Undergraduate Algebra

Robert

0th Edition

Contents

List of Theorems

Preface

This was originally a collection of notes for abstract algebra, but it has since evolved into a textbook. We will cover the theory of groups, rings, fields as well as modules.

The main motivation for writing such a textbook was to discuss the techniques used in the study of abstract algebra, as well as the motivations behind the concepts discussed. As such, we have adopted the more ambitious approach of discussing the ideas and motivations behind the topics while leaving proofs short and concise. We hope that the reader should come away with feeling that all the concepts here are the most natural thing you could possibly think of.

The only prerequisite for this book is good mathematical maturity and the techniques for writing proofs. It would help slightly if you have had linear algebra, as some of our examples depend on linear algebra. Of course, plenty of exercises and problems are included for the reader to practice their skills. The author recommends that the reader do every exercise (even the tedious ones!) and at at least attempt every problem. In general, the average problem will be slightly harder than the average exercise.

At the end of the book, we include references to some other good abstract algebra books, for those who wish to delve deeper into the theory.

This is a work in progress. Corrections and improvements are always appreciated. Please email any corrections to robert [dot] xiu [at] mail [dot] utoronto [dot] ca.

Acknowledgements

Writing a book is not a solo activity. I wish to thank some of my first readers: Robert Chung, Jae Hyeon Hyeoh, Eddison Pham who offered feedback and suggestions on exercises. Additionally, I would also like to thank other reviewers like Yulong Liu who has offered feedback regarding notations, typography and mathematical contents.

I'm also greatly indebted to other resources from which I've learnt this content from. In no particular order: [Gal20], [DF04], [Jac09]. Readers are greatly encouraged to check out these other books for a more thorough treatment on algebra.

August 2024
Toronto

Chapter 0

Preliminaries

We assume that the reader is already familiar with the basics of set theory and how to write proofs. More concretely, the reader should have a good grasp on functions and relations. We do request that the reader know about equivalence relations. Therefore, we will not treat them in this book. (If there is sufficient demand I will add these in)

In this book, the naturals start from zero. That is, $\mathbb{N} = \{ 0, 1, 2, \dots \}$. We denote the set of integers by $\mathbb{Z}$, the set of real numbers by $\mathbb{R}$, the set of rational numbers by $\mathbb{Q}$ and the set of complex numbers by $\mathbb{C}$.

We first begin with an axiom. This will help us with proving the division algorithm (Theorem 0.2) and the fact that the GCD is a linear combination (Theorem 0.3).

Axiom 0.1 (Well-ordering for naturals)**.** Let $S \subseteq \mathbb{N}$ be a nonempty set of natural numbers. Then, S has a smallest element.

Theorem 0.2 (Division algorithm)**.** Let $n, m \in \mathbb{Z}$ and $m > 0$. Then, there exists unique $q, r \in \mathbb{Z}$, where $0 \leq r < m$ such that $n = qm + r$.

Proof. Let

$$S = \{ n - qm : q \in \mathbb{Z}, n - qm \geq 0 \}.$$

Then S is nonempty as $n \in S$, so it has a smallest element r. Clearly $r < m$, for if $r \geq m$ then it would not be the smallest. Then $n - r$ must divide m, so let q be an integer such that $qm = n - r$. For uniqueness, suppose q', r', where $0 \leq r' < m$ satisfies $n = q'm + r'$. Then, $qm + r = q'm + r'$, so $m(q - q') = r' - r$. Observe that $-m < r' - r < m$, so $q - q' = 0$, and thus $r = r'$ as well. □

In the proof above, q is called the *quotient* and r is called the *remainder*. If the remainder r is zero, then m is said to **divide** n, and we write $m \mid n$.

We now give some motivation for what is going on in the proof above. The set S may seem mysterious, but let us quickly try to understand why it is defined as such. Let us suppose that we are dividing n by m. Recall from elementary school that when performing long division, we are interested in the largest multiple of m, say qm such that $n - qm$ is as small as possible. So S should contain the minimum value of $n - qm$ possible. This would be the remainder.

Theorem 0.3 (GCD is a linear combination)**.** Let $n, m \in \mathbb{Z}$ be nonzero integers. Then, there exists integers $s, t \in \mathbb{Z}$ such that $\gcd(n, m) = ns + mt$. Additionally, $\gcd(n, m)$ is the smallest positive integer of the form $ns + mt$.

Proof. Let

$$S = \{ na + mb : a, b \in \mathbb{Z}, na + mb > 0 \}.$$

Then S is nonempty, so it has a smallest element d, which is of the form $ns + mt$. We claim $d = \gcd(n, m)$. First, we show d divides both n and m. By Theorem 0.2, $n = qd + r$, where $0 \leq r < d$. If $r > 0$ then we have

$r = n - qd = n - q(ns + mt) = n(1 - qs) - m(qt)$. So $r \in S$ but $r < d$, a contradiction. A similar argument holds for m, so d divides both n and m. Let d' divide both n and m too, we show d' divides d to establish that d is in fact the gcd. Let $n = d'h$, and $m = d'k$. Then $d = (d'h)s + (d'k)t = d'(hs + kt)$ as desired. □

Once again we have constructed a rather mysterious looking set. However, such a set S is natural because we are trying to show that the gcd is the *smallest* positive integer that is a linear combination of n, m.

We say that 2 numbers n, m are **coprime** if $\gcd(n, m) = 1$. One corollary of this theorem is so important it is singled out.

Corollary 0.4 (Bezout's lemma). If $\gcd(n, m) = 1$, then there exists integers $s, t \in \mathbb{Z}$ such that $ns + mt = 1$.

And now a quick application of this corollary

Lemma 0.5 (Euclid's Lemma). *Let p be a prime and $p \mid ab$. Then $p \mid a$ or $p \mid b$.*

Proof. Suppose p does not divide a. Then, by Corollary 0.4, there are integers s, t such that $as + pt = 1$, so $b = bas + bpt$. Then p divides the right side of the equation, so it divides the left side too. □

This theorem tells us that we can factorize natural numbers into a product of primes in a unique way.

Theorem 0.6 (Fundamental Theorem of Arithmetic). Let $n \in \mathbb{N}$ and $n > 1$. Then n is prime, or is a unique product of primes.

Proof. Exercise for the reader. Use Lemma 0.5 and strong induction. □

All the results here are rather important especially in the study of finite group theory. As we go deeper into the book, we will invoke them with no explicit mention, so the reader is highly encouraged to keep these in mind.

Exercise 0.7 (Fundamental Theorem of Arithmetic). Prove Theorem 0.6

Exercise 0.8 (Generalized Euclid's lemma). Prove that if $p \mid a_1 \cdots a_n$ then $p \mid a_i$ for some a_i.

Exercise 0.9. Prove that there are infinitely many primes.

Chapter 1

Groups

1.1 Groups

Before we give the definition of a group, the reader might appreciate some motivation behind what a group is trying to capture. The axioms of a group are in the sense, all that you need for the equation $ax = b$ to have a unique solution. Of course, the reader may also be motivated by other examples, such as the rotations and reflections of a square, or other sorts of symmetries.

Definition 1.1 (Group). A group is a set G with a binary operation $\cdot : G \times G \to G$ such that

1. **(Associativity)** For all $x, y, z \in G$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
2. **(Identity)** There exists $e \in G$ such that for all $g \in G$, $e \cdot g = g \cdot e = g$.
3. **(Inverses)** For all $g \in G$, there exists $h \in G$ such that $g \cdot h = h \cdot g = e$.

Note that the order of properties 2 and 3 do matter. We cannot write property 3 before property 2. A remark about how the identity and inverse is written is order. We do need the fact that $e \cdot g = g \cdot e = g$, since if only $e \cdot g = g$ and $h \cdot g = e$ are given, this may not determine a group. [Jac09]

To make notation clearer, we shall write gh for $g \cdot h$. We may sometimes use addition to denote the group operation as well, writing $g + h$. Additionally, because of associativity, we can drop any brackets. This means that there is no ambiguity about what xyz is. Recall that when adding numbers, $(2 + 3 + 4) + 5 = (2 + 3) + (4 + 5)$. Of course, it follows that you can drop the brackets for finitely many elements.

Exercise 1.2. Let G be a group. Prove that associativity holds for finitely many elements $x_1, \ldots, x_n \in G$. For example, $(xy)(zw) = x((yz)w)$. (c.f. [DF04, Prop 1, p. 19])

Additionally, if we can commute elements under the group operation, the group is called Abelian. This is named in honor of the Norwegian mathematician Niels Abel, who contributed greatly to the development of group theory.

Definition 1.3 (Abelian group). Let G be a group. Then G is Abelian if for every $g, h \in G$, we have $gh = hg$.

Exercise 1.4. Show that the condition that $eg = ge = g$ (and similarly for inverses) can be replaced with simply $eg = g$ if we say that G is abelian.

At this point, the reader might be wondering whether the existence of identities and inverses necessarily guarantees that they are unique. This is indeed true.

Theorem 1.5 (Uniqueness of identity and inverses). Let G be a group. Then, the following are true.

1. The identity of G is unique.
2. If $g \in G$ has an inverse h, then it is unique.

Proof. (1) Let $e, e' \in G$ and suppose both e, e' are identities. Keeping in mind that they satisfy the property of being an identity, we have,

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

(2) Suppose h, h' are both inverses of g. Again keeping in mind that h, h' both satisfy the properties of being an inverse for g.

$$h = h(h'g) = h(gh') = (hg)h' = h'.$$

□

Henceforth we shall talk about "the" identity of a group, and "the" inverse of an element. If not explicitly mentioned, the identity of a group G will be denoted e. Additionally, if $g \in G$, then we shall denote the inverse of g by g^{-1}.

Let us now see some examples of groups.
Example 1.6 (Integers)**.** The integers form a group under usual addition. Clearly the identity under addition is 0. Inverses are obvious. //

We trust that the reader is mathematically mature enough to not be confused by the usage of $+$ for the group operation.
Example 1.7. The set of integers under usual multiplication is *not* a group. There is no multiplicative inverse for 2. //
Example 1.8 (Vector spaces)**.** Let V be a vector space over $\mathbb{R}$. Then V is a group under vector addition. //
Example 1.9 (General linear group)**.** Let $\mathbb{GL}_n(\mathbb{R})$ denote the set of $n \times n$ invertible matrices with real entries. Then this set is a group under the operation of matrix multiplication. //
Example 1.10 (Special linear group)**.** Let $\mathbb{SL}_n(\mathbb{R})$ denote the set of $n \times n$ matrices with real entries and determinant 1. This set forms a group under the operation of matrix multiplication. //
Example 1.11 (Dihedral group D_4)**.** Consider a square. We shall label the square's vertices in a counterclockwise direction. Let r denote a clockwise rotation and let s denote reflection on the vertical axis. The operation in this group shall be defined by applying successive transformations. So for instance, r^2 would be rotating clockwise, then rotating clockwise again. If we do instead rs, we would first flip the square on the vertical axis, then rotate the square clockwise. (The reader is highly encouraged to grab a piece of paper and do these operations for themselves.) The set of all these transformations forms a group under the operation of "doing a transformation after another". Of course, we need to add in the rotation by 0 degrees, which is the identity.

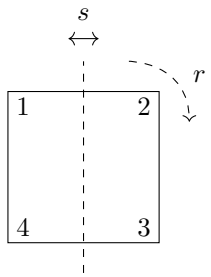


Figure 1.1: A square with some labels to help you visualize the dihedral group D_4

For better visuals, see [Gal20, Fig. 1.1, p. 28].

We can easily generalize this example. Given an n sided regular polygon, we can again let r denote rotation by $360/n$ degrees, and we let s denote reflection about some axis. The general construction of this is called the **dihedral group of an n-sided polygon** D_n. We also sometimes call this the dihedral group of order $2n$.

//
Example 1.12. The real numbers form a group under usual addition. The real numbers without 0 form another group under usual multiplication. //

Note that the previous example illustrates an important point. *The same (similar) set can be a different group when the operation is replaced.* This tells us that to specify a group, we need both the set, as well as the group operation. However, if the operation does not matter, or it is clear from context, we shall simply say that G is a group.

Exercise 1.13. Verify that all of the above examples which are claimed to be groups are indeed groups.
Exercise 1.14. Groups can be finite or infinite in size. Identify which of the above groups are finite and which are not.
Exercise 1.15. Not every group is Abelian. Identify which of the groups above are abelian and which are not.

We state a few more properties of groups. Many of the proofs below invoke the uniqueness of inverses, and the reader should keep this in mind as they read the proof.

Theorem 1.16. Let G be a group. Then, the following are true.

1. **(Generalized associativity)** For any $x_1, \ldots, x_n \in G$, the value of $x_1 \cdots x_n$ is independent of how it is bracketed.
2. If $g \in G$, then $\left(g^{-1}\right)^{-1} = g$.
3. **(Socks-shoes property)** If $g, h \in G$, then $(gh)^{-1} = h^{-1}g^{-1}$.
4. **(Cancellation)** Let $g, h, h' \in G$. If $gh = gh'$ then $h = h'$. This is called left cancellation. Additionally, if $hg = h'g$, then $h = h'$. This is called right cancellation.

Proof. (1) is Exercise 1.2.

(2) Write

$$\left(g^{-1}\right)\left(g^{-1}\right)^{-1} = e = g^{-1}g.$$

Then the result follows by uniqueness of inverses.

(3)

$$(gh)^{-1}(gh) = e = h^{-1}h = h^{-1}(g^{-1}g)h = (h^{-1}g^{-1})(gh).$$

(4) Exercise for reader. □

To ensure that the reader is adequately familiar with the techniques of the proof above, we include the following simple exercises.

Exercise 1.17. Prove part (4) of Theorem 1.16.

Exercise 1.18. Prove part 1-2 Theorem 1.16 again using Theorem 1.16 part (4).

Exercise 1.19. We called part 3 of Theorem 1.16 the socks-shoes property. Explain why we gave it that name.

At this point, it seems fitting to introduce an infinite family of examples of groups. We will be studying them closely in Chapter 2.

Example 1.20 (Integers mod n)**.** Let $\mathbb{Z}_n = \{0, \ldots, n-1\}$ be equipped with the operation of addition modulo n. That is, we define $+$ on $\mathbb{Z}_n$ to be given by $a + b = (a + b) \mod n$. This is called the *group of integers modulo n*, or alternatively *the cyclic group of order n*. We will soon see what this means. //

Throughout the section on group theory, whenever we write $\mathbb{Z}_n$, we are referring to the group of integers under addition modulo n.

Exercise 1.21. Verify that $\mathbb{Z}_n$ with the operation as defined above is indeed a group.

Example 1.22 (Group of units)**.** Let $U(n)$ denote the set of all nonnegative integers $k \leq n$ such that $\gcd(k, n) = 1$. Then $U(n)$ is a group under the operation of multiplication modulo n. That is, if $a, b \in U(n)$, $ab = a \cdot b \mod n$. //

We now give as an example, an infinite family of non abelian groups. This family of groups is important because in a sense, they contain every other finite group.

Example 1.23 (Symmetric groups)**.** Let $S = \{1, \ldots, n\}$. Then consider the set of all permutations of S (bijective functions from S to S). We shall call this set S_n, which stands for *symmetric group on n things*. This set is a group under function composition. //

Exercise 1.24. Prove that S_n is a group under function composition.

We will not have the reader prove that this is non abelian yet, until we develop more tools in Chapter 3.

It is common to perform repeated multiplication in groups with a single element. Nobody wants to write $ggggggg$. How shall we clean this up? Notation. Recall from elementary school that a^n is the act of multiplying a by itself n times. To better leverage our intuitions from these times, we can define similar notation for repeated multiplication in groups. Let G be a group and $g \in G$. We shall write

$$g^n = \underbrace{gg \cdots g}_{n \text{ times}}$$

to mean g multiplied by itself n times. If the group operation is denoted by addition, we write

$$n \cdot g = \underbrace{g + g + \cdots + g}_{n \text{ times}}$$

to mean g added to itself n times. In either way, these are the same concept. This does leave the small problem of leaving multiplying g by itself 0 times undefined. What should g multiplied by itself no times be? Drawing back from the intuition of exponentiation from elementary school, we may recall that raising a real number to the 0th power yields 1. But what is 1? Well, it is the multiplicative identity of the real numbers. This suggests a similar definition for groups. Thus, g^0 (or $0 \cdot g$) is *defined* to be e, the group identity.

Good notation should leverage existing intuitions and feel natural, and easy to work with. At this point, the reader is probably wondering whether this notation really does satisfy the usual properties of exponentiation. It turns out that these usual properties of exponentiation really only depend on associativity. Thus, we have the fact that $a^{n+m} = a^n \cdot a^m$. In Exercise 1.30, we shall see that $a^i a^j = a^{i+j}$ as well, thus the familiar intutition of repeated multiplication or addition of numbers carries over.

Example 1.25. Let G be the set of real numbers under multiplication, and consider the real number π. Notice that $\pi^0 = 1$, under usual exponentiation and our definition, and $\pi^n = \pi \cdots \pi$ n times, which again, agrees with the usual definition. //

Definition 1.26 (Order of an element)**.** If $g \in G$, then we denote $|g|$ to be the *least positive integer* n such that $g^n = e$.

Example 1.27. In the group $\{1, -1, i, -i\}$ under the operation of complex multiplication, the element i has order 4 as $i^4 = -1$ and 4 is the least positive integer for which this holds true for. //

Example 1.28. Let $G = \mathbb{Z}_6$. We leave the reader to calculate the order of every element. Note that the only possible orders of elements in this group are 1,2,3 and 6. We will see why this is true in Chapter 2. //

We shall also define the order of a group.

Definition 1.29 (Order of a group)**.** Let G be a group. Then $|G|$ is the number of elements in G if G is finite, or if G is infinite, it is ∞.

At this point, the reader may be wondering why the abuse of notation. Is this abuse of notation even justified? Or will it lead to confusion down the road? Unfortunately, at this stage, we aren't able to provide a good answer to why this notational abuse is justified. However, we promise the reader that in later chapters, such as Chapter 2, we will justify this.

We close off this section with some exercises and problems.

1.1.1 Problems

Exercise 1.30 (Power notation)**.**

1. Prove that $a^{i+j} = a^i a^j$ for all nonnegative integers i, j.
2. Prove that $a^{ij} = (a^i)^j$ for all nonnegative integers i, j.
3. Prove that $a^{-i} = (a^i)^{-1}$.
4. Prove that $a^{i+j} = a^i a^j$ and $a^{ij} = (a^i)^j$ for all integers i, j.

Exercise 1.31 (Order of an element is the same as the order of its inverse)**.** Show that $|a| = \left|a^{-1}\right|$

Exercise 1.32 (Divisors and orders)**.** Let G be a group, $a \in G$ and let $|a| = n$. Let d be a divisor of n. Prove that $\left|a^d\right| = n/d$.

Problem 1.1. Let G be a group and $a, b \in G$. Prove that $\left|aba^{-1}\right| = |b|$. Now show that $|ab| = |ba|$.

Problem 1.2. Let G be a group. Prove that if for every $g \in G$, we have $g^2 = e$, then G is Abelian.

Problem 1.3. Let S be a set with an associative and commutative binary operation $\cdot$ on it, with the additional property that given any $a, b \in S$, there exists $c \in S$ such that, $a \cdot c = b$. Prove that for all $x, y, z \in S$, if $x \cdot z = y \cdot z$, then $x = y$.

Problem 1.4. Suppose that G is a group such that $(ab)^i = a^i b^i$ for 3 consecutive integers i, for all $a, b \in G$. Prove that G is abelian.

