Lecture notes on elementary modern algebra

Benjamin J. Clark

Spring 2025

Contents

Chapter 0

Preliminaries

0.1 Special common operations

0.1.1 Modulo arithmetic

When working in finite groups (will be defined later) we want the operation of addition to remain closed. To accomplish this, we make addition "wrap back around" on itself. This is called modulo arithmetic.

Theorem 0.1.1 (The quotient remainder theorem)**.** *Given any integer n and positive integer d, there exists unique integers q and r with $0 \leq r < d$ such that*

$$n = dq + r.$$

Definition 0.1.2. Given an integer n and a positive integer d, if $n = dq + r$ for q r integers such that $0 \leq r < d$ then

$$n \text{ div } d = q$$
$$n \bmod d = r.$$

Example 0.1.3. Time is a common place to see modulo arithmetic. When we talk about hours in a day, we are doing modulo arithmetic. Consider it is 8pm, and we want to know what hour it will be 100 hours from now. Instead of directly counting, we can take $99 \mod 24 = 3$, then add the 3 hours to 8pm (which is really 20 hours into the day) to get 11pm. So hours in a day is modulo 24. △

We can use the quotient remainder theorem to take proofs involving an integer and break them into a finite number of cases based on the divisor d.

Definition 0.1.4. For any real number x, the **absolute value of** x, denoted $|x|$, is defined as follows:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0. \end{cases}$$

With this definition, we have the following common properties for all real numbers x, y:

1. $-|x| \leq x \leq |x|$.
2. $|-x| = |x|$.
3. $|x + y| \leq |x| + |y|$.

0.1.2 Complex numbers

Real numbers have a shortcoming when solving equations, consider $x^2 + 1 = 0$. What are the roots of x? Solving for x gives $\pm\sqrt{-1}$, but we know the square root function can't take negative numbers. So this equation has no solutions in the real numbers.

To fix this, we will define a new number system called the complex numbers.

Definition 0.1.5. The complex numbers are defined as a pair of real numbers a, b in the form $a + bi$ where $i = \sqrt{-1}$. Symbolically

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R} \text{ and } i = \sqrt{-1}\}.$$

For complex numbers $a + bi$ and $c + di$ we have

$$\begin{aligned}(a + bi) + (c + di) &= (a + c) + (b + d)i \\ (a + bi)(c + di) &= (ac - bd) + (ad + bd)i.\end{aligned}$$

So, addition is done by adding across and multiplication is done by expanding the two binomials, keeping in mind that $i^2 = -1$.

Complex numbers form an algebraically complete field, which for now just means all polynomials of degree n have n roots.

0.2 Proofs

0.2.1 Direct proof and counterexample.

Definition 0.2.1. An integer n is **even** if, and only if, n equals twice some integer. An integer n is **odd** if, and only if, n equals twice some integer plus 1. Symbolically this gives:

$$\begin{aligned}n \text{ is even} &\iff n = 2k \text{ for some integer } k. \\ n \text{ is odd} &\iff n = 2k + 1 \text{ for some integer } k.\end{aligned}$$

Definition 0.2.2. An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n. An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

Note that these two definitions give us ways to break up the integers. An integer can only be even or odd, but not both. Similarly, a positive integer can be either prime or composite, but not both.

Procedure 0.2.3 (Proving existential and disproving universal statements)**.** If you need to prove an existential statement of the form,

$$\exists x \in D \text{ such that } Q(x)$$

then all it takes is finding one $x \in D$ that makes $Q(x)$ true. Similarly, if you need to disprove a universal statement of the form

$$\forall x \in D, P(x),$$

then that is the same as proving the negation which is

$$\exists x \in D \text{ such that } \sim P(x).$$

△

So to disprove the universal statement we need to find one $x \in D$ such that $P(x)$ is false. When dealing with integers I would recommend $-1, 0, 1$ as easy options to start with.

Procedure 0.2.4 (Proving universal or disproving existential statements)**.** If we want to prove a statement of the form,

$$\forall x \in D, \text{ if } P(x) \text{ then } Q(x).$$

then below are a couple of the main type of proof strategies that can be used.

1. **Method of exhaustion**: If the domain D is finite or if you can split it into a finite number of cases, then the method of exhaustion can be used by checking each case.

   For example, when dealing with integers using that they are either even or odd is a common strategy.

2. **Direct proof**: Here we start with our if $P(x)$ as an assumption and use definitions, previous theorems, and other results to directly get to our conclusion. This is the most standard proof method and is often used with other strategies.

   The general form of this proof will start with

   > Let $x \in D$ such that $P(x)$ is true, then ...

   To show that a result is true for all elements in a set we need to use a variable to represent an arbitrary element and work only off the properties that all elements in the set have.

3. **Proof by contradiction**: Another common proof strategy is proof by contradiction. Here we are going to assume $\sim Q(x)$ and $P(x)$ then try to reach a logical contradiction. This strategy can be helpful since we get the extra information on x that $\sim Q(x)$ is true.

△

Theorem 0.2.5. *The sum of any two even integers is even.*

Proof. Suppose $m, n \in \mathbb{Z}$ such that m, n are even, then by the definition of being even $m = 2r$ and $n = 2s$ for some integers $r, s \in \mathbb{Z}$. With this we have

$$m + n = 2r + 2s = 2(r + s).$$

Let $t = r + s$ and note that t is an integer since it is the sum of integers. Hence, $m + n = 2t$ which is the definition of being even. □

While a lot of problems involving concepts from even/odd and primes seem easy to prove, they can be deceptively hard. A well known open problem in math is as follows

Conjecture 0.2.6 (Goldbach conjecture)**.** *Let $n \in \mathbb{Z}$ such that $n > 2$, then n is the sum of two prime numbers.*

0.2.2 General tips

Copy the statement of the theorem to be proved on your paper

This makes the theorem statement available for reference to anyone reading the proof.

Clearly mark the beginning of your proof with the word Proof

This word separates general discussion about the theorem from its actual proof.

Make your proof self-contained

Explain the meaning of each variable used in your proof. Begin proofs by introducing the initial variables to be used. This is similar to declaring variables and their data types at the beginning of a computer program.

Common words to start a proof are Assume, Let, If, Suppose.

Write your proof in complete, grammatically correct sentences

This does not mean that you should avoid using symbols and shorthand abbreviations, just that you should incorporate them into sentences.

Don't start your sentences with symbols. Try and prep the symbols with short phrases of where the sentence is going. Common words are Following, Since, This gives, We have, Now.

Keep your reader informed about the status of each statement in your proof

Your reader should never be in doubt about whether something in your proof has been assumed or established, or is still to be deduced. If something is assumed, preface it with a word like Suppose or Assume. If it is still to be shown, preface it with words like, We must show that or In other words, we must show that. This is especially important if you introduce a variable in rephrasing what you need to show. (See Common Mistakes.)

Give a reason for each assertion in your proof

Each assertion in a proof should come directly from the hypothesis of the theorem, or follow from the definition of one of the terms in the theorem, or be a result obtained earlier in the proof, or be a mathematical result that has previously been established or is agreed to be assumed. Indicate the reason for each step of your proof using phrases such as by hypothesis, by definition of ... by theorem ... and so forth.

It is best to refer to definitions and theorems by name or number. If you need to state one in the body of your proof, avoid using a variable when you write it because otherwise your proof could end up with a variable that has two conflicting meanings.

Proofs in more advanced mathematical contexts often omit reasons for some steps because it is assumed that students either understand them or can easily figure them out for themselves. However, in a course that introduces mathematical proof, you should make sure to provide the details of your arguments because you cannot guarantee that your readers have the necessary mathematical knowledge and sophistication to supply them on their own.

Include the "little words and phrases" that make the logic of your arguments clear

When writing a mathematical argument, especially a proof, indicate how each sentence is related to the previous one. Does it follow from the previous sentence or from a combination of the previous sentence and earlier ones? If so, start the sentence with the word Because or Since and state the reason why it follows, or write Then, or Thus, or So, or Hence, or Therefore, or Consequently, or It follows that, and include the reason at the end of the sentence.

If a sentence expresses a new thought or fact that does not follow as an immediate consequence of the preceding statement but is needed for a later part of a proof, introduce it by writing Observe that, or Note that, or Recall that, or But, or Now.

Sometimes in a proof, it is desirable to define a new variable in terms of previous variables. In such a case, introduce the new variable with the word Let.

Display equations and inequalities

The convention is to display equations and inequalities on separate lines to increase readability, both for other people and for ourselves so that we can more easily check our work for accuracy.

0.2.3 Common Mistakes

Arguing from examples

Looking at examples is one of the most helpful practices a problem solver can engage in, and is encouraged by all good mathematics teachers. However, it is a mistake to think that a general statement can be proved by showing it to be true for some individual cases. A property referred to in a universal statement may be true in many instances without being true in general.

Using the same letter to mean two different things

Think of the "scope" of a mathematical variable as covering the entire proof. Make sure to not double use the same letter or symbol, unless you clearly redefine it.

Jumping to a conclusion

To jump to a conclusion means to allege the truth of something without giving an adequate reason. Especially for early proofs, always justify every step you take.

Assuming what is to be proved

To assume what is to be proved is a variation of jumping to a conclusion. This can be difficult with early proof classes, as sometimes a theorem can be used on a proof which itself relies on the validity of what is trying to be proved. This can generally be avoided by justifying every step of the proof.

Use of any when the correct word is some

Sometimes the word some acts like an any in a statement, and other times it acts like a there exists. I generally only use some when writing the phrase "[statement is true] for some [value]".

Misuse of the word if

Another common error is not serious in itself, but it reflects imprecise thinking that sometimes leads to problems later in a proof. This error involves using the word if when the word because is really meant. Using the word "if" can sometimes lead to doubt on whether the value is known. I like to use "if" in proofs when I am doing a proof with cases.

0.2.4 Example proofs

Lemma 0.2.7. *If $p \in \mathbb{Z}$ is even, then p^2 is even.*

Proof. Let $p \in \mathbb{Z}$ be even, then by the definition of even $p = 2k$ for some $k \in \mathbb{Z}$. Now

$$p^2 = (2k)^2 = 4k^2 = 2(2k^2).$$

Letting $x = 2k^2$ we have $p^2 = 2x$ giving p^2 is even. □

Theorem 0.2.8. *$\sqrt{2}$ is irrational.*

Proof. Assume for contradiction that $\sqrt{2}$ is rational, then $\sqrt{2} = \frac{p}{q}$ for $p, q \in \mathbb{Z}$ where $q \neq 0$ and $\gcd\{p, q\} = 1$. This gives

$$\sqrt{2} = \frac{p}{q} \implies 2 = \frac{p^2}{q^2} \implies 2q^2 = p^2$$

which implies p^2 is even. Because p^2 is even p must be even. Following p is even $p = 2k$ for some $k \in \mathbb{Z}$. Now

$$\begin{aligned} 2q^2 = p^2 &\implies 2q^2 = (2k)^2 \\ &\implies 2q^2 = 4k^2 \\ &\implies q^2 = 2k^2. \end{aligned}$$

Therefore q is also even. However, this is a contradiction since we assumed $\gcd\{p, q\} = 1$. Thus $\sqrt{2}$ is irrational. □

Theorem 0.2.9. *For every integer n, $2n - 1$ is odd.*

Here are three different ways to prove this theorem.

Proof. If $n \in \mathbb{Z}$ is odd, then by the definition of odd $n = 2k + 1$ for some $k \in \mathbb{Z}$. Now

$$2n - 1 = 2(2k + 1) - 1 = 4k + 2 - 1 = 2(2k) + 1.$$

Let $x = 2k$ which is an integer. Therefore by the definition of being odd $2n - 1 = 2x + 1$ is odd.

If $n \in \mathbb{Z}$ is even, then by the definition of even $n = 2k$ for some $k \in \mathbb{Z}$. Now

$$2n - 1 = 2(2k) - 1 = 4k - 1 = 4k - 1 + 2 - 2 = 2(2k - 1) + 1.$$

Let $x = 2k - 1$ which is an integer. Therefore by the definition of being odd $2n - 1 = 2x + 1$ is odd. □

Proof. Assume for contradiction that $2n - 1$ is even for some integer $n \in \mathbb{Z}$, then $2n - 1 = 2k$ for some $k \in \mathbb{Z}$. Now

$$2n - 1 = 2k \implies 2n = 2k + 1 \implies n = k + \frac{1}{2}.$$

However this is a contradiction since we assumed n, k to be integers but $1/2$ is not an integer. Thus $2n - 1$ is odd. □

Proof. Let $n \in \mathbb{Z}$, then

$$2n - 1 = 2n + 2 - 2 - 1 = 2(n - 1) + 1.$$

Let $x = n - 1$ which is an integer. Therefore $2n - 1 = 2x + 1$ is odd. □

Theorem 0.2.10. *For every integer m, if m is even, then $3m + 5$ is odd.*

Proof. Let $m \in \mathbb{Z}$ such that m is even, then $m = 2k$ for some $k \in \mathbb{Z}$. Now

$$3m + 5 = 6k + 5 = 6k + 4 + 1 = 2(3k + 2) + 1.$$

Let $x = 3k + 2$ which is an integer. Therefore $3m + 5 = 2x + 1$ is odd. □

Theorem 0.2.11. *If k is any odd integer and m is any even integer, then $k^2 + m^2$ is odd.*

Proof. Let $k, m \in \mathbb{Z}$ such that k is odd and m is even, then $k = 2a + 1$ and $m = 2b$ for some $a, b \in \mathbb{Z}$. Now

$$k^2 + m^2 = (2a + 1)^2 + (2b)^2 = 4a^2 + 4a + 1 + 4b^2 = 2(2a^2 + 2a + 2b^2) + 1.$$

Let $x = 2a^2 + 2a + 2b^2$ which is an integer. Therefore $k^2 + m^2 = 2x + 1$ is odd. □

To show the statement "There exists an integer $m \geq 3$ such that $m^2 - 1$ is prime." is false we can take the negation and show it is true.

Theorem 0.2.12. *For all integers m, if $m \geq 3$ then $m^2 - 1$ is composite.*

Proof. Let $m \in \mathbb{Z}$ such that $m \geq 3$, then

$$m^2 - 1 = (m + 1)(m - 1).$$

Following that $m + 1$ and $m - 1$ are greater than 1 we have that $m^2 - 1$ is composite with factors of $m + 1$ and $m - 1$. □

To show the statement "There exists an integer n such that $6n^2 + 27$ is prime." is false we can take the negation and show it is true.

Theorem 0.2.13. *For all integers n, $6n^2 + 27$ is composite.*

Proof. Let $n \in \mathbb{Z}$, then

$$6n^2 + 27 = 3(2n^2 + 9).$$

Following 3 and $2n^2+9$ are integers greater than 1 we have $6n^2+27$ is composite with factors 3 and $2n^2 + 9$. □

To show the statement "There exists an integer $k \geq 4$ such that $2k^2 - 5k + 2$ is prime." is false we can take the negation and show it is true.

