \cap Z(G)| = p^j$ for some $j \geqslant 1$.

Lemma 5.27. *Let G be a group and $N \trianglelefteq G$. The conjugation action of G on itself induces an action by conjugation of G on N. In particular, N is the disjoint union of some of the conjugacy classes in G.*

Proof. Define the conjugation action of G on N by $g \cdot n = gng^{-1}$ for all $g \in G$ and $n \in N$. Since $N \trianglelefteq G$, this always gives us back an element of N, and thus the action is well-defined. We can think of this action as a restriction of the action of G on itself by conjugation, and thus the two properties in the definition of an action hold for the action of G by conjugation on N. Therefore, this is indeed an action. The orbits of elements $n \in N$ under this action are the conjugacy classes $[n]_c$, and we have just shown that for all $n \in N$, $[n]_c \subseteq N$. But every element in N belongs to some conjugacy class, thus the conjugacy classes of the elements of N partition N. □

Remark 5.28. Lemma 5.27 says that the orbits of the conjugation action of G on a normal subgroup N are just the orbits of the conjugation action of G on itself that contain elements of N (and must thus be completely contained in N). In contrast, if N is a normal subgroup of G, we can also consider the conjugation action of N on itself. If a and b are elements of N that are conjugate for the N-conjugation, then they must also be conjugate for the G-conjugation action, using the same element $n \in N$ such that $a = nbn^{-1}$. However, if a and b are conjugate for the G-conjugation, they might not necessarily be conjugate for the N-action, as all the elements $g \in G$ such that $a = gbg^{-1}$ could very well all be in $G \setminus N$.

We will see examples of this in the next section, where we will study the special case of the alternating group.

5.3 The alternating group

Since $A_n \leq S_n$, we know that *if* two elements of A_n are conjugate, *then* they have the same cycle type, as they are also conjugate elements of S_n, and thus we can apply Theorem 5.13. But as noted in Remark 5.28, there is no reason for the converse to hold: given $\alpha, \beta \in A_n$ of the same cycle type, the elements $\sigma \in S_n$ such that $\sigma\alpha\sigma^{-1} = \beta$ might all belong to $S_n \setminus A_n$. Indeed, we will see that this does happen in some cases.

Example 5.29. The two permutations (123) and (132) are not conjugates in A_3, despite having the same cycle type and thus being conjugate in A_3 by Theorem 5.13. One can check this easily, for example, by conjugating (123) by the 3 elements in A_3.

Lemma 5.30. *Let σ be an m-cycle in S_n. Then*

$$\sigma \in A_n \iff m \text{ is odd.}$$

Proof. Recall that by Exercise 6,

$$(i_1\, i_2\, \cdots\, i_m) = (i_1\, i_m)(i_1\, i_{m-1})(i_1\, i_3)(i_1\, i_2)$$

is a product of $m-1$ transpositions. Thus σ is even if and only if $m-1$ is even. □

Lemma 5.31 (Conjugacy classes of A_5)**.** *The conjugacy classes of A_5 are given by the following list:*

(1) The singleton $\{e\}$ is a conjugacy class.

(2) The conjugacy class of $(1\,2\,3\,4\,5)$ in A_5 has 12 elements.

(3) The conjugacy class of $(2\,1\,3\,4\,5)$ in A_5 has 12 elements, and it is disjoint from the conjugacy class of $(1\,2\,3\,4\,5)$.

(4) The collection of all three cycles, of which there are 20, forms a conjugacy class in A_5.

(5) The collection of all products of two disjoint transpositions, of which there are 15, forms one conjugacy class in A_5.

As a reality check, note that $12 + 12 + 20 + 15 + 1 = 60 = |A_5|$.

Proof. By Lemma 5.30, the cycle types of elements of A_5 are

- five cycles, of which there are $4! = 24$,
- three cycles, of which there are $\binom{5}{3}2 = 20$,
- products of two disjoint transpositions, of which there are $5 \cdot 3 = 15$, and
- the unique 1-cycle e, and indeed $[e]_c = \{e\}$.

By Theorem 5.13, we know that two permutations are conjugate in S_5 if and only if they have the same cycle type. It follows that the conjugacy classes in A_5 form a subset of the cycles types. The statement we are trying to prove asserts that the set of five cycles breaks apart into two conjugacy classes in A_5, whereas in all the other cases, the conjugacy classes remain whole.

Claim: Fix a 5-cycle σ. The conjugacy class of σ in A_5 has 12 elements.

By Lagrange's Theorem,

$$|C_{S_5}(\sigma)| = \frac{|S_5|}{[S_5 : C_{S_5}(\sigma)]}.$$

By Lemma 5.21,

$$[S_5 : C_{S_5}(\sigma)] = |[\sigma]_c|.$$

By Theorem 5.13, this is the number of 5-cycles in S_5, which is $4!$. Thus

$$|C_{S_5}(\sigma)| = \frac{5!}{4!} = 5.$$

Since every power of σ commutes with σ, and there are 5 such elements, we conclude that

$$C_{S_5}(\sigma) = \{e, \sigma, \sigma^2, \sigma^3, \sigma^4\}.$$

But these are all in A_5, and thus by Exercise 27 we conclude that

$$C_{A_5}(\sigma) = C_{S_5}(\sigma) \cap A_5 = \{e, \sigma, \sigma^2, \sigma^3, \sigma^4\}.$$

By LOIS, Lemma 5.21, and Lagrange's Theorem,

$$\text{the size of the conjugacy class of } \sigma \text{ in } A_5 = [A_5 : C_{A_5}(\sigma)] = \frac{|A_5|}{|C_{A_5}(\sigma)|} = \frac{60}{5} = 12.$$

This proves the claim.

We have now shown that the conjugacy class of each 5-cycle has 12 elements, and all twenty-four 5-cycles are in A_5. Thus there are two conjugacy classes of 5-cycles in A_5. This shows that σ is only conjugate in A_5 to half of the five cycles. If we pick two 5-cycles σ and τ that are not conjugate in A_5, then τ is conjugate to exactly 12 elements, which must be exactly the other 5-cycles that σ is not conjugate to.

One can see that in fact $(1\,2\,3\,4\,5)$ and $(2\,1\,3\,4\,5)$ are not conjugate. While they *are* conjugate *in* S_5, it is via the element $(1\,2)$, which is *not* in A_5. Suppose that $\alpha \in S_5$ is such that

$$\alpha(2\,1\,3\,4\,5)\alpha^{-1} = (1\,2\,3\,4\,5).$$

Note that $\tau = \alpha(1\,2)$ satisfies

$$\begin{aligned}
\tau(1\,2\,3\,4\,5) &= \alpha(1\,2)(1\,2\,3\,4\,5)\\
&= \alpha(2\,1\,3\,4\,5)\\
&= (2\,1\,3\,4\,5)\alpha\\
&= (1\,2\,3\,4\,5)(1\,2)\alpha\\
&= (1\,2\,3\,4\,5)\tau.
\end{aligned}$$

Thus $\alpha(1\,2) \in C_{S_5}(1\,2\,3\,4\,5)$, or equivalently,

$$\alpha \in (1\,2) \cdot C_{S_5}(2\,1\,3\,4\,5).$$

But note that we just proved that every element in $C_{S_5}(2\,1\,3\,4\,5)$ is in A_5, and thus even; this shows that every element in the coset

$$(1\,2) \cdot C_{S_5}(2\,1\,3\,4\,5)$$

is odd (as we multiplied by *one* transposition), and thus there are no such α in A_5. This proves (1) and (2).

Claim: All 20 three cycles are conjugate in A_5.

Given two three cycles $(a\,b\,c)$ and $(d\,e\,f)$ in S_5, we already know that they are both in A_5 and that there is a $\sigma \in S_5$ such that

$$\sigma(a\,b\,c)\sigma^{-1} = (d\,e\,f).$$

If $\sigma \notin A_5$, let $\{1, \ldots, 5\} \setminus \{a, b, c\} = \{x, y\}$. Then σ is a product of an odd number of transpositions, so $\sigma \cdot (x\,y) \in A_5$. Moreover, since $(x\,y)$ and $(a\,b\,c)$ are disjoint cycles, then by Lemma 1.35 they must commute, so that

$$(x\,y)(a\,b\,c)(x\,y))^{-1} = (a\,b\,c).$$

Therefore,

$$(\sigma \cdot (x\,y))(a\,b\,c)(\sigma \cdot (x\,y))^{-1} = (d\,e\,f),$$

so $(a\,b\,c)$ and $(d\,e\,f)$ are still conjugate in S_5. This proves the claim.

Claim: All products of two disjoint transpositions are conjugate in A_5.

Set $\alpha = (1\,2)(3\,4)$. The conjugacy class of α in S_5 consists of all the products of two disjoint two-cycles, and there are 15 such elements. By lois and Lemma 5.21,

$$15 = |\text{ the conjugacy class of } \alpha \text{ in } S_5 \,| = [S_5 : C_{S_5}(\alpha)] = \frac{120}{|C_{S_5}(\alpha)|}.$$

Thus

$$|C_{S_5}(\alpha)| = \frac{120}{15} = 8.$$

Since α commutes with e, α, $(1\,3)(2\,4)$ and $(1\,4)(2\,3)$ and each of these belongs to A_5, we must have $|C_{A_5}(\alpha)| \geqslant 4$. Since, by Exercise 27,

$$C_{A_5}(\alpha) = C_{S_5}(\alpha) \cap A_5,$$

it follows that $|C_{A_5}(\alpha)|$ must divide both 8 and 60, and so must be 1, 2 or 4. We conclude that $|C_{A_5}(\alpha)| = 4$. Thus α is conjugate in A_5 to $60/4 = 15$ elements. Since there are 15 products of disjoint two-cycles, they must all be conjugate to α, and thus the conjugacy class of α in A_5 is still the set of all 2-cycles. $\square$

Now that we have completely calculated all the conjugacy classes of A_5, our hard work will pay off: we can now prove a very important result in group theory.

Definition 5.32. A nontrivial group G is **simple** if it has no proper nontrivial normal subgroups.

Exercise 33. Let p be prime. Show that $\mathbb{Z}/p$ is a simple group.