Problem 1.5. Let G be a nonempty finite set that is closed under an associative binary operation such that for every $x, y, z \in G$,

1. **(Left cancellation)** if $xy = xz$ then $y = z$, and;
2. **(Right cancellation)** if $yx = zx$ then $y = z$.

Prove that G is a group. Find an example that if one of the cancellation laws were not assumed, that G is not a group. (Find an example without left cancellation and without right cancellation)

Problem 1.6 (Fundamental Group)**.** This exercise is best done with knowledge of topology.

Let X be a nonempty path-connected space, and $x_0 \in X$ be a point. Recall that a *loop* in X is a continuous map $p : [0, 1] \to X$ such that $p(0) = p(1)$.

1.2 Subgroups

In the previous section, the reader may have observed that some groups are seemingly contained in other groups. For example, the special linear group is a subset of the general linear group. The notion of a substructure is a very common theme throughout the study of abstract algebra. Before we give the definition of a subgroup, the reader should keep the idea of a subgroup being a smaller group contained in a bigger group in mind.

Definition 1.33 (Subgroup). Let G be a group. A subset $H \subseteq G$ is a **subgroup** of G if the following properties hold under the operation of G.

1. The identity of G is in H.
2. For all $x, y \in H$, $xy \in H$.
3. For all $x \in H$, $x^{-1} \in H$.

This tells us that if we restrict the operation of G to H, then H is still a group. We shall notate the situation of H being a subgroup of G by $H \leq G$. If H is a *proper* subgroup of G, it means that H is a proper subset of G, and we denote this by $H < G$.

Before we continue, we shall give some examples of subgroups.
Example 1.34. Any group is a subgroup of itself. //
Example 1.35 (Trivial example)**.** Let $G = \mathbb{Z}$ under usual addition and $H = \{0\}$. Then H is a subgroup of G. In general, if G is any group and $H = \{e\}$ then H is a subgroup of G, and it is called the *trivial subgroup of* G. //

A quick remark is that if G is a group with a single element, then G is called the *trivial group*.
Example 1.36 (Roots of unity)**.** Let $G = \mathbb{C} \setminus \{0\}$ with the operation of multiplication and let $H = \{1, -1, i, -i\}$. Then H is a proper subgroup of G. //
Example 1.37. Let $G = \mathbb{Z}_5$. Then the *only* subgroups of G are $\{0\}$ and G itself. //

We emphasize that $\mathbb{Z}_5$ really does only have 2 subgroups. The reason for this will be seen in the next section.

Note that some authors will define a subgroup of G to be a subset $H \subseteq G$ such that H is a group under the operation of G. This definition is equivalent to the one above. Note that restricting an associative binary operator on G to a subset of it still leaves it associative. The reader should verify this for themselves.

We now give some equivalent formulation of the definition of a subgroup in the form of a theorem. These are often called the subgroup tests (c.f. [Gal20]).

Theorem 1.38 (Subgroup tests). Let G be a group and $H \subseteq G$. Then, the following are equivalent.

1. H is a subgroup of G.
2. H is nonempty, for all $x, y \in H$ we have $xy \in H$. For all $x \in H$ we have $x^{-1} \in H$.
3. H is nonempty, and for all $x, y \in H$, we have $xy^{-1} \in H$.

Proof. We will not insult the reader's intelligence by providing a proof. □

Exercise 1.39. Prove Theorem 1.38.

Readers who have had linear algebra will recall that to test whether U is a subspace of a vector space V, we would check that U is nonempty, if $x + y \in U$ and $\lambda x \in U$ for some scalar λ. This will actually suffice to show that U is a subgroup of V has well.

In general, to test whether something is a subgroup, we can apply the following framework. Suppose G is a group and $H \subseteq G$ with some property P. We first check that H is nonempty. This usually involves verifying that $e \in G$ satisifies the property P. Next, we show that if x, y satisfy the property P, then xy^{-1} also satisfies the property P. We can then apply the subgroup test to conclude that H is a subgroup of G.

The reader is probably wondering why checking for existence of inverses is needed. After all, in linear algebra, when checking that U is a subspace, we didn't need to check that the additive inverse of $u \in U$, $-u$ is in U. This is because

this step was completed when we checked that U is closed under scalar multiplication. However, with groups, this is not sufficient.

Example 1.40 (Why are inverses needed)**.** Consider the set of natural numbers $\mathbb{N} \subseteq \mathbb{Z}$ where $\mathbb{Z}$ is the group of integers under addition. Then $\mathbb{N}$ is nonempty, contains the identity of $\mathbb{Z}$ and is closed under the operation of $\mathbb{Z}$, but does not contain inverses for any $n > 0$. //

However, if H is a *finite* subset of G, it is sufficient to check that H is closed under the operation of G.

Theorem 1.41. Let G be a group and $H \subseteq G$ be a *finite subset* of G. Then, H is a subgroup if and only if for all $x, y \in H$, $xy \in H$.

Proof. A good exercise. □

Exercise 1.42. Prove Theorem 1.41

We now introduce 2 more definitions, the centralizer of an element and the center of a group. These are both subgroups (exercise) and will be used in the future to prove the Sylow Theorems, and some other counting theorems.

Definition 1.43 (Centralizer)**.** Let G be a group and $a \in G$. Then define

$$C(a) = \{\, g \in G : ga = ag \,\}.$$

We call this the **centralizer of** a in G. This is the subgroup of all the elements that commute with a.

Exercise 1.44. Prove that $C(a)$ is a subgroup of G.

Definition 1.45 (Center of a group)**.** Let G be a group. Then define

$$Z(G) = \{\, g \in G : \forall x \in G, gx = xg \,\}.$$

We call this the **center of** G. This is the subgroup of the elements in G that commute with all other elements.

If the group is clear, we will sometimes simply write just C to indicate the center of the group.

Exercise 1.46. Prove that $Z(G)$ is a subgroup of G.

1.2.1 Problems

Exercise 1.47. Let G be a group and H, K be subgroups. Prove that $H \cap K$ is a subgroup of G. Now suppose H_α, $\alpha \in \Lambda$ is an arbitrary family of subgroups. Show that $\bigcap_{\alpha\in\Lambda} H_\alpha$ is a subgroup.

Exercise 1.48. Let G be a group and H, K be subgroups of G. Is $H \cup K$ always a subgroup of G? If so, prove it. If not, find a counterexample.

Exercise 1.49. Let G be an Abelian group and let $g \in G$. Let $n \in \mathbb{Z}$ be a fixed integer. Show that the set $H = \{\, x \in G : x^n = e \,\}$ is a subgroup of G. Is this true if G is not Abelian?

Exercise 1.50. Let G be a group and suppose that for all $x, y, z \in G$, if $xy = yz$ then $x = z$. Prove that G is Abelian.

Exercise 1.51. Let G be a group. Prove that $(ab)^2 = a^2b^2$ if and only if $ab = ba$. Prove that $(ab)^{-2} = b^{-2}a^{-2}$ if and only if $ab = ba$. [Gal20, Ex. 36, Ch 1, p. 56]

Exercise 1.52 (Conjugates)**.** Let G be a group and let $x \in G$. Let H be a subgroup of G. Define $xHx^{-1} = \{\, xhx^{-1} : h \in H \,\}$, which is called the *conjugate of* H *by* x. Show that

1. xHx^{-1} is a subgroup of G,
2. if H is cyclic then so is xHx^{-1},
3. if H is Abelian then so is xHx^{-1}.

We remark that conjugacy is an equivalence relation on G. Specifically, define $x \sim y$ if and only there exists $g \in G$ such that $x = gyg^{-1}$. This exercise is important because we will use this concept to prove the Sylow Theorems.

Exercise 1.53 (Centralizers and conjugates)**.** Let G be a group and let $x \in G$. Show that $g \in C(x)$ if and only if $gxg^{-1} = x$. Conclude that $C(x) = \{\, g \in G : gxg^{-1} = x \,\}$.

Problem 1.7. Prove that no group is the union of 2 proper subgroups. (No cheating and looking this up)

Problem 1.8. Does there exist an infinite group where every element has finite order?

1.3 Direct Products

In the previous section, we have seen groups contained within other groups, in the form of subgroups. Now we turn to the other aspect: building bigger groups from smaller groups.

Definition 1.54 (Direct Product)**.** Let G, H be groups. The **direct product of G and H** is defined to be the set

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

endowed with the group operation $(g, h)(g', h') = (gg', hh')$.

Recall from linear algebra that given vector spaces V, W, one can form the product of these vector spaces $V \times W$. This is the same notion. Some authors may call this the *external direct product* of groups [Gal20, Ch 8], and denote it with $G \oplus H$. The reader show now attempt the following exercises to gain some familiarity with this definition.
Exercise 1.55. Prove that the direct product of $G \times H$ is a group.
Exercise 1.56. Prove that if G, H are abelian then so is $G \times H$.
Exercise 1.57. Let $g \in G$ and $h \in H$. We shall note that $(g, h) \in G \times H$. Show that (e, h) and (g, e) commute with each other.
Exercise 1.58 (Order of elements in direct products)**.** Let $g \in G$ and $h \in H$, and consider $G \times H$. Prove that $|(g, h)| = \operatorname{lcm}(|g|, |h|)$.

Let us now see some examples of direct products.
Example 1.59. We take $\mathbb{Z}_2 \times \mathbb{Z}_2$. What does this group look like? We can write out the set explicitly, as it is small:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{ (0,0), (0,1), (1,0), (1,1) \}.$$

Although this group is abelian, notice that it is not cyclic. If it were cyclic then it would have an element of order 4, but no such element exists in this group. //
Example 1.60. Take $\mathbb{Z}_2 \times \mathbb{Z}_3$. Again, let us look at what this group looks like.

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{ (0,0), (0,1), (0,2), (1,0), (1,1), (1,2) \}.$$

There are 6 elements in this group. In fact, this group is cyclic! We leave the reader to find which element has order 6. //

A natural question is how do we deal with the product of more than 2 groups. Let's say we have groups G, H, K. There are two ways to think about this direct product: $(G \times H) \times K$ and $G \times (H \times K)$. Are these the same group? It turns out that the answer to this question is yes, but the reader will have to await for the definition of a group isomorphism to be able to prove this fact.

What about the infinite case? Suppose we have for each $n \in \mathbb{N}$, a group G_n. We can define the direct product in the same way as in Definition 1.54. The group operation also follows similarly.
Exercise 1.61. Formulate the definition of a direct product of infinitely many groups. Prove that this definition does indeed define a group.
Exercise 1.62. Is there an infinite group where every element has finite order?

1.4 Homomorphisms and Isomorphisms

One may say that algebra is the study of relations. At a higher level, we can even ask how are 2 groups related to each other.

In mathematics, the theme of a structure preserving transformation is common. You may have seen continuous and differentiable functions in middle school. These functions preserve certain properties of the real numbers. If you've had linear algebra, you might have seen linear transformations. Linear transformations preserve certain properties of vector spaces. We shall now introduce the notion of a group homomorphism, which preserves certain properties of groups.

Definition 1.63 (Group Homomorphism). Let G, H be groups. Then a **(group) homomorphism** is a function $\phi : G \to H$ such that for all $x, y \in G$,

$$\phi(xy) = \phi(x)\phi(y).$$

A **(group) isomorphism** is a group homomorphism that is bijective.

So a homomorphism is a function that preserves group operations. You can call this an operation-preserving map. Additionally, we shall say that G and H are isomorphic, or G is isomorphic to H if there is an isomorphism $\phi : G \to H$.

Definition 1.64 (Group Automorphism). Let G be a group. A **(group) automorphism** is an isomorphism $f : G \to G$.

So a group automorphism is a group isomorphism where the domain and the codomain are the same.

Before we continue, the reader should really appreciate how simple this definition is. With just the simple equation $\phi(xy) = \phi(x)\phi(y)$, we can capture all the algebraic properties we care about. As algebraists, we often talk about two groups being the "same". While they may not be equal as sets, if they are isomorphic, then every algebraic property you could care about is preserved.

Example 1.65 (Linear maps)**.** Let V, W be vector spaces and $T : V \to W$ be linear. Then T is a group homomorphism, when considering V, W as groups (under vector addition). If T is an isomorphism of vector spaces, then it is also necessarily a isomorphism of groups. //

Example 1.66 (Exponential)**.** Let $G = \mathbb{R}$ under addition, and $H = \mathbb{R}^+$, the positive reals, under multiplication. Define $\phi : G \to H$ by $\phi(x) = e^x$, the exponential function. Then, $\phi(x + y) = \phi(x)\phi(y)$ by properties of exponentials. In fact, this is an isomorphism. //

Exercise 1.67. Prove that ϕ as defined above is an isomorphism.

We shall immediately prove some useful properties of homomorphisms.

Theorem 1.68 (Properties of homomorphisms). Let G, H be groups and $\phi : G \to H$ be a group homomorphism. Then, the following are true.

1. $\phi(e) = \overline{e}$. That is, homomorphisms take the group identity to the identity.
2. $\phi(x^n) = \phi(x)^n$, for all $n \in \mathbb{Z}$.
3. If K is a subgroup of G, then $\phi[K]$ is a subgroup of H. Thus, the image of a subgroup is a subgroup.
4. If J is a subgroup of H, then $\phi^{-1}[J]$ is a subgroup of G. Thus, the preimage of a subgroup is a subgroup.
5. If K is a subgroup of G and K is Abelian, $\phi[K]$ is Abelian.

Proof. For property 1,

$$\overline{e}\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e).$$

The result follows by right-cancellation.

Properties 2-5 are exercises. □

Exercise 1.69. Prove property (2) of Theorem 1.68. *Hint: First show it for nonnegative n, then show that $\phi(g^{-1}) = \phi(g)^{-1}$.*

Exercise 1.70. Prove the rest of Theorem 1.68

Exercise 1.71. Let G be a group. The set of automorphisms on a group G is denoted $\mathrm{Aut}(G)$, and this is called the **group of automorphisms on** G.

For $g \in G$, define $\varphi_g : G \to G$ to be the function $\varphi_g(x) = gxg^{-1}$. Let $\mathrm{Inn}(G) = \{\, \varphi_g : g \in G \,\}$. This is called the **inner automorphism group on** G.

1. Prove that $\mathrm{Aut}(G)$ is a group under function composition.
2. Prove that φ_g is an automorphism. Conclude that $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$.

1.4.1 Problems

Exercise 1.72 (Product of groups is commutative)**.** Let G, H be groups. Prove that $G \times H$ is isomorphic to $H \times G$.
Exercise 1.73 (Product of groups is associative)**.** Let G, H, K be groups. Prove that $(G \times H) \times K$ is isomorphic to $G \times (H \times K)$.

Chapter 2

Cyclic groups

2.1 Cyclic groups

Groups are very general things, and thus we don't have much control over them. However, there are some groups which are much easier to understand and gain control over. These are the cyclic groups. Cyclic groups are very nice because any element in the cyclic group must be of a certain form. We thus open with the motivating example of the integers.

Example 2.1 (The integers)**.** Let $G = \mathbb{Z}$. Consider any integer $n \in \mathbb{Z}$. Since $n = 1 + \cdots + 1$, n times, we can write $n = n \cdot 1$. Every integer is of this form, a multiple of 1. Thus, $\mathbb{Z} = \{ n \cdot 1 : n \in \mathbb{Z} \}$. Alternatively, we could say that $n = -n \cdot -1$, and so $\mathbb{Z} = \{ n \cdot -1 : n \in \mathbb{Z} \}$. //

It seems that 1 and -1 *generate* the entire group of integers (under addition), and indeed this is true.

Definition 2.2 (Cyclic group)**.** Let G be a group. Then G is **cyclic** if there is a $g \in G$ such that $G = \{ g^n : n \in \mathbb{Z} \}$. Such an element g is called a **generator** of G.

If G is cyclic and g is a generator of G, we denote this situation with $G = \langle g \rangle$.

Example 2.3 (Cyclic subgroups)**.** Let G be a group and $g \in G$. Then, $\langle g \rangle$ is a subgroup of G. //

Exercise 2.4. Prove that $\langle g \rangle$ is a subgroup of G.

Example 2.5 (Integers modulo n)**.** Let $G = \mathbb{Z}_n$. Notice that this is again a cyclic group under addition modulo n. Of course, 1 remains a generator for G. However, unlike $\mathbb{Z}$, which only has 2 generators, $\mathbb{Z}_n$ could have more than one. We will see this in the next example. //

Example 2.6. Let $G = \mathbb{Z}_6$. Then $G = \langle 1 \rangle = \langle 5 \rangle$. However, 2 is not a generator of G as $\langle 2 \rangle = \{ 0, 2, 4 \}$ which is not all of $\mathbb{Z}_6$. //

Example 2.7 (Non-example of a cyclic group)**.** Let $G = U(8)$. Then, G is not cyclic, as $\langle 1 \rangle = \{ 1 \}$, $\langle 3 \rangle = \{ 1, 3 \}$, $\langle 5 \rangle = \{ 1, 5 \}$ and $\langle 7 \rangle = \{ 1, 7 \}$. //

Taking $G = \mathbb{Z}_6$, we notice that $4 \cdot 2 = 1 \cdot 2$. In general, we would like to be able to tell when a^i and a^j are the same element (and when they are not). The next theorem gives necessary and sufficient conditions to be able to determine this.

Theorem 2.8. Let G be a group and $a \in G$. If a has infinite order then $a^i = a^j$ if and only if $i = j$. If a has order n then $\langle a \rangle = \{ e, a, a^2, \ldots, a^{n-1} \}$ and $a^i = a^j$ if and only if n divides $i - j$.

Before starting the proof, a remark about what the statement $\langle a \rangle = \{ e, a, a^2, \ldots, a^{n-1} \}$ means. We are essentially saying that if a has order n, then the cyclic group generated by a has n distinct elements in it and it is *precisely* the set as written.

Proof. Suppose a has infinite order. Then $a^n = e$ if and only if $n = 0$. Since $a^i = a^j$ if and only if $a^{i-j} = e$, $i - j = 0$. Suppose a has order n. It is clear that $\{ e, a, a^2, \ldots, a^{n-1} \} \subseteq \langle a \rangle$. Now let $a^k \in \langle a \rangle$. Then using the division algorithm on k and n, $a^k = a^{qn+r} = a^{qn} a^r = a^r$. Keeping in mind that $0 \leq r < n$, $a^k \in \{ e, a, a^2, \ldots, a^{n-1} \}$. Now suppose

$a^i = a^j$, so $a^{i-j} = e$. Apply the division algorithm on $i - j$ to see that $e = a^{i-j} = a^{qn+r} = a^r$. Since n is the least positive integer for which $a^n = e$ and $r < n$, $r = 0$. The converse direction is similar. □

In Definition 1.29, we used the absolute value operation to refer to both the order of an element and the order of a group. We promised that we will justify that abuse of notation here. Let us now make good on our promise. Notice that as a consequence of this theorem we have $|a| = |\langle a \rangle|$. Thus, the order of an element a is precisely the order of the cyclic (sub)group that it generates.

Another consequence of this theorem is the following corollary.

Corollary 2.9. $a^k = e$ if and only if $|a|$ divides k.

Corollary 2.10. If G is a finite group and $a, b \in G$ where $ab = ba$, then $|ab|$ divides $|a||b|$.

In general, however, there is no relationship between $|ab|$ and $|a|, |b|$. The next exercise shows this.

Exercise 2.11. Let $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ be from $\mathbb{SL}_2(\mathbb{R})$. Compute $|A|, |B|$ and $|AB|$.