Theorem 0.2.14. *For all integers $k \geq 4$, $2k^2 - 5k + 2$ is composite.*

Proof. Let $k \in \mathbb{Z}$ such that $k \geq 4$, then

$$2k^2 - 5k + 2 = (2k - 1)(k - 2).$$

Following that $2k - 1$ and $k - 2$ are integers greater than 1 for $k \geq 4$ we have $2k^2 - 5k + 2$ is composite with factors $2k - 1$ and $k - 2$. □

Theorem 0.2.15. *Prove that the sum of any 3 consecutive integers is divisible by 3.*

Proof. Let $n \in \mathbb{Z}$, then 3 consecutive integers are $n - 1$, n, $n + 1$. Now

$$(n - 1) + n + n + 1 = 3n$$

which is divisible by 3. □

0.2.5 Mathematical Induction

Definition 0.2.16 (Principal of mathematical induction)**.** Let $P(n)$ be a property that is defined for integers n, and let a be a fixed integer. Suppose the following two statements are true:

1. $P(a)$ is true.
2. For every integer $k \geq a$, if $P(k)$ is true, then $P(k + 1)$ is true.

Then the statement

$$\text{for every integer } n \geq a, P(n)$$

is true.

Procedure 0.2.17 (Method of proof by mathematical induction)**.** To prove a statement of the form

> For every integer $n \geq a$, a property $P(a)$ is true

we can use mathematical induction. To do this, first we prove the base case. Which is show $P(a)$ is true, where a is the initial value the statement should hold on.

Then we need to prove the inductive step. Assume the result holds for some $k \geq a$, then we want to show that the result holds for $k + 1$.

Once you have shown these two things, the original statement is proven. △

Example 0.2.18. Prove that for $n \geq 1$ we have

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

△

Proof. For the base case, $n = 1$, we have

$$\sum_{k=1}^{1} k = 1 = \frac{1(2)}{2}.$$

Now for the inductive step we assume that the result holds for some $m \geq 1$, then

$$\begin{aligned}\sum_{k=1}^{m+1} k &= (m+1) + \sum_{k=1}^{m} k \\ &= (m+1) + \frac{m(m+1)}{2} \\ &= \frac{(m+1)(m+2)}{2}.\end{aligned}$$

□

0.2.6 Exercises

1. Prove that there is an integer $n > 5$ such that $2^n - 1$ is prime.
2. Prove that for every integer n, if $(n-1)/2$ is an integer, then n is odd.
3. Prove that the difference between the squares of any two consecutive integers is odd.
4. Prove the following by induction
   (a) $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$ for all $n \geq 1$.
   (b) $\sum_{k=1}^{n+1} k2^k = n2^{n+2} + 2$.
   (c) $\sum_{k=1}^{n} k(k!) = (n+1)! - 1$ for all $n \geq 1$.

0.2.7 Solutions

1. Prove that there is an integer $n > 5$ such that $2^n - 1$ is prime.
   Choose $n = 7$, then $2^7 - 1 = 127$ which is prime.
2. Prove that for every integer n, if $(n-1)/2$ is an integer, then n is odd.

   Proof. Let n be an integer such that $(n-1)/2$ is also an integer, then $(n-1)/2 = k$ for some integer k. Now,

   $$(n-1)/2 = k \implies n - 1 = 2k \implies n = 2k + 1.$$

   Following the definition of odd numbers, n is odd. □

3. Prove that the difference between the squares of any two consecutive integers is odd.

Proof. Let $n \in \mathbb{Z}$, then

$$(n+1)^2 - n^2 = n^2 + 2n + 1 - n^2 = 2n + 1.$$

By definition of odd numbers $2n+1$ is odd giving that $(n+1)^2 - n^2$ is odd. □

4. Prove the following by induction

   (a) $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$ for all $n \geq 1$.

   Proof. Proceed by induction, for the base case of $n = 1$ we have

   $$1^2 = 1 = \frac{1(2)(3)}{6}.$$

   For the inductive step, assume the result holds for some $n \geq 1$, then

   $$\begin{aligned} 1^2 + 2^2 + \cdots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{2n^3 + 3n^2 + n}{6} + \frac{6n^2 + 12n + 6}{6} \\ &= \frac{2n^3 + 9n^2 + 13n + 6}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6}. \end{aligned}$$ □

   (b) $\sum_{k=1}^{n+1} k2^k = n2^{n+2} + 2$.

   Proof. Proceed by induction, for the base case of $n = 1$ we have

   $$\sum_{k=1}^{2} k2^k = 1(2^1) + 2(2^2) = 10 = 1(2^{1+2}) + 2.$$

   For the inductive step assume the result holds for some $n \geq 1$, then

   $$\begin{aligned} \sum_{k=1}^{n+2} k2^k &= (n+2)2^{n+2} + \sum_{k=1}^{n+1} k2^k \\ &= (n+2)2^{n+2} + n2^{n+2} + 2 \\ &= (2n+2)2^{n+2} + 2 \\ &= (n+1)2^{n+3} + 2. \end{aligned}$$ □

   (c) $\sum_{k=1}^{n} k(k!) = (n+1)! - 1$ for all $n \geq 1$.

Proof. Proceed by induction, for the base case of $n = 1$ we have

$$\sum_{k=1}^{1} k(k!) = 1(1!) = 1 = 2! - 1.$$

For the inductive step assume the result holds for some $n \geq 1$, then

$$\begin{aligned}\sum_{k=1}^{n+1} k(k!) &= (n+1)(n+1)! + \sum_{k=1}^{n} k(k!) \\ &= (n+1)(n+1)! + (n+1)! - 1 \\ &= (n+2)(n+1)! - 1 \\ &= (n+2)! - 1.\end{aligned}$$

□

0.3 Set theory

0.3.1 Definition and basic properties of sets

Definition 0.3.1. A set is defined as a collection of elements. These elements can be (almost) anything, including other sets. There is no implicit order to the elements of a set, and duplicates are ignored.

Definition 0.3.2. One way to build sets is with **set-roster notation**, which is where we list all elements of the set or list the first few once the pattern is clear to the reader. For example, $\{1, 2, 3\}$ and $\{1, 2, 3, \dots\}$.

Another way to build sets is with **set-builder notation**, which is written as $\{x \in S \mid P(x)\}$ this is read as "x in S such that $P(x)$ is true" where $P(x)$ is some property of the statement that x must satisfy. For example, $\{x \in \mathbb{R} \mid x \geq 3\}$ which is the set of all real numbers that are greater than or equal to 3. Note that instead of the $\mid$ it is also common to use, : this can be especially helpful in situations involving absolute values like $\{x \in \mathbb{R} : |x| < 1\}$.

The most common sets when working with numbers are $\mathbb{N}$ the natural numbers, $\mathbb{Z}$ the integers, $\mathbb{Q}$ the rational numbers, and $\mathbb{R}$ the real numbers. We will generally exclude using $\mathbb{N}$ because it has two definitions that are used about the same, which are the nonnegative integers and the positive integers. The integers are the whole numbers, including negatives. We will use $\mathbb{Z}^+$ for the positive integers and $\mathbb{Z}^{\geq 0}$ for the nonnegative integers. Another set we care about is the **empty set**, which is defined to be the set of no elements, it is denoted $\emptyset$.

When working with sets, we often care about the idea of a **subset**, which is defined as a set that contained in another set and is denoted $A \subseteq B$. If this containment is strict, that is B contains more elements then A, we write $A \subset B$ and this is called a **proper subset**.

Two sets are called equal if and only if they contain all the same elements.

Definition 0.3.3. Given elements a, b, the symbol (a, b) denotes the **ordered pair** made from a and b with the added information that a is first and b is second.

Two ordered pairs are equal if and only if their first and second components are the same. That is, for $(a, b) = (c, d)$ we need $a = c$ and $b = d$.

The above definition can be extended to arbitrary dimension.

Definition 0.3.4. Let n be a positive integer and let $x_1, \ldots, x_n$ be elements. The **ordered n-tuple**, $(x_1, \ldots, x_n)$, consists of the above elements with the ordering that x_1 comes before x_2 and so on.

We can apply this idea of ordered pairs to construct a multiplication like operation for sets.

Definition 0.3.5. Given sets $A_1, A_2, \ldots, A_n$ the Cartesian product of $A_1, \ldots, A_n$ denoted $A_1 \times A_2 \times \cdots \times A_n$, is the set of all ordered tuples $(a_1, \ldots, a_n)$ where $a_1 \in A_1$ and so on. Symbolically, we can write this as

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) | a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.$$

Definition 0.3.6 (Common set operations)**.** Let A and B be subsets of a universal set U.

1. The **union** of A and B, denoted $A \cup B$, is the set of all elements that are in at least one of A or B.
2. The **intersection** of A and B, denoted $A \cap B$, is the set of all elements that are common to both A and B.
3. The **difference** of B minus A, denoted $B - A$, is the set of all elements that are in B and not in A.
4. The **complement** of A, denoted A^c, is the set of all elements in U that are not in A.

Definition 0.3.7 (Unions and intersections of an indexed collection of sets)**.** Given sets $A_0, A_1, A_2, \ldots$ that are subsets of a universal set U and given a nonnegative integer n,

$$\bigcup_{i=0}^{n} A_i = \{x \in U | x \in A_i \text{ for some } i = 0, 1, \ldots, n\}$$
$$\bigcap_{i=0}^{n} A_i = \{x \in U | x \in A_i \text{ for every } i = 0, 1, \ldots, n\}.$$

Definition 0.3.8 (Interval notation)**.** Given real numbers a and b with $a \leq b$:

$$(a, b) = \{x \in \mathbb{R} | a < x < b\} \qquad [a, b] = \{x \in \mathbb{R} | a \leq x \leq b\}$$
$$(a, b] = \{x \in \mathbb{R} | a < x \leq b\} \qquad [a, b) = \{x \in \mathbb{R} | a \leq x < b\}.$$

Definition 0.3.9. Two sets are called **disjoint** if and only if they have no elements in common.

We can extend this definition to a list of sets $A_1, A_2, A_3, \dots$ and say that all the A_i sets are **mutually disjoint** if all pairs of the sets are disjoint.

Definition 0.3.10. A collection of nonempty sets $\{A_1, A_2, \dots\}$ is a **partition** of a set A if and only if

1. A is the union of all the A_i
2. The sets $A_1, A_2, \dots$ are mutually disjoint.

Definition 0.3.11. Given a set A, the **power set** of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.

Theorem 0.3.12 (Set inclusion principals)**.** *Let A, B, C be sets, then*

1. $A \cap B \subseteq A$
2. $A \subseteq A \cup B$
3. *If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

Theorem 0.3.13 (Set Identities)**.** *Let $A, B, C \subset U$ where U is the universal set, then*

1. *Commutative laws:*
$$A \cup B = B \cup A \text{ and } A \cap B = B \cap A.$$
2. *Associative laws:*
$$(A \cup B) \cup C = A \cup (B \cup C) \text{ and } (A \cap B) \cap C = A \cap (B \cap C).$$
3. *Distributive laws:*
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
and
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$
4. *Identity laws:*
$$A \cup \emptyset = A \text{ and } A \cap U = A.$$
5. *Complement laws:*
$$A \cup A^c = U \text{ and } A \cap A^c = \emptyset.$$
6. *Double complement law:*
$$(A^c)^c = A.$$

7. *Idempotent laws:*
$$A \cup A = A \text{ and } A \cap A = A.$$

8. *Universal bound laws:*
$$A \cup U = U \text{ and } A \cap \emptyset = \emptyset.$$

9. *De Morgan's laws:*
$$(A \cup B)^c = A^c \cap B^c \text{ and } (A \cap B)^c = A^c \cup B^c.$$

10. *Absorption laws:*
$$A \cup (A \cap B) = A \text{ and } A \cap (A \cup B) = A.$$

11. *Complements of U and $\emptyset$:*
$$U^c = \emptyset \text{ and } \emptyset^c = U.$$

12. *Set difference law:*
$$A - B = A \cap B^c.$$

Theorem 0.3.14. *Let A be a set, then $\emptyset \subseteq A$.*

Theorem 0.3.15. *For all sets A, B, C, if $A \subseteq B$ and $B \subseteq C^c$, then $A \cap C = \emptyset$.*

0.3.2 Proofs on sets

Procedure 0.3.16. Given sets, A, B to prove that, $A \subseteq B$ we need to show for any element in A that element is in B. The standard way to do this is

1. Suppose that a is an unknown, but particular element of A.
2. Show that a is an element of B.

△

Procedure 0.3.17. Given sets A, B the standard way to prove that, $A = B$ is to prove $A \subseteq B$ and that $B \subseteq A$. △

One way to think of set relations is as a for all statement. That is for all sets we have this relation. So, to disprove a set relation we need to construct a counterexample.

Example 0.3.18. Disprove the following. For all sets A, B, C we have
$$(A - B) \cup (B - C) = A - C.$$

To start building the counterexample think about what each side is saying. On the right we have A with everything from C removed. However on the left we

have A with everything from B removed or B with everything from C removed. So if we have an element in C that is in A but not in B then it will break our equality. For example

$$\begin{aligned} A &= \{1\} \\ B &= \{2\} \\ C &= \{1\} \\ (A - B) \cup (B - C) &= \{1, 2\} \\ (A - C) &= \emptyset. \end{aligned}$$

△

Theorem 0.3.19. *Let $n \in \mathbb{Z}$ such that $n \geq 0$, if X is a set with n elements, then $\mathcal{P}(X)$ has 2^n elements.*

Proof. Let $n = 0$, then X is the set with no elements so its only subset is itself giving $\mathcal{P}(X)$ has 1 element. Now assume the result holds for some $m \geq 0$. If X has $m + 1$ elements, then it has at least one element $z \in X$. Consider $X - \{z\}$ this is a set with m elements so by our induction hypothesis $\mathcal{P}(X - \{z\})$ has 2^m subsets. Now to build $\mathcal{P}(X)$ we can either add z to each subset in $\mathcal{P}(X - \{z\})$ or not. This gives two possible choices for each element. Thus $\mathcal{P}(X)$ has $2(2^m) = 2^{m+1}$ elements. □

0.3.3 Exercises

1. Let $\mathbb{R}$ be the universal set and let

$$\begin{aligned} A &= \{x \in \mathbb{R} \mid -3 \leq x \leq 0\}, \\ B &= \{x \in \mathbb{R} \mid -1 < x < 2\}, \\ C &= \{x \in \mathbb{R} \mid 6 < x \leq 8\}. \end{aligned}$$

   Find the following

   (a) $A \cup B$
   (b) B^c
   (c) $A^c \cap B^c$
   (d) $(A \cap B)^c$

2. Let

$$\begin{aligned} A &= \{x \in \mathbb{Z} | x = 10b - 3 \text{ for some integer } b\} \\ B &= \{z \in \mathbb{Z} | z = 18c + 16 \text{ for some integer } c\}. \end{aligned}$$

   Prove or give a counter example to $A \subset B$, $B \subset A$, and $A = B$.

3. Is $\{\{a, d, e\}, \{b, c\}, \{d, f\}\}$ a partition of $\{a, b, c, d, e, f\}$. If so, justify. If not how can you make it one?

4. Let $A = \{1, 2\}$ and $B = \{2, 3\}$, then find the following.
   (a) $\mathcal{P}(\emptyset)$.
   (b) $\mathcal{P}(A)$.
   (c) $\mathcal{P}(A \cap B)$.
   (d) $\mathcal{P}(A \cup B)$.