Theorem 5.33. *The group A_5 is a simple group.*

Proof. Suppose $N \trianglelefteq A_5$. By Lagrange's Theorem, $|N|$ divides

$$|A_5| = \frac{5!}{2} = 60.$$

By Lemma 5.31, A_5 has only four nontrivial conjugacy classes, and they have order 12, 12, 15, and 20. By Lemma 5.27, $|N|$ is a union of conjugacy classes of A_5. Thus

$$|N| = 1 + \text{ the sum of a sublist of the list } 20, 12, 12, 15.$$

By checking the relatively small number of cases we see that $|N| = 1$ or $|N| = 60$ are the only possibilities, as the remaining options do not divide 60. $\square$

In fact, A_n is simple for all $n \geqslant 5$, but we will not prove this. In contrast, A_4 is not simple:

Example 5.34. The alternating group A_3 is simple and abelian since it has order 3.

Both A_1 and A_2 are the trivial group.

Exercise 34. Consider the subset of A_4 given by

$$V = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}.$$

Show that V is a normal subgroup of A_4.

Example 5.35. The alternating group A_4 is not simple, since it has 12 elements and a normal subgroup of order 4.

Thus the story goes:

Theorem 5.36. *Let $n \geqslant 3$. The alternating group A_n is simple if and only if $n \neq 4$.*

In fact, one can show that A_5 is the smallest nonabelian simple group, having 60 elements. This we will also not prove.

5.4 Other group actions with applications

Let's discuss a couple other group actions that often lead to useful information about the group doing the acting. The first one arises from the action of a group on the collection of left cosets of one of its subgroups. More precisely, let G be a group and H a subgroup, and let $\mathcal{L}$ denote the collection of left cosets of H in G:

$$\mathcal{L} = \{xH \mid x \in G\}.$$

When H is normal, $\mathcal{L}$ is the quotient group $\mathcal{L} = G/H$, but note that we are not assuming that H is normal. Then G acts on $\mathcal{L}$ via the rule

$$g \cdot (xH) := (gx)H.$$

This action is transitive: for all x,

$$xH = x \cdot (eH).$$

The stabilizer of the element $H \in \mathcal{L}$ is

$$\mathrm{Stab}_G(H) = \{x \in G \mid xH = H\} = H,$$

which is consistent with LOIS, as indeed

$$\mathrm{Orb}_G(H) = \mathcal{L}, \quad \text{so } |\operatorname{Orb}(H)| = |\mathcal{L}| = [G : H],$$

while

$$\mathrm{Stab}_G(H) = H, \quad \text{so } [G : \mathrm{Stab}_G(H)] = [G : H].$$

As with any group action, this action induces a homomorphism

$$\rho \colon G \to \mathrm{Perm}(\mathcal{L})$$

where for any g,

$$\begin{aligned} \mathrm{Perm}(\mathcal{L}) &\xrightarrow{\rho(g)} \mathrm{Perm}(\mathcal{L}) \\ xH &\longmapsto (gx)H. \end{aligned}$$

If $n = [G : H] = |\operatorname{Perm}(\mathcal{L})|$ is finite, then we have a homomorphism $\rho \colon G \to S_n$.

Lemma 5.37. *Let G be a group and H a subgroup of G. Consider the action of G on the set $\mathcal{L}$ of left cosets of H, and the corresponding permutation representation $\rho \colon G \to \mathrm{Perm}(\mathcal{L})$. Then*

$$\ker(\rho) = \bigcap_{x \in G} xHx^{-1}.$$

In particular, $\ker(\rho) \subseteq H$.

Note that $\bigcap_{x \in G} xHx^{-1}$ is the largest normal subgroup of G contained in H.

Proof. Note that

$$\begin{aligned} g \in \ker(\rho) &\iff (gx)H = xH \text{ for all } x \in G \\ &\iff x^{-1}gx \in H \text{ for all } x \in G \\ &\iff g \in xHx^{-1} \text{ for all } x \in G. \end{aligned}$$

Thus

$$\ker(g) = \bigcap_{x \in G} xHx^{-1}.$$

Since $eHe^{-1} = H$, we conclude that $\ker(g) \subseteq H$. $\square$

Remark 5.38. The action of G on the left cosets of H might be faithful or not. Lemma 5.37 says that the action is faitfull if and only if

$$\bigcap_{x \in G} xHx^{-1} = \{e\}.$$

If H is a normal subgroup of G, then in fact

$$\bigcap_{x \in G} xHx^{-1} = H,$$

and thus the action is not faithful unless $H = \{e\}$.

Remark 5.39. Consider the subgroup $H = \langle (12) \rangle$ of S_3. The action of S_3 on the left cosets of H is faithful: for example, taking $\sigma = (13)$ we have

$$\sigma H \sigma^{-1} = \{e, (12)(13)\} = \{e, (23)\},$$

and thus the permutation representation $\rho\colon S_3 \to S_3$ associated with the action has

$$\ker \rho \subseteq \sigma H \sigma^{-1} \cap H = \{e\}.$$

Theorem 5.40. *Let G be a finite group and H a subgroup of index p, where p is the smallest prime divisor of $|G|$. Then H is normal.*

Proof. The action of G on the set of left cosets of H in G by left multiplication induces a homomorphism $\rho\colon G \to S_p$. By Lemma 5.37, its kernel $N := \ker(\rho)$ is contained in H. By the First Isomorphism Theorem,

$$[G : N] = |G/N| = |\operatorname{im}(f)|.$$

By Lagrange's Theorem, since $\operatorname{im}(f)$ is a subgroup of S_p then $[G : N] = |\operatorname{im}(f)|$ divides $|S_p| = p!$. On the other hand, $[G : N]$ divides $|G|$ by Lagrange's Theorem. Since $[G : N]$ divides both $|G|$ and $p!$, it must divide $\gcd(|G|, p!)$. Since p is the smallest prime divisor of G, we must have

$$\gcd(|G|, p!) = p.$$

It follows that $[G : N]$ divides p, and hence $[G : N] = 1$ or $[G : N] = p$. But $N \subseteq H$, and H is a proper subgroup of G, so $N \neq G$, and thus $[G : N] \neq 1$. Therefore, we conclude that $[G : N] = p$. Since $N \subseteq H$ and $[G : H] = p = [G : N]$, we conclude that $H = N$. In particular, H must be a normal subgroup of G. $\square$

This generalizes Exercise 20, which says that any subgroup of index 2 is normal.

Another interesting action arises from the following.

Exercise 35. Let H be a subgroup of G.

(a) Fix $g \in G$. Prove that $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ is a subgroup of G of the same order as H.

Note: we are not assuming that H is finite, so you must show that there is a bijection between H and gHg^{-1}.

(b) Show that if H is the unique subgroup of G of order $|H|$, then $H \trianglelefteq G$.

So we can now define an action. Let G be a group and let

$$\mathcal{S}(G) = \{H \mid H \leq G\}$$

be the collection of all subgroups of G. Then G acts on $\mathcal{S}$ by

$$g \cdot H = gHg^{-1}.$$

Definition 5.41. Two subgroups A and B of a group G are **conjugate** if there exists $g \in G$ such that $A = gBg^{-1}$.

Equivalently, two subgroups are conjugate if they are in the same orbit by the following group action: the action of G on the set of its subgroups by conjugation.

Exercise 36. Let G be a group and let

$$\mathcal{S}(G) = \{H \mid H \leq G\}.$$

Check that the rule

$$g \cdot H = gHg^{-1}$$

defines an action of G on $\mathcal{S}(G)$. Moreover, prove that given any subgroup H of G, the stabilizer of H is given by $N_G(H)$.

The normalizer $N_G(H)$ is the largest subgroup of G that contains H as a normal subgroup, meaning that $H \trianglelefteq N_G(H)$.

Exercise 37. Let G be a group and H be a subgroup of G. Show that if K is any subgroup of G such that $H \trianglelefteq K$, then $K \leq N_G(H)$. In particular, $H \trianglelefteq G$ if and only if $N_G(H) = G$.

We can now show that the number of subgroups conjugate to a given subgroup is the index of its normalizer:

Lemma 5.42. *Let G be a group and H be a subgroup of G. The number of subgroups of G that are conjugate to H is equal to $[G : N_G(H)]$.*

Proof. The number of subgroups of G that are conjugate to H is just the size of the orbit of H under the action of G by conjugation on the set of subgroups of G. By LOIS, the number of elements in the orbit of H is the index of the stabilizer. Finally, by Exercise 36, the stabilizer of H is $N_G(H)$. $\square$

Here is an application of this action:

Lemma 5.43. *If G is finite and H is a proper subgroup of G, then*

$$G \neq \bigcup_x xHx^{-1}.$$

Proof. First, suppose that H is a normal. Then $H = xHx^{-1}$ for all $x \in G$, so

$$\bigcup_x xHx^{-1} = H \neq G.$$

Now assume that H is not normal, so that $N_G(H) \neq G$ and $[G : N_G(H)] \geqslant 2$. By Exercise 35, we have $|H| = |xHx^{-1}|$ for all x. Since there are $[G : N_G(H)]$ conjugates of H by Lemma 5.42, and since $e \in xHx^{-1}$ for all x, we get

$$\left| \bigcup_x xHx^{-1} \right| \leqslant [G : N_G(H)] \cdot |H|.$$

But in fact, this calculation can be improved, as there are at least two distinct conjugates of H and e is an element of all of them. This gives us

$$\left| \bigcup_x xHx^{-1} \right| \leqslant [G : N_G(H)] \cdot |H| - 1.$$

But $H \subseteq N_G(H)$ and so $[G : N_G(H)] \leq [G : H]$. We conclude that

$$\left| \bigcup_x xHx^{-1} \right| \leqslant [G : H] \cdot |H| - 1 = |G| - 1. \qquad \square$$

Since $|H| = |xHx^{-1}|$ for all $x \in G$, we can fix a natural number n, set

$$\mathcal{S}_n(G) := \{H \mid H \leq G \text{ and } |H| = n\},$$

and consider the action of G on $\mathcal{S}_n(G)$ by conjugation. This idea will be exploited in the next section.

Exercise 38. Show that if G is a finite group acting transitively on a set S with at least two elements, then there exists $g \in G$ with no fixed points, meaning $g \cdot s \neq s$ for all $s \in S$.

Chapter 6

Sylow Theory

Sylow Theory is a very powerful technique for analyzing finite groups of relatively small order. One aspect of Sylow theory is that it allows us to deduce, in certain special cases, the existence of a unique subgroup of a given order, and thus it allows one to construct a normal subgroup.

6.1 Cauchy's Theorem

We start by proving a very powerful statement: that every finite group whose order is divisible by p must have an element of order p.