Given cyclic subgroups $\langle a^i \rangle$ and $\langle a^j \rangle$, how do we determine whether they are the same? Given an element a and its order, can we determine $\left|a^k\right|$ for any k? The answers to all these questions is yes, and the following theorem illustrates this.

Theorem 2.12. Let $a \in G$ and $|a| = n$. Let $k > 0$. Let $d = \gcd(n, k)$. Then, we have

- $\langle a^k \rangle = \langle a^d \rangle$,
- $\left|a^k\right| = n/d$.

Proof. Let $k = dr$, so $a^k = a^{dr}$ which shows $\langle a^k \rangle \subseteq \langle a^d \rangle$. Now write $d = ns + kt$ (c.f. Theorem 0.3), then

$$a^d = a^{ns} a^{kt} = a^{kt}.$$

So $a^d \in \langle a^k \rangle$. Let's prove the second part. Firstly, $(a^d)^{n/d} = e$ so $\left|a^d\right| \leq n/d$. If $i < n/d$, then $(a^d)^i \neq e$ so this establishes $\left|a^d\right| = n/d$. The desired conclusion follows from the first part. □

The next corollary of this theorem tells us that in a finite cyclic group, the order of an element divides the order of the group.

Corollary 2.13 (Order of an element divides order of the group)**.** If G is a finite cyclic group and $a \in G$, then $|a|$ divides $|G|$.

It thus follows that the order of a cyclic subgroup of a finite cyclic group divides the order of the group. In a later chapter, we shall soon this is true in general for any finite group.

This corollary gives us a criterion for the equivalence of cyclic subgroups.

Corollary 2.14 (Criterion for equivalence of cyclic subgroups)**.** Suppose $a \in G$ has order n. Then, $\langle a^i \rangle = \langle a^j \rangle$ if and only if $\gcd(n, i) = \gcd(n, j)$.

Exercise 2.15. Prove this corollary.

We now have the tools to find all the generators of a finite cyclic group.

Corollary 2.16 (Criteria for being a generator)**.** Let $G = \langle a \rangle$ be a cyclic group of order n. Let b be an element of order m. Then, b generates G if and only if $\gcd(m, n) = 1$.

Since $\mathbb{Z}_n$ is always cyclic, we can always easily determine the generators of $\mathbb{Z}_n$.

A burning question in the reader's mind is on the kind and number of subgroups a group may contain. For example, we may be wondering if every subgroup of a cyclic group is cyclic. Intuitively, this should feel true.

Theorem 2.17. Every subgroup of a cyclic group is cyclic.

Proof. Let $G = \langle a \rangle$ and $H \subseteq G$ be a subgroup. Suppose H is not the trivial subgroup, for else it is trivially cyclic. Then there is some $t > 0$ such that $a^t \in H$. We now attempt to find a generator for H. Let m be the least positive integer such that $a^m \in H$. Obviously $\langle a^m \rangle \subseteq H$. Now let $a^k \in H$. Then write $a^k = a^{qm+r}$. Since m is the least, $r = 0$. Thus $a^k \in \langle a^m \rangle$ and so $\langle a^m \rangle \supseteq H$. □

We remark that we make use of the well ordering principle here, so make sure you have spotted it!

This theorem tells us exactly what the subgroups of a cyclic group are, and how to find them. We will invoke Theorem 2.12 many times in the proof, so keep that in mind. Additionally, if d divides n, we note that $\gcd(d, n) = d$.

Theorem 2.18 (Fundamental Theorem of Cyclic Groups)**.** Let $G = \langle a \rangle$ be a finite cyclic group of order n. Then, if d divides n, there is *exactly one* subgroup of order d. Moreover, these are the *only* subgroups of G.

Proof. Suppose d divides n. It is clear that $\langle a^{n/d} \rangle$ is a subgroup of order d. Let $H = \langle a^k \rangle$ be a subgroup of order d, we shall show $H = \langle a^{n/d} \rangle$. Since $\langle a^k \rangle = \langle a^j \rangle$ where $j = \gcd(n, k)$ and $\langle a^j \rangle$ has order $n/j = d$ it follows that $n/d = j$ so $\langle a^k \rangle = \langle a^{n/d} \rangle$. The final claim follows from Theorem 2.17 and Corollary 2.13. □

With this theorem, it is now very easy to find all the subgroups of $\mathbb{Z}_n$.
Exercise 2.19. Formulate a corollary that classifies the subgroups of $\mathbb{Z}_n$.

Since cyclic groups are so nice, they should behave nicely under homomorphisms and isomorphisms as well.

Proposition 2.20 (Properties of cyclic groups under homomorphisms)**.** Let $\phi : G \to H$ be a group homomorphism, and G be a cyclic group. Then, the following are true.

1. If $G = \langle g \rangle$, then $\phi[G] = \langle \phi(g) \rangle$. In other words, ϕ takes generators to generators.

Proof. If $\phi(x) \in \phi[G]$, then there is some integer n such that $x = g^n$. Thus, we have $\phi(x) = \phi(g^n) = \phi(g)^n$. □

Proposition 2.21 (Properties of cyclic groups under isomorphisms)**.** Let $\phi : G \to H$ be a group isomorphism, and let G be a cyclic group. Then, the following are true.

1. H is cyclic.

Proof. (1) follows from Proposition 2.20(1) □

Thus, if G is a cyclic group of order n, it is isomorphic to $\mathbb{Z}_n$.
Exercise 2.22. Show that any cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

We can thus say that there is only one cyclic group of order n up to isomorphism, which means precisely that any cyclic group of order n is isomorphic to any other cyclic group of order n. This means that any question about finite cyclic groups can be answered by studying $\mathbb{Z}_n$ instead.

2.1.1 Exercises and Problems

Exercise 2.23 (Criterion for element to be identity)**.** Prove that if $a^k = e$, then k divides $|a|$.
Exercise 2.24. Show that if G has order 3, then it must be cyclic.
Exercise 2.25. Show that if $a \in G$, then $\langle a \rangle$ is a subgroup of $C(a)$.
Exercise 2.26. Let G be a group and $a \in G$. Show that $\langle a \rangle = \langle a^{-1} \rangle$.
Exercise 2.27. Let $G = \mathbb{Z}$ and let $m, n \in \mathbb{Z}$. Consider $\langle m \rangle$ and $\langle n \rangle$ as subgroups of G. Find a generator of $\langle m \rangle \cap \langle n \rangle$.
Exercise 2.28. Show that $\mathbb{Q}$ under multiplication is not cyclic.
Exercise 2.29. Let G be a cyclic group of order 15 and let $x \in G$. Suppose that *exactly two* of x^3, x^5 and x^9 are equal. Determine $\left|x^{13}\right|$.
Exercise 2.30. Prove that an infinite group has infinitely many subgroups. *Warning: Do not assume that an infinite group must have an element of infinite order.*
Exercise 2.31. Let n be an natural number. Find a group that has exactly n subgroups.
Problem 2.1. Let G be a group with more than one element, and suppose that G has no proper nontrivial subgroups. Show that G is a finite group and $|G|$ is prime.
Problem 2.2. Let G be a finite group. Prove that G is the union of proper subgroups if and only if G is not cyclic.

Given a cyclic group, a question is to determine how many generators it has. We already have Corollary 2.16, which gives us necessary and sufficient conditions for an element to be a generator. At this point, the reader should recall the definition of $U(n)$. It appears that every element of $U(n)$ is a generator of $\mathbb{Z}_n$, and these are the only generators. Is this true?

Proposition 2.32 (Number of generators)**.** Let G be a cyclic group of order n. Then, G has exactly $|U(n)|$ generators.

Proof. Let $g \in G$ and $m = |g|$. Notice that g generates G if and only if $\gcd(m, n) = 1$, which is true if and only if $m \in U(n)$. □

2.2 Euler totient function

We have spent a large amount of time working with $\mathbb{Z}_n$. This feels very number theoretic, and the reader may very well be wondering[1] about the connection between group theory and number theory. We shall scratch the surface of this connection by using group theory to prove some facts about a common function used in number theory, the Euler totient function.
Warning. *Do not think about skipping this section. There are important theorems in here.*

Definition 2.33 (Euler totient function)**.** We define the Euler totient function $\varphi(n)$ to be the number of natural numbers less than or equal to n that are coprime to n.

It is immediate, by definition, that $\varphi(n) = |U(n)|$.

Those who have had number theory may be familiar with the following proposition. You might also recall how much of a pain these are to prove with number theory. Are we going to subject you to the same pain as you have previously experienced? No. We are going to show how we can use group theory to deal with these facts.

Proposition 2.34. Let φ denote the Euler totient function. Then,

1. If a is coprime to b, $\varphi(ab) = \varphi(a)\varphi(b)$
2. Let p be a prime. Then, $\varphi(p^n) = p^n - p^{n-1}$.

Proof. (1) will follow from the more general statement that $U(ab) \cong U(a) \times U(b)$. (2) will follow from the more general statement that $U(p^n) \cong \mathbb{Z}_{p^n - p^{n-1}}$ for an odd prime, and $U(2^n) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$ when $p = 2$. Thus we shall prove the more general statements instead. □

[1] If you're not wondering about it, you might try to skip this section. Heed the warning, and do not skip it.

A common theme in algebra is trying to break down larger structures into smaller, more understandable structures. We began with number theory, by factorizing numbers into primes and studying the primes to gain control over all numbers. In group theory, we can try to understand a group in terms of its subgroups. We shall now prove a theorem that lets us "factorize" $U(n)$.

Theorem 2.35 (Structure of $U(n)$)**.** Let a, b be coprime. Then, $U(ab) \cong U(a) \times U(b)$.

Proof. Notice that the mapping $n \mapsto (n \bmod a, n \bmod b)$ is an isomorphism from $U(ab)$ to $U(a) \times U(b)$. □

The reader should find that the choice of the isomorphism very natural. This choice is natural in part because we didn't really have any other good options to choose.

Exercise 2.36. Check that the mapping which is claimed to be isomorphisms are indeed isomorphisms.

2.2.1 Problems and Exercises

Exercise 2.37 (Automorphisms on finite cyclic groups)**.** Prove that $\mathrm{Aut}(\mathbb{Z}_n)$ is isomorphic to $U(n)$. *Hint: Consider the mapping $\varphi \mapsto \varphi(1)$. Here, φ is an automorphism on $\mathbb{Z}_n$.*

2.3 Group presentations and generators

Group presentations are a tool for us to describe all the elements of a group. We have already made use of them to talk about the dihedral group. We shall only give a light overview here; they will be treated more formally later on.

Definition 2.38 (Generator)**.** Let G be a group and let $S \subseteq G$. Then if every $g \in G$ has the property that g can be written as the finite product of elements of S and their inverses, then S is called a set of **generators for** G. We thus say that G is *generated by* S.

We leave it to the exercises to formalize this notion. For now, an intuitive understanding will suffice. Let us now discuss notation. If S is a set of generators for G, we shall write $G = \langle S \rangle$. If S is a finite set, say $S = \{ g_1, \ldots, g_n \}$, then we shall write $G = \langle g_1, \ldots, g_n \rangle$ instead.

Definition 2.39 (Relation)**.** Let G be a group and suppose S generates G. Any equation that generators satisfy is a called a **relation**.

Example 2.40 (Presentation of $\mathbb{Z}$)**.** The reader has probably already guessed this. Every element of $\mathbb{Z}$ is of the form $1 + \cdots + 1$ where you add 1 to itself n times to obtain n. It thus follows that $\mathbb{Z} = \langle 1 \rangle$. We also notice that we can actually write any element as $-(-1 + \cdots + -1)$, adding -1 to itself n times and taking the inverse of it. Thus $\mathbb{Z} = \langle -1 \rangle$ too. It's not too hard to see that any other element of $\mathbb{Z}$ cannot be a generator of $\mathbb{Z}$. //

Our main focus here shall be on the presentation of D_n. Before we can find ourselves a presentation for D_n, we must first take a look at some of the properties of D_n. Consider a regular n-gon, and let r be a rotation of $360/n$ degrees counterclockwise. Let s be reflection across the line between the vertex 1 and the origin. For a helpful visual, see Figure 2.1.

Now, the following details can be easily deduced. We leave the details to the reader in Exercise 2.45.

1. The order of r is n. This says that every rotation is distinct.
2. The order of s is 2. This says that applying the reflection twice leaves the n-gon unchanged.
3. For any i, $s \neq r^i$. This says that a rotation is never a reflection.
4. Whenever $i \neq j$, $sr^i \neq sr^j$ for $i, j \in \{ 0, \ldots, n-1 \}$. As such,

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

   This means every element of D_n can be written *uniquely* in the form sr^k for some $k \in \{ 0, \ldots, n-1 \}$.
5. $r^j s = sr^{-j}$ for $j \in \{ 0, \ldots, n-1 \}$. This is better understood by seeing that $rs = sr^{-1}$. The reader is encouraged to pull out something that's square (or rectangular) and try this for themselves.

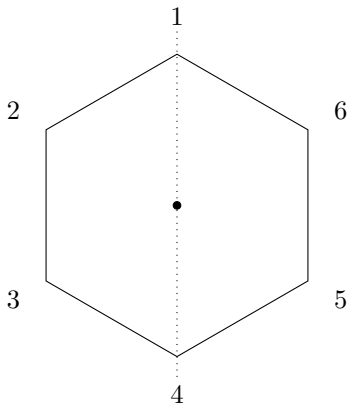


Figure 2.1: Labelled hexagon

With these facts, we are now ready to construct a presentation of D_n. From 4, every element of D_n can be written with r and s, so we would have 2 generators: r, s. At this point, we have no relations yet, but it seems sensible that we should write down the relations $r^n = e$ and $s^2 = e$. For our last relation, we shall write down $r^j s = sr^{n-j}$, a slight modification of number 5. Our choice for this relation is forced by the fact that the other facts simply say that something is not equal to something else. We now present[2] to the reader, the presentation of D_n.

Example 2.41 (Presentation of D_n)**.** The usual presentation of D_n is given by

$$D_n = \langle r, s \mid r^n = s^2 = e,\ sr^j = r^{-j}s \rangle.$$

Intuitively, r is a rotation and s is a reflection. We leave it to the reader to check that this presentation actually gives us D_n.

Of course, there are other presentations, such as

$$D_n = \langle a, b \mid a^2 = b^2 = (ab)^n = e \rangle.$$

You can think about it as $a = s$ and $b = sr$ where s, r are from the first presentation. //

Group presentations are nice because they're a compact way to describe a group. Unfortunately, there are some caveats to group presentations. Due to the flexibility of group presentations, we do not require that the generators come from some preexisting group. What this means is that we can write down some presentation like $\langle a, b \mid a^4 = b^2 = e \rangle$ and consider all the strings formed by a and b and their formal inverses[3]. What this means is that this presentation defines a group G where the set is all finite strings with letters a, b and letters a^{-1}, b^{-1}, with the property that aa^{-1}, $a^{-1}a$ and $bb^{-1}, b^{-1}b$ are removed from the string. For example, the string $aab^{-1}ba$ is equal to aaa. The same conventions apply: if we have $aaaa \cdots a$ n times, we would write a^n instead. Such a construction is called a *free group*. The relations then specify what strings are equal in this group. We will return to the concept of free groups in a latter chapter, but because of this, if we are given an arbitrary presentation, it can be difficult or impossible to distinguish between distinct elements. In the example with D_n, we worked backwards by deducing facts that the generators must satisfy and property 4 told us that everything in D_n was able to be uniquely expressed in terms of the generators and relations, but this may not be true for an arbitrary group presentation. This has some nasty consequences.

Example 2.42 (A group presentation that leads to an infinite group)**.** Consider the presentations

$$\langle a, b \mid a^2 = b^2 = (ab)^2 = e \rangle \tag{2.1}$$

$$\langle a, b \mid a^3 = b^3 = (ab)^3 = e \rangle \tag{2.2}$$

What do you think the order of Equation (2.1) is? 2? 4? It turns out that this is a group of order 4. (Actually this turns out to be D_2. See Exercise 2.47) Now what about Equation (2.2)? Is it 3? 9? No! It's an infinite group. As such, one must not get misled by things like

$$\langle x, y, z \mid x^n = y^k = z^m = e, \cdots \rangle$$

and conclude that the group is necessarily finite. //

[2] lmao

[3] This is a horrible name and very pedagogically disastrous, I'll need to change this soon

Another important remark is in order. Given a group presentation, we cannot assume that the relations as written are the only relations. That is, there may be some hidden relations.

Example 2.43. This is taken from [DF04, Eqn 1.2, p. 26]. Let

$$X_n = \langle x, y \mid x^n = y^2 = 1,\ xy = yx^2 \rangle.$$

Although X_n looks like a group that has order $2n$. This is not true. The problematic relationship is $xy = yx^2$. Let's now see why this causes problems. First, notice that y has order 2, so that $y^2 = e$. Now we consider the relationship $x = xy^2$. Now, $y^2 = yy$, so then we have

$$x = (xy)y = (yx^2)y = (yx)(xy) = (yx)(yx^2) = y(xy)x^2 = y(yx^2)(x^2) = x^4.$$

So this tells us that $x^3 = e$. So the order of X_n can be at most 6. //

Example 2.44 (A group with an elaborate presentation that degenerates)**.** This example is from [DF04, Eqn 1.3, p. 27]. Let

$$Y = \langle u, v \mid u^4 = v^3 = 1,\ uv = v^2u^2 \rangle.$$

While the first relation may suggest that Y has order 12, Y turns out to actually be the trivial group. A sketch of this proof is given in Exercise 2.48. //

Now why does this not happen with the presentation we gave for D_n? The reason is because we crafted a presentation from properties that the group already satisfies. As such, we have demonstrated that there is a group with generators r, s that satisfy the relations as given in the standard presentation. This tells us that a group which satisfies the relations of the standard presentation of D_n would have at least order $2n$, since it would contain D_n. It can also be proven that any group with the presentation as given would have order at most $2n$, so necessarily this presentation gives us the dihedral group.

2.3.1 Problems and Exercises

Exercise 2.45 (Properties of D_n)**.** Prove the following properties about D_n.

1. The order of r is n.
2. The order of s is 2.
3. For any i, $s \neq r^i$.
4. Whenever $i \neq j$, $sr^i \neq sr^j$ for $i, j \in \{0, \ldots, n-1\}$.
5. $r^j s = sr^{-j}$ for $j \in \{0, \ldots, n-1\}$. A good strategy is to prove that $rs = sr^{-1}$ first, then apply induction on j.

Exercise 2.46. Find a presentation of $\mathbb{Z}_n$.

Exercise 2.47. Show that the presentation in Equation (2.1) gives the dihedral group D_2, but that the presentation in Equation (2.2) is a presentation of an infinite group.

Exercise 2.48. We shall prove that Y as defined in Example 2.44 is the trivial group.

1. Show that $v^2 = v^{-1}$.
2. Prove that $v^{-1}u^3v = u^3$. To get started, notice that $v^{-1} = v^2$, and so $v^2u^3v = (v^2u^2)(uv)$. You will need to make use of part 1 again.
3. Prove that u^3 and v commute.
4. Prove that Y is abelian. Note that it suffices to show that u and v commute (why?). Try to prove that $u^9 = u$, and then apply (2)
5. Prove that $uv = e$, $u = e$ and $v = e$. Conclude that Y is the trivial group.