5. Prove the following
$$(A - B) \cup (C - B) = (A \cup C) - B$$

6. Find a counterexample to the following
   (a) $(A \cup B) \cap C = A \cup (B \cap C)$
   (b) If $B \cup C \subseteq A$, then $(A - B) \cap (A - C) = \emptyset$.

0.3.4 Solutions

1. Let $\mathbb{R}$ be the universal set and let
$$A = \{x \in \mathbb{R} \mid -3 \leq x \leq 0\},$$
$$B = \{x \in \mathbb{R} \mid -1 < x < 2\},$$
$$C = \{x \in \mathbb{R} \mid 6 < x \leq 8\}.$$
   Find the following
   (a) $A \cup B$ $[-3, 2)$ or $\{x \in \mathbb{R} \mid -3 \leq x < 2\}$.
   (b) B^c $(-\infty, -1] \cup [2, \infty)$ or $\{x \in \mathbb{R} \mid x \leq -1 \text{ or } x \geq 2\}$.
   (c) $A^c \cap B^c$ $(-\infty, -3] \cup [2, \infty)$
   (d) $(A \cap B)^c$ $(-\infty, -1] \cup (0, \infty)$

2. Let
$$A = \{x \in \mathbb{Z} | x = 10b - 3 \text{ for some integer } b\}$$
$$B = \{z \in \mathbb{Z} | z = 18c + 16 \text{ for some integer } c\}.$$
   Prove or give a counter example to $A \subseteq B$, $B \subseteq A$, and $A = B$.
   We know $-3 \in A$ since $-3 = 10(0) - 3$. For -3 to be in B we need $-3 = 18c + 16 \implies -19 = 18c$ for some integer $c \in \mathbb{Z}$. However, this is a contradiction since -19 is not divisible by 18. This gives that A is not a subset of B. Note this also shows that A is not equal to B.
   Taking a similar approach to showing that B is not a subset of A. Let $16 \in B$, then for 16 to be in A we need $16 = 10b - 3 \implies 19 = 10b$. However, this can't happen since 19 is not divisible by 10.

3. Is $\{\{a,d,e\},\{b,c\},\{d,f\}\}$ a partition of $\{a,b,c,d,e,f\}$. If so, justify. If not, how can you make it one?

   This is not a partition. While the sets $\{a,d,e\},\{b,c\},\{d,f\}$ do union to $\{a,b,c,d,e,f\}$, we have a duplicate d in sets $\{d,f\}$ and $\{a,d,e\}$.

   To fix this, we can simply remove the duplicate d. An example would be $\{\{a,d,e\},\{b,c\},\{f\}\}$.

4. Let $A=\{1,2\}$ and $B=\{2,3\}$, then find the following.

   (a) $\mathcal{P}(\emptyset)$

   Note that the power set is a set containing sets and that it always contains the set itself. In this case, that is the only subset giving

   $$\mathcal{P}(\emptyset)=\{\emptyset\}.$$

   (b) $\mathcal{P}(A)$.

   $$\mathcal{P}(A)=\{\{1,2\},\{1\},\{2\},\emptyset\}.$$

   (c) $\mathcal{P}(A\cap B)$.

   $$\mathcal{P}(A\cap B)=\{\{2\},\emptyset\}.$$

   (d) $\mathcal{P}(A\cup B)$.

   $$\mathcal{P}(A)=\{\{1,2,3\},\{1,2\},\{1,3\},\{2,3\},\{1\},\{2\},\{3\},\emptyset\}.$$

5. Prove the following $(A-B)\cup(C-B)=(A\cup C)-B$

   Proof.

   $$\begin{aligned}(A-B)\cup(C-B)&=(A\cap B^c)\cup(C\cap B^c) && \text{(Set difference law)}\\ &=(A\cup C)\cap B^c && \text{(Distributive law)}\\ &=(A\cup C)-B. && \text{(Set difference law)}\end{aligned}$$

   □

6. Find a counterexample to the following

   (a) $(A\cup B)\cap C=A\cup(B\cap C)$

   $$A=\{1\},\ B=\{2\},\ C=\{3\}$$
   $$(A\cup B)\cap C=\emptyset$$
   $$A\cup(B\cap C)=\{1\}.$$

(b) If $B \cup C \subseteq A$, then $(A - B) \cap (A - C) = \emptyset$.

$$A = \{1\},\ B = \emptyset,\ C = \emptyset$$
$$B \cup C = \emptyset \subseteq A$$
$$(A - B) \cap (A - C) = \{1\}.$$

0.4 Relations

0.4.1 Properties of relations

Definition 0.4.1. Let A and B be sets A relation R from A to B is a subset of $A \times B$. We use xRy to mean $(x, y) \in R$. The set A is called the domain and B is called the co-domain.

Definition 0.4.2. Let R be a relation from A to B. Define the inverse relation R^{-1} from B to A as

$$R^{-1} = \{(y, x) \in B \times A \mid (x, y) \in R\}.$$

Example 0.4.3. Let $A = \{2, 3, 4\}$ and $B = \{2, 6, 8\}$, then

$$A \times B = \{(2,2), (2,6), (2,8), (3,2), (3,6), (3,8), (4,2), (4,6), (4,8)\}.$$

If we have

$$R = \{(2,2), (2,6), (2,8), (3,6), (4,8)\},$$

then

$$R^{-1} = \{(2,2), (6,2), (8,2), (6,3), (8,4)\}.$$

△

Definition 0.4.4. A relation on a set A is a relation from A to A.

Definition 0.4.5. Given sets $A_1, A_2, \ldots, A_n$ an n-ary relation R is a subset of $A_1 \times \cdots \times A_n$.

0.4.2 Reflexivity, Symmetry, and Transitivity

Definition 0.4.6. Let R be a relation on a set A.

1. R is **reflexive** if and only if for every $x \in A$, xRx.
2. R is **symmetric** if and only if for every $x, y \in A$, if xRy then yRx.
3. R is **transitive** if and only if for every $x, y, z \in A$, if xRy and yRz then xRz.

Example 0.4.7. Let $A = \{0, 1, 2, 3\}$ and define the following relations

$$R = \{(0,0), (0,1), (0,3), (1,0), (1,1), (2,2), (3,0), (3,3)\},$$
$$S = \{(0,1), (2,3)\},$$
$$T = \{(0,0)\}.$$

Are R, S, T transitive, reflexive or symmetric?

R is reflexive and is symmetric, but is not transitive since $(1,0) \in R$ and $(0,3) \in R$, but $(1,3) \notin R$.

S is not reflexive since $(0,0) \notin S$. S is not symmetric since $(0,1) \in S$, but $(1,0) \notin S$. S is transitive since there are no points such that $(x,y) \in S$ and $(y,z) \in S$.

T is transitive, is not reflexive and symmetric. △

Example 0.4.8. Let R be a relation on the real numbers where xRy if and only if $x = y$, then R is symmetric, reflexive, and transitive. △

Definition 0.4.9. Let A be a set and R a relation on A. The **transitive closure** of R is the relation R^t on A that satisfies the following three properties:

1. R^t is transitive.
2. $R \subseteq R^t$.
3. If S is any other transitive relation that contains R, then $R^t \subseteq S$.

Example 0.4.10. Let $A = \{0, 1, 2, 3\}$ and consider R defined on A as follows:

$$R = \{(0,1), (1,2)\}.$$

Then

$$R^t = \{(0,1), (1,2), (0,2)\}.$$

△

0.4.3 Equivalence relations

Definition 0.4.11. Given a partition of a set A, the **relation induced by the partition**, R, is defined on A as follows: For every $x, y \in A$, $(x,y) \in R$ if x and y are contained in the same subset of the partition.

Example 0.4.12. Let $A = \{0, 1, 2, 3, 4\}$ and consider the partition

$$\{0, 3, 4\},\ \{1\},\ \{2\}.$$

The relation R induced by this partition is

$$\{(0,0), (0,3), (0,4), (3,0), (3,3), (3,4), (4,0), (4,3), (4,4), (1,1), (2,2)\}$$

△

Theorem 0.4.13. *Let A be a set with a partition and let R be the relation induced by the partition. Then R is reflexive, symmetric, and transitive.*

Definition 0.4.14. Let A be a set and R a relation on A, then R is an **equivalence relation** if and only if R is reflexive, symmetric, and transitive.

Note that the above theorem and definition can be combined since they connected with if and only if statements. So we could say that R is an equivalence relation on a set A if and only if R is a relation induced by a partition of A.

Using this if you are asked to show a relation is an equivalence relation one option is to show that there exists a partition of the set such that the relation is induced on it.

Definition 0.4.15. Suppose A is a set and R is an equivalence relation on A. For each element $a \in A$, the **equivalence class of** a, denoted $[a]$ is the set of all elements $x \in A$ such that $(x, a) \in R$. The element a is called the **representative** for the equivalence class $[a]$.

Another way to think about equivalence classes is with partitions. If we have a set A and a partition, then for some $a \in A$ the equivalence class $[a]$ is the set in the partition where a is in.

Example 0.4.16. Let $A = \{0, 1, 2, 3, 4\}$ with the partition

$$\{0, 3, 4\},\ \{1\},\ \{2\},$$

then the equivalence classes of A are

$$\begin{aligned}[0] = [3] = [4] &= \{0, 3, 4\} \\ [1] &= \{1\} \\ [2] &= \{2\}.\end{aligned}$$

△

Example 0.4.17. Consider $\mathbb{Z}$ which can be partitioned into the even and odd numbers, then the equivalence classes of that partition are

$$\begin{aligned}[0] &= \{\dots, -4, -2, 0, 2, 4, \dots\} \\ [1] &= \{\dots, -3, -1, 1, 3, \dots\}.\end{aligned}$$

We can also write

$$\mathbb{Z} = [0] \cup [1].$$

△

Lemma 0.4.18. *Suppose A is a set, R is an equivalence relation on A, and $a, b \in A$. If $(a, b) \in R$, then $[a] = [b]$.*

Lemma 0.4.19. *Suppose A is a set, R is an equivalence relation on A, and $a, b \in A$. Either $[a] \cap [b] = \emptyset$ or $[a] \cap [b] = [a]$.*

Definition 0.4.20. Let $m, n \in \mathbb{Z}$ and let $d \in \mathbb{Z}^+$. We say that m is **congruent** to n modulo d and write

$$m \equiv n \bmod d$$

if and only if

$$d \mid (m - n).$$

Using the definition above we can form partitions of the integers with congruence equivalence classes. We already saw this with the even and odd integers where they are congruent modulo 2.

Example 0.4.21. Let $d \in \mathbb{Z}^+$ and let R be the relation defined by

$$(x, y) \in R \iff x \equiv y \bmod d,$$

then R is an equivalence relation. △

Example 0.4.22. Let $A = \mathbb{Z} \times (\mathbb{Z} - \{0\})$, then define the relation

$$((a, b), (c, d)) \in R \iff \frac{a}{b} = \frac{c}{d} \iff ad = bc.$$

This relation R is an equivalence class and is a way to define the rational numbers. Consider

$$\left[\frac{1}{2}\right] = \left\{\frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \dots\right\}$$

△

0.4.4 Exercises

1. Let $A = \{-1, 1, 2, 4\}$ and $B = \{1, 2\}$ and define relations R and S from A to B as follows: For every $(x, y) \in A \times B$.

   $$(x, y) \in R \iff |x| = |y|$$
   $$(x, y) \in S \iff x - y \text{ is even.}$$

   State which ordered pairs are in $A \times B$, R, S, $R \cup S$, and $R \cap S$.

2. Let C be the circle relation on the set of real numbers: For every $x, y \in \mathbb{R}$, $(x, y) \in C$ if and only if $x^2 + y^2 = 1$. Determine if C is reflexive, transitive, and symmetric.

3. If R and S are reflexive, then is $R \cap S$ reflexive?

4. If R and S are reflexive, then is $R \cup S$ reflexive?

5. Let $X = \{-1, 0, 1\}$, let $A = \mathcal{P}(X)$, and define R to be a relation on A such that

   $(s, t) \in R \iff$ the sum of the elements in s equals the sum of the elements in t.

   Find the distinct equivalence classes of R.

6. Let $A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$ and define R on A to be

$$(m, n) \in R \iff 4|(m^2 - n^2).$$

Find the distinct equivalence classes of R.

0.4.5 Solutions

1. Let $A = \{-1, 1, 2, 4\}$ and $B = \{1, 2\}$ and define relations R and S from A to B as follows: For every $(x, y) \in A \times B$.

$$(x, y) \in R \iff |x| = |y|$$
$$(x, y) \in S \iff x - y \text{ is even.}$$

State which ordered pairs are in $A \times B$, R, S, $R \cup S$, and $R \cap S$.

$$A \times B = \{(-1, 1), (-1, 2), (1, 1), (1, 2), (2, 1), (2, 2), (4, 1), (4, 2)\}$$
$$R = \{(-1, 1), (1, 1), (2, 2)\}$$
$$S = \{(-1, 1), (1, 1), (2, 2), (4, 2)\}$$
$$R \cup S = \{(-1, 1), (1, 1), (2, 2), (4, 2)\}$$
$$R \cap S = \{(-1, 1), (1, 1), (2, 2)\}.$$

2. Let C be the circle relation on the set of real numbers: For every $x, y \in \mathbb{R}$, $(x, y) \in C$ if and only if $x^2 + y^2 = 1$. Determine if C is reflexive, transitive, and symmetric.

   C is not reflexive, consider $(1, 1) \notin C$.

   C is symmetric, since x and y are real numbers so we can swap any (x, y) with (y, x).

   C is not transitive. Let $x = 1$, $y = 0$, and $z = 1$, then $(x, y) \in C$ and $(y, z) \in C$, but $(x, z) \notin C$.

3. If R and S are reflexive, then is $R \cap S$ reflexive?

   Yes, since R and S are reflexive, then they both must contain $(x, x) \in A \times A$ for every $x \in A$. So their intersection still contains all those pairs.

4. If R and S are reflexive, then is $R \cup S$ reflexive?

   Yes, similar reasoning to the previous question.

5. Let $X = \{-1, 0, 1\}$, let $A = \mathcal{P}(X)$, and define R to be a relation on A such that

   $(s, t) \in R \iff$ the sum of the elements in s equals the sum of the elements in t.

Find the distinct equivalence classes of R.

First building $\mathcal{P}(X)$ we get

$$\mathcal{P}(x) = \{\{-1\}, \{0\}, \{1\}, \{-1, 0\}, \{-1, 1\}, \{0, 1\}, \{-1, 0, 1\}, \emptyset\}.$$

Remember the trick to checking your work on the power set is there should be 2^n elements, so in this case 8 subsets.