Theorem 6.1 (Cauchy's Theorem)**.** *If G is a finite group and p is a prime number dividing $|G|$, then G has an element of order p. In fact, there are at least $p-1$ elements of order p.*

Proof. Let S denote the set of ordered p-tuples of elements of G whose product is e:

$$S = \{(x_1, \ldots, x_p) \mid x_i \in G \text{ and } x_1 x_2 \cdots x_p = e\}.$$

Consider

$$G^{p-1} := \underbrace{G \times \cdots \times G}_{p-1 \text{ factors}}$$

and the map

$$\begin{aligned} G^{p-1} &\xrightarrow{\quad\phi\quad} S \\ (x_1, \ldots, x_{p-1}) &\longmapsto (x_1, \ldots, x_{p-1}, x_{p-1}^{-1} \cdots x_1^{-1}). \end{aligned}$$

Given the definition of S, the map ϕ does indeed land in S. Moreover, ϕ is bijective since the map $\psi\colon S \to G^{p-1}$ given by

$$\psi(x_1, \ldots, x_p) = (x_1, \ldots, x_{p-1})$$

is a two-sided inverse of the map above. Therefore, $|S| = |G^{p-1}| = |G|^{p-1}$.

Let C_p denote cyclic subgroup of S_p of order p generated by the p-cycle

$$\sigma = (1\,2\,\cdots\,p).$$

The following rule gives an action of C_p on S:

$$\sigma^i \cdot (x_1, \dots, x_p) := (x_{\sigma^i(1)}, \dots, x_{\sigma^i(p)}) = (x_{1+i}, x_{2+i}, \dots, x_{p+i}),$$

where the indices are taken modulo p. We should check that this is indeed an action. On the one hand, σ^0 is the identity map, so

$$e \cdot (x_1, \dots, x_p) = \sigma^0 \cdot (x_1, \dots, x_p) = (x_{\sigma^0(1)}, \dots, x_{\sigma^0(p)}) = (x_1, \dots, x_p).$$

Moreover,

$$\sigma^i \cdot \big(\sigma^j \cdot (x_1, \dots, x_p)\big) = \sigma^i \cdot (x_{1+j}, x_{2+j}, \dots, x_{p+j}) = (x_{1+j+i}, x_{2+j+i}, \dots, x_{p+j+i}),$$

while

$$(\sigma^i \sigma^j) \cdot (x_1, \dots, x_p) = \sigma^{i+j} \cdot (x_1, \dots, x_p) = (x_{1+i+j}, x_{2+i+j}, \dots, x_{p+i+j}).$$

Thus

$$\sigma^i \cdot \big(\sigma^j \cdot (x_1, \dots, x_p)\big) = (\sigma^i \sigma^j) \cdot (x_1, \dots, x_p),$$

and we have shown that this is indeed an action.

Now let us consider the fixed points of this action. If

$$\sigma \cdot (x_1, \dots, x_p) = (x_1, \dots, x_p),$$

then $x_{i+1} = x_i$ for $1 \leqslant i \leqslant p$, so it follows that

$$x_1 = x_2 = \cdots = x_p.$$

Thus if $\sigma \cdot (x_1, \dots, x_p) = (x_1, \dots, x_p)$, then $(x_1, \dots, x_p)$ corresponds to an element x such that $x^p = x_1 \cdots x_p = e$. On the other hand, if σ fixes $(x_1, \dots, x_p)$, then so does any element of C_p. Therefore, a fixed point for this action corresponds to an element x such that $x^p = e$. The element $(e, e, \dots, e)$ is a fixed point. Any other fixed point, meaning an orbit of size one, corresponds to an element of G order p, thus we wish to show that there is at least one fixed point besides $(e, \dots, e)$.

By the Orbit-Stabilizer Theorem, the size of every orbit divides $|C_p| = p$. Since p is prime, every orbit for this action has size 1 or p. By the Orbit Equation,

$$|S| = \# \text{ fixed points } + p \cdot \# \text{ orbits of size } p$$

Since p divides $|S|$, we conclude that p divides the number of fixed points. We already know that there is at least one fixed point, $(e, \dots, e)$. Thus there must be at least one other fixed point; in fact, at least $p - 1$ others, since the number of fixed points must then be at least p. $\square$

We now know that if p divides $|G|$, then G has an element of order p. However, this is not true if n divides $|G|$ but n is not prime. In fact, G may not even have any subgroup of order n.

Exercise 39. Prove that the converse to Lagrange's theorem is false: find a group G and an integer $d > 0$ such that d divides the order of G but G does not have any subgroup of order d.

6.2 The Main Theorem of Sylow Theory

Definition 6.2. Let G be a finite group and p a prime. Write the order of G as $|G| = p^e m$ where $p \nmid m$. A **p-subgroup** of G is a subgroup of G of order p^k for some k. A **Sylow p-subgroup** of G is a subgroup $H \leq G$ such that $|H| = p^e$.

Thus a Sylow p-subgroup of G is a subgroup whose order is the highest conceivable power of p according to Lagrange's Theorem.

Definition 6.3. We will denote the collection of all Sylow p-subgroups of G by $\mathrm{Syl}_p(G)$.

This is, of course, not very interesting unless $e > 0$. Nevertheless, we allow that case.

Remark 6.4. When p does not divide $|G|$, we have $e = 0$ and G has a unique Sylow p-subgroup, namely $\{e\}$, which indeed has order $p^0 = 1$.

Note that even if p does divide $|G|$, it is a priori possible that $n_p = 0$ for some groups G and primes p. We will prove this is not possible, and that is actually one of the hardest things to prove to establish Sylow theory.

Example 6.5. Let $p > 2$ be a prime and consider the group D_p. The subgroup $\langle r \rangle$ is a Sylow p-subgroup, as it has order p and $|D_p| = 2p$. In fact, this is the only Sylow p-subgroup of D_p, as by Exercise 18 every group of order p is cyclic, and the only elements of order p in D_p are r and its powers.

In D_n for n odd, each of the subgroups $\langle sr^j \rangle$, for $j = 0, \ldots, n-1$ is a Sylow 2-subgroup. Since n is odd, only the reflections have order 2, and we have listed all the subgroups generated by reflections, so we conclude that the number of Sylow 2-subgroups is n.

Example 6.6. If G is cyclic of finite order, there is a unique Sylow p-subgroup for each p, since by Theorem 3.29 there is a unique subgroup of each order that divides $|G|$: if $G = \langle x \rangle$ and $|x| = p^e m$ with $p \nmid m$, then the unique Sylow p-subgroup of G is $\langle x^m \rangle$.

Let G be a finite group and p is a prime that divides $|G|$. Then G acts on its Sylow p-subgroups of G via conjugation. As of now, for all we know, this might be the action on the empty set. Sylow Theory is all about understanding this action very well. Before we can prove the main theorem, we need a technical lemma.

Lemma 6.7. *Let G be a finite group, p a prime, P a Sylow p-subgroup of G, and Q any p-subgroup of G. Then $Q \cap N_G(P) = Q \cap P$.*

Proof. ($\subseteq$) Since $P \leq N_G(P)$, then $Q \cap P \leq Q \cap N_G(P)$.

($\supseteq$) Let $H := Q \cap N_G(P)$. Since $H \subseteq N_G(P)$, then $PH = HP$, so by Exercise 24 we get that PH is a subgroup of G. By Corollary 4.49, we have

$$|PH| = \frac{|P| \cdot |H|}{|P \cap H|}$$

and since each of $|P|$, $|H|$, and $|P \cap H|$ is a power of p, we conclude that the order of PH is also a power of p. In particular, PH is a p-subgroup of G. On the other hand, $P \leq PH$ and P is already a p-subgroup of the largest possible order, so we must have $P = PH$. Note that $H \leq PH$ always holds. We conclude that $H \leq P$ and thus $H \leq Q \cap P$. $\square$

Theorem 6.8 (Main Theorem of Sylow Theory)**.** *Let p be prime. Assume G is a group of order $p^e m$, where p is prime, $e \geqslant 0$, and $\gcd(p, m) = 1$.*

(1) There exists at least one Sylow p-subgroup of G. In short, $\mathrm{Syl}_p(G) \neq \emptyset$.

(2) If P is a Sylow p-subgroup of G and $Q \leq G$ is any p-subgroup of G, then $Q \leq gPg^{-1}$ for some $g \in G$. Moreover, any two Sylow p-subgroups are conjugate and the action of G on $\mathrm{Syl}_p(G)$ by conjugation is transitive.

(3) We have

$$|\,\mathrm{Syl}_p(G)| \equiv 1 \mod p.$$

(4) For any $P \in \mathrm{Syl}_p(G)$,

$$|\,\mathrm{Syl}_p(G)| = [G : N_G(P)],$$

and hence

$$|\,\mathrm{Syl}_p(G)| \text{ divides } m.$$

Proof. First we will prove G contains a subgroup of order p^e by induction on $|G| = p^e m$.

When $|G| = 1$, $\{e\}$ is a Sylow p-subgroup, as noted in Remark 6.4. In fact, this argument applies for whenever $e = 0$, so we may thus assume through the rest of the proof that p does divide $|G|$. So suppose that p divides $|G|$ and every group of order $n < |G|$ has a Sylow p-subgroup. We will consider two cases, depending on whether p divides $|\,\mathrm{Z}(G)|$.

If p divides $|\,\mathrm{Z}(G)|$, then by Cauchy's Theorem there is an element $z \in \mathrm{Z}(G)$ of order p. Set $N := \langle z \rangle$. Since $z \in \mathrm{Z}(G)$, then for all $g \in G$ we have

$$gz^i g^{-1} = z^i \in N,$$

and thus $N \trianglelefteq G$. Since

$$|G/N| = \frac{|G|}{|N|} = \frac{p^e m}{p} = p^{e-1} m,$$

by induction hypothesis G/N has a subgroup of order p^{e-1}, which must then have index m. By the Lattice Isomorphism Theorem, this subgroup corresponds to a subgroup of G of index m, hence of order p^e.

Now assume p does not divide $|\,\mathrm{Z}(G)|$, and consider the Class Equation for G: $g_1, \ldots, g_k$ are a complete list of noncentral conjugacy class representatives, without repetition of any class, we have

$$|G| = |\,\mathrm{Z}(G)| + \sum_{i=1}^{k} [G : C_G(g_i)].$$

Suppose that p divides $[G : C_G(g_i)]$ for all i. Since p also divides $|G|$, then this would imply that p divides $|\,\mathrm{Z}(G)|$, but we assumed that p does not divide $|\,\mathrm{Z}(G)|$. We conclude that p does not divide $[G : C_G(g_i)]$ for some i.