Problem 2.3. Let G be a finitely generated group, and suppose that $[G : H]$ is finite. Prove that H is finitely generated. *(You might need the content from Chapter 4 to do this.)*

Bonus: Try to find a proof of this fact using algebraic topology

Chapter 3

Permutation Groups

3.1 Permutations and cycles

Now that we have looked at a bunch of abelian groups, let us look at some non abelian groups. In particular, we will be looking at an infinite familiy of non abelian groups, called permutation groups. The importance of permutation groups cannot be overstated. In a sense, every group is contained within a permutation group. This will be the content of Cayley's Theorem.

Definition 3.1 (Permutation). Let S be a set. Then a **permutation** (of S) is a bijection $\sigma : S \to S$.

We leave the reader to come with some examples of permutations.
Exercise 3.2. Let $S = \{1, 2, 3\}$. Find every permutation of S.

We have previously seen in Example 1.23 that if $S = \{1, \dots, n\}$, then the set of permutations of S forms a group under function composition. In fact, given any set A, the set of permutations on S forms a group under function composition. We denote this set with S_A, or $\mathrm{Sym}(A)$, to avoid things like S_S (which is confusing). This is called the *group of symemtries on the set* A. Of course, when n is a positive integer, we also have S_n, the group of symmetries on n things[1].
Exercise 3.3. Let S be *any* set. Prove that the set of permutations on S forms a group under function composition.

We remark that the structure of the group S_A only depends on the cardinality of A, and not on what is in A. That is, if $|A| = |B|$ then S_A is isomorphic to S_B. We defer a proof of this to Exercise 3.28. As such when considering permutations on finite sets of size n, we only need to consider permutations on the set $\{1, \dots, n\}$.

We will focus our efforts on permutations of finite sets for now. Recall that S_n denotes the set of permutations on n things. Since the main property of an n-element set is that it contains n elements, we shall let S_n refer to the group of permutations on the set $\{1, \cdots, n\}$. To aid in our study of permutation groups, we shall introduce some notation to describe the elements of permutation groups, called *cycle notation*. To understand this notation, let us begin with an example.

Let $\sigma \in S_6$ be defined by $\sigma(1) = 3$, $\sigma(2) = 4$, $\sigma(3) = 5$, $\sigma(4) = 6$, $\sigma(5) = 1$, $\sigma(6) = 2$. So, 1 goes to 3, 3 goes to 5 and 5 goes to 1. We can write this down as $(1, 3, 5)$. Additionally, 2 goes to 4 and 4 goes to 6, and 6 goes to 2. We similarly write this down as $(2, 4, 6)$. Thus, expressing σ in cycle notation, we get $\sigma = (1, 3, 5)(2, 4, 6)$.

We remark that given $\sigma \in S_n$, if $n < 10$, it is common to omit the commas in the cycle notation as there is no ambiguity about what is going on. So for instance, our σ above could be written as $(135)(246)$.

Let us see how to evaluate σ at a particular value. Suppoe that we didn't know what $\sigma(5)$ was but we do know that $\sigma = (135)(246)$. We first apply the cycle (246) to 5. Since 5 appears nowhere in this cycle, it comes out as a 5. Now we apply the cycle (135) to 5. Since 5 is at the end of the cycle, it goes to 1, so application of (135) to 5 yields 1.

[1] Actually, it turns out that natural numbers are sets, since they are ordinals. So the notation S_n and S_A is not abusive. But if you don't know about this fact, then it is abusive notation.

$$5 \overset{(246)}{\longmapsto} 5 \overset{(135)}{\longmapsto} 1$$

Now, let $\tau = (123)$. We shall now describe how to compose the permutations σ and τ. In this case, the obvious answer is the correct one, so we have

$$\sigma\tau = \underbrace{(135)}_{\sigma}\underbrace{(246)(123)}_{\tau}.$$

As such, we compose cycles *right to left*. This agrees with how we do function composition. (The reader should be warned that some authors compose cycles left to right instead. Note that this is stupid.)

However, this form is not very helpful for determining the properties of $\sigma\tau$. It is much better if we can express $\sigma\tau$ in terms of disjoint cycles.

Definition 3.4 (Disjoint cycles). Let $\alpha = (a_1, \ldots, a_n)$ and $\beta = (b_1, \ldots, b_m)$. Then α and β are said to be **disjoint** if $a_i \neq b_j$ for all i, j.

In other words, two cycles are disjoint if they share no elements in common. For example, the cycles (123) and (456) are disjoint, but the cycles (134) and (235) are not.

So to express $\sigma\tau$ in terms of disjoint cycles, we simply need to find out where all the elements go. Unfortunately, the best way to do so is to simply evaluate $\sigma\tau$ at every element. We shall do one evaluation and leave the rest for the reader to practice. Let us follow where the element 3 goes.

$$3 \overset{(123)}{\longmapsto} 1 \overset{(246)}{\longmapsto} 1 \overset{(135)}{\longmapsto} 3$$

So $\sigma(3) = 3$.

Exercise 3.5. Figure out where the rest of the elements go. Write down $\sigma\tau$ in cycle notation.

We now finish our discussion of cycle notation by remarking that cycles with only one entry are often omitted. For example, instead of writing (1)(23)(4)(56), one would write (23)(56) instead. Any missing element is fixed by the permutation. Of course, we have to write something down for the identity permutation, so we could say that the identity permutation is (1) or (3) or whatever.

We now begin our investigation into permutations. The following theorem justifies the preceding discussion on writing permutations as cycles. While reading the proof, the reader should keep in mind the cycle decomposition algorithm.

Theorem 3.6 (Existence of cycle decomposition). Every permutation of a finite set admits a cycle decomposition. In other words, if $\sigma \in S_n$ then σ is either a cycle, or a product of disjoint cycles.

Proof. Let $S = \{1, \ldots, n\}$ let σ be a permutation on S. Pick $a_1 \in S$. Set $a_n = \sigma(a_{n-1})$, so $a_n = \sigma^{n-1}(a_1)$. This sequence is finite since all the elements are in S. Thus, there are indices i, j, where $i < j$ and $a_i = a_j$. So $a_1 = \sigma^{j-i}(a_1)$. Now set $\alpha = (a_1, \ldots, a_{j-i})$. If $S \setminus \{a_k\}_1^{j-i}$ is empty we are done. If not, pick $b_1 \in S \setminus \{a_k\}_1^{j-i}$ and repeat the same procedure. Let β be the cycle formed from doing this. We now prove that β and α are disjoint cycles (the general case follows easily). Suppose not. Say x shows up in both α and β. If $x = \beta^k(b_1) = \alpha^m(a_1)$, then this means that $x = \sigma^k(b_1) = \sigma^m(a_1)$, but then we would have $\sigma^{m-k}(a_1) = b_1$, so b_1 shows up in the sequence (a_n). But this contradicts $b_1 \in S \setminus (a_n)$. □

The astute reader may have already noticed the following fact: If α, β are disjoint cycles then the order in which they are evaluated does not matter.

Theorem 3.7 (Disjoint cycles commute). If α and β are disjoint cycles, then $\alpha\beta = \beta\alpha$.

Proof. We shall not rob the reader of the joy of discovering the proof of this theorem on their own. □

Exercise 3.8. Prove Theorem 3.7.

Disjoint cycles have yet another advantage up their sleeve: we are able to quickly determine their order.

Theorem 3.9 (Order of 2 disjoint cycles is lcm of their length)**.** Suppose α and β are disjoint cycles of length m and n respectively. Then,

$$|\alpha\beta| = \operatorname{lcm}(|\alpha|, |\beta|).$$

Proof. Since n, m are the orders of α, β respectively, we let $l = \operatorname{lcm}(n, m)$. Then, $(\alpha\beta)^l = \alpha^l\beta^l = e$ by Theorem 3.7, so $|\alpha\beta| \leq l$. If $k \leq l$ and k is the order of $\alpha\beta$ then we have n and m both dividing k, so k is a common multiple of n and m. Thus $k = l$. □

Exercise 3.10. Prove that if α is a cycle of length n, then $|\alpha| = n$.
Exercise 3.11. Generalize Theorem 3.9.

Given a permutation, we would like to write it as a product of 2-cycles. It is always possible to do so.

Proposition 3.12 (Existence of 2-cycle decomposition)**.** If σ is a permutation on the set $\{1, \ldots, n\}$ then σ can be decomposed as the product of 2-cycles.

Proof. Suppose σ is a cycle. Let $\sigma = (a_1, \ldots, a_k)$. Then direct computation shows that

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

The proof of the general case can be easily obtained by using Theorem 3.6. □

Definition 3.13 (Even/Odd Permutation)**.** Let σ be a permutation on a finite set. Then, σ is **even** if it admits a 2-cycle decomposition into an even number of 2-cycles.

An odd permutation is defined similarly. We call the oddness or evenness of a permutation its *parity*.

One may be wondering whether a 2-cycle decomposition is unique. Unfortunately, this is not true.
Example 3.14 (Non-uniqueness of 2-cycle decomposition)**.**

$$(12345) = (54)(53)(52)(51)$$
$$(12345) = (54)(52)(21)(25)(23)(13).$$

A simpler example would be $(123) = (13)(12) = (12)(23) = (23)(13)$. //

Can a permutation be both even or odd? No. In fact, if a permutation can be decomposed as an even number of 2 cycles, then any 2-cycle decomposition of this permutation must also result in an even number of 2 cycles.

Let us first find out the parity of the identity permutation. Since $e = (12)(12)$ it makes sense that it should be even. It turns out that this is true. Unfortunately, the following proof is very long and painful.

Alternative proofs of the fact that the parity of permutation is well-defined can be found in Exercise 3.33 or Exercise 3.34.

Proposition 3.15 (Identity permutation is even)**.** Let e be the identity permutation. If $e = \alpha_1 \cdots \alpha_n$ where α_i is a 2-cycle, then n is even.

Proof. Suppose otherwise. Say $\beta_1 \cdots \beta_n = e$ where n is odd. Note that $n > 1$. Without loss of generality assume $\beta_1 = (ab)$. Then there is some 2-cycle β_i, $i > 1$, which contains a, otherwise this product will send a to b.

We make a few additional assumptions, which can be done without loss of generality:

1. Assume that i is the smallest such index which contains a;
2. assume that this product is one with the fewest number of a's as a entry in any cycle.

If $i = 2$, then $\beta_1\beta_2$ is $(ab)(ab)$ or $(ab)(ac)$ where $c \neq b$. (Note that if it is of the form $(ab)(ca)$ then we have $(ca) = (ac)$ anyway.) In the first case, $(ab)(ab)$ is the identity, so we now have the identity being a product of an odd number of 2-cycles, with fewer appearances of a's, contradicting assumption 2. In the latter, we have $(ab)(ac) = (ac)(bc)$. We may replace $\beta_1\beta_2$ with $\beta_1'\beta_2' = (ab)(bc)$ in our product. This contradicts assumption 2 again. Since $i = 2$ gives us contradictions, let's assume $i > 2$. Now, β_{i-1} does not contain a, by assumption 1, but it has to contain c. If this is not true, β_i and β_{i-1} are disjoint. We now see that □

Theorem 3.16 (Parity of a permutation is well-defined). If σ is a permutation (on a finite set), then it is either even or odd.

Proof. Let $\sigma = \alpha_1 \cdots \alpha_k$ $\sigma = \gamma_1 \cdots \gamma_m$ be 2-cycle decompositions of σ. Then, keeping in mind a 2-cycle is its own inverse,

$$e = \sigma\sigma^{-1} = (\alpha_1 \cdots \alpha_k)(\gamma_m \cdots \gamma_1).$$

So Proposition 3.15 this implies $k + m$ is even. So k, m are both odd or both even. □

The set of even permutations of a permutation group is extremely important, and so it deserves its own name. Although we will not see its importance at the moment[2], it is worth introducing it at this point.

Definition 3.17 (Alternating group). Let A_n denote the set of even permutations of S_n.

You probably already suspect that A_n is a group now.
Exercise 3.18. Prove that A_n is a subgroup of S_n.

You might be thinking to yourself that there should be as many even permutations as odd permutations. This is indeed true. If $n > 1$, then A_n has order $n!/2$.
Exercise 3.19. Prove that $|A_n| = n!/2$ when $n > 1$.

Hint: If α is even, then $(12)\alpha$ is odd. Additionally, if $\alpha \neq \beta$ then $(12)\alpha \neq (12)\beta$.

3.2 Group actions

We open the discussion about group actions with a motivating example. Let $G = \{ r^0, r^1, r^2, r^3 \}$ where r is rotation clockwise by 90 degrees. Consider the diagram of the square, and follow where the dot goes.

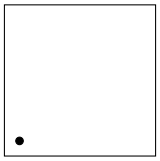


Figure 3.1: Helpful square to visualize rotation group acting on square.

In some sense, the group of rotations is acting on the square, changing its position. We can perhaps envision a rotation as some kind of function on the square. Let S represent the square. Imagine labelling each of the edges of the square by 1,2,3,4. So we can think of rotating the square by 90 degrees as $r(S)$, whatever that means. Now, if we do $r(r(S))$, that is rotating by 180 degrees. But if we do $r^2(S)$, it is also rotating by 180 degrees. In the former, we apply the rotation action and then the rotation action, but in the latter, we multiply r with itself in the group G and then apply the action of the result on S. Naturally, it should make sense that these notions agree. Now, let's take a look at how the identity rotation acts on the square. Notice that the rotation by 0 degrees fixes every edge of the square.

As another example, let us consider a tuple (1,2,3). We can rearrange the components in the tuple, to be something like (2,1,3) or like (3,2,1). Now, we know that the act of rearranging something is simply a permutation. In this example, if σ is the permutation that sends 1 to 2, 2 to 1 and 3 to itself, then $(\sigma(1), \sigma(2), \sigma(3)) = (2, 1, 3)$. It's not too hard to figure out how to extend this idea to any other $\sigma \in S_3$.

[2]The alternating group has no nontrivial proper normal subgroups. You might have seen this called a *simple group*. There is a rather famous theorem that classifies all the finite simple groups. The alternating groups form an infinite family of finite simple groups.

Definition 3.20 (Group action)**.** Let G be a group and S a set. Then a **action of G on S** is a function $f : G \times S \to S$ such that:

1. **(Associativity)** For all $g, h \in G$ and $s \in S$, $f(gh, s) = f(g, f(h, s))$.
2. **(Identity)** For all $s \in S$, $f(e, s) = s$.

As you can see above, writing $f(g, s)$ gets annoying very fast. Thus, whenever the group action is clear, we shall use $g \cdot s$, to mean $f(g, s)$. When there is no danger of confusing the group action with group multiplication, we shall write gs instead.

We shall now see some examples of group actions.

Example 3.21 (Symmetric group)**.** Let $S = \{ 1, \ldots, n \}$ and let $G = S_n$. Then we can define an action of G on S by declaring $\sigma \cdot s := \sigma(s)$. //

Example 3.22. Let $S = \mathbb{R}$ be the real numbers, and let $G = \mathbb{Z}$. We can define an action of G on S by declaring $n \cdot r = n + r$. //

Example 3.23 (Group acting on itself)**.** Let G be a group. Now, if we momentarily forget that G is a group, G is also a set. Thus, we can define a very natural group action on G by $g \cdot h := gh$. So G acts on G by left multiplication. //

Definition 3.24 (Orbit)**.** Let G act on S. For $s \in S$, we define the **orbit of s** to be

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

So the orbit is the image of G under the function $g \mapsto f(g, s)$.

Definition 3.25 (Stabilizer)**.** Let G act on S. For $s \in S$, we define the **stabilizer of s** to be

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

So the stabilizer of s is the set of all $g \in G$ that fixes s under the group action. Of course, a natural question is whether the stabilizer is a subgroup. The following exercise answers that question.

Exercise 3.26. Prove that the stabilizer of s is a subgroup.

A burning question at this point might be the following: Aren't group actions kind of just like permutations? Indeed, this is an excellent question, as we have put in the chapter on permutation groups. Suppose G acts on X. Let us fix a $g \in G$. Consider the function $f : X \to X$ given by $x \mapsto g \cdot x$. It turns out that f is a bijection, and thus f is a permutation of X. Now, let us call σ_g the function that applies the action of g on X, i.e. $\sigma_g(x) = g \cdot x$. It seems that we can construct a map from G into S_X. Of course, this map would be $g \mapsto \sigma_g$. Since we are studying group theory, it is natural to wonder whether this is a homomorphism. Indeed, it is. See Exercise 3.35.

Our study of permutation groups takes a temporary hiatus with the following theorem. If it seems trivial to you, it's due to the power of excellent definitions. This shows us the power of group actions and once again reminds us the importance of constructing good definitions.

Theorem 3.27 (Cayley's Theorem)**.** Every group is isomorphic to a group of permutations.

Proof. See Exercise 3.36. □

3.3 Problems

Exercise 3.28 (Structure of permutation group)**.** Recall that the cardinality of a set A is equal to the cardinality of a set B if there exists a bijection from A to B. Let A, B be sets and suppose that the cardinality of A equals to the cardinality of B. Thus we may let $\gamma : A \to B$ be a bijection. Show that S_A is isomorphic to S_B.

Hint: Think about how a permutation of A can be changed into a permutation of B, and conversely.

Exercise 3.29. Suppose H is a subgroup of S_n and H has odd order. Prove that H is a subgroup of A_n.

Exercise 3.30. Prove that if σ is a permutation with odd order, then σ is even.

Exercise 3.31. Show that if $n \geq 3$, then $Z_(S_n)$ is trivial.

Exercise 3.32. Let $\alpha \in S_n$. Without using Lagrange's theorem, prove that the order of α divides S_n.

Exercise 3.33 (An alternative proof that the sign of a permutation is well-defined)**.** We give an alternative proof that the sign of a permutation is well-defined, due to [Jac09, p. 50].

Recall that an n-cycle can be decomposed into $n-1$ transpositions. If γ is an n-cycle, let $\tilde{N}(\gamma) = n-1$, the number of transpositions that γ is a product of. Given some $\alpha \in S_n$, let

$$\alpha = \gamma_1 \cdots \gamma_n,$$

be the disjoint cycle decomposition of α. Now we can define $N(\alpha) = \sum_{i=1}^{n} \tilde{N}(\gamma_i)$.

More concretely, if γ_i is a u_i cycle, then $N(\alpha) = \sum_{i=1}^{n} u_i - 1$. Also note that $N(e) = 0$.

(a) Show that $N(\alpha)$ is uniquely determined by α.

(b) Let $a, b, c_1, \ldots, c_h, d_1, \ldots, d_k$ be distinct elements, where $h, k \geq 0$. Verify that

$$(ab)(ac_1 \cdots c_h b d_1 \cdots d_k) = (bd_1 \cdots d_k)(ac_1 \cdots c_h).$$

(c) Let $p = (ac_1 \cdots c_h b d_1 \cdots d_k)$. Check that $N(p) = h + k + 1$, and that $N((ab)p) = h + k$.

(d) Let α be some permutation. Show that $N((ab)\alpha) = N(\alpha) - 1$ if a, b occur in the same cycle in the decomposition of α into disjoint cycles, and $N((ab)\alpha) = N(\alpha) + 1$ if a, b occur in different cycles.

(e) Suppose that α is a product of m transpositions. Prove that $N(\alpha) = \sum_{i=1}^{m} \varepsilon_i$, where $\varepsilon_i = \pm 1$. *Hint: Decompose α into disjoint cycles first to make life easy.*

(f) Prove that $N(\alpha)$ and m have the same parity, i.e. $N(\alpha)$ is even if and only if m is even.