Now to build the equivalence classes we could find all entrys the are related. However for this problem we can assume the relation R is an equivalence relation, so just start building the equivalence classes. So $[\{-1\}]$ is the equivalence class where the sum of the entries is -1 which gives

$$[\{-1\}] = \{\{-1\}, \{0, -1\}\}.$$

To get the next equivalence class take an element of $\mathcal{P}(X)$ that is not in $[\{-1\}]$ like $[\{0\}]$ which gives

$$[\{0\}] = \{\{0\}, \{-1, 1\}, \{-1, 0, 1\}\}.$$

The next element that is not in $[\{-1\}]$ or $[\{0\}]$ is $\{1\}$, so we can build

$$[\{1\}] = \{\{1\}, \{0, 1\}\}.$$

Finally, we are missing $\emptyset$, so we give it its own equivalence class. This gives

$$\begin{aligned} [\{-1\}] &= \{\{-1\}, \{0, -1\}\} \\ [\{0\}] &= \{\{0\}, \{-1, 1\}, \{-1, 0, 1\}\} \\ [\{1\}] &= \{\{1\}, \{0, 1\}\} \\ [\emptyset] &= \{\emptyset\}. \end{aligned}$$

as our distinct equivalence classes.

6. Let $A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$ and define R on A to be

$$(m, n) \in R \iff 4|(m^2 - n^2).$$

Find the distinct equivalence classes of R.

Similar to last time we can assume R is an equivalence relation and just start building the classes. So take -4 and we want to find which numbers are related. This gives

$$[-4] = \{-4, -2, 0, 2, 4\}.$$

Removing those from A the next element not in $[-4]$ is

$$[-3] = \{-3, -1, 1, 3\}$$

These two equivalence classes cover all the elements.

0.5 Functions

Definition 0.5.1. A **function F from a set A to a set B** is a relation with domain A and co-domain B that satisfies the following two properties:

1. For every element $x \in A$, there is an element $y \in B$ such that $(x, y) \in F$.
2. For all elements $x \in A$ and $y \in B$, if $(x, y) \in F$ and $(x, z) \in F$ then $y = z$.

For functions, we frequently use the notation $F(x)$ where $x \in A$ and $F(x) \in B$.

Example 0.5.2. Define a relation C from $\mathbb{R}$ to $\mathbb{R}$ as follows: For any $(x, y) \in \mathbb{R} \times \mathbb{R}$, $(x, y) \in C$ means that $x^2 + y^2 = 1$.

The domain and co-domain of C are both $\mathbb{R}$.

In its current form C does not satisfy the requirement of being a function since a single input could have two outputs. To see this, consider $x = 0$.

To make C into a function, we could apply a restriction to the co-domain. If we instead defined C from $\mathbb{R}$ to $\mathbb{R}^+$, then C satisfies the requirements of being a function. △

Definition 0.5.3 (Equality of functions)**.** Let $\alpha : A \to B$ and $\beta : A \to B$, then $\alpha = \beta$ if $\alpha(a) = \beta(a)$ for all $a \in A$.

Definition 0.5.4. Let $f : A \to B$ be a function. We say that the *image* of $a \in A$ under f is the element $b \in B$ such that $f(a) = b$. We can also take the images of sets, for a set $A' \subseteq A$ the image $f(A') = \{f(a) \mid a \in A'\}$.

Definition 0.5.5. Let $\phi : A \to B$ and $\psi : B \to C$. The composition $\psi\phi$ is the mapping from A to C defined by $(\psi\phi)(a) = \psi(\phi(a))$ for all $a \in A$.

You will likely have seen the notation $(f \circ g)(x) = f(g(x))$ for this class, we will omit the circle and just write $(fg)(x)$.

Note that generally for functions f and g, fg is not the same as gf.

Definition 0.5.6. A function $\phi : A \to B$ is called *one-to-one* or *injective* if for every $a_1, a_2 \in A$ if $\phi(a_1) = \phi(a_2)$ then $a_1 = a_2$.

A requirement of being a function is that every input has exactly one output, for that function to be one-to-one every output must have exactly one input. Note however that the function ϕ does not need to reach every value of B.

Definition 0.5.7. A function $\phi : A \to B$ is said to be *onto* B or just onto, if for every $b \in B$ there exists a $a \in A$ such that $\phi(a) = b$. This is also known as *surjective*.

Onto is the property that allows us to say that the function "covers" the set B. If a function is onto, we know that every output has an associated input. However, be careful as being onto might still allow for multiple inputs to have the same output.

Definition 0.5.8. A function that is both one-to-one and onto is called a bijection.

Bijections form a special type of function since, as you will see formally in the next theorem, they allow for the inverse of the function to be well-defined. One way to think of bijections is that they preserve the "structure" of the set. Or that, both of the two sets are the same under the view of the bijection.

Theorem 0.5.9. *Given functions $\alpha : A \to B$, $\beta : B \to C$, and $\gamma : C \to D$, then*

1. *$\gamma(\beta\alpha) = (\gamma\beta)\alpha$ (associativity).*
2. *If α and β are one-to-one, then $\beta\alpha$ is one-to-one.*
3. *If α and β are onto, then $\beta\alpha$ is onto.*
4. *If α and β are bijective, then $\beta\alpha$ is bijective.*
5. *If α is a bijection, then there is a function $\alpha^{-1} : B \to A$ such that $(\alpha^{-1}\alpha)(a) = a$ for all $a \in A$ and $(\alpha\alpha^{-1})(b) = b$ for all $b \in B$.*

0.5.1 Exercises

1. Show that $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is neither one-to-one or onto. Give a domain/co-domain restriction that makes it one-to-one and onto.
2. Prove that $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x + 1$ forms a bijection.
3. Prove there is a bijection between $\mathbb{N}$ and $\mathbb{Z}$.
4. How many distinct bijections are there between sets $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$? In general, how many bijections are there between two sets of size n?
5. Suppose that α, β, and γ are functions over a set A. If $\alpha\gamma = \beta\gamma$ and γ is a bijection, then prove that $\alpha = \beta$.

0.5.2 Solutions

1. Show that $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is neither one-to-one or onto. Give a domain/co-domain restriction that makes it one-to-one and onto.

   We can do a proof by counter example for both one-to-one and onto.

   Proof. Consider $x = 1$ and $x = -1$, through f both get mapped to 1. Thus, the function f is not one-to-one.

   For onto, consider the output of -1 to reach this we need an x such that $x^2 = -1$ which implies $x = \sqrt{-1}$. We know that $\sqrt{-1}$ is not a real number, so it is not in our domain. Thus f is not onto. □

2. Prove that $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x + 1$ forms a bijection.

   Proof. To prove that f forms a bijection we will first show that it is one-to-one, then onto. Let $a_1, a_2 \in \mathbb{R}$ such that $f(a_1) = f(a_2)$ this implies that $2a_1 + 1 = 2a_2 + 1$ which gives $a_1 = a_2$ as desired.

   For showing that it is onto, let $b \in \mathbb{R}$, then we are looking for an $a \in \mathbb{R}$ such that $f(a) = b$. Let $a = (b-1)/2$, then $f(a) = 2(b-1)/2 + 1 = b$. Following f is one-to-one and onto we have that f is a bijection. □

3. Prove there is a bijection between $\mathbb{N}$ and $\mathbb{Z}$.

   Proof. Define $f : \mathbb{N} \to \mathbb{Z}$ such that

$$f(x) = \begin{cases} -(x/2) & \text{if } x \text{ is even,} \\ (x+1)/2 & \text{if } x \text{ is odd.} \end{cases}$$

   The claim to prove is that f is a bijection. First for one-to-one note that if $f(x) \leq 0$, then x is even. If $f(x) > 0$, then x is odd. Now let $a_1, a_2 \in \mathbb{N}$ such that $f(a_1) = f(a_2)$, then we will continue by cases, If $f(a_1) > 0$, then a_1 and a_2 are both odd giving that

$$f(a_1) = f(a_2) \implies \frac{a_1 + 1}{2} + \frac{a_2 + 1}{2} \implies a_1 = a_2.$$

   If $f(a_2) \leq 0$, then a_1 and a_2 are both even giving that

$$f(a_1) = f(a_2) \implies -(a_1/2) = -(a_2/2) \implies a_1 = a_2.$$

   Thus f is one-to-one.

   For onto let $b \in \mathbb{Z}$ if $b > 0$, then consider $2b - 1$ which is an odd natural number. Now $f(2b-1) = (2b - 1 + 1)/2 = b$. If $b \leq 0$, then consider $-2b$ which is an even natural number. With this we have, $f(-2b) = -(-2b/2) = b$. This gives that f is also onto. Therefore, f is a bijection. □

4. How many distinct bijections are there between sets $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$? In general, how many bijections are there between two sets of size n?

   Between sets A and B there are 6 possible bijections. To see this, first consider where we can map 1 from set A. It can go to either a, b, or c giving 3 possible choices. Now 2 can be mapped to either of the two choices that 1 was not mapped to, giving an additional two choices. Finally, 3 is fully locked in to the final choice. This give $3(2)(1) = 6$ total bijections.

   The same argument as above can be used to generalize the problem. In this case the first choice will have n options, the ith choice will have $n - i$ options and the final choice will have 1 option. This gives a total of $n!$ different bijections.

5. Suppose that α, β, and γ are functions over a set A. If $\alpha\gamma = \beta\gamma$ and γ is a bijection, then prove that $\alpha = \beta$.

   To show that two functions are equal, we need to show that for every $x \in A$ we have that $\alpha(x) = \beta(x)$. In this case, a contradiction proof works fairly well.

   Proof. Assume for contradiction that $\alpha \neq \beta$, then there exists a $x \in A$ such that $\alpha(x) \neq \beta(x)$. Following γ is a bijection, there exists a $y \in A$ such that $\gamma(y) = x$. From assumptions, we have that, $\alpha(\gamma(y)) = \beta(\gamma(y))$ which implies that $\alpha(x) = \beta(x)$. Thus, we have a contradiction, since $\alpha(x)$ can't be both equal and not equal to $\beta(x)$. □

Chapter 1

Groups

1.1 Definition and examples

Before we formally start talking about a group, we need to define a special type of relation.

Definition 1.1.1. Let G be a set. A *binary operation* on G is a function that assigns each ordered pair of elements of G an element of G

So a binary operation, in its most general form, is a relation on a single set that is closed. Note that this definition does not require inverses, associativity, commutativity, or other common function/relation properties.

Example 1.1.2. The usual addition operation over the integers is a binary operation, that is, $a + b \in \mathbb{Z}$ for all $a, b \in \mathbb{Z}$. Another way to write this would be $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

The usual division operation over the integers is not a binary operation, since it is not closed. As an example, $3/2 = 1.5 \notin \mathbb{Z}$. △

Definition 1.1.3. Let G be a set together with a binary operation that assigns to each ordered pair (a, b) of elements of G an element in G denoted ab. We say G is a *group* under this operation if the following three properties are satisfied.

1. Associativity: For all $a, b, c \in G$ we have $(ab)c = a(bc)$.
2. Identity: There exists an element, $e \in G$, such that $ae = ea = a$ for all $a \in G$.
3. Inverses: For each element, $a \in G$ there is an element $b \in G$ such that $ab = ba = e$.

Note, when checking whether something is a group, we need to satisfy the above three properties and closure of the binary operation.

Generally a group is not commutative, if it is commutative, then it is called a commutative group or abelian group. Similarly, if a group is not commutative, then it is either called a non-commutative group or non-abelian.

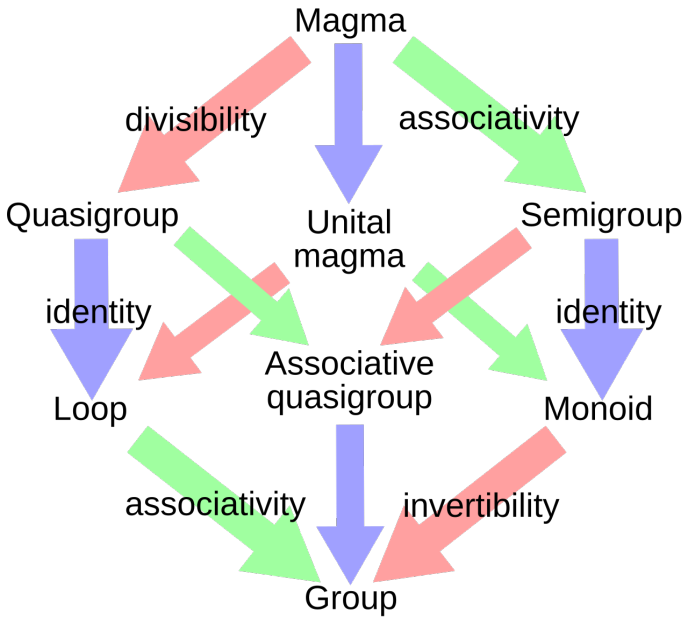


Figure 1.1: Types of pseudo-groups missing key parts.

As we shall see, a group is an extremely general object, this allows us to study seemingly different objects and associate them both with groups, then use those groups to derive similarities.

If you are curious about why we want these criteria for groups or what happens when certain criteria are dropped, I would recommend the Wikipedia page on algebraic structures; en.wikipedia.org/wiki/Algebraic_structure. The following image, pulled from that page, gives the names of the associated "pseudo-groups".

Question 1.1.4. Find/build an example of a group.

Question 1.1.5. Are the following groups? Are they abelian?

1. The set of rational numbers under ordinary addition.
2. The set of integers under multiplication.
3. The set of real numbers under multiplication.
4. The set $\{1, 2, \ldots, n-1\}$ under multiplication modulo n.

Example 1.1.6. The set of integers, rational numbers, and real numbers are all groups under ordinary addition. In each case, the identity is 0. △

Example 1.1.7. The set of integers under multiplication is not a group. It has an identity, 1, is associative, and is a closed operation, but it does not have inverses. △

Example 1.1.8. The set $\mathbb{R}^*$ of nonzero real numbers is a group under ordinary multiplication. The identity is 1 and the inverse of a is $1/a$. △

Example 1.1.9. The set

$$GL(2,\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in \mathbb{R}, ad-bc \neq 0 \right\}$$

under regular matrix multiplication forms a non-abelian group. △

The above groups is a very special non-abelian group called the general linear group of 2 by 2 matrices over the reals. We can generalize this to n by n matrices and it still holds as a group as long as the determinant is non-zero.

Example 1.1.10. The set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ for $n \geq 1$ is a group under addition modulo n. The inverse of j is $n - j$. △

Theorem 1.1.11 (Unique identity)**.** *In a group G, there is only one identity element.*

Theorem 1.1.12 (Cancellation laws)**.** *In a group G, the right and left cancellation laws hold; that is $ba = ca$ implies $b = c$, and $ab = ac$ implies $b = c$.*

Theorem 1.1.13 (Unique inverse)**.** *For each element a in a group G, there is a unique element $b \in G$ such that $ab = ba = e$*

Theorem 1.1.14 (Socks-shoes property)**.** *For group elements a and b, $(ab)^{-1} = b^{-1}a^{-1}$.*

1.2 Multiplication table

When working with finite groups, or infrequently infinite groups, it can be helpful to build the group's corresponding multiplication table. This is the same multiplication table you are probably thinking of for integers, now applied to an arbitrary set and an arbitrary group operation.

Example 1.2.1. The set $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ with the binary operation of multiplication mod p is a group denoted $U(p)$ when p is prime. We will prove this later. For now consider $U(7)$, it has the multiplication table in Figure 1.2

U(7)

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Figure 1.2: Multiplication table for $U(7)$

Cranking this up to $U(13)$ gives Figure 1.3.