Note that $[G : C_G(g_i)]$ divides $|G|$ by Lagrange's Theorem, and thus it must divide m. Set

$$d := \frac{m}{[G : C_G(g_i)]}.$$

Then

$$|C_G(g_i)| = \frac{|G|}{[G : C_G(g_i)]} = \frac{p^e m}{[G : C_G(g_i)]} = p^e d,$$

and note that p does not divide d since it does not divide m. Since g_i is not central, then $e \notin C_G(g_i)$, and in particular $|C_G(g_i)| < |G|$. By induction hypothesis, $C_G(g_i)$ contains a subgroup S of order p^e. But S is also a subgroup of G, and it has order p^e, as desired. This completes the proof of (1): we have shown that G contains a subgroup of order p^e.

To prove (2) and (3), let P be a Sylow p-subgroup and let Q be any p-subgroup. Let $\mathcal{S}_P$ denote the collection of all conjugates of P:

$$\mathcal{S}_P := \{gPg^{-1} \mid g \in G\}.$$

By definition, G acts transitively on $\mathcal{S}_P$ by conjugation. Restricting that action to Q, we get an action of Q on $\mathcal{S}_P$, though note that we do now know if that action is transitive. The key to proving parts (2) and (3) of the Sylow Theorem is to analyze the action of Q on $\mathcal{S}_P$.

Let $\mathcal{O}_1, \ldots, \mathcal{O}_s$ be the distinct orbits of the action of Q on $\mathcal{S}_P$, and for each i pick a representative $P_i \in O_i$. Note that

$$\begin{aligned}
\mathrm{Stab}_Q(P_i) &= \{q \in Q \mid qP_iq^{-1} = P_i\} && \text{by the definition of the action}\\
&= N_Q(P_i) && \text{by definition of normalizer}\\
&= Q \cap N_G(P_i) && \text{by Exercise 27}\\
&= Q \cap P_i && \text{by Lemma 6.7.}
\end{aligned}$$

By LOIS, we have $|\mathcal{O}_i| = [Q : Q \cap P_i]$, and thus by the Orbit Equation

$$|\mathcal{S}_P| = \sum_{i=1}^{s} [Q : Q \cap P_i]. \tag{6.2.1}$$

This equation 6.2.1 holds for any p-subgroup Q of G. In particular, we can take $Q = P_1$. In this case, the first term in the sum is $[Q : Q \cap P_i] = 1$ and, for all $i \neq 1$ we have

$$Q \cap P_i = P_1 \cap P_i \neq P_1 = Q \implies [Q : Q \cap P_i] > 1.$$

But $|Q|$ is a power of p, so $[Q : Q \cap P_i]$ must be divisible by p for all i. We conclude that

$$|\mathcal{S}_P| \equiv 1 \pmod{p}. \tag{6.2.2}$$

Note, however, that this does not yet prove part (3), since we do not yet know that $\mathcal{S}_P$ consists of *all* the Sylow p-subgroups. But we do have all the pieces we need to prove part (2). Suppose, by way of contradiction, that Q is a p-subgroup of G that is not contained in any of the subgroups in $\mathcal{S}_P$. Then $Q \cap P_i \neq Q$ for all i, and thus every term on the right-hand side of

$$|\mathcal{S}_P| = \sum_{i=1}^{s} [Q : Q \cap P_i]$$

is divisible by p, contrary to (6.2.2). We conclude that Q must be contained in at least one of the subgroups in $\mathcal{S}_P$. This proves the first part of (2).

Moreover, if we take Q to be a Sylow p-subgroup of G, then $Q \leq gPg^{-1}$ for some g, but Q and P are both Sylow p-subgroups of G, so by Exercise 35

$$|Q| = |P| = |gPg^{-1}|.$$

We conclude that $Q = gPg^{-1}$ is conjugate to P. In particular, the conjugation action of G on $\operatorname{Syl}_p(G)$ is transitive, and this finishes the proof of (2).

This proves, in particular, that $\mathcal{S}_P$ in fact does consist of all Sylow p-subgroups, we can now also conclude part (3) from (6.2.2).

Finally, for any $P \in \operatorname{Syl}_p(G)$, the stabilizer of P for the action of G on $\operatorname{Syl}_p(G)$ by conjugation is $N_G(P)$. Since we now know the action is transitive, the Orbit-Stabilizer Theorem says that

$$|\operatorname{Syl}_p(G)| = [G : N_G(P)].$$

Moreover, since $P \leq N_G(P)$ and $|P| = p^e$, it follows that p divides $|N_G(P)|$, so

$$|N_G(P)| = p^e d$$

for some d that divides m. We conclude that

$$[G : N_G(P)] = \frac{|G|}{|N_G(P)} = \frac{p^e m}{p^e d} = \frac{m}{d},$$

so $[G : N_G(P)]$ divides m. □

Remark 6.9. In general, Cauchy's Theorem can be deduced from part one of the Sylow Theorem. However, we used Cauchy's Theorem to prove the Sylow Theorem, so it is important to see that Cauchy's Theorem can be proven independently of Sylow theory.

To see how Cauchy's Theorem follows from the Main Theorem of Sylow Theory, suppose that the prime p divides $|G|$. Then by Theorem 6.8 there exists a Sylow p-subgroup P of G. Pick any nontrivial element $x \in P$. Then $|x| = p^j$ for some $j \geqslant 1$, since by Lagrange's Theorem $|x|$ must divide $|P| = p^e$. Then $y = x^{p^{j-1}}$ has order p:

$$y^p = \left(x^{p^{j-1}}\right)^p = x^{p \cdot p^{j-1}} = x^{p^j} = e,$$

Moreover, $y^i \neq e$ for $2 \leqslant i < p$, as otherwise

$$|x| \leqslant ip^{j-1} < p^j.$$

Remark 6.10. Let G be a group. We saw in Exercise 35 that if H is the unique subgroup of finite order n, then H is must be a normal subgroup of G. One consequence of the Main Theorem of Sylow Theory is a sort of converse to this: if G has multiple Sylow p-subgroups, then G has no normal Sylow p-subgroups, since any two Sylow p-subgroups must be conjugate to each other.

These are

6.3 Using Sylow Theory

Using the Main Theorem of Sylow Theory, we can often find the exact number of Sylow p-subgroups, sometimes leading us to find normal subgroups. In particular, these techniques can be used to show that there are no normal subgroups of a particular order, as the next example will illustrate.

Example 6.11 (No simple groups of order 12)**.** Let us prove that there are no simple groups of order 12. To do that, let G be any group of order $12 = 2^2 \cdot 3$. We will prove that G must have either a normal subgroup of order 3 or a normal subgroups of oder 4.

First, consider $n_2 = |\operatorname{Syl}_2(G)|$. By the Main Theorem of Sylow Theory, $n_2 \equiv 1 \pmod 2$ and n_2 divides 3. This gives us $n_2 \in \{1, 3\}$. Similarly, $n_3 = |\operatorname{Syl}_3(G)|$ satisfies

$$n_3 \equiv 1 \pmod 3 \quad \text{and} \quad n_3 \mid 4,$$

so $n_3 \in \{1, 4\}$. If either of these numbers is 1, we have a unique subgroup of order 4 or of order 3, and such a subgroup must be normal.

Suppose that $n_3 \neq 1$, which leaves us with $n_3 = 4$. Let P_1, P_2, P_3, and P_4 be the Sylow 3-subgroups of G. Consider any $i \neq j$. Since $P_i \cap P_j$ is a subgroup of P_i, its order must divide 3. On the other hand, P_i and P_j are distinct groups of order 3, so $|P_i \cap P_j| < 3$, and we conclude that $|P_i \cap P_j| = 1$. Therefore, $P_i \cap P_j = \{e\}$ for all $i \neq j$. Thus the *set*

$$T := \bigcup_{i=1}^{4} P_i$$

has 9 elements: the identity e and 8 other distinct elements. Since each P_i has order 3, those 8 elements must all have order 3. Note, moreover, that any other potential element of order 3 would generate its own Sylow 3-subgroup, so this is a complete count of all the elements of order 3. We conclude that there are 8 elements of order 3 in G.

In particular, there are 9 elements in G that are either the identity or have order 3, and thus there are only $12 - 9 = 3$ elements in G of order not 3, say a, b, c.

Now consider any Sylow 2-subgroup Q, which has 4 elements. None of its elements has order 3, so we must have $Q = \{e, a, b, c\}$. In particular, this shows that there is a unique Sylow 2-subgroup, which must then be normal.

Remark 6.12 (Warning!)**.** In Example 6.11, it would not be so easy to count elements of order 2 and 4. We do know that every element in

$$S := \bigcup_{i} Q_i$$

has order 1, 2, or 4, but the size of this set is harder to calculate. The issue is that $Q_i \cap Q_j$ might have order 2 for distinc i and j. The best we can say for sure is that S has at least $4 + 4 - 2 = 6$ elements.

More generally, if P and Q are both subgroups of G of prime order p, we can say that $P \cap Q = \{e\}$ using the same argument we employed in Example 6.11. However, if P and Q are two subgroups of order p^e with $e \geqslant 2$, we can no longer guarantee that $P \cap Q = \{e\}$.

Example 6.13 (No simple groups of order 80)**.** Let G be a group of order $80 = 5 \cdot 16$, and let $n_2 = |\operatorname{Syl}_2(G)|$ and $n_5 = |\operatorname{Syl}_5(G)|$. By the Main Theorem of Sylow Theory,

$$n_2 \equiv 1 \pmod 2 \quad \text{and} \quad n_2 \mid 5 \implies n_2 \in \{1, 5\}$$

and

$$n_5 \equiv 1 \pmod 5 \quad \text{and} \quad n_5 \mid 16 \implies n_5 \in \{1, 16\}.$$

If either $n_2 = 1$ or $n_5 = 1$, then the unique Sylow 2-subgroup or 5-subgroup would be normal. If G is a simple group, then we must have

$$n_2 = 5 \quad \text{and} \quad n_5 = 16.$$

While the counting trick we used in Example 6.11 would work, let us try on a different tactic here.