Exercise 3.34 (Another proof that the sign of a permutation is well-defined)**.** Let T be the set of all polynomials in $x_1, \ldots, x_n$. For $\sigma \in S_n$, define a group action on T by $\sigma \cdot x_i = x_{\sigma(i)}$ and extending this in a natural way, so for instance, we have $\sigma \cdot (4x_i + 3x_i x_j) = 4x_{\sigma(i)} + 3x_{\sigma(i)} x_{\sigma(j)}$. Let $\Delta = \prod_{i>j} (x_i - x_j)$, where i, j runs from 1 to n.

1. Prove that the group action defined is actually a group action.
2. Show that if τ is a transposition, $\tau \cdot \Delta = -\Delta$.
3. Prove that if σ can be decomposed into an even number of transpositions, then any decomposition of σ into transpositions yields an even number of permutations.

Exercise 3.35 (Group actions and the symmetric group)**.** Let G act on X. For a fixed $g \in G$, define $\sigma_g(x) = g \cdot x$.

1. For every $g \in G$, show that σ_g is a bijection.
2. Show that the map $g \mapsto \sigma_g$ is a homomorphism. (i.e. $\sigma_g \sigma_h = \sigma_{gh}$)

Exercise 3.36 (Cayley's Theorem)**.** Prove Cayley's Theorem.

Exercise 3.37 (Orbits partition a set)**.** Let G be a group acting on a set S. Define $\sim$ on S by

$$x \sim y \iff x \in \mathrm{orb}_G(y).$$

Show that $\sim$ is an equivalence relation, and that the equivalence class of x under $\sim$, $[x]_\sim$ is precisely $\mathrm{orb}_G(x)$.

Chapter 4

Lagrange's Theorem

One of the central problems in group theory is to understand the structure of a group by understanding the structure of its subgroups. Of course, this is a very difficult question to answer. Given a group G, how can we possibly hope to find all of its subgroups? Admittedly, we only have to check a finite number of sets, namely elements of $\mathcal{P}(G)$. We can even dispose of a bunch of sets quite fast (any sets not containing the identity). But that's still a lot! Can we narrow our search more?

We do have a sufficient condition for something to be a subgroup, namely, the definition. But that doesn't help us much, since we would still need to manually check whether something is a subgroup. What about a necessary condition? Do subgroups have any properties that they must satisfy? Turning our attention temporarily to cyclic groups, we notice that the subgroups of all cyclic groups have orders the divisor of the order of the whole group. So the orders of subgroups of cyclic groups divides the order of the group. Is this true in general?

The answer to this question is yes. Lagrange's Theorem tells us that the order of a subgroup must divide the order of a group. Of course, this only holds for finite groups.

How should we prove something like this? Let G be a finite group and let H be a subgroup of G. If we can somehow bundle together the elements of a group into piles of $|H|$, the result should follow. But what is the correct way to bundle them? To find out how to do so, let us look at some examples.

Let $G = \mathbb{Z}_{10}$. We know all the subgroups of G, since G is cyclic. Let us consider the subgroup of G that consists of all the even numbers. Now, we know that there are just as many odd numbers. Indeed, if $H = \{0, 2, 4, 6, 8\}$, then the odd numbers would be $\{1, 3, 5, 7, 9\}$. Now, notice that if we take each element of H and add 1 to it, i.e. $1 + H$, we would arrive at the set of odd numbers. It also appears that $1 + H$ is disjoint from H. Motivated by this example, we turn our attention to the subgroup $H = \{0, 5\}$. In a similar fashion, we can consider $1 + H = \{1, 6\}$, $2 + H = \{2, 7\}$ as well as $3 + H, 4 + H$. What is $5 + H$? It appears that $5 + H$ is just H, and $6 + H$ is just $1 + H$. So it appears that if $h \in H$, then $h + H = H$. Another interesting observation we can make is that $g + H$ and $g' + H$ appear to be either equal to each other, or disjoint.

We summarize our observations:

1. The sets of the form $g + H$ seem to all have the same size
2. We either have $g + H = g' + H$ or they are disjoint

At this point, these are all conjectural. So let us now make this precise.

Definition 4.1 (Coset). Let G be a group and let H be a subgroup of G. A (left) coset of H, denoted gH is the set

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

Why are cosets important? It turns out that cosets form a partition of G, and that the size of a coset is precisely the size of the subgroup H. The language of partitions is equivalence relations, and we shall now talk about them.

Recall that an equivalence relation $\sim$ on G is a relation that is reflexive, symmetric and transitive. Equivalence

relations give rise to partitions. If $\sim$ is an equivalence relation on G and $g \in G$, then the set

$$[g]_\sim = \{\, a \in G : a \sim g \,\}$$

denotes the equivalence class of g under $\sim$. If the equivalence relation is clear, we shall simply write $[g]$.

Proposition 4.2 (Coset is an equivalence relation)**.** Let G be a finite group and H a subgroup of G. Define the equivalence relation $\sim$ on G by $a \sim b$ if and only if $a^{-1}b \in H$. Then, $\sim$ is an equivalence relation and $aH = [a]$, where $[a]$ is the equivalence class of a under $\sim$.

Proof. Exercise. □

Exercise 4.3. Prove Proposition 4.2.

Note that we can declare a similar equivalence relation by saying that $a \sim b$ if and only if there is some $h \in H$ such that $a = hb$.

Theorem 4.4 (Properties of cosets)**.** Let G be a finite group and let H be a subgroup of G. Then, the following are true.

1. $a \in aH$.
2. $aH = H$ if and only if $a \in H$.
3. $aH = bH$ if and only if $a^{-1}b \in H$.
4. $aH = Ha$ if and only if $aHa^{-1} = H$.
5. $|aH| = |bH|$. In other words, different cosets have the same size.
6. aH is a subgroup if and only if $a \in H$.
7. $aH = bH$ or aH is disjoint from bH

Proof.

1. Notice $a = ae \in aH$.
2. This follows from Proposition 4.2.
3. Follows from 2.
4. Exercise.
5. Define a bijection from aH to bH by sending $x \in aH$ to $ba^{-1}x$.
6. Use 2 and 3.
7. Being in the same coset is an equivalence relation.

□

Exercise 4.5. Fill in the details of the proof of Theorem 4.4.

Now, take a good look at property number 5 of Theorem 4.4. This is the key idea here. It tells us that the equivalence classes of the coset relation all have the same size. We are now ready to prove Lagrange's Theorem. With the coset equivalence relation, we cut up G into pieces of size $|H|$.

Theorem 4.6 (Lagrange's Theorem)**.** Let G be a finite group of order n. Let H be a subgroup of G. Then, $|H|$ divides n.

Proof. See Exercise 4.7. □

Exercise 4.7. Prove Theorem 4.6. You will need Proposition 4.2 and property 5 in Theorem 4.4.

We again direct our attention to the power of definitions. Having the correct choice of equivalence relation made the proof of Lagrange's Theorem very easy. As such, it would do a lot of good to understand how such an equivalence relation was chosen. Lagrange's theorem now motivates the following definition: the *index of a subgroup*. If H is a subgroup of G, then we let $[G : H]$ denote the number of left cosets of H. This is called the *index of H in G*. We leave it to the reader to verify that $[G : H]$ is the same number if we used right cosets instead of left. If there are infinitely many cosets, we write $[G : H] = \infty$.

We now state some corollaries of Lagrange's Theorem. While obvious, they are still good to mention.

Corollary 4.8 (Consequences of Lagrange's Theorem)**.** Let G be a finite group. Then, the following are true.

1. If $g \in G$, $|g|$ divides $|G|$.
2. If G has prime order then it is cyclic.
3. If $g \in G$, then $g^{|G|} = e$.

Exercise 4.9. Prove Corollary 4.8.

To really demonstrate the power of Lagrange's theorem, we shall see some applications of it. The first application is in number theory.

Corollary 4.10 (Fermat's Little Theorem)**.** Let p be a prime, and let a be an integer. Then, $a^p \bmod p = a \bmod p$.

Proof. To do this, we study the behavior of an element of $U(p)$. Recall that $U(p) = \{1, \ldots, p-1\}$, which has order $p-1$. If $a \in U(p)$, we would have $a^{|U(p)|} = 1$, so $a^p = a$. If a is not in $U(p)$, then use the division algorithm on a (divide it by p). □

Exercise 4.11. Fill in the details of Corollary 4.10.

Lagrange's theorem also gives us a useful counting theorem which tells us what the sizes of subgroups can be.

Theorem 4.12 (HK theorem)**.** Let H, K be finite subgroups of some group G. Define $HK = \{hk : h \in H, k \in K\}$. Then,

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Let's talk strategy. Of course, HK has $|H| \cdot |K|$ products, but they may not be distinct group elements. What this means is that we could have $hk = h'k'$ where $h \neq h', k \neq k'$. The formula suggests that duplicates occur in multiples of $|H \cap K|$. We need some way to tie each product in HK to every single element of $|H \cap K|$. The first observation comes from noticing that if $t \in H \cap K$, then $hk = (ht)(t^{-1}k)$.

Proof. Let $h \in H, k \in K$. If $t \in H \cap K$, then $hk = (ht)(t^{-1}k)$. This tells us that every element of HK is represented by at least $|H \cap K|$ products in HK. Suppose $hk = h'k'$, then,

$$tt^{-1} = h^{-1}h'k'k^{-1}.$$

So if $t = h^{-1}h' = kk'^{-1}$, then it all works out. This shows that every element in HK is represented by precisely $|H \cap K|$ products. □

The proof here actually leads to a proof of a more general fact, which is outlined in Exercise 4.19.

Let us now see another application of Lagrange's theorem. This time, we classify all groups of order $2p$ where p is some odd prime.

Theorem 4.13 (Classification of groups of order $2p$)**.** Let p be a prime such that $p > 2$. Let G be a group of order $2p$. Then G is isomorphic to $\mathbb{Z}_{2p}$ or D_p.

Proof. See Exercise 4.16. □

Counting can be useful. We now make use of Lagrange's theorem to prove a fact about group actions.

Theorem 4.14 (Orbit-Stabilizer Theorem)**.** Let G be a finite group acting on a set S. Then,

$$|G| = |\mathrm{orb}_G(s)||\mathrm{stab}_G(s)|.$$

Proof. The stabilizer of s is a subgroup of G. It will suffice to provide a bijection between left cosets of $\mathrm{stab}_G(s)$ and elements in $\mathrm{orb}_G(s)$. The map $\varphi : g\,\mathrm{stab}_G(s) \mapsto g \cdot s$ will do. We leave the details to the reader in Exercise 4.17. □

4.0.1 Exercises and Problems

Exercise 4.15. Suppose that G is finite. Let $H \leq G$ and $K \leq H$. Show that $[G : K] = [G : H][H : K]$.
Exercise 4.16. Prove Theorem 4.13 by following the steps below.

1. Assume that G has no element of order $2p$. Show that G must have an element of order p, call it a.
2. Find an element of order 2, call it b.
3. Show that a and b satisfy the relations of D_p: in particular, $a^j b = ba^{-j}$ for $j \in \{1, \ldots, p-1\}$.
4. Show that every element of G can be uniquely expressed in the form $a^j b^k$.
5. Conclude that G is isomorphic to D_p.

Exercise 4.17 (Orbit-Stabilizer Theorem)**.** Complete the proof of Theorem 4.14. In particular, show that the map φ as defined is well-defined and a bijection. Note that the facts in Exercise 3.37 will be needed.
Exercise 4.18. Prove that the rotation group of a cube is S_4.
Exercise 4.19 (Generalization of HK theorem)**.** Let H, K be subgroups of G, and $\alpha : H \times K \to G$ be the map defined by $\alpha(h, k) = hk$. Prove that $\alpha^{-1}(hk) = \{(ht, t^{-1}k) : t \in H \cap K\}$, and that additionally the cardinality of $\alpha^{-1}(hk)$ equals to the cardinality of $H \cap K$. Conclude that if H, K are finite, then $|HK| = |H||K|/(|H \cap K|)$.

See [Jac09, Exercise 9, p. 58]
Exercise 4.20 (Index is multiplicative)**.** Let G be a group (not necessarily finite) and let $H \leq K \leq G$. Prove that $[G : H] = [G : K][K : H]$. Do not assume that any of the indices are finite.

Hint: There is a canonical surjection p from left cosets of H to left cosets of K. Consider the size of $p^{-1}[\{gK\}]$.

Chapter 5

Normal Subgroups and Homomorphisms

At the end of Chapter 1, we briefly discussed homomorphisms. We shall now study a closely related concept: normal subgroups. The study of normal subgroups is closely connected with the study of group homomorphisms.

Definition 5.1 (Normal subgroup)**.** A subgroup N of a group G is **normal** if for all $g \in G$,

$$gN = Ng.$$

Notationally, we will write $N \trianglelefteq G$. When we wish to additionally say that $N \neq G$, we shall write $N \triangleleft G$.

That is to say, the left coset of N is equal to the right coset of N. An equivalent criterion is given below, which may be taken to be the definition of normality. The definition above was chosen due to ease of application.

Lemma 5.2. *Let G be a group and N a subgroup of G. Then N is normal in G if and only if for all $g \in G$,*

$$gNg^{-1} \subseteq N.$$

Proof. See Exercise 5.3. □

Exercise 5.3. Prove Lemma 5.2
Warning. *This does not imply that $gn = ng$ for every $n \in N$.*

Let us now see examples of normal subgroups.

Example 5.4. Any subgroup of an Abelian group is normal. Moreover, any nontrivial group always has at least 2 normal subgroups. Which ones?[1] //

Example 5.5. Let $D_4 = \langle s, r : r^4 = s^2 = 1, sr^j = r^{-j}s\rangle$ be the dihedral group of order 8. Then D_4 has a normal subgroup, namely $N = \langle r\rangle$, the subgroup of rotations. This will actually follow from Example 5.7, but we can directly verify this fact here. Let us pick $g \in D_4$, and notice that if g is a pure rotation, $gN \in N$ and so $gN = Ng$. Let us assume that $g = s$ (the general case follows easily from this - why?), then using the group relation $sr^j = r^{-j}s$, we quickly observe that $sN = Ns$. //

At this point, the reader may be wondering whether "is a normal subgroup of" is a transitive relation. This may feel intuitively true; after all, the relation of being a subgroup of is in fact transitive. Unfortunately, this is untrue.

Example 5.6 (Normality is not transitive)**.** Let $G = D_4$. Let $H = \langle r^2, s\rangle$ and let $K = \langle s\rangle$. Then $K \trianglelefteq H \trianglelefteq G$, but K is not normal in G, since $rsr^{-1} = sr^2 \notin K$. //

Example 5.7 (Index 2 subgroups are normal)**.** Any subgroup of index 2 is normal. In other words, if H is a subgroup of G, and $|G/H| = 2$, then H is normal in G. See Exercise 5.34 for more details. //

Example 5.8 (Alternating group)**.** Recall that A_n is the alternating group, the subgroup of all the even permutations in S_n. Leveraging Example 5.7, we can swiftly say that A_n is normal in S_n. //

Recall that given subgroups H, K of a group G, it may not be true that HK is a subgroup of G. However, if H is instead a normal subgroup of G, then this will be true.

[1] The whole group and the trivial subgroup.

Example 5.9 ("Product" of subgroup with a normal subgroup is a subgroup)**.** Let H be normal in G and K a subgroup of G. Of course HK is nonempty. Given elements $a = h_1k_1, b = h_2k_2 \in HK$, we notice that $ab^{-1} = h_1(k_1k_2^{-1}h_2^{-1})$. Consider the expression in parentheses. Since H is normal in G there is some h' such that $k_1k_2^{-1}h_2^{-1} = h'k_1k_2^{-1}$. So this means $ab^{-1} = h_1h'k_1k_2^{-1}$ which is in HK.

We have thus proven the following proposition: Let H be normal in G and K be a subgroup of G. Then, HK is a subgroup of G. //

Warning. *If H is not normal, then HK may not be a subgroup. Let $G = D_3$, let $H = \{e, s\}$ and let $K = \{e, rs\}$. Then, $HK = \{e, s, rs, srs = r^{-1}\}$, which cannot be a subgroup due Lagrange's Theorem.*

5.1 Quotient groups

We have previously discussed a product of groups. This concept was rather simple. But what about the quotient of groups. Can we "divide" a group by another group?

To explain the concept of quotient groups, we shall turn first to modular arithmetic. Let us consider the set $\mathbb{Z}$, and we declare the equivalence relation $x \sim y$ if and only if $x \mod 3 = y \mod 3$. This partitions $\mathbb{Z}$ into the following sets:

$$\begin{aligned} 0 + 3\mathbb{Z} &= \{0, \pm 3, \pm 6, \cdots\} \\ 1 + 3\mathbb{Z} &= \{1, \pm 4, \pm 7, \cdots\} \\ 2 + 3\mathbb{Z} &= \{2, \pm 5, \pm 8, \cdots\}. \end{aligned}$$

When we add 1 and 1 modulo 3, we get 2 modulo 3. Notice that if we add up the stuff in the set $1 + 3\mathbb{Z}$ to themselves, we also obtain $2 + 3\mathbb{Z}$. This suggests that we should perhaps define the group operation in $\mathbb{Z}/\sim$ by setting $(x + N) + (y + N) = x + y + N$, where $N = 3\mathbb{Z}$.

Can we replicate this construction for any subgroup of $\mathbb{Z}$ whatsoever? It turns out that the answer is yes. What about for a general group? Can we replicate this idea? Yes, but we would require that the subgroup be normal. Of course, in abelian groups, every subgroup is normal. But it turns out that in order for the operation to be well defined it was sufficient to assume that the subgroup is normal.

Theorem 5.10 (Existence of quotient groups)**.** Let G be a group and N be a normal subgroup of G. Then the set G/N with the operation $(xN)(yN) := xyN$ is a group.

Proof. We first show that this operation is well defined. Suppose $xN = x'N$ and $yN = y'N$. Then there is some $n_1, n_2 \in N$ such that $x' = xn_1, y' = yn_2$. So $x'y'N = xn_1yn_2N = xn_1yN = xn_1Ny = xyN$. (Recall that in Chapter 4 we proved some properties about cosets). We leave it to the reader to verify that this operation is associative, has identity and inverses. □

Interestingly enough, the converse is true: If the operation $xNyN := xyN$ defines a group (on the set of left cosets G/N), then N is normal in G. We leave this as a good exercise in Exercise 5.27. Additionally, note that if N is not normal, then the product operation as defined there may not yield a left coset.

Example 5.11. In S_3, let $H = \{(1), (12)\}$. Then $(13)H(23)H$ is not equal to $(13)(23)H$. //

We now make some remarks about notation. It may seem confusing that $gNhN = ghN$, but since G/N is a group, we should view gN and hN as elements of the group G/N. If you find this confusing, you may instead treat gN as $\tilde{g}$ and $\tilde{h}$, although be aware that this technique may lead to you forgetting about the properties of cosets.

The next theorem gives us a criterion for determining if G is not Abelian.

Theorem 5.12. If $G/Z(G)$ is cyclic, then G is Abelian.

Proof. Firstly, $Z(G)$ is normal (Exercise 5.25). If G is Abelian then $Z(G) = G$, it thus suffices to show that $G/Z(G)$ is the trivial group. Suppose $gZ(G)$ generates $G/Z(G)$. If $a \in G$, then $aZ(G) = g^iZ(G)$ for some i, so that $a = g^iz$ for some $z \in Z(G)$. We observe that this implies a commutes with g, since g^i and z both commute with g. But this shows that every element of G commutes with g, so that $g \in Z(G)$. □

The quotient group $G/Z(G)$ is also useful for other purposes.

Proposition 5.13. Let G be a group. Then $G/Z(G)$ is isomorphic to $\mathrm{Inn}(G)$.