U(13)

*	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	1	3	5	7	9	11
3	3	6	9	12	2	5	8	11	1	4	7	10
4	4	8	12	3	7	11	2	6	10	1	5	9
5	5	10	2	7	12	4	9	1	6	11	3	8
6	6	12	5	11	4	10	3	9	2	8	1	7
7	7	1	8	2	9	3	10	4	11	5	12	6
8	8	3	11	6	1	9	4	12	7	2	10	5
9	9	5	1	10	6	2	11	7	3	12	8	4
10	10	7	4	1	11	8	5	2	12	9	6	3
11	11	9	7	5	3	1	12	10	8	6	4	2
12	12	11	10	9	8	7	6	5	4	3	2	1

Figure 1.3: Multiplication table for $U(13)$

△

The multiplication table can tell you several things about the group, most importantly, if the generated matrix is symmetric then the corresponding group is commutative.

1.3 Subgroups

Definition 1.3.1 (Order of a group)**.** The number of elements of a group is called its *order*. We will use $|G|$ to denote the order of G.

Definition 1.3.2 (Order of an element)**.** The *order* of an element g in a group G is the smallest positive integer n such that $g^n = e$. If no such integer exists, we say that g has *infinite order*. The order of an element is denoted $|g|$.

Example 1.3.3. Consider $\mathbb{Z}_{10}$ under addition modulo 10. Since $2(5) = 0$ and 5 is the smallest integer to get 2 to 0 we know that $|2| = 5$. △

Definition 1.3.4 (Subgroup)**.** If a subset H of a group G is itself a group under the operation of G, we say that H is a *subgroup* of G. The notation $\leq$ ($<$) is used to denote a subgroup (proper subgroup).

The subgroup $\{e\}$ is called the *trivial subgroup*, any other subgroup is called *nontrivial*.

Note: A subgroup requires the same operation as the original group, so $\mathbb{Z}_n$ with the operation addition modulo n is not a subgroup of $\mathbb{Z}$ with usual addition.

Theorem 1.3.5 (One-step subgroup test)**.** *Let Gbe a group and H a nonempty subset of G. If ab^{-1} is in H whenever a and b are in H, then H is a subgroup of G.*

This is called the one-step subgroup test, however there are two things to check. First make sure that H is nonempty, then check that ab^{-1} is in H.

Example 1.3.6. Let G be a commutative group under multiplication with identity e. Then $H = \{x^2 \mid x \in G\}$ is a subgroup of G.

To prove this, first note that H is nonempty since $e^2 = e$. Now let $a^2, b^2 \in H$ such that $a, b \in G$, then we want to show that $a^2(b^2)^{-1} \in H$. To do this, note that

$$\begin{aligned} a^2(b^2)^{-1} &= aab^{-1}b^{-1} \\ &= (ab^{-1})(ab^{-1}) && \text{(Group is commutative)} \\ &= (ab^{-1})^2. \end{aligned}$$

Thus, $a^2(b^2)^{-1} = (ab^{-1})^2$ which is the square of some element in G giving that $a^2(b^2)^{-1} \in H$. △

Sometimes it is difficult to show that the operation is both closed under multiplication and inverses in the same step. To help with that, you can use the two-step subgroup test given below. Note that similar to the one-step subgroup test it takes 3 steps.

Theorem 1.3.7 (Two-step subgroup test)**.** *Let G be a group and let H be a nonempty subset of G. If ab is in H whenever a and b are in H, and a^{-1} is in H whenever a is in H, then H is a subgroup of G.*

When working with finite sets, you can use a simplified test given below. The idea for this test is that inverses are naturally given by the order of the elements in the set when those orders are finite.

Theorem 1.3.8 (Finite subgroup test)**.** *Let H be a nonempty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.*

Definition 1.3.9 (Center of a group)**.** The *center*, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G. That is

$$Z(G) = \{a \in G \mid ax = xa \text{ for all } x \in G\}.$$

Example 1.3.10. The center for $GL(n, \mathbb{R})$ (invertible matrices under ordinary matrix multiplication), is the set

$$\{sI_n \mid s \in \mathbb{R}^*\}.$$

△

Example 1.3.11. For any commutative group, the center is the group itself. △

Theorem 1.3.12. *The center of a group G is a subgroup of G.*

Definition 1.3.13 (Centralizer of a in G)**.** Let a be a fixed element of a group G. The *centralizer* of a in G, $C(a)$, is the set of all elements in G that commute with a. That is

$$C(a) = \{g \in G \mid ag = ga\}$$

Theorem 1.3.14. *For each a in a group G, the centralizer of a is a subgroup of G.*

1.4 Exercises

1. In the group $\mathbb{Z}_{12}$ (integers from 0 to 11 under addition modulo 12), find $|a|$, $|b|$, and $|a + b|$ for each of the following

   (a) $a = 6$, $b = 2$
   (b) $a = 3$, $b = 8$
   (c) $a = 5$, $b = 4$

   Does there seem to be any relationship between $|a|$, $|b|$, and $|a + b|$?

2. If a, b, and c are group elements and $|a| = 6$ and $|b| = 7$, then express $(a^4c^{-2}b^4)^{-1}$ without using negative exponents.

3. Prove in any group, an element and its inverse have the same order.

4. For any group elements a and b, prove that $|ab| = |ba|$.

5. Prove that a group with two elements of order 2 that commute must have a subgroup of order 4.

6. Let $H = \{a + bi | a, b \in \mathbb{R}, ab \geq 0\}$. Prove or disprove that H is a subgroup of $\mathbb{C}$ (complex numbers) under addition.

1.5 Solutions

1. In the group $\mathbb{Z}_{12}$ (integers from 0 to 11 under addition modulo 12), find $|a|$, $|b|$, and $|a+b|$ for each of the following

   (a) $a = 6$, $b = 2$

   To find, $|a|$ we want to find the n such that a^n or na equals e. We can directly compute this

   $$a^1 = 6$$
   $$a^2 = 12 \bmod 12 = 0$$

   Similarly for b gives

   $$b^1 = 2$$
   $$b^2 = 4$$
   $$b^3 = 6$$
   $$b^4 = 8$$
   $$b^5 = 10$$
   $$b^6 = 0.$$

   Thus $|a| = 2$ and $|b| = 6$.

   (b) $a = 3$, $b = 8$

   Take a similar approach to part (a) giving

   $$a^1 = 3$$
   $$a^2 = 6$$
   $$a^3 = 9$$
   $$a^4 = 12 \bmod 12 = 0$$

   and

   $$b^1 = 8$$
   $$b^2 = 16 \bmod 12 = 4$$
   $$b^3 = 24 \bmod 12 = 0.$$

   This gives $|a| = 4$ and $|b| = 3$.

   (c) $a = 5$, $b = 4$

Again similar to part (a) we have

$$\begin{aligned} a^1 &= 5 \\ a^2 &= 10 \\ a^3 &= 15 \bmod 12 = 3 \\ a^4 &= 20 \bmod 12 = 8 \\ a^5 &= 25 \bmod 12 = 1 \\ a^6 &= 30 \bmod 12 = 6 \\ a^7 &= 35 \bmod 12 = 11 \\ a^8 &= 40 \bmod 12 = 4 \\ a^9 &= 45 \bmod 12 = 9 \\ a^{10} &= 50 \bmod 12 = 2 \\ a^{11} &= 55 \bmod 12 = 7 \\ a^{12} &= 60 \bmod 12 = 0 \end{aligned}$$

and

$$\begin{aligned} b^1 &= 4 \\ b^2 &= 8 \\ b^3 &= 12 \bmod 12 = 0. \end{aligned}$$

This gives that $|a| = 12$ and $|b| = 3$. We will talk about a in the next section, but a forms a generator for the group.

Does there seem to be any relationship between $|a|$, $|b|$, and $|a + b|$?

In general there is no connection between $|a|$, $|b|$, and $|a + b|$.

2. If a, b, and c are group elements and $|a| = 6$ and $|b| = 7$, then express $(a^4c^{-2}b^4)^{-1}$ without using negative exponents.

   First we can apply the socks and shoes theorem to distribute the inverse, this gives

   $$(a^4c^{-2}b^4)^{-1} = b^{-4}c^2a^{-4}.$$

   Now consider b^{-4}, following $|b| = 7$ we know that $b^{-1} = b^6$. Taking this 4 times gives

   $$b^{-4} = (b^6)^4 = b^{36} = b^35b = (b^7)^5b = e^5b = b.$$

   A similar argument for a gives

   $$a^{-4} = (a^5)^4 = a^{20} = (a^6)^3a^2 = a^2.$$

   Substituting these in gives $b^{-4}c^2a^{-4} = bc^2a^2$.

3. Prove, in any group, an element and its inverse have the same order.

Proof. Let $a \in G$ such that $|a| = n$ and $|a^{-1}| = m$, then $a^{-1} = a^{n-1}$. Now, $(a^{-1})^m = a^{-m} = e$ gives that $a^{-m+1} = (a^{-1})^{-1} = a$. Thus, we have

$$aa^{-1} = e \implies a^{-m+1}a^{n-1} = e \implies -m + 1 + n - 1 = 0 \implies m = n.$$

□

4. For any group elements a and b, prove that $|ab| = |ba|$.

Proof. Let $a, b \in G$ with $|ab| = n$ and $|ba| = m$, then

$$\begin{aligned}(ba)^m = e &\implies b(ab)^{m-1}a = e \\ &\implies (ab)^{m-1} = b^{-1}a^{-1} \\ &\implies (ab)^{m-1} = (ab)^{-1}.\end{aligned}$$

Also note that following $|ab| = n$ we have $(ab)^n = e$ giving that $(ab)^{n-1} = (ab)^{-1}$. Thus, we have that

$$(ab)^{m-1} = (ab)^{-1} = (ab)^{n-1}$$

which gives that $m = n$. □

5. Prove that a group with two elements of order 2 that commute must have a subgroup of order 4.

Let $a, b \in G$ such that $a^2 = e$, $b^2 = e$, and $ab = ba$. Consider now the set $\{e, a, b, ab\}$ with the group operation, call this H. We will prove that this forms a subgroup.

Proof. First H is nonempty since it has 4 elements in it. Now we can apply the finite subgroup test. Here are all the possible combinations,

$$\begin{aligned}aa = e \in H \\ ab \in H \\ a(ab) = eb = b \in H \\ ba = ab \in H \\ bb = e \in H \\ b(ab) = ab^2 = a \in H.\end{aligned}$$

Thus H is closed under the operation, giving that it is a subgroup of G. □

6. Let $H = \{a + bi | a, b \in \mathbb{R}, ab \geq 0\}$. Prove or disprove that H is a subgroup of $\mathbb{C}$ (complex numbers) under addition.

   H is not a subgroup of the complex numbers under addition.

   Proof. Consider $10 + 1i$ and $-1 - 10i$ where we can see that both are in H. Now $(10 + 1i) + (-1 - 10i) = 9 - 9i \notin H$ following $9(-9) < 0$. □

Chapter 2

Special types of groups

2.1 Cyclic groups

Definition 2.1.1 (Cyclic group)**.** A group G is called *cyclic* if there is an element a in G such that $G = \{a^n \mid n \in \mathbb{Z}\}$.

The element a is called the *generator* of G and we denote $\langle a \rangle$ to be equal to G.

Example 2.1.2. The group $\mathbb{Z}_n$ for $n \geq 1$ is a cyclic under addition modulo n. The generator 1 is always an option, but there may be more depending on the value of n.

The group $\mathbb{Z}_8$ has the generators 1,3,5,7. You can verify this by taking powers (multiplication) of these numbers to see that they generate the whole set. △

Theorem 2.1.3. *Let G be a group, and let a belong to G, then we have the following two statements based on the order of a.*

1. *If a has infinite order, then $a^i = a^j$ if and only if $i = j$.*
2. *If a has a finite 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 $i - j$.*

Proof. If a has infinite order, note that $a^i = a^j$ implies, $a^{i-j} = e$ which gives that $i = j$. Doing the same in reverse gives the result.

Assume $|a| = n$. Note first that the elements $e, a, \ldots, a^{n-1}$ are in $\langle a \rangle$. Now let a^k be some element in $\langle a \rangle$. By the division algorithm, there exists integers q and r such that

$$k = qn + r \text{ with } 0 \leq r < n.$$

Then $a^k = a^{qn}a^r = a^r$. This gives that $a^k \in \{e, a, \ldots, a^{n-1}\}$.

Next, we assume that $a^i = a^j$ and we want to prove that n divides $i - j$. We begin by observing that $a^i = a^j$ implies $a^{i-j} = e$. We will again use the division algorithm, this time on $i - j$ giving

$$i - j = qn + r \text{ with } 0 \leq r < n.$$

Then $a^{i-j} = a^r$ by similar logic to above. However, $a^{i-j} = e$ and n thus $a^r = e$. Therefore, $i - j = qn$ giving that n divides $i - j$. □

Corollary 2.1.4. *For any group element a, $|a| = |\langle a \rangle|$.*

Corollary 2.1.5. *Let G be a group and let a be an element of order n in G. If $a^k = e$, then n divides k.*

Corollary 2.1.6. *If a and b belong to a finite group and $ab = ba$, then $|ab|$ divides $|a||b|$.*

Theorem 2.1.7. *Let a be an element of order n in a group and let k be a positive integer. Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n,k)$.*

Corollary 2.1.8. *In a finite cyclic group, the order of an element divides the order of the group.*

Corollary 2.1.9. *Let $|a| = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ if and only if $\gcd(n,i) = \gcd(n,j)$, and $|a^i| = |a^j|$ if and only if $\gcd(n,i) = \gcd(n,j)$.*

Corollary 2.1.10. *An integer k in $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ if and only if $\gcd(n,k) = 1$.*

Theorem 2.1.11 (Fundamental theorem of cyclic groups)**.** *Let G be a cyclic group, then the following three statements hold.*

1. *Every subgroup of G is cyclic.*
2. *If $|G| = n$, then the order of any subgroup divides n.*
3. *If $|G| = n$, then for any $k|n$, the subgroup $\langle a^{n/k} \rangle$ is the unique subgroup of order k.*

Proof. (1) Let $H \leq G$. If $H = \{e\}$ then we're done so, assume $H \neq \{e\}$. Choose $a^m \in H$ with $m \leq n$. Clearly $\langle a^m \rangle \leq H$. For any, $a^k \in H$ we can put $k = qm + r$ with $0 \leq r < m$ so $r = k - qm$ and then $a^r = a^k (g^m)^{-q} \in H$ and so $r = 0$. Now $a^k = (a^m)^q$ and hence $a^k \in \langle a^m \rangle$.

(2) Suppose that $G = \langle a \rangle$, $|G| = n$, and that H is a subgroup of G, then by part (1) we have that $H = \langle a^m \rangle$, where m is the least positive integer such that $a^m \in H$. By the same argument as in part (1) with a^n instead of a^k we have that $a^n = a^{mq}$ which implies m divides n.