Consider the action of G on $\operatorname{Syl}_2(G)$ by conjugation, and let

$$\rho\colon G \to S_5$$

be the associated permutation representation. The action is transitive by the Main Theorem of Sylow Theory, so the map ρ is nontrivial. By Lemma 3.8, $\operatorname{im}(\rho)$ is a subgroup of S_5, and thus by Lagrange's Theorem the order of $\operatorname{im}(\rho)$ divides $|S_5|$. However, $|G| = 80$ does not divide $120 = |S_5|$, so the image of ρ cannot have 80 elements, and in particular ρ cannot be injective. It follows that $\ker(\rho)$ is a nontrivial, proper normal subgroup of G, a contradiction.

Chapter 7

Products and finitely generated abelian groups

In this chapter, we will discuss how to build new groups from old ones, and completely classify all finitely generated abelian groups.

7.1 Direct products of groups

Definition 7.1. Let I be a set and consider a group G_i for each $i \in I$. The **direct product** of the groups $\{G_i\}_{i\in I}$, denoted by

$$\prod_{i\in I} G_i,$$

is the group with underlying set the Cartesian product

$$\prod_{i\in I} G_i$$

equipped with the operation defined by

$$(g_i)_{i\in I}(h_i)_{i\in I} = (g_i h_i)_{i\in I}.$$

The **direct sum** of the groups G_i is the subgroup of the direct product of $\{G_i\}_{i\in I}$ given by

$$\bigoplus_{i\in i} G_i := \{(g_i)_{i\in I} \in \prod_{i\in I} G_i \mid g_i = e_{G_i} \text{ for all but finitely many } i \in I\}.$$

In particular, the direct sum of $\{G_i\}_{i\in I}$ has the same operation as the direct product.

When I is finite, say $I = \{1, \dots, n\}$, we write

$$G_1 \times \cdots \times G_n := \prod_{i=1}^{n} G_i.$$

Remark 7.2. When I is finite, the direct sum and the direct product of $\{G_i\}_{i\in I}$ coincide. This is the case we will be most interested in.

Exercise 40. The direct product of a collection of groups is a group, and the direct sum is a subgroup of the direct product.

Remark 7.3. If $G_1, \ldots, G_n$ are all finite groups, then

$$|G_1 \times \cdots \times G_n| = |G_1| \cdots |G_n|.$$

Exercise 41. Let $\{G_i\}_{i \in I}$ be a collection of abelian groups. Show that

$$\prod_{i \in I} G_i$$

is an abelian group.

Exercise 42. Let G and H be groups, and $g \in G$ and $h \in H$.

(a) Show that if $|g|$ and $|h|$ are both finite, then $|(g,h)| = \operatorname{lcm}(|g|, |h|)$.

(b) Show that if at least one of g or h has infinite order, then (g,h) also has infinite order.

Lemma 7.4. *If* $\gcd(m,n) = 1$*, then* $\mathbb{Z}/m \times \mathbb{Z}/n \cong \mathbb{Z}/mn$*.*

Proof. By Exercise 42,

$$|(1,1)| = \operatorname{lcm}(m,n) = mn.$$

But $\mathbb{Z}/m \times \mathbb{Z}/n \cong \mathbb{Z}/mn$ has order mn, so $(1,1)$ is a generator for the group, which must then be cyclic. By Theorem 3.41, all cyclic groups of order mn are isomorphic to $\mathbb{Z}/mn$, so

$$\mathbb{Z}/m \times \mathbb{Z}/n \cong \mathbb{Z}/mn.$$

□

Exercise 43. Show that the converse holds: for all integers $m, n > 1$, if

$$\mathbb{Z}/m \times \mathbb{Z}/n \cong \mathbb{Z}/mn,$$

then $\gcd(m,n) = 1$.

Recall that we saw in Exercise 24 that given a group G and subgroups H and K, if H is normal then HK is a subgroup of G. In fact, we can saw more:

Theorem 7.5 (Recognition theorem for direct products)**.** *Suppose G is a group with normal subgroups $H \trianglelefteq G$ and $K \trianglelefteq G$ such that $H \cap K = \{e\}$. Then $HK \cong H \times K$ via the isomorphism $\theta \colon H \times K \to HK$ given by*

$$\theta(h,k) = hk.$$

Moreover,

$$H \cong \{(h,e) \mid h \in H\} \leq H \times K$$

and

$$K \cong \{(e,k) \mid k \in K\} \leq H \times K.$$

Proof. By Exercise 24, the hypothesis implies $HK \leq G$. Moreover, consider any $h \in H$ and any $k \in K$. Since H is a normal subgroup,

$$khk^{-1} \in H, \text{ say}$$

so also

$$[k,h] = khk^{-1}h^{-1} \in H.$$

But K is also a normal subgroup, so similarly we obtain

$$[k,h] \in K.$$

Therefore,

$$[k,h] \in H \cap K = \{e\},$$

so $[k,h] = e$. We conclude that

$$hk = kh \quad \text{ for all } h \in H, k \in K.$$

The function θ defined above must then satisfy

$$\begin{aligned}
\theta((h_1,k_1)(h_2,k_2)) &= \theta(h_1h_2, k_1k_2) \\
&= (h_1h_2)(k_1k_2) && \text{by definition of } \theta \\
&= h_1(h_2k_1)k_2 \\
&= (h_1k_1)(h_2k_2) && \text{since } h_2k_1 = k_1h_2 \\
&= \theta(h_1,k_1)\theta(h_2,k_2) && \text{by definition of } \theta
\end{aligned}$$

and thus θ is a homomorphism. Its kernel is

$$\ker(\theta) = \{(k,h) \mid k = h^{-1}\} = \{(e,e)\}$$

since $H \cap K = \{e\}$. Moreover, θ is surjective, as any element in HK is of the form $hk \in HK$, and

$$\theta(h,k) = hk.$$

This proves θ is an isomorphism. Finally, restricting the codomain to any subgroup L of G and the domain to $\theta^{-1}(L)$ gives an isomorphism between L and $\theta^{-1}(L)$, so in particular

$$H \cong \theta^{-1}(H) = \{(h,e) \mid h \in H\} \leq H \times K$$

and

$$K \cong \theta^{-1}(K) = \{(e,k) \mid k \in K\} \leq H \times K.$$

□

Remark 7.6. If $H \trianglelefteq G$ and $K \trianglelefteq G$ are such that $H \cap K = \{e\}$, then each elements of HK is *uniquely* of the form hk. This is a consequence of the fact that the map θ is a bijection.

Definition 7.7. Let G be a group. If $H \trianglelefteq G$ and $K \trianglelefteq G$ are such that $H \cap K = \{e\}$, then the subgroup HK of G is called the **internal direct product** of H and K, while the group $H \times K$ is called the **external direct product** of H and K.

Example 7.8. Let $G = D_n$, $H = \langle r \rangle$ and $K = \langle s \rangle$. Then $H \cap K = \{e\}$, $HK = G$, and $H \trianglelefteq G$, but K is not normal in G. So Theorem 7.5 does not apply to say that G is isomorphic to $H \times K$. In fact, G is *not* isomorphic to $H \times K$, since $H \times K$ is abelian, while G is not. As we shall see, G is the semidirect product of H and K.

7.2 Semidirect products

Remark 7.9. Let G be a group. Suppose we are given subgroups $H \trianglelefteq G$ and $K \leq G$ such that $H \cap K = \{e\}$ but K is not normal. Then we still have $HK \leq G$, but it is not necessarily true that the map $\theta : H \times K \to HK$ defined by $\theta(h,k) = hk$ is a group homomorphism. The issue is that given $h \in H$ and $k \in K$, while

$$khk^{-1} \in H \implies kh = h'k \text{ for some } h' \in H,$$

we can no longer guarantee that $kh = hk$. So given $h_1, h_2 \in H$ and $k_1, k_2 \in K$, suppose that $k_1 h_1 = h_2' k_1$. For θ to be a homomorphism, we would need the following:

$$\theta(h_1, k_1)\theta(h_2, k_2) = (h_1 k_1)(h_2 k_2) = h_1 h_2' k_1 k_2 = \theta(h_1 h_2', k_1 k_2).$$

This we would need

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2', k_1 k_2).$$

This motivates the following definition:

Definition 7.10. Let H and K be groups and let $\rho \colon K \to \mathrm{Aut}(H)$ be a homomorphism. The (external) **semidirect product** induced by ρ is the set $H \times K$ equipped with the binary operation defined by

$$(h_1, k_2)(h_2, k_2) := (h_1 \rho(k_1)(h_2), k_1 k_2).$$

This group is denoted by $H \rtimes_\rho K$.

The underlying set of $H \rtimes_\rho K$ is the same as the direct product, but it is the operation that differs.

Remark 7.11. Note in particular that if K and K are finite, then $|H \rtimes_\rho K| = |H| \cdot |K|$.

Remark 7.12. If $\rho : K \to \mathrm{Aut}(H)$ is a nontrivial homomorphism, then the semidirect product $H \rtimes_\rho K$ is *never* abelian. Indeed, all we need is to consider any $k \in K$ such that $\rho(k) \neq \mathrm{id}_H$, so that $\rho(k)(h) \neq h$ for some $h \in H$, and note that

$$(e,k)(h,e) = (\rho(k)(h), k) \quad \text{while} \quad (h,e)(e,k) = (h\rho(e)(e), k) = (h,k).$$

The proof that the semidirect product is indeed a group is straightforward but a bit messy, as we need to check all the group axioms.