5.2 Homomorphisms and the first isomorphism theorem

Recall that we defined group homomorphisms in Definition 1.63. We now undertake a deeper study of them.

First, let us start with a definition that is likely familiar to you, if you've had linear algebra.

Definition 5.14 (Kernel of a homomorphism)**.** Let $\phi : G \to H$ be a group homomorphism. The **kernel of** ϕ is the set of all g which are mapped to the identity by ϕ;

$$\ker \phi := \{\, g \in G : \phi(g) = e \,\}.$$

The image of a homomorphism will be simply denoted $\phi[G]$, since it is not sufficiently important in group theory to get a special designation. Let us now see a few more properties of homomorphisms. Recall that we have proven more properties previously on Theorem 1.68 and Proposition 2.20.

Proposition 5.15. Let $\phi : G \to H$ be a homomorphism. Then, the following properties are true:

1. $\ker \phi$ is a subgroup of G;
2. $\phi(g) = \phi(h)$ if and only if $g \ker \phi = h \ker \phi$.
3. If $h \in \phi[G]$ and $\phi(g) = h$, then $\phi^{-1}[\{\, h \,\}] = g \ker \phi$.
4. If N is normal in G, then $\phi[N]$ is normal in $\phi[G]$.
5. $\phi[Z(G)]$ is a subgroup of $Z(\phi[G])$.
6. If K is normal in H, then $\phi^{-1}[K]$ is normal in G.
7. If $\ker \phi$ is finite and has n things in it, then ϕ is an n to 1 mapping.

Proof. We leave the proof of (1) to the reader. For (2), notice that $\phi(g) = \phi(h)$ if and only if $\phi(gh^{-1}) = e$. This is true if and only if $gh^{-1} \in \ker \phi$, if and only if $g \ker \phi = h \ker \phi$. Everything else shall be left to the reader. □

The reader may have also observed that property (2) seems very indicative of a equivalence relation. See Exercise 5.28 for more details.

Property (6) of Proposition 5.15 can be used to deduce the following very important property of kernels.

Corollary 5.16 (Kernels are normal)**.** If ϕ is a homomorphism then $\ker \phi$ is normal.

Proof. Consider $\phi^{-1}[\{\, e \,\}]$. □

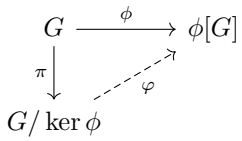
5.3 Isomorphism Theorems

We have previously mentioned that the study of normal subgroups is the same as the study of homomorphisms. Let us now make this notion precise with the First Isomorphism Theorem. This is sometimes called the Fundamental Theorem of Group Homomorphisms, which really goes to show just how important this theorem is.

Theorem 5.17 (First Isomorphism Theorem)**.** Suppose G is a group and $\phi : G \to H$ is a homomorphism. Then the group $G/\ker \phi$ is isomorphic to $\phi[G]$ by the isomorphism $\varphi(g \ker \phi) = \phi(g)$.

Proof. See Exercise 5.29. □

We may depict the relationship of this theorem with the following commutative diagram:



Here, π denotes the natural projection which sends the element g to the left coset $g \ker \phi$, i.e. $\pi(g) = g \ker \phi$. The commutative diagram can be read as saying that $\phi = \varphi \circ \pi$. We won't go into too much detail into how to read commutative diagrams here for now.

Using the first isomorphism theorem, we can turn back to our motivating example for the study of normal subgroups, and see what we mean by $\mathbb{Z}/3\mathbb{Z}$ is really just $\mathbb{Z}_3$.

Example 5.18. Let n be a positive integer. Define $\phi(m) = m \mod n$. Then ϕ is easily seen to be a (surjective) group homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_n$ and the kernel of ϕ is $n\mathbb{Z}$. So the first isomorphism theorem tells us that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. //

The first isomorphism theorem makes computations involving kernels and homomorphisms much easier.

Example 5.19. Let G be the general linear group of 2 by 2 matrices over $\mathbb{R}$, and let N be the special linear group of 2 by 2 matrices over $\mathbb{R}$. Let ϕ be the determinant function. Notice that ϕ is a surjective group homomorphism onto the group of nonzero real numbers under multiplication, and the kernel of ϕ is precisely N. Thus this shows that G/N is isomorphic to the nonzero reals under multiplication. //

Although we have labelled the following as theorems, they really are corollaries to Theorem 5.17.

Theorem 5.20 (Second Isomorphism Theorem)**.** Suppose K is a subgroup of G, and N is normal in G. Then $K/(K \cap N)$ is isomorphic to KN/N.

Proof. See Exercise 5.30. Note that by Example 5.9, we have the fact that KN is a subgroup of G. □

Theorem 5.21 (Third Isomorphism Theorem)**.** Suppose M, N are normal in G and that N is a subgroup of M. Then $(G/N)/(M/N)$ is isomorphic to G/M.

Proof. See Exercise 5.31. □

The reader may be wondering whether all normal subgroups are kernels of some sort of homomorphism. The answer is yes. If N is a normal subgroup of G, let us define[2] $\pi : G \to G/N$ by $\pi(g) = gN$. We leave it to the reader (Exercise 5.32) to verify this is indeed a homomorphism, and it has kernel N.

We now make use of the concept of factor groups to prove the following useful theorem. This theorem is used to prove the Sylow Theorem's.

Theorem 5.22 (Cauchy's Theorem (for finite abelian groups))**.** Let G be a finite abelian group and let p be a prime that divides $|G|$. Then, G contains an element of order p.

Proof. We induct on the order of G. Let $|G| = n$. Clearly if $|G| = 1$ it is trivial. Suppose the statement is true when $|G| < n$. Let $a \in G$, $a \neq e$. If $|a| = r$ and p divides r, then the element $a^{r/p}$ has order p. If not, then p, r are coprime. Let us consider $G/\langle a \rangle$. This group has order $|G|/r$, and necessarily p divides the order of this group. Thus there is some $b\langle a \rangle \in G/\langle a \rangle$ which has order p. Let $|b| = s$; we claim p divides s. Indeed, $(a\langle a \rangle)^s = a^s \langle a \rangle = \langle a \rangle$, and $a^p \langle a \rangle = \langle a \rangle$. So p divides s. Now $b^{s/p}$ has order p. □

[2]The reason for the use of the symbol π is because we are essentially projecting the elements down to G/N. Sometimes this is called the natural homomorphism from G to G/N. I'm not sure if this is categorically natural, so let me know.

5.4 Exercises and Problems

Exercise 5.23. Let G be a group and let $x, y \in G$. Let H be a subgroup of G. Show that if $xH = Hy$, then $xHy^{-1} \subseteq H$.

Exercise 5.24 (Internal direct products)**.** Let G be a group. We say that G is the **internal direct product of H and K** and write $G = H \times K$ if

1. H, K are normal subgroups of G,
2. $HK = G$,
3. $H \cap K = \{ e \}$.

Note that this seemes similar to a vector space being a direct sum of subspaces.

Show that G is isomorphic to $H \times K$. This justifies the abuse of the group product notation. Extend this to the case where G is an internal direct product of a finite number of groups.

Exercise 5.25 (Center is always normal)**.** Let G be a group. Show that $Z(G)$ is normal subgroup of G. In addition, prove that if H is a subgroup of $Z(G)$, then H is normal in G.

Exercise 5.26 (Stronger version of Theorem 5.12)**.** Let G be a group. Let H be a subgroup of $Z(G)$. Show that if G/H is cyclic, then G is Abelian.

Exercise 5.27 (Converse of Theorem 5.10)**.** Suppose G is a group and N is a subgroup of G such that for all $x, y \in G$, we have $xNyN = xyN$. Show that N is normal.

Exercise 5.28. Let $\phi : G \to H$ be a homomorphism. Define the equivalence relation $\sim$ on G by $x \sim y$ if and only if $\phi(x) = \phi(y)$. Prove that $\sim$ is an equivalence relation, and the equivalence class $[g]_\sim$ is precisely $g \ker \phi$.

Exercise 5.29. Prove the First Isomorphism Theorem (Theorem 5.17).

Exercise 5.30. Prove the Second Isomorphism Theorem (Theorem 5.20).

Exercise 5.31. Prove the Third Isomorphism Theorem (Theorem 5.21).

Exercise 5.32 (Every normal subgroup is a kernel)**.** If N is a normal subgroup of G, let us define $\pi : G \to G/N$ by $\pi(g) = gN$. Prove that π is a homomorphism and it has kernel N.

Exercise 5.33. Prove that $\mathbb{Q}$ under addition has no proper subgroup with finite index.

Exercise 5.34 (Index 2 subgroups are normal)**.** Let G be a group and H be a subgroup such that $[G : H] = 2$. Prove that H is normal in G. *Hint: Think about the pigeonhole principle*

Exercise 5.35. Show that the intersection of any arbitrary collection of normal subgroups is normal.

Note: The tools to do the following exercise have not been developed in this book yet.

Exercise 5.36. Show that if $\{ N_\alpha : \alpha \in \Lambda \}$ is a collection of normal subgroups of G, then $\langle N_\alpha : \alpha \in \Lambda \rangle$, the smallest normal subgroup that contains all N_α, is normal in G.

For an added challenge, do this with the intersection definition.

Chapter 6

Group actions

6.1 Group actions

We teased the concept of group actions in Chapter 3; now we come back to it. The abstract study of groups is a rather modern treatment. Historically, group theory only dealt with the theory of groups of permutations. However, it turns out that studying how a group acts on a set can be very insightful into the properties of groups. We already know of one example: Cayley's Theorem. We also can understand Lagrange's Theorem in the language of group actions. Later on, we will prove a partial converse to Lagrange's Theorem - the Sylow Theorems. All this is to say that the study of group actions is worthwhile.

For convenience, we shall restate the definition of a group action. At this point, the reader is likely to be sufficiently used to abstract concepts that there can be no confusion with the group action and the group multiplication.

Definition 6.1 (Group action)**.** A **group action** of G on a set S is a function $\cdot : G \times S \to S$ satisfying the following properties:

(1) **(Associativity)** For all $g, h \in G$ and $x \in S$, we have $gh \cdot x = g \cdot (h \cdot x)$.

(2) **(Identity)** For all $x \in S$, we have $e \cdot x = x$.

Sometimes, when it is clear, we will omit the use of $\cdot$, and just write gx to indicate $g \cdot x$. (Warning: Some authors such as [Jac09] are quite abusive with this notation.)

We wish to investigate further the properties of the function $\cdot$ which is defined by the action of G on S. Let G be a group and suppose G acts on S. The function $\cdot$ takes in 2 arguments; a group element and an element of S. To best investigate this function, we should probably do it by fixing one of the arguments. For now, fix some $g \in G$, and let $m_g : S \to S$ be the function given by $m_g(x) = g \cdot x$. Is m_g injective or surjective? Yes.
Exercise 6.2. Show that m_g is bijective.

The above discussion shows us that for each g, the function m_g is a bijection, hence a permutation. What we can do now is define a function $T : G \to \mathrm{Sym}(S)$ (here $\mathrm{Sym}(S)$ is the set of permutations on S), which takes $T(g) = m_g$. Both the domain and codomain of T are groups. Is T a group homomorphism? For that to hold we need $m_g \circ m_h = m_{gh}$. But this is immediate from the definition of a group action. Thus, we have a positive answer. We leave it for the reader to verify this claim.
Exercise 6.3. Check that T as defined above is indeed a group homomorphism.

After all that work, we can conclude that any group action induces a group homomorphism of G into $\mathrm{Sym}(S)$. In this case, we call the homomorphism T, the *homomorphism induced by the action of G on S*. If the context is clear, we shall simply say *action induced homomorphism* The image of the group G under T, $T[G] \subseteq \mathrm{Sym}(S)$, we shall call the *associated transformation group*.

All this discussion begs the following question: If we have a group G and a set S, and we are given a homomorphism $\varphi : G \to \mathrm{Sym}\, S$, is there some way we can define an action of G on S using φ? The answer is positive as well (see Exercise 6.22. If you think you have an idea of how to define it, don't go to the exercise yet. Try to come up with it

yourself before looking at the exercise.)

Definition 6.4 (Effective action)**.** Let G act on S, and let T be the action induced homomorphism. Then we say that G **acts effectively on** S if T is injective.

Previously, we have defined the kernel of a group action to be the set

$$\{ g \in G : g \cdot x = x \text{ for every } x \in S \}.$$

We will now show that the name "kernel" is not an abuse of notation - this set is exactly equal to the kernel of the homomorphism induced by the action of G.

Exercise 6.5. Let G act on S. Let $T : G \to \mathrm{Sym}(S)$ be the homomorphism induced by the action of G on S. Show that $\ker T$ is exactly equal to the kernel of the action of G on S.

We now look at examples of group actions.

Example 6.6 (Group acting on itself by left translation)**.** This example really illustrates the power of group actions - it yields the proof of Cayley's Theorem (Exercise 3.36). Let G be a group and let $S = G$. We shall define an action $\cdot : G \times S \to S$ by $g \cdot x = gx$. This action is called **the action of G on itself by left translation (or left multiplication)**. Note that on the right side, gx is the group multiplication. On the left side, $g \cdot x$ is the group action. The proof of Cayley's Theorem yields the fact that the induced homomorphism $T : G \to \mathrm{Sym}(G)$ is injective. The group of symmetries which G is isomorphic to is actually its image $T[G]$. //

Example 6.7 (Group acting on itself by right translations)**.** We can let G act on itself with right multiplications in a similar way. However, we have to be careful. Notice if we define $g \cdot x = xg$, then we have $(gh) \cdot x = xgh$, and $g \cdot (h \cdot x) = xhg$. If G is not abelian then these may not be equal. However, we can repair the issue by instead defining $g \cdot x = xg^{-1}$. Then, we have $gh \cdot x = x(gh)^{-1} = xh^{-1}g^{-1} = g \cdot (h \cdot x)$. This action is called the **action of G on itself by right translations**. We leave it for the reader to verify that this action is effective. //

Example 6.8 (Group acting on itself by conjugations)**.** Another important action of G on itself is what we shall call G **acting on itself by conjugations**. This will be essential in our proof of the Sylow Theorems. Let $S = G$. Define an action $\cdot : G \times S \to S$ by $g \cdot x = gxg^{-1}$. We can also denote this with ${}^g x$. We leave it to the reader to check that conjugation is an action. We also leave it to the reader to verify that the kernel of this action is $Z(G)$ (see Exercise 6.20).

//

Example 6.9 (Restricting the action)**.** Let G be a group acting on a set S. If H is a subgroup of G, then H also acts on S, by restricting the action of G to H, i.e. $\cdot|_H : H \times S \to S$. //

Example 6.10 (Actions on coset space)**.** Let G be a group, and let H be a subgroup of G. Recall that G/H denotes the set of all left cosets of H, i.e. $G/H = \{ xH : x \in G \}$. There is a canonical action of G on G/H given by setting $g \cdot xH = (gx)H$. We shall call this the **action of G on G/H by left translations**. We leave it to the reader to show that the kernel of this action is the set of all $g \in G$ such that $g \in \bigcap_{x \in G} xHx^{-1}$. //

Recall that we defined the

Definition 6.11 (Orbit of an element)**.** Let G act on a set S, and let $x \in S$. The **orbit of x (under the action of G)** is the set

$$\mathrm{Orb}_G(x) = \{ g \cdot x : g \in G \}.$$

We will write $\mathrm{Orb}(x)$ whenever the group G is clear. This is sometimes denoted $\mathcal{O}_x$[1], or $G \cdot x$.

The orbits of Example 6.10 are rather interesting. Pick some $xH \in G/H$, and let us consider what $\mathrm{Orb}(xH)$ will be. If yH is any other coset, then we have $yx^{-1} \cdot xH = yH$. What this means is $\mathrm{Orb}(xH)$ is all of the coset space G/H. We call group actions where this happens transitive actions.

Definition 6.12 (Transitive group action)**.** Let G act on S. Then we say G **acts transitively on** S if there exists $x \in S$, such that $\mathrm{Orb}(x) = S$.

Notice that if there is a single $x \in S$ with orbit being all of S, then for any $x \in S$, $G \cdot x = S$.

Exercise 6.13. Show that if there is some $x \in S$ such that $G \cdot x = S$, then for every $y \in S$, $G \cdot y = S$.

[1] We will not use $\mathcal{O}_x$ since this notation is bad. However, [DF04] does.

We make a trivial but important observation that if Σ is some orbit, then G acts transitively on Σ. Let's take a look at some transitive actions.

Example 6.14. Let S_n act on the set $\{1, \ldots, n\}$ in the obvious way (i.e. $\sigma \cdot x = \sigma(x)$). Then S_n acts transitively on this set, as you should verify. //

Example 6.15. Let G act on itself by left multiplications, as in Example 6.6. Then this action is transitive, since if $x \in G$, we have $yx^{-1} \cdot x = y$, so that $G \cdot x = G$. //

Example 6.16. Similarly, the action of G on itself by right translations is transitive. //

Of course, not all group actions are transitive.

Example 6.17 (A non-transitive group action)**.** Let $O(n)$ be the orthogonal group of $\mathbb{R}^n$. Recall that elements of $O(n)$ are isometries (distance-preserving linear maps). Consider some vector $v \in \mathbb{R}^n$ with norm 1. Then for any $T \in O(n)$, it follows that $\|T(v)\| = 1$. Thus any vector with norm that is not 1 is not in the orbit of this v. //

6.1.1 Problems and Exercises

Exercise 6.18 (Left translations)**.** Check that Example 6.6 is indeed a group action. Also verify that

Exercise 6.19. Verify that the actions defined in Examples 6.6 to 6.10. are actually group actions.

Exercise 6.20 (Kernel of conjugation)**.** Prove that the kernel of the action of G on itself by conjugation as defined in Example 6.8 is the center of G, $Z(G)$. Conclude that this action is effective if and only if $Z(G)$ is trivial.

Exercise 6.21 (Action of a group on coset space)**.** Let G be a group and let H be a subgroup of G. Let G act on G/H canonically (as in Example 6.10).

(i) Check that this action is transitive.

(ii) Show that the kernel of this action is precisely $\bigcap_{x \in G} xHx^{-1}$. To get started, note that $gxH = xH$ if and only if $x^{-1}gx \in H$ for all x.

(iii) Show that G acts on G/H effectively if and only if H contains no nontrivial subgroups that are normal in G. (*Hint: The kernel of the action is the largest normal subgroup of G contained in H*)

Exercise 6.22 (Group actions induced by homomorphisms)**.** Let G be a group, and let S be a set. Let $\varphi : G \to \mathrm{Sym}(S)$ be a homomorphism of G into the group of symmetries on the set S.

Define the function $\cdot : G \times S \to S$ by $g \cdot x = \varphi(g)(x)$. Here, $\varphi(g)$ is a permutation on S. Verify that $\cdot$ is an action of G on S.

6.2 Transitive actions and counting

Transitive actions are special, in the sense that there is really only "one". In particular, if G acts on S transitively, then we can study this action by studying how G acts on a coset space G/H. To make this notion precise, we shall define essentially what is an "isomorphism" of group actions.

Definition 6.23 (Equivalent actions)**.** Let G act on S with $\cdot_1$ and S' with $\cdot_2$. We say that the actions of G on S and S' are **equivalent** if there is a bijection $\beta : S \to S'$ such that

$$g \cdot_2 \beta(x) = \beta(g \cdot_1 x).$$

We can express this diagramatically with

$$\begin{array}{ccc} S & \xrightarrow{g\cdot -} & S \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\beta} \\ S' & \xrightarrow[g\times -]{} & S' \end{array}$$

Here, g is fixed, and $\cdot, \times$ are actions of G on S and S' respectively. The map $g \cdot -$ is the map $s \mapsto g \cdot s$ (likewise with $g \times -$). We can understand this intuitively as saying that it does not matter whether we first do the action in S and move to S', or whether we first move over to S' and do the action in S'.