(3) Let k be a positive divisor of n. From Theorem 2.1.7 the group $\langle a^{n/k} \rangle$ has order

$$\frac{n}{\gcd(n, n/k)} = \frac{n}{n/k} = k.$$

Now to show it is unique, let $H = \langle a^m \rangle$ be any subgroup of order k. By part (2) we know that m is a divisor of n. This gives $m = \gcd(n,m)$ and by Theorem 2.1.7

$$k = |a^m| = |a^{\gcd(n,m)}| = \frac{n}{\gcd(n,m)} = \frac{n}{m}.$$

Thus $m = n/k$ giving that $H = \langle a^m \rangle = \langle a^{n/k} \rangle$. □

Corollary 2.1.12. *For each positive divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k. Moreover, these subgroups are all the subgroups of $\mathbb{Z}_n$.*

Definition 2.1.13. Let $\phi(n)$ denote the *Euler totient function.* Define $\phi(1) = 1$, and for any $n > 1$ define $\phi(n)$ to be the number of positive integers less than n that are relatively prime to n.

Theorem 2.1.14. *If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.*

Corollary 2.1.15. *In a finite group, the number of elements of order d is a multiple of $\phi(d)$.*

2.1.1 Exercises

1. Find all the generators of $\mathbb{Z}_6$, $\mathbb{Z}_8$, and $\mathbb{Z}_{20}$.
2. List all the elements of order 8 in $\mathbb{Z}_{8000000}$. How do you know your list is complete?
3. Let G be a group and let a be an element of G.
   (a) If $a^{12} = e$, what can we say about the order of a?
   (b) Suppose that $|G| = 24$ and that G is cyclic. If $a^8 \neq e$ and $a^{12} \neq e$, show that $\langle a \rangle = G$.
4. Prove that a group of order 3 must be cyclic.
5. Let G be a group with $a \in G$. Prove that $\langle a \rangle = \langle a^{-1} \rangle$.

2.1.2 Solutions

1. Find all the generators of $\mathbb{Z}_6$, $\mathbb{Z}_8$, and $\mathbb{Z}_{20}$.

   The generators of $\mathbb{Z}_6$ are $1, 5$, we can see this by applying Theorem 2.1.7 and looking for values where the gcd is 1.

   The generators of $\mathbb{Z}_8$ are $1, 3, 5, 7$.

   The generators of $\mathbb{Z}_{20}$ are $1, 3, 9, 7, 11, 13, 17, 19$

2. List all the elements of order 8 in $\mathbb{Z}_{8000000}$. How do you know your list is complete?

   The elements of order 8 in $\mathbb{Z}_{8000000}$ can be found using the fundamental theorem of cyclic groups part (3). In this case, we will want

   $$\langle 1^{8000000/8} \rangle = \langle 1^{1000000} \rangle = \{0, 1000000, 2000000, \ldots, 7000000\}.$$

   From this group we can take the generators which are

   $$1000000, 3000000, 5000000, \text{ and } 7000000.$$

3. Let G be a group and let a be an element of G.

   (a) If $a^{12} = e$, what can we say about the order of a?

   First, we can say that the order of a is less than or equal to 12.

   Next by Theorem 2.1.3 we know that either the order of a is 12 or the real order n divides 12. In this case that leaves $1, 2, 3, 4, 6, 12$ as possible orders.

   (b) Suppose that $|G| = 24$ and that G is cyclic. If $a^8 \neq e$ and $a^{12} \neq e$, show that $\langle a \rangle = G$.

   First note that following $a^8 \neq e$ we know that $|a| \neq 1, 2, 4, 8$ since any of those orders share a common factor with 8 and would cause $a^8 = e$. Next note that following $a^{12} \neq e$ we know that $|a| \neq 1, 2, 3, 4, 6, 12$. This leaves $5, 7, 9, 10, 11, 13, \ldots, 24$ as possible orders of a. However, by the fundamental theorem of cyclic groups the order of the subgroup must divide 24. In this case only 24 does that so $|a| = 24$ which implies $\langle a \rangle = G$.

4. Prove that a group of order 3 must be cyclic.

   Proof. Consider the set $\{1, 2, 3\}$ and let 1 be the identity element. Now, either $2^2 = 3$ or $2^2 = 1$. In the former case, the group is cyclic since the order of every element in a finite group must be less than the size of the group, giving that $2^3 = 1$. In the latter case, we can take the same approach on 3. This leaves the case where $2^2 = 1$ and $3^2 = 1$. In this case, consider ab in either of the three cases where it gets mapped, we have either a or b acting as the identity. Following the identity is unique, this must really be a group of two elements, which is a contradiction. □

5. Let G be a group with $a \in G$. Prove that $\langle a \rangle = \langle a^{-1} \rangle$.

   Proof. Last class we proved that a and a^{-1} have the same order. Thus, the result follows by the fundamental theorem of cyclic groups part (3) and by Corollary 2.1.4. □

2.2 Permutation groups

Definition 2.2.1. A *permutation* of a set A is a bijection from A to A.

Definition 2.2.2. A *permutation group* of a set A is a set of permutations of A that forms a group under function composition.

Example 2.2.3. We could define a permutation α on the set $\{1, 2, 3, 4\}$ by specifying

$$\alpha(1) = 2, \quad \alpha(2) = 3, \quad \alpha(3) = 1, \quad \alpha(4) = 4.$$

A more convenient way to express this correspondence is to write α in array from as

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}.$$

In this notation the top line is the starting point and the bottom line is where they are sent. △

2.2.1 Cycle notation

A permutation always breaks the set-up into distinct cycles. Because of this, we can use a further shorthand when writing out permutations called cycle notation. To see this, consider the permutation

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}.$$

In cycle notation this could be written as $\alpha = (1, 2)(3, 4, 6)(5)$ since we have a cycle between 1 and 2, a cycle between 3,4,6, and a cycle between 5. When we have cycles of length 1 we drop them. Thus, we would write this as $\alpha = (1, 2)(3, 4, 6)$. Finally, if it does not cause ambiguity we can drop the commas, leaving $\alpha = (12)(346)$.

In this form, an expression of the form $(a_1 a_2 \dots a_m)$ is a cycle of length m or m-cycle.

To compose permutations we write out all of their cycles then moving from right to left attempt to simplify them such that they are in cycle disjoint form, no element can be in multiple cycles. To do this take each element in the set and tracing it from right to left, see where it ends. This will build the beginnings of a cycle. Once that cycle loops back on itself, start a new one until all elements are represented.

Example 2.2.4. Consider

$$\alpha = (13)(27)(456)(8) \text{ and } \beta = (1237)(648)(5)$$

in the set $\{1, 2, \dots, 8\}$. To compose $\alpha\beta$ first write out their cycles

$$\alpha\beta = (13)(27)(456)(8)(1237)(648)(5).$$

Now for each element we will move right to left. So first note that 1 goes to 2 in the third from right cycle. Then 2 goes to 7 in the second to last cycle. Thus, when building the composition we take (17 to start. Now we track where 7 goes. In this case, 7 goes to 1 and 1 goes to 3. Giving (173. Continue this process for all 8 elements yields the composition (1732)(48)(56). △

2.2.2 Properties of permutations

Theorem 2.2.5. *Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.*

Theorem 2.2.6. *If the pair of cycles $\alpha = (a_1, \ldots, a_m)$ and $\beta = (b_1, \ldots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.*

Proof. Let $\alpha = (a_1, \ldots, a_m)$ and $\beta = (b_1, \ldots, b_n)$ be disjoint permutations of a set

$$S = \{a_1, \ldots, a_m, b_1, \ldots, b_n, c_1 \ldots, c_k\}$$

where the c_j are fixed by both α and β. To prove $\alpha\beta = \beta\alpha$ we need to show that they are equal for every value $x \in S$. We will proceed by cases. If $x = a_i$, then

$$\alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1},$$

since β fixes all a_i elements. For the same reason,

$$\beta(\alpha(a_i)) = \beta(a_{i+1}) = a_{i+1}.$$

A similar argument shows that if $x = b_i$ the commutativity holds. Finally, if $x = c_i$ we have

$$\alpha(\beta(c_i)) = c_i = \beta(\alpha(c_i))$$

since both α and β fix c_i. □

Theorem 2.2.7 (Order of a permutation)**.** *The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.*

Example 2.2.8. Consider the following examples for the set $\{1, 2, \ldots, 8\}$,

$$\begin{aligned} |(132)(45)| &= 6 \\ |(1432)(56)| &= 4 \\ |(123)(456)(78)| &= 6 \\ |(123)(145)| = |(14523)| &= 5. \end{aligned}$$

△

2.2.3 Even odd permutations

Theorem 2.2.9. *Every permutation in S_n, $n > 1$, is a product of 2-cycles.*

Proof. Consider $\alpha = (a_1, \ldots a_n)$, then a direct computation shows that

$$\alpha = (a_1 a_n)(a_1 a_{n-1}) \ldots (a_1 a_2).$$

□

Theorem 2.2.10. *If a permutation α can be expressed as a product of an even (odd) number of 2-cycles, then every decomposition of α into a product of 2-cycles must be even (odd).*

Definition 2.2.11. A permutation that can be expressed as a product of an even number of 2-cycles is called an *even* permutation. A permutation that be expressed as an odd number of 2-cycles is called an *odd* permutation.

Note that by Theorem 2.2.10 every permutation can be uniquely defined as either odd or even.

2.3 Symmetric groups

Definition 2.3.1. Let $n \in \mathbb{N}$. Let $X = \{1, \ldots, n\}$, then, the *symmetric group*, S_n, is the set of all permutations from X to X with the binary operation is the composition of permutations.

Theorem 2.3.2. *For $n \in \mathbb{N}$, $|S_n| = n!$.*

Proof. The number of elements in S_n is equal to the number of permutations of n elements. For counting the number of permutations, we will follow a combinatorial approach. First, note that we have n places to map the first element. Next, with that first spot picked, we have $n-1$ remaining choices for the second element to get mapped to. Continuing this process gives $n(n-1)(n-2)\ldots(2)(1)$ choices. □

Example 2.3.3. The set S_3 is all bijections of the set $\{1, 2, 3\}$ with function composition as its group action. The six elements are

$$
\begin{aligned}
e &= \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} \\
\alpha &= \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \\
\alpha^2 &= \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \\
\beta &= \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \\
\alpha\beta &= \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \\
\alpha^2\beta &= \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}.
\end{aligned}
$$

Note that, $\beta\alpha \neq \alpha\beta$ so S_3 is non-commutative. △

Example 2.3.4. Determine the possible orders of elements of S_7.

Note first that there are $7! = 5040$ elements in S_7 so checking them all by hand is impractical. Instead to do this, we can use Theorem 2.2.7 and look at the different possible cycle lengths. We will abbriviate an n-cycle by (n). This

gives

$$
\begin{array}{l}
(7)\\
(6)(1)\\
(5)(2)\\
(5)(1)(1)\\
(4)(3)\\
(4)(2)(1)\\
(4)(1)(1)(1)\\
(3)(3)(1)\\
(3)(2)(2)\\
(3)(2)(1)(1)\\
(3)(1)(1)(1)(1)\\
(2)(2)(2)(1)\\
(2)(2)(1)(1)(1)\\
(2)(1)(1)(1)(1)(1)\\
(1)(1)(1)(1)(1)(1)(1)
\end{array}
$$

Going down the list the unique least common multiples are 7, 6, 10, 5, 12, 4, 3, 2, and 1. Thus, the possible orders of the elements of S_7 are

$$1, 2, 3, 4, 5, 6, 7, 10, 12.$$

△

Theorem 2.3.5. *The set of even permutations in S_n forms a subgroup of S_n.*

2.3.1 Exercises

1. Let
$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix} \text{ and } \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{bmatrix}.$$
Compute each of the following
   (a) α^{-1}
   (b) $\beta\alpha$
   (c) $\alpha\beta$

2. Write each of the following permutations as a product of disjoint cycles
   (a) (1235)(413)
   (b) (13256)(23)(46512)
   (c) (12)(13)(23)(142)

3. What are the possible orders for the elements in S_6?

4. Suppose α is a mapping from a set S to itself such that $\alpha(\alpha(x)) = x$ for all x in S. Prove that α is a bijection.

5. Give two reasons why the set of odd permutations in S_n do not form a subgroup.

6. If α is an even permutation of S_n, then prove that α^{-1} is an even permutation.

   If α is an odd permutation of S_n, then prove that α^{-1} is an odd permutation.

2.3.2 Solutions

1. Let
$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix} \text{ and } \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{bmatrix}.$$
   Compute each of the following

   (a) α^{-1}

   For computing α^{-1} we can think of flipping the matrix then sorting the top row entries. This gives
$$\alpha^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix}.$$

   (b) $\beta\alpha$

   For computing $\beta\alpha$ we have a couple of approachs. First we can turn these into cycle notation and follow the example in the above section. Another way is to think of stacking the matrices, then tracing downwards where the values go. This gives
$$\beta\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 2 & 3 & 4 & 5 \end{bmatrix}.$$

   (c) $\alpha\beta$

   Same as the previous part, but now take β first giving
$$\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 1 & 5 & 3 & 4 \end{bmatrix}.$$

2. Write each of the following permutations as a product of disjoint cycles

(a) (1235)(413)

Here we take the same approach as the example in this section. First see where 1 gets mapped to. From the right most cycle it goes to 3, then from the other cycle 3 goes to 5. Giving (15 as our starting piece. Do the same for the rest of the elements giving

$$(1235)(413) = (15)(234).$$

(b) (13256)(23)(46512)

Same as the previous part yielding

$$(13256)(23)(46512) = (124)(35).$$

(c) (12)(13)(23)(142)

Same as part 1 giving

$$(12)(13)(23)(142) = (14)(13).$$

3. What are the possible orders for the elements in S_6?

   This is very similar to the example we did. We want to use the fact that the order of a permutation is the least common multiple of the cycle lengths. So writing out all the possible cycle lengths for 6 gives

   $$\begin{gathered}(6)\\(5)(1)\\(4)(2)\\(4)(1)(1)\\(3)(3)\\(3)(2)(1)\\(3)(1)(1)(1)\\(2)(2)(2)\\(2)(2)(1)(1)\\(2)(1)(1)(1)(1)\\(1)(1)(1)(1)(1)(1)\end{gathered}$$

   The unique options for least common multiple are then $1, 2, 3, 4, 5, 6$ which are our possible orders.

4. Suppose α is a mapping from a set S to itself such that $\alpha(\alpha(x)) = x$ for all x in S. Prove that α is a bijection.

Proof. To prove a bijection, we need to show that it is one-to-one and onto. For one-to-one let $x, y \in S$ such that $\alpha(x) = \alpha(y)$, then consider taking α of both sides. Since α is a well-defined function, we know that will map both to the same place. This gives,

$$\alpha(x) = \alpha(y) \implies \alpha(\alpha(x)) = \alpha(\alpha(y)) \implies x = y.$$

Hence, α is one-to-one.

For onto, let $y \in S$, the let $x = \alpha(y)$. Again taking α of both sides gives $\alpha(x) = y$. Thus, we can reach every point in S by α giving that α is onto. □

5. Give two reasons why the set of odd permutations in S_n do not form a subgroup.

   First consider the identity permutation, e. We can express it as

   $$e = (12)(12)(13)(13)\cdots(1n)(1n).$$

   This is an even permutation, and hence the first reason the set of odd permutation do not form a group is that they are missing the identity element.