Theorem 7.13. *If H and K are groups and $\rho \colon K \to \mathrm{Aut}(H)$ is a homomorphism, then $H \rtimes_\rho K$ is a group, H and K are isomorphic to subgroups of $H \rtimes_\rho K$, as follows:*

$$H \cong \{(h,e) \mid h \in H\} \trianglelefteq H \rtimes_\rho K \text{ and } K \cong \{(e,k) \mid k \in K\} \leq H \rtimes_\rho K.$$

Moreover,

$$\frac{(H \rtimes_\rho K)}{\{(h,e) \mid h \in H\}} \cong K.$$

Proof. First, we show that the operation is associative. Indeed,

$$\begin{aligned}(y_1, x_1)\left((y_2, x_2)(y_3, x_3)\right) &= (y_1, x_1)(y_2\rho(x_2)(y_3), x_2x_3)\\ &= \left(y_1\rho(x_1)\left(y_2\rho(x_2)(y_3)\right), x_1x_2x_3\right)\\ &= (y_1\rho(x_1)(y_2)(\rho(x_1)\circ\rho(x_2))(y_3), x_1x_2x_3)\\ &= (y_1\rho(x_1)(y_2)\rho(x_1x_2)(y_3), x_1x_2x_3)\\ &= (y_1\rho(x_1)(y_2), x_1x_2)(y_3, x_3)\\ &= \left((y_1, x_1)(y_2, x_2)\right)(y_3, x_3).\end{aligned}$$

To show that (e, e) is a two-sided identity, consider any $h \in H$ and $k \in K$. Since $\rho(k) \in \mathrm{Aut}(H)$, then $\rho(k)(e) = e$, and thus

$$(h, k)(e, e) = (h\rho(k)(e), ke) = (he, ke) = (h, k).$$

Moreover, $\rho(e) = \mathrm{id}_H$, and thus $\rho(e)(y) = \mathrm{id}_H(y) = y$ for any $y \in K$, so that

$$(e, e)(h, k) = (e\rho(e)(h), ek) = (eh, ek) = (h, k).$$

Finally, for any $x \in H$ and $y \in K$ we have

$$\begin{aligned}(x, y)(\rho(y^{-1})(x^{-1}), y^{-1}) &= \left(x\,\rho(y)\left(\rho(y^{-1})(x^{-1})\right), yy^{-1}\right)\\ &= (x(\rho(y)\circ\rho(y^{-1}))(x^{-1}), e)\\ &= (x\rho(e)(x^{-1}), e) && \text{since } \rho \text{ is a homomorphism}\\ &= (xx^{-1}, e) && \text{since } \rho(e) = \mathrm{id}_H\\ &= (e, e),\end{aligned}$$

and similarly,

$$\begin{aligned}(\rho(y^{-1})(x^{-1}), y^{-1})(x, y) &= (\rho(y^{-1})(x^{-1})\rho(y^{-1})(x), y^{-1}y)\\ &= (\rho(y^{-1})(x^{-1}x), e) && \text{since } \rho(y^{-1}) \text{ is a homomorphism}\\ &= (\rho(y^{-1})(e), e)\\ &= (e, e) && \text{since } \rho(y^{-1}) \text{ is a homomorphism}\end{aligned}$$

Thus (x, y) has an inverse, given by

$$(x, y)^{-1} = (\rho(x^{-1})(y^{-1}), x^{-1}).$$

This completes the proof that the semidirect product is a group.

To show that $\quad H \cong \{(h, e) \mid h \in H\} \trianglelefteq H \rtimes_\rho K \quad$ and $\quad K \cong \{(e, k) \mid k \in K\} \leq H \rtimes_\rho K,$

define the function

$$i\colon H \to H \rtimes_\rho K \quad \text{given by } i(y) = (y, e).$$

Then i is a homomorphism:

$$i(y_1)i(y_2) = (y_1, e)(y_2, e) = (y_1\rho(e)(y_2), ee) = (y_1y_2, e) = i(y_1y_2),$$

Moreover, i is injective by construction, and hence its image is isomorphic to H by the First Isomorphism Theorem. We can describe $\mathrm{im}(i)$ as the set of all elements whose second component is e. The image $\mathrm{im}(i)$ is normal since the second component of

$$(h,k)(a,e)(h,k)^{-1} = (h,k)(a,e)(\rho(k^{-1})(h^{-1}), h^{-1})$$

is

$$kek^{-1} = e,$$

which shows that any for any $(a,e) \in \mathrm{im}(H)$ and any $(h,k) \in H \rtimes_\rho K$,

$$(h,k)(a,e)(h,k)^{-1} \in \mathrm{im}(i).$$

Let us write the image of i, which we now know is a normal subgroup of $H \rtimes_\rho K$, as

$$H' := \mathrm{im}(i) = \{(y,e) \mid y \in H\} \trianglelefteq H \rtimes_\rho K.$$

The function

$$j\colon K \to H \rtimes_\rho K \quad \text{given by } j(x) = (e,x)$$

is also an injective homomorphism (exercise!), and thus its image

$$K' := \{(e,x) \mid x \in H\} \leq H \rtimes_\rho K$$

is isomorphic to K.

Finally, it is easy to see that $H'K' = H \rtimes_\rho K$ and $H' \cap K' = \{e\}$. Putting this all together we have shown that

- $H' \trianglelefteq H \rtimes_\rho K$,
- $K' \leq H \rtimes_\rho K$,
- $H'K' = H \rtimes_\rho K$, and
- $H' \cap K' = \{e\}$.

Finally, consider the projection onto the second factor

$$\pi_2\colon H \rtimes_\rho K \to K,$$

which is the map given by

$$\pi_2(x,y) = y.$$

This is a group homomorphism, since the second component of $(x_1,y_1)(x_2,y_2)$ is y_1y_2, and thus

$$\pi_2((x_1,y_1)(x_2,y_2)) = y_1y_2 = \pi_2(y_1)\pi_2(y_2).$$

Moreover, π_2 is surjective by definition. Finally,

$$\ker(\pi_2) = \{(y, e_K) \mid y \in H\} = H' \cong H.$$

By the First Isomorphism Theorem, we conclude that

$$(H \rtimes_\rho K)/H' \cong K. \qquad \square$$

In Theorem 7.13, we showed that $\{(h,e) \mid h \in H\}$ is a normal subgroup of $H \rtimes_\rho K$. However, $\{(e,k) \mid k \in K\}$ is typically *not* a normal subgroup of $H \rtimes_\rho K$. We will see a concrete example of this below in Example 7.22.

Example 7.14. Given any two groups H and K, we can always take ρ to be the trivial homomorphism. In that case, $K \rtimes_\rho H$ is just the usual direct product: for all $h \in H$ and all $k \in K$, $\rho(k) = \mathrm{id}_H$, so

$$(h,k)(h',k') = (h\rho(k)(h'), kk') = (hh', kk').$$

To better understand semidirect products, we should first better understand what it means to have a homomorphism $K \to \mathrm{Aut}(H)$.

Definition 7.15. Let G and H be groups. A (left) **action of G on H via automorphisms** is a pairing $G \times H \to H$, written as $(g,h) \mapsto g \cdot h$, such that

- For all $g_1, g_2 \in G$ and $h \in H$, $g_1 \cdot (g_2 \cdot h) = (g_1 \cdot_G g_2) \cdot h$.
- For all $h \in H$, $e_G \cdot h = h$.
- For all $g \in G$ and all $h_1, h_2 \in H$, $g \cdot (h_1 \cdot_H h_2) = (g \cdot h_1) \cdot_H (g \cdot h_2)$.

Remark 7.16. Note that the first two axioms are just the axioms for a group action. So given a group action of G on H, let $\rho\colon G \to \mathrm{Perm}(H)$ be the corresponding permutation representation. If the action satisfies the third axiom in Definition 7.15, then that means that for each $g \in G$, $\rho(g)$ satisfies

$$\rho(g)(h_1 \cdot_H h_2) = \rho(g)(h_1)\, \rho(g)(h_2).$$

This condition simply says that $\rho(g)$ must be a homomorphism. Since $\rho(g)$ is already a bijection, we conclude that $\rho(g)$ must be an automorphism of H. Conversely, given any homomorphism $\rho\colon K \to \mathrm{Aut}(H)$, we can define a group action of K on H via automorphisms by setting

$$k \cdot h := \rho(k)(h).$$

Since $\mathrm{Aut}(H) \subseteq \mathrm{Perm}(H)$, we can extend ρ to a homomorphism $K \to \mathrm{Perm}(H)$, which we saw in Lemma 2.3 is equivalent to the action of K on H we just defined. That action satisfies

$$\begin{aligned} k \cdot (h_1 \cdot_H h_2) &= \rho(k)(h_1 \cdot_H h_2) \\ &= \rho(k)(h_1) \cdot_H \rho(k)(h_2) \quad \text{since } \rho \text{ is a homomorphism} \\ &= (k \cdot h_1) \cdot_H (k \cdot h_2) \end{aligned}$$

In conclusion, we can now say that to give an action of G on H via automorphisms is to give a group homomorphism

$$\rho\colon G \to \mathrm{Aut}(H).$$

Moreover, given a group K acting on a group H by automorphisms, we get an induced semidirect product $H \rtimes_\rho K$, where $\rho\colon K \to \mathrm{Aut}(H)$ is the corresponding homomorphism.

Remark 7.17. It is sometimes useful to write ${}^g h$ for $g \cdot h$. With this notation, the axioms become:

$${}^{g_1}({}^{g_2}h) = {}^{g_1 g_2}h \qquad {}^e h = h \qquad {}^g(h_1 h_2) = {}^g h_1 {}^g h_2.$$

Exercise 44 (Conjugation action by automorphisms)**.** Fix a group G, a normal subgroup $H \trianglelefteq G$ and a subgroup $K \leq G$. Show that the rule

$$k \cdot h = khk^{-1}$$

for $k \in K$ and $h \in H$ determines an action of K on H via automorphisms, and the associated homomorphism $\rho\colon K \to \mathrm{Aut}(H)$ is given by

$$\rho(k)(h) = khk^{-1}.$$

Studying semidirect products is a great motivation to studying automorphism groups.

Exercise 45. Let C_n denote the cyclic group of order $n \geqslant 2$, and consider the group

$$(\mathbb{Z}/n)^\times = \{[j]_n \mid \gcd(j,n) = 1\}$$

with the binary operation given by the usual multiplication. Prove that

$$\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n)^\times.$$

Remark 7.18. We can now count the number of elements in $\mathrm{Aut}(C_n)$, since it is the number of integers $1 \leqslant i < n$ that are coprime with n. This number is given by what is know as the **Euler φ function**,

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

Equivalently, if $n = p_1^{a_1} \cdots p_k^{a_k}$, where $p_1, \ldots, p_k$ are distinct primes and each $a_i \geqslant 1$, then

$$\varphi(n) = \prod_{i=1}^{k} \left(p_i^{a_i - 1}(p_i - 1)\right).$$

In particular, if p is prime then $|\mathrm{Aut}(\mathbb{Z}/p)| = p - 1$.

Example 7.19. Let $K = \langle x \rangle$ be the cyclic of order 2 and $H = \langle y \rangle$ be the cyclic of order n for some $n \geqslant 2$. By the UMP for cyclic groups, to give a homomorphism out of K is to pick the image i of the generator x, which must satisfy $i^2 = e$. In particular, i must be either the identity or an element of order 2.

