Undergraduate Algebra

Robert

June 2024

Abstract

This is a collection of notes for abstract algebra, but it could be interpreted as a textbook, as we include exercises. We will cover the theory of groups, rings, fields as well as modules.

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.

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.

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.

Contents

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.

The next example is an important infinite family of finite groups. We will be studying them closely in
Example 1.20 (Integers mod n)**.** Let $\mathbb{Z}_n = \{0, \dots, n-1\}$ 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 $a, b \in U(n)$, $ab = a \cdot b \mod n$. //

The next example is also rather important.
Example 1.23 (Symmetric groups)**.** Let $S = \{1, \dots, n\}$. 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 now introduce some notation. 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. Recall from elementary school that a^n is the act of multiplying a by itself n times. We also have that $a^{n+m} = a^n \cdot a^m$. In exercise 1.28, 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.

Definition 1.25 (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 1.26. 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. //

We will immediately begin to abuse notation.

Definition 1.27 (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 ∞.

We close off this section with some exercises and problems.

1.1.1 Problems

Exercise 1.28 (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 1.29 (Order of an element is the same as the order of its inverse)**.** Show that $|a| = \left|a^{-1}\right|$

Exercise 1.30 (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 1.31 (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 1.32. Any group is a subgroup of itself. //
Example 1.33 (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 1.34 (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 1.35. 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 1.36 (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 1.37. Prove theorem 1.36.

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 1.38 (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 1.39. 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 1.40. Prove theorem 1.39

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 1.41 (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 1.42. Prove that $C(a)$ is a subgroup of G.

Definition 1.43 (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 1.44. Prove that $Z(G)$ is a subgroup of G.

1.2.1 Problems

Exercise 1.45. 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 1.46. 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 1.47. 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 1.48 (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?

This problem is a bit trickier, and you may need knowledge from later chapters.

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. □

As a consequence of this theorem we have $|a| = |\langle a \rangle|$. 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. 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. We mentioned in the beginning that cyclic subgroups are very nice, and they are indeed so.

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 k be an integer such that $a^k \in H$. Then write $a^k = a^{qm+r}$. Since m is the least, $r = 0$. Thus $a^k \in \langle a^m \rangle$ and so $\langle a^m \rangle \supseteq H$. □

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. □

We leave the reader to formulate a corollary that tells us what the subgroups of $\mathbb{Z}_n$ are.
Exercise 2.19. Formulate a corollary that classifies the subgroups of $\mathbb{Z}_n$.

2.0.1 Problems

Exercise 2.20. Show that if G has order 3, then it must be cyclic.
Exercise 2.21. Show that if $a \in G$, then $\langle a \rangle$ is a subgroup of $C(a)$.
Exercise 2.22. Let G be a group and $a \in G$. Show that $\langle a \rangle = \langle a^{-1} \rangle$.
Exercise 2.23. 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 2.24. Show that $\mathbb{Q}$ under multiplication is not cyclic.
Exercise 2.25. 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 $\left|x^{13}\right|$.
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 subgroup if and only if G is not cyclic.

Chapter 3

Rings

TBD

Chapter 4

Field Extensions and Splitting Fields

4.1 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 4.1. 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 4.2. $\mathbb{C}$ is clearly an extension field of $\mathbb{R}$. Additionally, $\mathbb{R}$ is an extension field of $\mathbb{Q}$. //

Example 4.3. 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 4.4 (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 4.5. 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. //

4.2 Splitting Fields

Definition 4.6. 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 4.7 (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 4.8. 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 4.9 (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 4.4.

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 4.4, 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 4.10. 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.