   Next, let α, β be two odd length permutations. Then $\alpha\beta$ can be expressed by the odd number of α 2-cycles followed by the odd number of β 2-cycles. Since an odd plus an odd is even, this implies that the composition of two odd permutations is even. Thus, the second reason it is not a subgroup is not being closed under the operation of function composition.

6. If α is an even permutation of S_n, then prove that α^{-1} is an even permutation.

   If α is an odd permutation of S_n, then prove that α^{-1} is an odd permutation.

   Proof. If α is an even permutation, then first note that $\alpha\alpha^{-1} = e$ which is an even permutation. Hence, we have an even number times a number giving an even number. Thus α^{-1} is even.

   Similarly, if α is an odd permutation, then $\alpha\alpha^{-1} = e$ is even. This forces α^{-1} to be odd, since we have an odd times a number is even. □

2.4 Alternating groups

Definition 2.4.1. The *alternating groups*, A_n, are the set of all even permutations associated with composition.

Theorem 2.4.2. *A_n is a subgroup of the symmetric group S_n.*

Example 2.4.3. The alternating group of three elements can be described using cycle notation as the permutations

$$A_3 = \{(1), (123), (321)\}$$

△

Theorem 2.4.4. *The order of A_n is $n!/2$.*

The names for the symmetric group and alternating group come from the study of polynomials. A multivariable polynomial is called symmetric if we can swap any of the variables without changing the polynomial, consider $p(x, y, z) = xyz$. An alternating polynomial is then one where changing any variable causes the polynomial to change sign, consider $f(x, y, z) = (x - y)(x - z)(y - z)$.

The alternating groups will play an important role later, as we shall see they are one of the fundamental building blocks of finite groups.

Theorem 2.4.5. *The alternating group is non-commutative for $n \geq 4$.*

Proof. Consider, A_4 which is defined as the permutations

$$e,\ (12)(34),\ (13)(24),\ (14)(23),\ (123),\ (124),$$
$$(134),\ (234),\ (432),\ (431),\ (421),\ (321)$$

of $\{1, 2, 3, 4\}$.

Let $a = (12)(34)$ and $b = (41)(42)$. Their products are then

$$ab = (12)(34)(41)(42) = (1342)$$

and

$$ba = (41)(42)(12)(34) = (1432).$$

Thus $ab \neq ba$ for $n = 4$. Now for A_n with $n > 4$ note that the elements of A_4 (with the rest of the entries fixed) are all in A_n. Thus A_n is non-commutative for $n \geq 4$. □

2.5 Dihedral groups

Definition 2.5.1. The *dihedral group* D_n is defined to be the group of possible symmetries of a n sided regular polygon. We can view this symbolically as

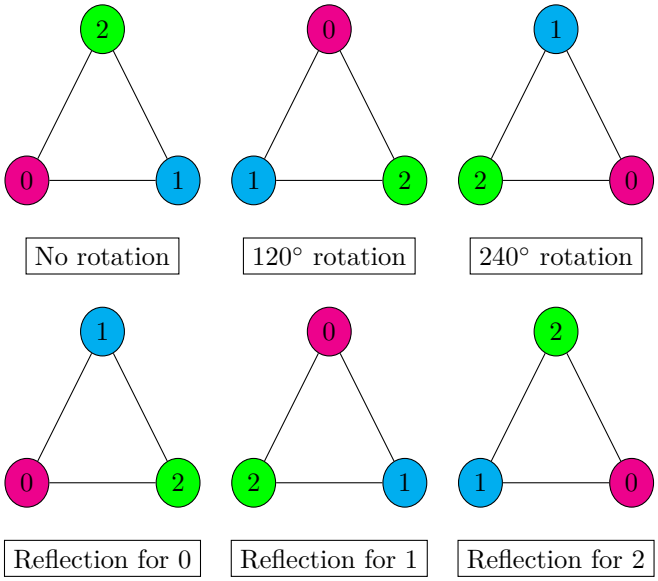
$$D_n = \{r, s \mid s^2 = e, r^n = e, srs = r^{-1}\} = \{e, r, r^2, r^3, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}.$$

Example 2.5.2. For D_3 we can express it as

$$D_3 = \{e, r, r^2, s, rs\}$$

Geometrically, we can view this where r is a 120-degree rotation of an equilateral triangle. The element s would then be a reflection across one of the vertices.

There should be three of these reflections, but instead you can rotate then reflect. This is captured through rs. Visually, we can see all these group elements below.



△

Theorem 2.5.3. *Dihedral groups are non-commutative for $n \geq 3$.*

The proof is similar to why the alternating groups are non-commutative. There is an example at $n = 3$, then all larger values of n have this as part of them.

Theorem 2.5.4. *For the dihedral group D_n and elements r, s as from the definition, we have the following*

1. $r^k s = sr^{-k}$.
2. *The order of r^k is $n/\gcd(k, n)$.*

Proof. For the first piece, we have

$$r^k s = er^k s = s^2 r^k s = ssr^k s = sr^{-k}.$$

Now for part 2. We will show that $r^k = e$ if and only if $n|k$. To do this, let $k \in \mathbb{Z}$ such that $r^k = e$, then by the division algorithm $k = qn + s$. This gives,

$$e = r^k = r^{qn} r^s = er^s = r^s$$

which implies $s = 0$ since n is the order of r. Thus $n|k$. Conversely, let $k = nq$, then the result follows from $r^k = r^{nq} = e$. Finally, note that by the definition of greatest common divisor $m = n/\gcd(k, n)$ is the smallest number such that $n|km$. □

2.5.1 Exercises

1. Let $\beta = (123)(145)$. Write β^{99} in disjoint cycle form.
2. Show that A_5 has 24 elements of order 5, 20 elements of order 3, and 15 elements of order 2.
3. Viewing D_4 as the symmetries of a square with vertices labeled, $1, 2, 3, 4$ what are the symmetries that correspond to even permutations?
4. Determine integers n for which $H = \{\alpha \in A_n \mid \alpha^2 = e\}$ is a subgroup of A_n.
5. Find the center of D_n.

2.5.2 Solutions

1. Let $\beta = (123)(145)$. Write β^{99} in disjoint cycle form.

   First we need to make β in disjoint cycle form, which is $\beta = (14523)$. Now we know that $\beta^5 = e$ by Theorem 2.2.7. With this

   $$\beta^{99} = \beta^{95}\beta^4 = \beta^4 = \beta^{-1} = (13254).$$

2. Show that A_5 has 24 elements of order 5, 20 elements of order 3, and 15 elements of order 2.

   The group A_5 has 60 elements, so we can't easily write them all out. First consider all the elements of S_5 as we have done in previous examples, this gives the partition list

   (5)
   (4)(1)
   (3)(2)
   (3)(1)(1)
   (2)(2)(1)
   (2)(1)(1)(1)
   (1)(1)(1)(1)(1)

   All the 5 cycles are in A_5 this is because they can all be written as $(a_1a_5)(a_1a_4)(a_1a_3)(a_1)(a_2)$ which is even. Now to count the number of those we have the first element can get mapped anywhere but itself, this leaves 4 choices, the second element can get mapped anywhere but itself and back giving 3 choices. Continuing, this gives $4! = 24$ order 5 elements.

   We know the elements with partition (4)(1) are not in A_5 by the same construction as above. Similarly, for (3)(2) elements. Now (3)(1)(1) is

open. For it, we have 5 choices for the first fixed element, and 4 choices for the next one. Once these are picked, there is only one cycle that works. Hence, there are 20 elements of order 3.

Finally, for the order 2 elements, we only need to consider the (2)(2)(1) options. Here we can count them by taking the 5 ways to pick the solo element times the 3 choose 2 ways of picking the other 4 (it is 3 choose 2 since we always lock in 1 element). This gives 15 options of order 2.

3. Viewing D_4 as the symmetries of a square with vertices labeled, $1, 2, 3, 4$ what are the symmetries that correspond to even permutations?

   Applying one or three rotations results in a 4-cycle, which works out to be odd. However, two rotations work. If we apply a flip across the 1 diagonal it works, and if we flip across the 4 diagonal it works. The other flips do not. This gives the symmetries

   $$e, r^2, s, r^2 s.$$

4. Determine integers n for which $H = \{\alpha \in A_n \mid \alpha^2 = e\}$ is a subgroup of A_n.

5. Find the center of D_n.

Chapter 3

Group morphisms and combining groups

3.1 Definitions

Definition 3.1.1. (Homomorphism) Let G and H be groups. A *homomorphism* from G to H is a function $\phi : G \to H$ such that

$$\phi(gh) = \phi(g)\phi(h) \quad \text{for all } g, h \in G.$$

Example 3.1.2. Let $G = (\mathbb{Z}, +)$ and $H = (\mathbb{Z}_n, +)$, then define $\phi : G \to H$ such that $\phi(x) = x \bmod n$. We have then that ϕ is a homomorphism.

To show this, consider

$$\phi(x + y) = x + y \bmod n = \phi(x) + \phi(y).$$

Note that ϕ is onto but not one-to-one. △

Definition 3.1.3. (Isomorphism) Let G and H be groups. An *isomorphism* from G to H is a function $\phi : G \to H$ that is a homomorphism and a bijection.

Definition 3.1.4. (Automorphism) Let G be a group and ϕ be an isomorphism from G to itself, then ϕ is called an *automorphism*.

Example 3.1.5. Let $G = (\mathbb{R}, +)$ and $H = (\mathbb{R}^+, \times)$ (positive real numbers under multiplication), then define $\phi : G \to H$ to be $\phi(x) = 2^x$. We have then that ϕ is an isomorphism from G to H.

To show one-to-one consider $x, y \in G$ such that $2^x = 2^y$, then $\log_2(2^x) = \log_2(2^y)$ giving that $x = y$. To show onto, let y be some positive real number, then define $x = \log_2(y)$ and we have that $\phi(x) = y$. Finally, to show it is operation preserving, we have

$$\phi(x + y) = 2^{x+y} = 2^x 2^y = \phi(x)\phi(y)$$

for all $x, y \in G$. △

Procedure 3.1.6. There are 4 steps to proving that two groups, G and H, are isomorphic.

1. Define a candidate mapping, ϕ, from G to H.
2. Prove that ϕ is one-to-one.
3. Prove that ϕ is onto.
4. Prove that ϕ is operation preserving, that is $\phi(a)\phi(b) = \phi(ab)$ for all $a, b \in G$.

For a homomorphism, we just need steps 1 and 4. △

Definition 3.1.7. Two groups G, H are called *isomorphic* (*homeomorphic*) if there exists an isomorphism (homomorphism) between them. This is denoted $G \cong H$.

I tend to think of a homomorphism as an embedding of G into H. We may lose information in this process, but some properties that we care about might still be there. An isomorphism is more of a comparison, showing that we can embed each group into each other in a way that no information is lost.

3.2 Properties of isomorphisms

Theorem 3.2.1 (Properties of isomorphisms acting on elements.)**.** *Let G, H be groups and ϕ be a isomorphism from G to H, then*

1. *$\phi(e_1) = e_2$, where e_1 is the identity of G and e_2 is the identity of H.*
2. *$\phi(g^n) = \phi(g)^n$, $n \in \mathbb{Z}$ and $g \in G$.*
3. *$gh = hg$ if and only if $\phi(g)\phi(h) = \phi(h)\phi(g)$ for all $g, h \in G$.*
4. *If G is finite, then G and H have exactly the same number of elements of finite order.*

Theorem 3.2.2 (Properties of isomorphisms acting on Groups)**.** *Let G, H be groups and ϕ be a isomorphism from G to H, then*

1. *ϕ^{-1} is an isomorphism from H to G.*
2. *G is commutative if and only if H is commutative.*
3. *G is cyclic if and only if H is cyclic.*
4. *If K is a subgroup of G, then $\phi(K) = \{\phi(k) \mid k \in K\}$ is a subgroup of H.*
5. *$\phi(Z(G)) = Z(H)$.*

Corollary 3.2.3. *Let G, H be groups and ϕ be a homomorphism from G to H. If $g \in G$ has finite order, then $\phi(g)$ has finite order and $|\phi(g)|$ divides $|g|$.*

Theorem 3.2.4. *Let G be a group with $g \in G$, then*

1. *If $|g|$ is infinite, then $\langle g \rangle \cong (\mathbb{Z}, +)$.*
2. *If $|g| = n$ is finite, then $\langle g \rangle \cong \mathbb{Z}_n$.*

Theorem 3.2.5. *(Cayley's theorem) Every group is isomorphic to a group of permutations.*

3.2.1 Exercises

1. Find an isomorphism from the group of integers under addition to the group of even integers under addition.
2. Let G be a group. Prove that the mapping $\alpha(g) = g^{-1}$ for all $g \in G$ is an automorphism if and only if G is commutative.
3. Let ϕ be an automorphism of a group G. Prove that $H = \{x \in G \mid \phi(x) = x\}$ is a subgroup of G.
4. Give an example of a cyclic group of smallest order that contains a subgroup isomorphic to $\mathbb{Z}_{12}$ and a subgroup isomorphic to $\mathbb{Z}_{20}$.
5. Prove that $\mathbb{R}$ under addition is not isomorphic to $\mathbb{R}^*$ under multiplication.

3.2.2 Solutions

1. Find an isomorphism from the group of integers under addition to the group of even integers under addition.

   First we need the mapping from the two sets. In this case we want an arbitrary integer to become even, so an easy choice is $f(x) = 2x$.

   To show this is an isomorphism we first need to show that it is a bijection. Let $x, y \in \mathbb{Z}$ such that $f(x) = f(y)$, then $2x = 2y$ giving that $x = y$ so the function is one-to-one. For onto let y be an arbitrary even integer, then let $x = y/2$. Putting x through f gives $f(x) = y$, so we are onto.

   The last step is to show that f is operation preserving. To do this let $x, y \in \mathbb{Z}$, then

   $$f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y).$$

   Thus f is an isomorphism.

2. Let G be a group. Prove that the mapping $\alpha(g) = g^{-1}$ for all $g \in G$ is an automorphism if and only if G is commutative.

   Proof. Let $\alpha(g) = g^{-1}$ be an automorphism, then

   $$gh = \alpha(g^{-1})\alpha(h^{-1}) = \alpha(g^{-1}h^{-1}) = \alpha((hg)^{-1}) = hg.$$

Thus G is commutative.

Conversely, if G is commutative, then for any $g \in G$ we know g has an inverse, let $x = g^{-1}$, then $\alpha(x) = g$ giving that α is onto. Let $g, h \in G$ such that $\alpha(g) = \alpha(h)$, then $g^{-1} = h^{-1}$ which following inverses are unique implies $h = g$. Finally for operation preserving we have

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

Thus α is an isomorphism from G to G giving that it is an automorphism. □

3. Let ϕ be an automorphism of a group G. Prove that $H = \{x \in G \mid \phi(x) = x\}$ is a subgroup of G.

Proof. To prove H is a subgroup, we can employee the 2-step subgroup test. First, note that $\phi(e) = e$ since an automorphism must map the identity to itself. This gives that H is nonempty.