Recall we have defined the

Definition 6.24 (Stabilizer of an element)**.** Let G act on S and let $x \in S$. Then the **stabilizer of** x is the set

$$\mathrm{Stab}(x) = \{\, g \in G : g \cdot x = x \,\}.$$

The last use of stabilizers was in Theorem 4.14. The ideas from this theorem will come to light in the proceeding discussion. It turns out that the stabilizer is exactly what we need to show that transitive actions are equivalent to the action of a group on some coset space.

Suppose G acts transitively on S. Pick some element $x \in S$, and let $H = \mathrm{Stab}(x)$. What do the left cosets of H represent? Well, if $h \in H$, then $h \cdot x = x$. So given some $g \in G$, then $(gh) \cdot x = g \cdot x$. Now, suppose that $g' \in G$ has the property that $g' \cdot x = g \cdot x$. This tells us that $g^{-1}g' \cdot x = x$, so that $g^{-1}g' \in H$. Equivalently, this means $g' \in gH$. We thus see that gH is the set of all the $g' \in G$ that takes x to $g \cdot x$, (i.e. $g' \cdot x = g \cdot x$ for all $g' \in H$). Now, for each $gH \in G/H$, let's associate to it the element of S, $g \cdot x$. This actually defines a map $gH \mapsto g \cdot x$ (which is well-defined, of course), with codomain in S. Does this map hit everything in S? Well, since G acts transitively on S, given any element $y \in S$, there is some g' such that $g' \cdot x = y$. This g' lives in some left coset of H. This shows that the map is actually surjective. At this point we may have an inkling that a coset gH represents exactly one element of S, namely the element $g \cdot x$. Is that true? Suppose that aH and bH both represent the element $y \in S$. This means that $a \cdot y = b \cdot y$. Now, using the same line of reasoning as above, when investigating what left cosets of H represent, we see that $b^{-1}a \cdot y = y$, so that $a \in bH$. This means $aH = bH$.

The discussion above has proven the following

Theorem 6.25 (Transitive actions are equivalent to actions on coset space)**.** Let G act on S transitively. Let $x \in S$ be some element, and let $H = \mathrm{Stab}(x)$. Then, the action of G on S is equivalent to the action of G on G/H.

Proof. Fix $x \in S$, and let $\alpha : G \to S$ be defined by $\alpha(g) = g \cdot x$. Note that α is surjective, since the action is transitive. Thus let $\overline{G} = \{\, \alpha^{-1}(x) : x \in S \,\}$. An element $\overline{g} \in \overline{G}$ is the set $\overline{g} = \{\, a \in G : \alpha(a) = \alpha(g) \,\} = \{\, a \in G : a \cdot x = g \cdot x \,\}$. We now let $\overline{\alpha} : \overline{G} \to S$ be the map defined by $\overline{\alpha}(\overline{g}) = \alpha(g)$. This map is obviously well-defined. We claim that $\overline{\alpha}$ is bijective. Surjectivity is due to surjectivity of α. We leave it for the reader to check injectivity.

We next check that $\overline{g}$ is the left coset $g\,\mathrm{Stab}(x)$. This will show that $\overline{G} = G/\mathrm{Stab}(x)$ and so the map $\overline{\alpha}$ takes $g\,\mathrm{Stab}(x)$ to $g \cdot x$. An element a is in $\overline{g}$ if and only if $a \cdot x = g \cdot x$ if and only if $g^{-1}a \cdot x = x$, which is equivalent to $g^{-1}a \in \mathrm{Stab}(x)$. This is equivalent to $a \in g\,\mathrm{Stab}(x)$.

All that remains is to check that $\overline{\alpha}$ is indeed an equivalence of actions. We leave this for the reader. □

Exercise 6.26. Complete the proof of Theorem 6.25.

If G is a finite group, then we obtain an important

Corollary 6.27. Let G be a finite group acting transitively on a set S. Then, for any $x \in S$,

$$|S| = [G : \mathrm{Stab}(x)].$$

Proof. This follows immediately since $\overline{\alpha}$ is a bijection of G/H to S. □

Consequently, if a finite group acts transitively on a set, then the set is finite, and the cardinality of that set divides $|G|$. Of course, not all actions are transitive. Let G be a finite group acting on a finite set S. We have previously shown in Exercise 3.37 that orbits partition S. Since S is finite we can write

$$S = \mathrm{Orb}(x_1) \cup \mathrm{Orb}(x_2) \cup \cdots \cup \mathrm{Orb}(x_k), \tag{6.1}$$

where x_k are representatives of orbits. We have previously remarked that G acts transitively on $\mathrm{Orb}(x_i)$, so in particular for any $y \in \mathrm{Orb}(x_i)$, then $|\mathrm{Orb}(x_i)| = [G : \mathrm{Stab}(y)]$. Since $x_i \in \mathrm{Orb}(x_i)$ we can simply say $|\mathrm{Orb}(x_i)| = [G : \mathrm{Stab}(x_i)]$. As such, we can say that

$$|S| = \sum_{x_i \in \{\, x_1, \ldots, x_k \,\}} [G : \mathrm{Stab}(x_i)] \tag{6.2}$$

where the set $\{ x_1, \ldots, x_k \}$ is a set of representatives of the orbits. We also remark that each term we sum over, the $[G : \mathrm{Stab}(x_i)]$'s are divisors of $|G|$.

At this point, the reader is likely curious how stabilizers of different elements within an orbit are related. Let O be some orbit and say we had $x, y \in O$. How is $\mathrm{Stab}(x)$ related to $\mathrm{Stab}(y)$? Since x and y lie in the same orbit, we have $y = g \cdot x$ for some g. Now, $a \cdot y = y$ if and only if $a \cdot (g \cdot x) = y$. We can apply g^{-1} on both sides to obtain $(g^{-1}ag) \cdot x = g^{-1} \cdot y = x$. So, $a \in \mathrm{Stab}(y)$ if and only if $g^{-1}ag \in \mathrm{Stab}(x)$. This is equivalent to saying that $a \in g\,\mathrm{Stab}(x)g^{-1}$. We shall write this as

$$\mathrm{Stab}(g \cdot x) = g\,\mathrm{Stab}(x)g^{-1}. \tag{6.3}$$

As such, if x and y lie in the same orbit, then their stabilizers are conjugate. Consequently, if the action is transitive, all stabilizers are conjugate to each other.

Exercise 6.28. Prove the claim in Equation (6.3).

6.2.1 Problems and exercises

Exercise 6.29 (Orbit-stabilizer is a corollary)**.** Show how the Orbit-Stabilizer Theorem (Theorem 4.14) can be obtained as a corollary to Theorem 6.25.

Exercise 6.30. Let G be a finite group and let H be a subgroup of G such that $[G : H] = n$. Show that there is a normal subgroup N of G such that $N \subseteq H$ and $[G : N]$ is a divisor of $n!$. *(Hint: Let G act on G/H by left translations. See Example 6.10)*

Exercise 6.31 (Generalization of index 2 subgroups are normal)**.** Let G be a finite group. Let p be the *smallest* prime dividing $|G|$. Show that if H is a subgroup of G such that $[G : H] = p$, then H is normal. *(Hint: Again let G act on G/H by left translations.)*

Exercise 6.32 (Classification of groups of order p^2)**.** Let p be a prime. Prove that if G has order p^2, G is abelian. Show that there are only 2 groups of order p^2 up to isomorphism.

Exercise 6.33 (Semidirect products)**.** Let H, K be groups. We say that H *acts on K by automorphisms* if H acts on K with $\cdot$, and for every $h \in H$, the map $k \mapsto h \cdot k$ is an automorphism of K.

Suppose H acts on K by automorphisms. Let $G = K \times H$ (cartesian product). Define a binary operation on G by

$$(k_1, h_1)(k_2, h_2) = (k_1(h_1 \cdot k_2), h_1h_2),$$

with $e_G = (e_K, e_H)$.

(i) Show that G is a group under the operation defined above.

(ii) Show that the map $h \mapsto (e_K, h)$ from H into $K \times H$ is an injective homomorphism.

(iii) Show that the map $k \mapsto (k, e_H)$ from K to $K \times H$ is an injective homomorphism, and that the image of K under this map is a normal subgroup.

(iv) Suppose H, K are finite. Show that $|G| = |K||H|$.

The construction above is called the **semi-direct product** of K and H. We will see this construction soon.

Exercise 6.34 (Primitive actions)**.** Let G be a group acting on S. Let S be a set with at least 2 elements, and let $\pi(S)$ be a partition of S. We shall say that $\pi(S)$ is **stabilized by the action of G on S** if for every $A \in \pi(S)$ and $g \in G$, then $gA = \{ g \cdot a : a \in A \} \in \pi(S)$.

There are always at least 2 partitions of S that have this property: The trivial partition of S given by $\pi_0(S) = \{ S \}$ and the partition of S into singletons, given by $\pi_1(S) = \{ s : s \in S \}$. Let us call an action of G on S **primitive** if $\pi_0(S)$ and $\pi_1(S)$ are the only partitions with this property.

(i) Show that G acts imprimitively on S if and only if there is an $A \subset S$ with at least 2 elements such that for any $g \in G$, either $gA = A$ or $gA \cap A = \varnothing$. Such a proper subset of S is called a **block**.

(ii) Show that G acts primitively on S if and only if the only blocks of S are singletons or S itself.

6.3 The class equation and Sylow theorems

Our study into group actions has proven rather fruitful into extracting insights about the structure of a group, especially when the group is finite. We first observed that if G acts on itself by left translations, we have Cayley's

Theorem, telling us that every group is really just a group of permutations. Now, we shall let G act on itself by conjugations. We have lightly explored this in Example 6.8. This action will be immensely useful for us when we prove the Sylow Theorems.

Recall that Lagrange's theorem states if we have a finite group, the order of any of its subgroups must divide the order of the group. The converse is not true: given some divisor of the order of a finite group, there may not necessarily be a subgroup of that order. Not to be discourage, we shall relax the conditions on the converse slightly, and ask a weaker question: Given some prime p that divides the order of a finite group G, is there necessarily a subgroup of that order? We know this question is answered positively if G is abelian by Cauchy's Theorem for finite abelian groups (Theorem 5.22). But it turns out it is true for all groups in general. In fact, something much more can be said. Namely, if p^k is a divisor of the order of a finite group G, then there is a subgroup of order p^k. This is the content of Sylow's first theorem.

Given a group action of G on a set S, we have a partitioning of S into orbits. In the finite case we can write it as in Equation (6.1). We shall study the orbits of G when it acts on itself by conjugation. This orbit is so important, it gets its own name,

Definition 6.35 (Conjugacy class)**.** Let G act on itself by conjugation and let $x \in G$. The **conjugacy class of** x is the orbit of x under the action of conjugation, i.e.

$$\{ gxg^{-1} : g \in G \}.$$

The collection of all these orbits is called the set of conjugacy classes of G.

From the previous section, we have an enumeration of the set G acts on (Equation (6.2)). Let G be a finite group, and let G act on itself by conjugations. Given some $x \in G$, what is $\mathrm{Stab}(x)$? An element $g \in G$ stabilizes x if and only if $gxg^{-1} = x$. From Exercise 1.53, this is equivalent to $g \in C(x)$. Thus $\mathrm{Stab}(x)$ is exactly equal to $C(x)$. We can thus rewrite Equation (6.2) as

$$|G| = \sum_{x_i \in \{ x_1, \ldots, x_k \}} [G : C(x_i)], \tag{6.4}$$

where $\{ x_1, \ldots, x_k \}$ is a set of representatives of all the conjugacy classes of G. However, this formula has some redundancy. It is quite possible that $C(x_i) = G$, in which case we have $[G : C(x_i)] = 1$. However, notice that $C(x_i) = G$ is equivalent to saying that x_i commutes with everything in G. This means that $x_i \in Z(G)$ if and only if $C(x_i) = G$. Actually, this means that every element of $Z(G)$ represents a conjugacy class. So instead of adding a bunch of ones (caused by $[G : C(x_i)] = 1$) for each $x_i \in Z(G)$, we might as well remove those x_i's from our set of representatives and just add $|Z(G)|$ all at once. This leaves us with the **class equation of the finite group** G.

$$|G| = |C| + \sum_{y_i \in \{ y_1, \ldots, y_m \}} [G : C(y_i)]. \tag{6.5}$$

Note that the set $\{ y_1, \ldots, y_m \}$ is a set of representatives of conjugacy classes of G such that the conjugacy class determined by y_i has more than one element, i.e. the orbit of y_i under the action of conjugation has more than one element. In particular, that means $[G : C(y_i)] > 1$.

The technique of using Equation (6.2) yields many rather useful results. We shall demonstrate the utility of the technique by using the class equation (Equation (6.5)) to prove the following rather useful

Proposition 6.36. If G is a finite group and G has prime power order, then $Z(G)$ is nontrivial

Proof. Suppose that $|G| = p^k$ for some $k > 0$. We consider the class equation Equation (6.5). On the left side, we have $|G|$ being divisible by p. On the right side, all the terms must be a power of p, since C is a subgroup of G, and each $C(y_j)$ is also a subgroup of G. Now, since $[G : C(y_j)] > 1$, we know that each of those terms is divisible by p. We can rearrange it and we have

$$|G| - \sum [G : C(y_j)] = |C|.$$

Thus p divides $|C|$, so the conclusion follows. □

We now use the class equation to prove

Theorem 6.37 (Sylow's First Theorem)**.** Let G be a finite group. Let p be a prime, let $k \geq 0$, and suppose that p^k divides $|G|$. Then, G has a subgroup of order p^k.

Proof. Let G have order n. We shall induct on the order of G. Clearly if G has order 1 it is trivial. Suppose the result is true for all groups of order $< n$. Consider the class equation Equation (6.5): $|G| = |C| + \sum[G : C(y_j)]$. If p does not divide $|C|$, then there is some j such that p does not divide $[G : C(y_j)]$. This implies that p^k divides $|C(y_j)|$, since $|G| = |C(y_j)| \cdot [G : C(y_j)]$. Since $C(y_j)$ is not all of G, it has order $< n$ and so it contains a subgroup of order p^k. If p does divide $|C|$, then by Theorem 5.22, there is some element $z \in C$ such that $|z| = p$. Now, $\langle z \rangle$ is normal in G (since any subgroup of C is normal), and $G/\langle z \rangle$ has order n/p, which is divisible by p^{k-1}[2]. By induction, $G/\langle z \rangle$ has a subgroup of order p^{k-1}, which is of the form $H/\langle z \rangle$ for some $H \leq G$, such that $H \supseteq \langle c \rangle$. Then we have

$$|H| = [H : \langle z \rangle] \cdot |\langle z \rangle| = p^{k-1} \cdot p = p^k.$$

□

A useful corollary is

Corollary 6.38 (Cauchy's Theorem for finite groups)**.** Let G be a finite group and p a prime dividing the order of G. Then, G contains an element of order p.

Proof. Immediate. □

With this theorem, we are now allowed to define what is known as a

Definition 6.39 (Sylow p-subgroup)**.** Let G be a finite group and suppose p^m is the largest power of p that divides $|G|$, i.e. $p^m \mid |G|$ and $p^{m+1} \nmid |G|$. If H is a subgroup of G of order p^m, then H is called a **Sylow p-subgroup** of G.

These are the largest subgroups of prime power order contained in G. We know these must exist because of Theorem 6.37. Sylow's Second Theorem gives us some insight into the properties of these subgroups.

Theorem 6.40 (Sylow's Second Theorem)**.** Let G be a finite group.

(1) Sylow p-subgroups of G are conjugates; that is, given Sylow p-subgroups P_1, P_2, there is some $a \in G$ such that $P_2 = aP_1a^{-1}$.

(2) If P is *any* Sylow p-subgroup, then the number of Sylow p-subgroups divides $[G : P]$. Additionally, this number is congruent to 1 modulo p.

(3) If H is a subgroup of prime power order, then it is contained in a Sylow p-subgroup.

Before we embark on the proof, let's discuss the strategy. The first part of Theorem 6.40 seems to suggest that we should consider the action of G on Sylow p-subgroups of G by conjugation. But is this even a valid action?

Let's consider the general situation. Let Γ be the set of all subgroups of G. Can we let G act on Γ by conjugation? Well, if $g \in G$, and H is a subgroup of G, then gHg^{-1} is still a subgroup of G. From here, it is not too hard to see that conjugation defines an action of G on Γ. Moreover, $\left|gHg^{-1}\right| = |H|$, since conjugation by a fixed element is an automorphism. This shows that the conjugate of a Sylow p-subgroup remains a Sylow p-subgroup (Exercise 6.42). Hence the action of G on Γ by conjugation induces an action of G on Π.

Anyway, before we proceed with the proof, we will need the following

Lemma 6.41. *Let P be a Sylow p-subgroup of G, and $H \leq G$ have order p^j such that $H \subseteq N(P)$. Then $H \subseteq P$.*

[2]There is a small technicality here since we only assumed $k \geq 0$, and so p^{0-1} is nonsense. However the case when $k = 0$ is a triviality, so it is ignored. We might as well say $k > 0$, but eh.

Proof. We have H being a subgroup of $N(P)$, and P is normal in $N(P)$. This implies HP is a subgroup with $HP/P \cong H/H \cap P$. Hence HP is isomorphic to a factor grop of H, so HP has prime power order p^k. Moreover, $|HP| = p^k|P|$. But P is a Sylow p-subgroup so we must have $k = 0$. This implies HP is P, and so $H \subseteq P$. □

If P is a Sylow p-subgroup of G, then P is the only Sylow p-subgroup of $N(P)$, by the lemma.

Proof of Theorem 6.40. Let Π be the set of Sylow p-subgroups of G. Consider the action of G on Π by conjugation. Let $\Sigma = G \cdot P$ be an orbit under this action, and consider the action of P on Σ. This partitions Σ into P-orbits. Call the set of these P-orbits $\mathcal{U}$. Notice that $\{P\} \in \mathcal{U}$. We next claim that this orbit is the only singleton P-orbit in Σ; if $\{P'\} \in \Sigma$, then conjugation by elements of P fixes P', hence $P \subseteq N(P')$. Thus $P = P'$ since P is the only Sylow p-subgroup of $N(P')$. Now let $\mathcal{O} \in \mathcal{U}$, and consider $|\mathcal{O}|$. It must be a power of p, since $|\mathcal{O}|$ divides $|P|$. This proves that $|\Sigma| \equiv 1 \pmod{p}$. We now show that $\Pi = \Sigma$, which will prove (2). If not, there is a $Q \in \Pi \notin \Sigma$. Use the argument above on this Q; this shows there are no Q-orbits in Σ of cardinality 1, giving $|\Sigma| \equiv 0 \pmod{p}$. This contradicts $|\Sigma| \equiv 1 \pmod{p}$. Hence $\Sigma = \Pi$ and so G acts transitively on Π. We have now proven (1). (2) is proven with the additional observation that $|\Pi| = [G : N(P)]$. To prove (3), let $H \leq G$ with order p^k. Restrict the action of G on Π to H acting on Π. The H-orbits have cardinality a power of p, and since $|\Pi| \equiv 1 \pmod{p}$, there is a singleton orbit $\{P\}$. Then $H \subseteq N(P)$ and by Lemma 6.41, $H \subseteq P$. □

6.3.1 Problems and exercises

Exercise 6.42 (Conjugate of Sylow p-subgroup is a Sylow p-subgroup)**.** Let G be a finite group, let $g \in G$ and let P be a Sylow p-subgroup. Show that gPg^{-1} is a Sylow p-subgroup.
Exercise 6.43. Show that there are no simple groups of order 148 or of order 56.
Exercise 6.44. Show that there is no simple group of order pq where p, q are primes (not necessarily distinct).
Exercise 6.45. Classify all groups of order 15.