Since H is abelian, the inverse map $f\colon H \longrightarrow H$ given by $f(a) = a^{-1}$ is an automorphism of H; we showed this in Problem Set 2.[1] This automorphism f is not the identity but it is its own inverse, so it has order 2. Therefore, by the UMP for cyclic groups, there is a homomorphism

$$\rho\colon K \to \mathrm{Aut}(H) \quad \text{with} \quad \rho(x)(y) = y^{-1}.$$

Consider the semidirect product $H \rtimes_\rho K$. The elements of $H \rtimes_\rho K$ are the tuples (y^i, x^j) for $0 \leqslant i \leqslant n-1$ and $0 \leqslant j \leqslant 1$. In particular, $|H \rtimes_\rho K| = 2n$. Set

$$\tilde{y} = (y, e_K) \in G \quad \text{and} \quad \tilde{x} = (e_H, x) \in G.$$

[1] In fact, we can say more: By Exercise 45, $\mathrm{Aut}(H) \cong (\mathbb{Z}/n)^\times$. In particular, -1 is an element of $(\mathbb{Z}/n)^\times$, and the associated automorphism sends y to y^{-1}.

Then $\tilde{y}^n = (y, e_K)^n = (y^n, e_K) = (e_H, e_K) = e_G$ and $\tilde{x}^2 = (e_H, x)^2 = (e_H, x^2) = (e_H, e_K) = e_G$. Moreover,

$$\tilde{x}\tilde{y}\tilde{x}\tilde{y} = (e_H, x)(y, e_K)(e_H, x)(y, e_K) = (\rho(x)(y), x)(\rho(x)(y), x) = (y^{-1}, x)(y^{-1}, x) = (y^{-1}y, e) = e_G.$$

Looks familiar? Indeed, using our presentation for D_n from Theorem 1.66 and the UMP for presentations from Theorem 4.61, we have a homomorphism

$$\theta\colon D_n \longrightarrow G \quad \text{given by} \quad \theta(r) = (y, e_K) \text{ and } \theta(s) = (x, e_H).$$

Moreover, θ is surjective since

$$\theta(r^i s^j) = (y^i, x^j) \text{ for all } 0 \leqslant i \leqslant n-1, 0 \leqslant j \leqslant 1.$$

Since $|D_n| = |G| = 2n$, this surjection must also be a bijection, and we conclude that θ is an isomorphism. So the dihedral group is a semidirect product of the cyclic of order n and the cyclic group of order 2 respectively:

$$D_n \cong \langle y \rangle \rtimes_\rho \langle x \rangle$$

where ρ is the inverse map as described above.

So given any group, how can we recognize it is in fact a semidirect product?

Theorem 7.20 (Recognition theorem for internal semidirect products)**.** *Let G be a group. Suppose we are given subgroups H and K of G such that*

$$H \trianglelefteq G \qquad HK = G \qquad \textit{and} \qquad H \cap K = \{e\}.$$

Let $\rho\colon K \to \operatorname{Aut}(H)$ be the permutation representation of the action of K on H via automorphisms given by conjugation in G, meaning that

$$\rho(k)(h) = khk^{-1}.$$

Then

$$G \cong H \rtimes_\rho K$$

via the isomorphism $\theta\colon H \rtimes_\rho K \to G$ given by $\theta(x, y) = xy$. Moreover,

$$H \cong \{(h, e) \in H \rtimes_\rho K \mid h \in H\} \quad \textit{and} \quad K \cong \{(e, k) \in H \rtimes_\rho K \mid k \in K\}.$$

Proof. First, we show that θ is a group homomorphism. Indeed,

$$\begin{aligned}\theta((y_1, x_1)(y_2, x_2)) &= \theta(y_1\rho(x_1)(y_2), x_1x_2) \\ &= y_1(x_1y_2x_1^{-1})x_1x_2 \\ &= y_1x_1y_2x_2 \\ &= \theta(y_1, x_1)\theta(y_2, x_2).\end{aligned}$$

Since $H \cap K = \{e\}$, the kernel of θ is

$$\ker(\theta) = \{(y, x) \in H \rtimes_\rho K \mid y = x^{-1}\} = \{e\}.$$

By construction, the image of θ is $KH = G$. Therefore, θ is an isomorphism. Finally,

$$\theta^{-1}(H) = \{(h, e) \mid h \in H\} \quad \text{and} \quad \theta^{-1}(K) = \{(e, k) \mid k \in K\}. \qquad \square$$

Definition 7.21. Given subgroups H and K of G such that $H \trianglelefteq G$, $HK = G$, and $H \cap K = \{e\}$, we say that G is the **internal semidirect product** of H and K.

Example 7.22. Consider $G = D_n$ and its subgroups $H = \langle r \rangle$ and $K = \langle s \rangle$. Then $H \trianglelefteq G$, $K \leq G$, $HK = G$ and $H \cap K = \{e\}$. By Theorem 7.20, $G \cong H \rtimes_\rho K$, where $\rho\colon K \to \operatorname{Aut}(H)$

$$\rho(s)(r^i) = sr^is^{-1} = r^{n-i}.$$

The last equality is Exercise 10. Note in particular that K is *not* a normal subgroup of G. We had already seen in Example 7.8 that G is not the internal direct product of H and K, but now know it is their internal semidirect product. We also already knew that D_n is a semidirect product by Example 7.19.

For a fixed pair of groups H and K, different actions of K on H via automorphisms can result in isomorphic semidirect products. Indeed, determining when $K \rtimes_\rho H \cong K \rtimes_{\rho'} H$ is in general a tricky business. Here is an example of this:

Example 7.23. Let $n \geqslant 3$ and consider $G = S_n$, $H = A_n$, and $K = \langle (1\,2) \rangle$. Then $H \trianglelefteq G$, $K \leq G$, $HK = G$ and $K \cap H = \{e\}$. Note that $H \cong C_2$ is the cyclic group with 2 elements. By Theorem 7.20,

$$S_n \cong A_n \rtimes_\rho C_2$$

where $\rho\colon C_2 \longrightarrow \operatorname{Aut}(A_n)$ sends x to conjugation by $(1\,2)$.

Now take $H' = \langle (1\,3) \rangle = (1\,2\,3)\langle (1\,2) \rangle (1\,2\,3)^{-1}$. Then

$$S_n \cong A_n \rtimes_{\rho'} C_2$$

where $\rho' : C_2 \to \operatorname{Aut}(A_n)$ sends x to conjugation by $(1\,3)$.

However, the actions determined by ρ and ρ' are not identical. For example,

$$\rho(x)(1\,2) = (1\,2) \quad \text{and} \quad \rho'(x)(1\,2) = (2\,3).$$

Yet

$$A_n \rtimes_\rho H \cong S_n \cong A_n \rtimes_{\rho'} H'.$$

One good reason why this happened in this case is that H and H' are conjugate in S_n.

Exercise 46. Let K be a finite cyclic group and let H be an arbitrary group. Suppose $\phi : K \to \operatorname{Aut}(H)$ and $\theta : K \to \operatorname{Aut}(H)$ are homomorphisms whose images are conjugate subgroups of $\operatorname{Aut}(H)$. Then $H \rtimes_\phi K \cong H \rtimes_\theta K$.

Example 7.24. Let K be a cyclic group of prime order p and H be a group such that $\operatorname{Aut}(H)$ has a unique subgroup of order p. Suppose $\phi\colon K \to \operatorname{Aut}(H)$ and $\theta\colon K \to \operatorname{Aut}(H)$ are any two *nontrivial* maps. Then ϕ and θ are injective, since K is simple and the kernel would be a proper normal subgroup. Hence, the images of ϕ and θ are both the unique subgroup of $\operatorname{Aut}(H)$ of order p, and in particular they must be equal. Thus Exercise 46 applies to give $H \rtimes_\phi K \cong H \rtimes_\theta K$.

7.3 Finitely generated groups

Recall that a group G is finitely generated if it $G = \langle A \rangle$, where A is a finite set.

Remark 7.25. Any finite group G is finitely generated, since we can take $A = G$. However, a finitely generated group need not be finite: for example $\mathbb{Z}$ is even cyclic but infinite.

The main theorem of this section is a special case of a much more general theorem we will prove in the Spring: the classification of finitely generated modules over PIDs. Thus we leave the proof for next semester.

Theorem 7.26 (The Fundamental Theorem of Finitely Generated Abelian Groups: Invariant Factor Form)**.** *Let G be a finitely generated abelian group. There exist integers $r \geqslant 0$, $t \geqslant 0$, and $n_i \geqslant 2$ for $1 \leqslant i \leqslant t$, satisfying $n_1 \mid n_2 \mid \cdots \mid n_t$ such that*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_t.$$

Moreover, the list $r, s, n_1, \ldots, n_t$ is uniquely determined by G.

Definition 7.27. In Theorem 7.26, the number r is the **rank** of G, the numbers $n_1, \ldots, n_t$ are the **invariant factors** of G, and the decomposition of G is the **invariant factor decomposition** of G.

Remark 7.28. A finitely generated abelian group is finite if and only if its rank is 0. A special case of the classification theorem is that if G is a finite abelian group then

$$G \cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_t$$

for a unique list of integers $n_i \geqslant 2$ such that n_{i+1} divides n_i for each i.

Here is another version of the classification theorem:

Theorem 7.29 (The Fundamental Theorem of Finitely Generated Abelian Groups: Elementary Divisor Form)**.** *Let G be a finitely generated abelian group. Then there exist integers $r \geqslant 0$ and $s \geqslant 0$, not necessarily distinct positive prime integers $p_1, \cdots, p_s$, and integers $a_i \geqslant 1$ for $1 \leqslant i \leqslant s$ such that*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/p_1^{a_1} \times \cdots \times \mathbb{Z}/p_s^{a_s}.$$

Moreover, r and s are uniquely determined by G, and the list of prime powers $p_1^{a_1}, \ldots, p_s^{a_s}$ is unique up to the ordering.

Definition 7.30. In Theorem 7.29, the number r is the **rank** of G, the $p_i^{a_i}$ are the **elementary divisors** of G, and the decomposition of G is called the **elementary divisor decomposition** of G.

The two forms of the classification theorem are equivalent, which we can prove using the following:

Theorem 7.31 (CRT)**.** *Suppose $m = p_1^{e_1} \cdots p_l^{e_l}$ for distinct primes $p_1, \dots, p_l$. Then there is an isomorphism*

$$\phi\colon \mathbb{Z}/m \xrightarrow{\cong} \mathbb{Z}/(p_1^{e_1}) \times \cdots \times \mathbb{Z}/(p_l^{e_l})$$

given by

$$\phi([j]_m) = ([j]_{p_1{}^{e_1}}, \cdots, [j]_{p_l{}^{e_l}})$$

where $[j]_b$ denote the class of an integer j in $\mathbb{Z}/b$.

