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.

July 3, 2024
Toronto, ON

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. Let n be an integer. Let D_n be the set of symmetries of a regular n-sided polygon. **TODO: This example needs to be improved** //
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 $gggggggg$. 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.

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.

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 $y \in xHx^{-1}$. This exercise is important because we will use this concept to prove the Sylow Theorems.

Problem 1.3. Prove that no group is the union of 2 proper subgroups. (No cheating and looking this up)

Problem 1.4. 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 1.53 (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 1.54. Prove that the direct product of $G \times H$ is a group.

Exercise 1.55. Prove that if G, H are abelian then so is $G \times H$.

Exercise 1.56. 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 1.57 (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 1.58. 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 1.59. 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 1.53. The group operation also follows similarly.

Exercise 1.60. Formulate the definition of a direct product of infinitely many groups. Prove that this definition does indeed define a group.

Exercise 1.61. 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 1.62 (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 $\phi : G \to H$.

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 1.63 (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 1.64 (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 1.65. Prove that ϕ as defined above is an isomorphism.

We shall immediately prove some useful properties of homomorphisms.

Theorem 1.66 (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 1.67. Prove property (2) of Theorem 1.66. *Hint: First show it for nonnegative n, then show that $\phi(g^{-1}) = \phi(g)^{-1}$.*

Exercise 1.68. Prove the rest of Theorem 1.66

1.4.1 Problems

Exercise 1.69 (Product of groups is commutative)**.** Let G, H be groups. Prove that $G \times H$ is isomorphic to $H \times G$.

Exercise 1.70 (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

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 trivial. □

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.

2.0.1 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 $m \in U(n)$. □

2.1 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. □

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.

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

Chapter 3

Permutation Groups

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 $S = \{1, \ldots, n\}$, 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.
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 3.20. As such when considering permutations on finite sets of size n, we only need to consider permutations on the set $\{1, \ldots, n\}$.

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.

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

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

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

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 $l = \text{lcm}(n, m)$. 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)**.**

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

//

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.
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. Painful. **TODO: Insert proof** □

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[1], 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.

[1]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.

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 $(12)\alpha \neq (12)\beta$.

3.1 Group actions

To be done

3.2 Problems

Exercise 3.20 (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 3.21. Suppose H is a subgroup of S_n and H has odd order. Prove that H is a subgroup of A_n.
Exercise 3.22. Prove that if σ is a permutation with odd order, then σ is even.
Exercise 3.23. Show that if $n \geq 3$, then $Z_(S_n)$ is trivial.
Exercise 3.24. Let $\alpha \in S_n$. Without using Lagrange's theorem, prove that the order of α divides S_n.

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.

One cannot talk about finite group theory without mention of Lagrange's Theorem. This is arguably the most important theorem in finite group theory. In a sense, it restricts the sizes of the subgroups of a group. 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? Here is one way.

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.

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.

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 $a \in H$.

Proof. 1. Obvious.

2. Clearly.
3. Follows from 2.
4. Easy to see.
5. Define a bijection from aH to bH by sending $x \in aH$ to $ba^{-1}x$.
6. Clearly.

□

Since writing "obvious" and "clearly" for a proof doesn't really constitute a proof, we have the following exercise.
Exercise 4.5. Prove 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. Exercise. □

Exercise 4.7. Prove Theorem 4.6

One thing you may have noticed is that the proof of Lagrange's Theorem was rather trivial. How does such a powerful theorem have such a trivial proof? The key answer lies in how the definitions were formulated.

We now state some corollaries of Lagrange's Theorem. These are obvious.

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.

Let us now see an application of Lagrange's Theorem.

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. □

Exercise 4.11. Fill in the details of Corollary 4.10.

Chapter 5

Rings

TBD

Chapter 6

Field Extensions and Splitting Fields

6.1 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 6.1. 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 6.2. $\mathbb{C}$ is clearly an extension field of $\mathbb{R}$. Additionally, $\mathbb{R}$ is an extension field of $\mathbb{Q}$. //

Example 6.3. 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 6.4 (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 6.5. 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. //

6.2 Splitting Fields

Definition 6.6. 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 6.7 (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 6.8. 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 6.9 (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 6.4.

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 6.4, 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 6.10. 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.