Chapter 7

Classification of finite abelian groups

7.1 Classification of finite abelian groups

Of all the groups, the finite abelian groups are relatively nice behaved, because they're abelian. What is even nicer behaved are the finite cyclic groups. Since they're so nicely behaved, it would be nice if we could understand everything about them. The theorem we present in this chapter will go a long way to dealing with this.

To motivate the theorem, recall that the fundamental theorem of arithmetic tells us that every number can be factorized uniquely as a product of primes, i.e. $n = p_1^{k_1} \cdots p_m^{k_m}$, where the p_i's are distinct primes. It turns out that we can do something similar for groups. We first state the theorem; the proof is difficult. Before embarking on this proof, please check out Exercise 5.24.

Theorem 7.1 (Classification of finite abelian groups)**.** Every finite abelian group is a unique product of cyclic groups of prime power order.

Now let's see what this means. Let G be a finite abelian group of order n. Then, Theorem 7.1 says that

$$G \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}.$$

However, note that *the p_i's may not be distinct primes.* However, this "factorization" is unique, meaning that if

$$G \cong \mathbb{Z}_{q_1^{l_1}} \times \cdots \times \mathbb{Z}_{q_n^{l_n}},$$

where q_i's are primes, then $n = m$, and $\{ p_1, \ldots, p_n \} = \{ q_1, \ldots, q_m \}$, and if $p_j = q_i$ then their powers are the same too.

This theorem is extremely powerful. It is extremely easy to determine *all* Abelian groups of a certain order. In contrast, classifying non abelian groups is extremely difficult. We additionally obtain a partial converse to Lagrange's theorem as a corollary.

Corollary 7.2 (Subgroups of finite abelian groups)**.** Let G be a finite abelian group and m divide the order of G. Then G has a subgroup of order m.

Proof. See Exercise 7.8. □

We will now prove the theorem. This proof comes from [Gal20, Ch 11]. We first "factorize" the group G using primes. We will encounter the following lemma but stated more generally; it is essentially Sylow's First Theorem.

Lemma 7.3 (Sylow's First Theorem for Abelian groups)**.** *Let G be a finite abelian group of order $p^n m$ where p does not divide m. Then, $G = H \times K$[1], where $H = \{ x \in G : x^{p^n} = e \}$ and $K = \{ x \in G : x^m = e \}$. Additionally, $|H| = p^n$.*

[1] This is an internal direct product. See Exercise 5.24 for the definition of an internal direct product.

Proof. Obviously H and K are subgroups. Let us show that $H \cap K = \{ e \}$ and $HK = G$. The fact that $H \cap K = \{ e \}$ is trivial. By Bezout's lemma, let s, t be integers such that $1 = sm + tp^n$. For any $x \in G$, we have

$$x = x^{sm+tp^n} = x^{sm} x^{tp^n}.$$

Then observe that $(x^{sm})^{p^n} = x^{smp^n} = e$ so $x^{sm} \in H$. A similar idea holds to show $x^{tp^n} \in K$. This shows $G = HK$. To prove the order statement, notice that

$$p^n m = |HK| = \frac{|H||K|}{|H \cap K|},$$

by Theorem 4.12, so that $|H||K| = p^n m$. Now, by Cauchy's Theorem (for finite abelian groups) (Theorem 5.22) and Corollary 2.9, if p divides $|K|$ then there would be an element of order p in K, call it k. But then $k^m = e$ and p does not divide m so that is not possible. Thus p does not divide $|K|$. So p divides $|H|$, thus $|H| = p^n$. □

We apply the lemma in the following form.

Corollary 7.4. Suppose G is an abelian group where $|G| = p_1^{k_1} \cdots p_n^{k_n}$. Define $G(p_i) = \left\{ x \in G : x^{p_i^{n_i}} = e \right\}$. Then, $G = G(p_1) \times \cdots \times G(p_n)$, and $|G(p_i)| = p_i^{k_i}$.

Proof. Induction. □

Next, we show that if an abelian group G has prime power order, we can "factorize" it with one of the factors being cyclic.

Lemma 7.5. *Suppose G is an Abelian group of order p^n. Let $a \in G$ be an element of maximum order. Then, $G = \langle a \rangle \times K$ for some subgroup K of G.*

Proof. We induct on n. If $n = 1$, it is trivial. Assume the lemma is true for all abelian groups of order p^k where $k < n$. Let a be an element of maximum order, say $|a| = p^m$. This means that $x^{p^m} = e$ for all $x \in G$. Assume $m < n$, else it is trivial. Let b be an element of minimum order such that $b \notin \langle a \rangle$. We claim that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Firstly, b^p has order $|b|/p$. Since b is of minimum order with $b \notin \langle a \rangle$, we know that b^p having a smaller order will satisfy $b^p \in \langle a \rangle$, so let $b^p = a^i$. Now, since $e = (b^p)^m = (b^p)^{p^{m-1}} = (a^i)^{p^{m-1}}$, we know that a^i does not generate $\langle a \rangle$, so that $\gcd(i, p^m) \neq 1$ (by Corollary 2.16). Thus p divides i, so let $i = pj$. Then $b^p = a^{pj}$. Let us consider the element $c = a^{-j} b$ (for reasons that will become clear shortly). Note that $c \notin \langle a \rangle$. Also, $c^p = a^{-jp} b^p = a^{-i} b^p = b^{-p} b^p = e$. This shows c has order p, and $c \notin \langle a \rangle$. Since b is an element of minimum order such that $b \notin \langle a \rangle$, we know b has order p. We have now shown the claim, since if $g \in \langle a \rangle \cap \langle b \rangle$, but $g \neq e$, then g generates $\langle b \rangle$, but then $b \in \langle a \rangle$, a contradiction.

We still need to show $\langle a \rangle \langle b \rangle = G$. To do so, we study a factor group and use induction. Let $\overline{G} = G/\langle b \rangle$. Let $\overline{x}$ denote the coset $x\langle b \rangle \in \overline{G}$. It's not hard to see that $|\overline{a}| = |a|$. If not, we have $\overline{a}^{p^{m-1}} = \overline{e}$. This shows that $a^{p^{m-1}} \in \langle b \rangle$, but then we would have $\langle a \rangle \cap \langle b \rangle$ having nontrivial intersection, since $a^{p^{m-1}} \neq e$. As such, $\overline{a}$ is an element of maximum order in $\overline{G}$. By induction, this tells us that $\overline{G} = \langle \overline{a} \rangle \times \overline{K}$ where $\overline{K} \leq \overline{G}$. Letting $\pi : G \to \overline{G}$ be the homomorphism defined by $\pi(g) = g\langle b \rangle$, we see that $K := \pi^{-1}\left[\overline{K}\right]$ is a subgroup of G. Now, we claim that $\langle a \rangle \cap K = \{e\}$. If $x \in \langle a \rangle \cap K$, then $\overline{x} \in \langle \overline{a} \rangle \cap \overline{K} = \{\overline{e}\} = \{e\langle b \rangle\}$. In particular we have $\overline{x} = \langle b \rangle$, but this means $x \in \langle b \rangle$, and since $x \in \langle a \rangle$, it must be that $x = e$. Now consider the order of K, and notice that $|G| = |\langle a \rangle| \cdot |K|$, so it must be that $G = \langle a \rangle K$. □

The above lemma implies the following:

Lemma 7.6. *Let G be an abelian group of prime power order. Then, it is an (internal) direct product of cyclic groups.*

Proof. Use Lemma 7.5 and induction on order of G. □

We now need to deal with uniqueness.

Lemma 7.7. *Let G be a finite abelian group with order p^n. If $G = H_1 \times \cdots \times H_m$, and $G = K_1 \times \cdots \times H_n$, where all H_i, K_j are nontrivial cyclic subgroups such that $|H_1| \geq \cdots \geq |H_i| \geq |H_{i+1}| \geq \cdots$, $|K_1| \geq \cdots \geq |K_j| \geq |K_{j+1}| \geq \cdots$, then $n = m$, and $|H_i| = |K_i|$ for all i.*

Proof. We start by induction on order of G. □

We end off this chapter with some closing remarks. Firstly, the group $\langle a \rangle$ in Lemma 7.5 would be a Sylow p-subgroup of G.

Secondly, this theorem can be derived as a corollary of a more general theorem, the classfiication of finitely generated abelian groups. This theorem can be derived as a corollary of a even more general theorem, the classification of finitely generated modules over a principal ideal domain. We will take up these theorems in the future, but for now these facts are just interesting to note.

7.1.1 Exercises and Problems

Exercise 7.8 (Subgroups of finite abelian groups)**.** Prove Corollary 7.2. A sketch is given in the next paragraph.

Let G be a finite abelian group of order n. We perform induction on n. When $n = 1$ or $m = 1$ it is trivial. Suppose the theorem is true for all abelian groups of order less than n. Let p be a prime dividing m, so that G has a subgroup of order p, say K (by Cauchy's Theorem). Then G/K has order n/p, and by the inductive hypothesis there is some subgroup of G/K of the form H/K that has order m/p.

Chapter 8

Rings

8.1 Introduction to Rings

At this point, we have now studied one kind of algebraic structure - groups. Groups are rather general things, but their flexibility means that we can say less about them. We now introduce a second kind of algebraic structure – rings.

Consider the integers, $\mathbb{Z}$. Within the integers, we have 2 operations: that of addition, and of multiplication. Adding 2 integers certainly yields another integer, and multiplying two integers also yields another integer. From elementary school, we also know that given integers a, b, c, we have

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$

the distributive law. We also have the property that 1 multiplied by any integer simply yields that integer itself.

Motivated by this example, we can now define a

Definition 8.1 (Ring). A **ring** is a set R equipped with 2 binary operations $+, \cdot$ such that R forms an abelian group under $+$, and

1. **(Associativity)** For all $a, b, c \in R$, we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
2. **(Distributivity)** For all $a, b, c \in R$, we have

   $$a \cdot (b + c) = a \cdot b + a \cdot c \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

   The former is called left distributivity, and the latter is right distributivity.
3. **(Unity)** There is an element $1 \in R$ such that for all $a \in R$, $1 \cdot a = a \cdot 1 = a$.

Whenever possible, we shall drop the use of $\cdot$ to make it less messy, and simply write $a(b + c)$ to mean $a \cdot (b + c)$. Note that what we have just defined here is a ring with unity. Some authors (e.g. [Gal20]) defines what is generally called a Rng, a ring without unity.

Given some $a \in R$, if there is an element b such that $ab = ba = 1$, then a is said to be a *unit* and we write $b = a^{-1}$. The following proposition justifies this notation.

Proposition 8.2 (Uniqueness of units and unity). Let R be a ring. Then, the unity of R is unique, and units are unique.

Proof. Repeat the proof for groups. □

Example 8.3 (The integers)**.** It is not too hard to verify that $\mathbb{Z}$ forms a ring. In fact, it is arguably the most important ring of all. //

The multiplication in a ring need not be commutative at all. If a ring has commutative multiplication, we call it a commutative ring.

Example 8.4 (Square matrices)**.** Let $\mathcal{M}_n(\mathbb{F})$ denote the set of $n \times n$ matrices with entries from $\mathbb{F}$. For a concrete example, let $\mathbb{F} = \mathbb{R}$, and let $R = \mathcal{M}_n(\mathbb{R})$. Then R forms a ring under usual matrix addition and multiplication. This ring is also noncommutative when $n > 1$, which we leave for the reader to verify. //

Example 8.5 (Any field)**.** Any field whatsoever is a ring. Some fields that may come to your mind are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. It is not too hard to check that these are all in fact, rings. We also have the relationship $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, and they are all subrings of each other in that way. //

We haven't defined what a subring is yet, but we shall now. Intuitively, a subring S of a ring R should form a ring as well, but with the operations of R. That means S has to contain the additive identity of R, the multiplicative identity of R, and remain closed under addition and multiplication.

Exercise 8.6. Formulate the definition of a subring.

We shall now see some basic properties of rings. These properties will allow us to use the familiar rules from multiplication and subtraction of integers that we are used to.

Proposition 8.7 (Basic properties of rings)**.** Let R be a ring, and let $a, b, c \in R$. Then, the following are true:

1. $a0 = 0a = 0$;
2. $a(-b) = (-a)b = -(ab)$;
3. $(-a)(-b) = ab$;
4. $a(b-c) = ab - ac$, $(b-c)a = ba - ca$;
5. $(-1)a = -a$;
6. $(-1)(-1) = 1$.

Proof. We will prove this without making use of the element $1 \in R$, so that this proposition remains true for rngs. For the first one, notice that

$$0 + a0 = a0 = a(0+0) = a0 + a0.$$

Subtract $a0$ on both sides to obtain the result. The other way is similar.

For 2, we have

$$a(-b) + ab = a(-b+b) = a0 = 0.$$

Adding $-(ab)$ to both sides yields $a(-b) = -(ab)$. Switch the roles of a and b to get the other one. □

Exercise 8.8. Complete the proof of Proposition 8.7 without making use of the unity 1, except in rules 5 and 6.

This proposition is useful and not difficult to prove.

Proposition 8.9 (Subring test)**.** Let $S \subseteq R$ be a subset of R. Then S is a subring of R if and only if S contains 1, and given $a, b \in S$, we have $a - b \in S$ and $ab \in S$.

Exercise 8.10. Supply the proof of Proposition 8.9.

Chapter 9

Fields

9.1 Extension fields

Given a polynomial, is it possible to find a field in which that polynomial has a root? For example, consider the polynomial $x^2 + 1$.

Definition 9.1. Let F be a field. If $E \supseteq F$ is a field and the operations of E restricted to F are the same as the operations of F, then E is an **extension field** of F.

If E is an extension field of F, we can say that E is an extension of F, or E extends F. Note the abuse of notation here again: F may not actually be a subset of E, but if it is isomorphic to a subfield of E it is good enough.

Example 9.2. $\mathbb{C}$ is clearly an extension field of $\mathbb{R}$. Additionally, $\mathbb{R}$ is an extension field of $\mathbb{Q}$. //

Example 9.3. Let F be a field and let $p \in F[x]$ be irreducible over F. Then, $F[x]/\langle p \rangle$ is an extension field of F. Notice that we can embed F as a subfield of $F/\langle p \rangle$ by the map

$$x \mapsto x + \langle p \rangle.$$

It is not too hard to see that this map is an isomorphism onto its image. We will use this example to motivate the following theorem. //

Theorem 9.4 (Existence of Extension Fields). Let F be a field and let $f \in F[x]$ be a nonconstant polynomial. Then there exists an extension field E of F such that f has a root in E.

Proof. Let $p(x)$ be an irreducible factor of f. This exists as $F[x]$ is a UFD. It suffices to produce an extension field of F where p has a root in. Let $E = F[x]/\langle p \rangle$. Then F embeds into E. Now, we see that $x + \langle p \rangle$ is a root of p in E. Write $p(x) = \sum_{i=0}^{n} a_i x^i$, then

$$p(x + \langle p \rangle) = \sum_{i=0}^{n} a_i (x + \langle p \rangle)^i = \left(\sum_{i=0}^{n} a_i x^i \right) + \langle p \rangle = \langle p \rangle.$$

□

Note that if D is an integral domain and $p \in D[x]$, then there is an extension field of $Q(D)$ that contains a root of p. This means that there is an extension field that contains D. This need not be true if D is not an integral domain.

Example 9.5. Let $f(x) = 2x + 1$ in $\mathbb{Z}_4[x]$. Then given any ring $R \supseteq \mathbb{Z}_4$, f has no roots in R. //

9.2 Splitting Fields

Definition 9.6. Let F be a field, and let E be an extension of F. Then we *define* $F(a_1, \ldots, a_n)$ to be the *smallest* subfield of E that contains F and $\{ a_1, \ldots, a_n \}$.

It immediately follows that $F(a_1, \ldots, a_n)$ is the intersection of all subfields of E that contain F and $\{ a_1, \ldots, a_n \}$. We warn the reader that it is important that we have an extension field to talk about. For example, it is nonsensical to write something like $\mathbb{Q}(\text{apple})$ when we don't have any field that contains apple in it.

Definition 9.7 (Polynomial splitting)**.** Let F be a field and let E be an extension of F. Let $f \in F[x]$. Then f **splits** in E if it can be factorized into linear factors, i.e. we have $a \in F$, $a_i \in E$ such that

$$f(x) = a(x - a_1) \cdots (x - a_n).$$

We say that E is a **splitting field for** f if $E = F(a_1, \ldots, a_n)$.

In other words, E is a splitting field for f it is the smallest field that contains F and all roots of f. We remark that whether a polynomial splits depends on which field the polynomial comes from.

Example 9.8. Let $f(x) = x^2 + 1$ in $\mathbb{Q}[x]$. Then $\mathbb{C}$ is *not* a splitting field of f over $\mathbb{Q}$, since we can find a smaller field that still contains roots of f, namely, $\mathbb{Q}[x]/\langle f \rangle$. //

It would be pretty stupid if splitting fields did not exist. Luckily they do.

Theorem 9.9 (Splitting fields exist)**.** Let F be a field and $f \in F[x]$ be nonconstant. Then there is a splitting field of f over F.

The proof of the theorem is simple: induction on $\deg f$ and use Theorem 9.4.

Proof. We go by induction[1] on $\deg f$. If $\deg f = 1$ it is trivial: $f(x) = (x - a)$ for some $a \in F$. Now suppose the theorem is true for all polynomials of degree less than $\deg f$ and all fields. By Theorem 9.4, there is an extension field $E \supseteq F$ such that f has a root in E. Let this root be a_1. Then we factorize f over E, so write $f(x) = (x - a_1)g(x)$, where $g(x) \in E[x]$. Thus there is a splitting field $K \supseteq E$ of g over E. K has all roots of g, say they are $a_2, \ldots, a_n$. Since $E \supseteq F$, K contains a_1, F and $a_2, \ldots, a_n$. So we can take the splitting field to be $F(a_1, \ldots, a_n)$. □

Now we can finally give some examples of splitting fields.

Example 9.10. Let $f(x) = x^2 + 1$, but this time considered as an element of $\mathbb{R}[x]$. Then $\mathbb{C}$ is a splitting field of f over $\mathbb{R}$. Notice that $\mathbb{R}[x]/\langle f \rangle$ also is a splitting field of f. Are these the same splitting field? We will answer this soon. //

[1] Note that strong induction is used here, since $\deg g$ may not necessarily be $\deg f - 1$. If I am wrong, please correct me.

Bibliography

[DF04] David Steven Dummit and Richard M. Foote. *Abstract algebra*. 3rd ed. Hoboken, NJ: Wiley, 2004. ISBN: 9780471433347.

[Jac09] Nathan Jacobson. *Basic algebra*. 2nd ed., Dover ed. Dover books on mathematics. Mineola, N.Y: Dover Publications, 2009. ISBN: 9780486471891.

[Gal20] Joseph A. Gallian. *Contemporary abstract algebra*. Tenth edition. Boca Raton: Chapman & Hall/CRC, 2020. ISBN: 9781003142331.