Proof. Using the UMP for infinite cyclic groups, we let

$$\psi\colon \mathbb{Z} \longrightarrow \mathbb{Z}/(p_1^{e_1}) \times \cdots \times \mathbb{Z}/(p_l^{e_l})$$

be the unique homomorphism that sends 1 to $([1]_{p_1{}^{e_1}}, \cdots, [1]_{p_l{}^{e_l}})$. Then

$$\psi(j) = ([j]_{p_1{}^{e_1}}, \cdots, [j]_{p_l{}^{e_l}}).$$

Note that $m \in \ker(\psi)$, and so $\langle m \rangle \subseteq \ker(\psi)$. Conversely, if $\psi(n) = 0$, then $p_i^{e_i} \mid n$ for all i and since $p_1^{e_1}, \dots, p_l^{e_l}$ are pairwise relatively prime, it follows that $m \mid n$. This proves $\ker(\psi) = \langle m \rangle$. By the UMP for quotient groups, there is an induced injective homomorphism ϕ as in the statement. Finally, ϕ must also be surjective for cardinality reasons. $\square$

Rather than a careful proof that the two versions of the classification theorem are equivalent, we will now see in examples how the CRT allows us to go between invariant factors and elementary divisors.

Example 7.32 (Converting elementary divisors to invariant factors)**.** Suppose G is a finitely generated abelian group of rank 3 with elementary divisors $4, 8, 9, 27, 25$. This means that

$$G \cong \mathbb{Z}^3 \times \mathbb{Z}/4 \times \mathbb{Z}/8 \times \mathbb{Z}/9 \times \mathbb{Z}/27 \times \mathbb{Z}/25.$$

Let us find the invariant factors of G.

By the CRT,

$$\mathbb{Z}/8 \times \mathbb{Z}/27 \times \mathbb{Z}/25 \cong \mathbb{Z}/(8 \cdot 27 \cdot 25)$$

and

$$\mathbb{Z}/4 \times \mathbb{Z}/9 \cong \mathbb{Z}/(4 \cdot 9),$$

so that

$$G \cong \mathbb{Z}^3 \times \mathbb{Z}/(8 \cdot 27 \cdot 25) \times \mathbb{Z}/(4 \cdot 9) = \mathbb{Z}^3 \times \mathbb{Z}/5400 \times \mathbb{Z}/36.$$

Since $36 \mid 5400$, we conclude that G has rank 3 and invariant factors 5400 and 36.

Since $n_2 = (4 \cdot 9) \mid n_1 = (8 \cdot 27 \cdot 25)$, this is in invariant factor form, and hence the rank of A is 3 and the invariant factors of A are $4 \cdot 9$ and $8 \cdot 27 \cdot 25$.

Example 7.33 (Converting invariant factors to elementary divisors)**.** Let

$$G \cong \mathbb{Z}^4 \times \mathbb{Z}/6 \times \mathbb{Z}/36 \times \mathbb{Z}/180.$$

Then by the CRT,

$$G \cong \mathbb{Z}^4 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/4 \times \mathbb{Z}/9 \times \mathbb{Z}/4 \times \mathbb{Z}/5 \times \mathbb{Z}/9,$$

given the elementary divisor form.

Example 7.34. Let $G = \mathbb{Z}/60 \times \mathbb{Z}/50$. This group is finite and abelian, and thus $r = 0$, but not in either invariant factor nor elementary divisor factorization.

Applying the CRT to $60 = 12 \cdot 5 = 2^2 \cdot 3 \cdot 5$ and $50 = 2 \cdot 5^2$, we have

$$\mathbb{Z}/60 \cong \mathbb{Z}/4 \times \mathbb{Z}/3 \times \mathbb{Z}/5 \quad \text{and} \quad \mathbb{Z}/50 \cong \mathbb{Z}/2 \times \mathbb{Z}/25$$

so

$$G \cong \mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/3 \times \mathbb{Z}/5 \times \mathbb{Z}/25.$$

This gives the elementary divisor decomposition: G has rank 0 and elementary divisors 2, 4, 3, 5, and 25. Applying the CRT again, in a different way, gives

$$G \cong \mathbb{Z}/(4 \cdot 3 \cdot 25) \times \mathbb{Z}/(2 \cdot 5) = \mathbb{Z}/300 \times \mathbb{Z}/10.$$

This is the invariant factor decomposition: G has rank 0 and invariant factors 10 and 300.

This classification makes the classification of finite abelian groups a very quick matter.

Example 7.35. Let us classify the abelian groups of order 75. First, note that $75 = 5^2 \cdot 3$. The two possible elementary divisor decompositions are

$$\mathbb{Z}/25 \times \mathbb{Z}/3 \text{ or } \mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/3.$$

Note that the two groups above are not isomorphic. This is part of the theorem, but to see this directly, note that there is an element of order 25 in $\mathbb{Z}/25 \times \mathbb{Z}/3$, namely $([1]_{25}, [0]_3)$ whereas every element $(a, b, c) \in \mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/3$ has order

$$|(a, b, c)| = \operatorname{lcm}(|a|, |b|, |c|) \leqslant 3 \cdot 5 = 15,$$

since $|a|, |b| \in \{1, 5\}$ and $|c| \in \{1, 3\}$.

Alternatively, the two possible invariant factor decompositions are

$$\mathbb{Z}/75 \quad \text{or} \quad \mathbb{Z}/15 \times \mathbb{Z}/5.$$

They are also not isomorphic, as the second option has no elements of order 75.

Remark 7.36. Let $n = p_1^{e_1} \cdots p_k^{e_k}$ for *distinct* positive prime integers $p_1, \ldots, p_k$ and integers $e_i \geqslant 1$. The classification of finitely generated abelian groups implies that there are $p(e_1) \cdots p(e_k)$ isomorphism classes of abelian groups of order n, where $p(m)$ is the number of partitions of m. For example, for $n = 2^4 \cdot 3^5 \cdot 5^2$ there are

$$p(4)p(6)p(2) = 5 \cdot 7 \cdot 2 = 70$$

abelian groups of order n up to isomorphism.

7.4 Classification of finite groups of certain orders

We can now combine the ideas from Sylow theory, (semi)direct products and the classification theorem for finitely generated abelian groups to classify the isomorphism classes of groups of small order.

You have already done some examples of this kind..

Exercise 47. Show that any group of order 6 is isomorphic either to $\mathbb{Z}/6$ or to D_6.

We will find the following facts very useful for this type of problems.

Exercise 48. If p is prime, then $\mathrm{Aut}(C_p) \cong \mathbb{Z}/p^\times$ is cyclic of order $p-1$.

Exercise 49. Let p be a prime integer. Show that

$$\mathrm{Aut}(\underbrace{\mathbb{Z}/p \times \cdots \times \mathbb{Z}/p}_{n \text{ factors}}) \cong \mathrm{GL}_n(\mathbb{Z}/p)$$

and that these groups have order $(p^n-1)(p^n-p)(p^n-p^2)\cdots(p^n-p^{n-1})$.

Theorem 7.37. *Let $p < q$ be primes.*

(1) If p does not divide $q-1$, there is a unique group of order pq up to isomorphism, the cyclic group C_{pq}.

(2) If p divides $q-1$, there are exactly two groups of order pq up to isomorphism, the cyclic group C_{pq} and a nonabelian group.

Proof. Let G be a group of order pq and let H and K be Sylow subgroups of order q and p respectively.

Let $n_q = |\operatorname{Syl}_q(G)|$. Since $n_q \equiv 1 \pmod{q}$, $n_q \mid p$, and $q > p$, we have $n_q = 1$ and thus H is a normal subgroup.[2] Thus HK is a subgroup of G. By Lagrange's theorem, $|H \cap K| \mid |H|$ and $|H \cap K| \mid |K|$. Therefore, $H \cap K = \{e_G\}$. From here it follows that

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{q \cdot p}{1} = pq = |G|$$

and so $HK = G$. The recognition theorem for semidirect products thus yields that

$$G \cong H \rtimes_\rho K$$

for some homomorphism $\rho\colon K \longrightarrow \mathrm{Aut}(H)$. Note that H and K are cyclic, since they have prime order. Let us identify H with $C_q = \langle x \mid x^q \rangle$ and K with $C_p = \langle y \mid y^p \rangle$. Then

$$G \cong C_q \rtimes_\rho C_p, \text{ for some homomorphism } \rho : C_p \to \mathrm{Aut}(C_q).$$

So we just need to classify all such semidirect products up to isomorphism.

[2]Alternatively, H is normal since $[G : H] = p$ is the smallest prime that divides $|G|$.

Now, by the UMP of cyclic groups, the homomorphism $\rho\colon C_p \longrightarrow \mathrm{Aut}(C_q)$ is uniquely determined by the image of the generator x, which must be an element $\alpha \in \mathrm{Aut}(C_q)$ with $\alpha^p = \mathrm{id}$. Given such an α, we have $\rho(y) = \alpha$ and more generally $\rho(y^i) = \alpha^{\circ i}$.

By Exercise 48, $\mathrm{Aut}(C_q)$ is cyclic of order $q-1$. On the other hand, the order of the image of ρ must divide both p and $q-1$. In particular, there is a nontrivial automorphism ρ if and only if $p \mid q-1$.

If p does not divide $q-1$, then ρ is trivial, and by the CRT we have

$$G \cong C_q \times C_q \cong C_{pq}.$$

If p does divide $q-1$, there is at least one nontrivial ρ. We still have $G \cong C_{pq}$ if ρ is trivial. When ρ is nontrivial, G is not abelian, giving us at least two isomorphism classes. It remains to show that if ρ_1 and ρ_2 are any two nontrivial homomorphisms from C_p to $\mathrm{Aut}(C_q)$, then the resulting semidirect products are isomorphic.

Since $\mathrm{Aut}(C_q)$ is a cyclic group and p divides its order, it has a unique subgroup of order p. Thus, we conclude that $\mathrm{im}(\rho_1) = \mathrm{im}(\rho_2)$, so that by (a special case of) Exercise 46 we have

$$C_q \rtimes_{\rho_1} C_p \cong C_q \rtimes_{\rho_2} C_p. \qquad \square$$

Example 7.38. If $p = 2$ and q is any odd prime, then there are two groups of order $2q$ up to isomorphism: C_{2q} and D_q.

Index