Next, let $x, y \in H$, then $\phi(xy) = \phi(x)\phi(y) = xy$ giving that $xy \in H$.

Finally, let $x \in H$, then $\phi(x^{-1}) = \phi(x)^{-1} = x^{-1}$ giving that $x^{-1} \in H$. Thus, by the 2-step subgroup test H is a subgroup of G. □

4. Give an example of a cyclic group of smallest order that contains a subgroup isomorphic to $\mathbb{Z}_{12}$ and a subgroup isomorphic to $\mathbb{Z}_{20}$.

To build this cyclic group we can use the Fundamental theorem of cyclic groups part 3. We need our group of size n to have divisors of size 12 and of size 20. Thus, we can take the least common multiple of 12 and 20 which is 60. This tells us that the smallest cyclic group that has both $\mathbb{Z}_{12}$ and $\mathbb{Z}_{20}$ as subgroups must be order 60. Since all finite cyclic groups are isomorphic to $\mathbb{Z}_n$ this gives our example as $\mathbb{Z}_{60}$.

5. Prove that $\mathbb{R}$ under addition is not isomorphic to $\mathbb{R}^*$ under multiplication.

Proof. Assume for contradiction that ϕ is an isomorphism from $\mathbb{R}$ to $\mathbb{R}^*$. Consider $-1 \in \mathbb{R}^*$ we know that $(-1)^2 = 1$ so the order of -1 is 2. From Theorem 3.2.1 we know that $\mathbb{R}$ must also have an element of order 2. That is $x + x = 0$, however, the only x that satisfies this equation is $x = 0$ which is order 1. Thus, we have a contradiction since $\mathbb{R}$ does not have any order 2 elements. □

3.3 Kernel and image of a group homomorphism

Definition 3.3.1. Let $\phi : G \to H$, then

1. The *kernel* of ϕ is defined as $\ker(\phi) = \{g \in G \mid \phi(g) = e\}$.
2. The image of ϕ is defined as $im(\phi) = \{h \in G \mid \phi(g) = h, g \in G\}$.

Example 3.3.2. Let $\phi : GL(2,\mathbb{R}) \to \mathbb{R}^*$ be defined by $\phi(A) = \det A$, then ϕ is a homomorphism, the kernel is $SL(2,\mathbb{R})$, and the image is $\mathbb{R}^*$

To show the above claims, first let $A, B \in GL(2,\mathbb{R})$, then

$$\phi(AB) = \det(AB) = \det(A)\det(B) = \phi(A)\phi(B).$$

This gives that ϕ is a homomorphism. For the kernel, we are looking for all matrices in $GL(2,\mathbb{R})$ which get mapped to 1 (the identity element of $\mathbb{R}^*$. This is exactly $SL(2,\mathbb{R})$ since this set is defined as matrices with determinant equal to 1. Finally, we can consider the matrix

$$A = \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix} \in GL(2,\mathbb{R})$$

the determinant of A is a which can be used to cover all of $\mathbb{R}^*$. △

Theorem 3.3.3. *Let $\phi : G \to H$ be a homomorphism. Then $\ker(\phi)$ is a subgroup of G and $im(\phi)$ is a subgroup of H.*

Proof. To prove these, we will use the 1-step subgroup test. First note that $\ker(\phi)$ is nonempty since $\phi(e) = e$. Now let $a, b \in \ker(\phi)$, then we want to show $ab^{-1} \in \ker(\phi)$. For this we have

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = e.$$

Thus $\ker(\phi)$ is a subgroup of G.

Now for the image being a subgroup of H. Again by the 1-step subgroup test, first we have $\phi(e) = e$ giving that $\text{im}(\phi)$ is nonempty. Let $a, b \in \text{im}(\phi)$, then define $x, y \in G$ such that $\phi(x) = a$ and $\phi(y) = b$. This gives

$$ab^{-1} = \phi(x)\phi(y)^{-1} = \phi(xy^{-1})$$

hence ab^{-1} is the output from some entry $xy^{-1} \in G$ implying that $ab^{-1} \in H$. □

Theorem 3.3.4. *Let $\phi : G \to H$ be a homomorphism, then $\ker(\phi) = \{e\}$ if and only if ϕ is injective.*

Theorem 3.3.5. *Let $\phi : G \to H$ be a homomorphism, and let K be the kernel of ϕ. Then for any $k \in K$ and $x \in G$, we have $xkx^{-1} \in K$.*

3.4 Automorphism groups

Definition 3.4.1 (Inner automorphism)**.** Let G be a group, and let $a \in G$. The function ϕ_a defined by $\phi_a(x) = axa^{-1}$ for all $x \in G$ is called the *inner automorphism* of G induced by a.

Example 3.4.2. Let P be an arbitrary permutation matrix. Then PAP^{-1} is an inner automorphism of $GL(n, \mathbb{R})$. △

Definition 3.4.3. The set of automorphisms of a group, G, is denoted $\mathrm{Aut}(G)$, the operation will be function composition.

Similarly, the set of inner automorphisms will be defined $\mathrm{Inn}(G)$, with the operation again being function composition.

Theorem 3.4.4. *The set of automorphisms of a group and the set of inner automorphisms of a group are both groups under the operation of function composition.*

Example 3.4.5. Consider S_4 and a subgroup

$$H = \{(1),\ (1234),\ (13)(24),\ (1432),\ (12)(34),\ (24),\ (14)(23),\ (13)\}$$

from this we have

$$(12)H(21) = \{(1),\ (1342),\ (14)(23),\ (1234),\ (12)(34),\ (14),\ (13)(24),\ (23)\}$$
$$(123)H(321) = \{(1),\ (1423),\ (12)(34),\ (1324),\ (14)(23),\ (34),\ (13)(24),\ (12)\}$$

are isomorphic to H △

Inner automorphisms are a convent way of generating isomorphic groups that are not identical.

3.4.1 Exercises

1. Suppose that $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ is an automorphism and $\phi(5) = 5$. What are the possibilities for $\phi(x)$? Hint: Consider where the generators of $\mathbb{Z}_{10}$ could be mapped.

2. If $a, b \in S_n$ for $n \geq 3$, prove that $\phi_a = \phi_b$ implies that $a = b$. Hint: The center of S_n is $\{e\}$ for $n \geq 3$.

3. Prove that the set of inner automorphisms with function composition of a group G forms a group.

3.4.2 Solutions

1. Suppose that $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ is an automorphism and $\phi(5) = 5$. What are the possibilities for $\phi(x)$? Hint: Consider where the generators of $\mathbb{Z}_{10}$ could be mapped.

   Following $\phi(g^n) = \phi(g)^n$ for isomorphisms we want to track what can happen to the generators of $\mathbb{Z}_{10}$. In this case, those are $1, 3, 7, 9$. This

restricts us to only automorphisms that map $1, 3, 7, 9$ to other elements in that set. Consider

$$\begin{aligned}\phi_1(x) = x &\implies \phi(5) = 5,\\ \phi_3(x) = 3x &\implies \phi(5) = 15 \bmod 10 = 5,\\ \phi_7(x) = 7x &\implies \phi(5) = 35 \bmod 10 = 5,\\ \phi_9(x) = 9x &\implies \phi(5) = 45 \bmod 10 = 5\end{aligned}$$

Hence the automorphisms given above are all valid.

2. If $a, b \in S_n$ for $n \geq 3$, prove that $\phi_a = \phi_b$ implies that $a = b$. Hint: The center of S_n is $\{e\}$ for $n \geq 3$.

   If $\phi_a = \phi_b$ for all $a, b \in S_n$, then consider $\phi_b(a) = bab^{-1} = \phi_a(a) = aaa^{-1} = a$ and $\phi_b(b) = b = \phi_a(b) = aba^{-1}$. Now we have

   $$a = bab^{-1} = (aba^{-1})a(aba^{-1})^{-1} = ababa^{-1}a^{-1}$$

3. Prove that the set of inner automorphisms with function composition of a group G forms a group.

   Proof. First we need to show that $\text{Inn}(G)$ has an identity element. Consider $\phi_e(x) = exe^{-1} = x$ and we have $\phi_e \in \text{Inn}(G)$. Now let $\phi_g, \phi_h \in \text{Inn}(G)$, then

   $$\phi_g\phi_h(x) = ghxg^{-1}h^{-1} = (gh)x(gh)^{-1} = \phi_{gh}$$

   giving that $\text{Inn}(G)$ is closed under the operation. Finally, note that the automorphisms are associative following function composition is associative. □

3.5 Product of groups

Definition 3.5.1. Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The *external direct product* of $G_1, G_2, \ldots, G_n$, written as $G_1 \times G_2 \times \cdots \times G_n$, is the set of all n-tuples for which the ith component is an element of G_i and the operation is componentwise.

Symbolically

$$G_1 \times \cdots \times G_n = \{(g_1, \ldots, g_n) \mid g_1 \in G_1, g_2 \in G_2, \ldots, g_n \in G_n\}$$

where $(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1h_1, \ldots, g_nh_n)$.

The direct product of groups should look very similar to the Cartesian product of sets. Essentially we are building tuples where the binary operation is just componentwise whatever the group operation is.

Note that there are several notations for direct product, a common alternative is $\oplus$.

Example 3.5.2. Consider $\mathbb{Z}_3$ and $\mathbb{Z}_2$, then

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

where the group operation is addition modulo 3 in the first entry and addition modulo 2 in the second entry. Note that

$$\mathbb{Z}_3 \times \mathbb{Z}_2 \neq \mathbb{Z}_2 \times \mathbb{Z}_3.$$

△

Theorem 3.5.3. *Let G, H be groups and $E = \{e\}$ be the trivial group, then $G \times H \cong H \times G$ and $G \times E \cong G$.*

Example 3.5.4. Let's revisit the Klein 4 group. We defined the group as $K_4 = \{e, a, b, c\}$ where $a^2 = e$, $b^2 = e$, $c^2 = e$, $ab = c$, $ac = b$, and $bc = a$.

The Klein 4 group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. To see this, let $\phi : K_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ where

$$\phi(e) = (0,0),\ \phi(a) = (0,1),\ \phi(b) = (1,0),\ \text{and } \phi(c) = (1,1).$$

Now

$$\begin{aligned}
\phi(e) = \phi(a^2) &= (0,1)^2 = (0,0)\\
\phi(e) = \phi(b^2) &= (1,0)^2 = (0,0)\\
\phi(e) = \phi(c^2) &= (1,1)^2 = (0,0)\\
\phi(c) = \phi(ab) &= (0,1)(1,0) = (1,1)\\
\phi(b) = \phi(ac) &= (0,1)(1,1) = (1,0)\\
\phi(a) = \phi(bc) &= (1,0)(1,1) = (0,1).
\end{aligned}$$

△

Theorem 3.5.5. *The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components. Or in symbols*

$$|(g_1, g_2, \ldots, g_n)| = lcm(|g_1|, |g_2|, \ldots, |g_n|).$$

Theorem 3.5.6. *Let G and H be finite cyclic groups. Then $G \times H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime.*

3.5.1 Exercises

1. Show that $G \times H$ is commutative if and only if G and H are commutative.
2. Prove that $\mathbb{Z} \times \mathbb{Z}$ is not cyclic.
3. Is $\mathbb{Z}_3 \times \mathbb{Z}_9$ isomorphic to $\mathbb{Z}_{27}$?
4. Prove that the complex numbers under addition are isomorphic to $\mathbb{R} \times \mathbb{R}$.
5. Find all subgroups of order 4 in $\mathbb{Z}_4 \times \mathbb{Z}_4$.
6. Give an example of an infinite non-commutative group that has exactly 6 elements of finite order.

3.5.2 Solutions

1. Show that $G \times H$ is commutative if and only if G and H are commutative.

   Proof. If $G \times H$ is commutative, then let $a, c \in G$ and $b, d \in H$. Now construct $x, y \in G \times H$ such that $x = (a, b)$ and $y = (c, d)$. We then have that $xy = yx$ which gives that componentwise $ac = ca$ and $bd = db$. Thus G and H are arbitrary.

   Conversely, if G and H are commutative, then let $x, y \in G \times H$ such that $x = (a, b)$ and $y = (c, d)$, then

   $$xy = (a, b)(c, d) = (ac, bd) = (ca, db) = (c, d)(a, b) = ya.$$

   □

2. Prove that $\mathbb{Z} \times \mathbb{Z}$ is not cyclic.

   Proof. For a group to be cyclic, we need some element $g \in G$ such that $\langle g \rangle = G$. Assume for contradiction here that there exists $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ such that $\langle (a, b) \rangle = \mathbb{Z} \times \mathbb{Z}$. Now consider the points $(1, 1)$ and $(2, 1)$. Following (a, b) is the generator, we have that $(na, nb) = (1, 1)$ for some $n \in \mathbb{Z}$ and we also have that $(ma, mb) = (2, 1)$ for some $m \in \mathbb{Z}$. This gives that $nb = 1 = mb$ which implies $n = m$. However, this is a contradiction with the fact that $na = 1 \neq 2 = ma$. Thus, we can't have a generator and $\mathbb{Z} \times \mathbb{Z}$ is not cyclic. □

3. Is $\mathbb{Z}_3 \times \mathbb{Z}_9$ isomorphic to $\mathbb{Z}_{27}$?

   No, to see this consider the possible orders of the elements in $\mathbb{Z}_3 \times \mathbb{Z}_9$, from a Theorem in this section we know the possibilities are the least common multiples of elements from each part. This gives the options for $\mathbb{Z}_3$ as 1,3 and the options for $\mathbb{Z}_9$ as 1,3,9. Notice that the largest, least common multiple we can make is 9. Hence, the largest order element from $\mathbb{Z}_3 \times \mathbb{Z}_9$ is 9. Now for $\mathbb{Z}_{27}$ we know that 1 has order 27. Thus, the two groups can't be isomorphic.

   As an alternative proof. We have that the product of two groups is cyclic if and only if they are cyclic and relatively prime. In this case, 3 and 9 are not relatively prime, thus it is not cyclic. From a previous theorem, for two groups to be isomorphic they must either both be cyclic or neither be cyclic.

4. Prove that the complex numbers under addition are isomorphic to $\mathbb{R} \times \mathbb{R}$.

   The mapping we will use is $\phi(a + bi) = (a, b)$. To show this is an isomorphism we will show it is operation preserving, one-to-one, and onto. For operation preserving let $a + bi, c + di \in \mathbb{C}$, then

   $$\phi(a + bi) + \phi(c + di) = (a, b) + (c, d) = (a + c, b + d) = \phi(a + c + (b + d)i)$$

For one-to-one, let $a+bi, c+di \in \mathbb{C}$ such that $\phi(a+bi) = \phi(c+di)$. This implies that $a = c$ and $b = d$ which gives our result.

For onto, let $(a, b) \in \mathbb{R} \times \mathbb{R}$, then let $x = a + bi$ and we have

$$\phi(x) = \phi(a + bi) = (a, b).$$

5. Find all subgroups of order 4 in $\mathbb{Z}_4 \times \mathbb{Z}_4$.

   First note that there are 3 subgroups of $\mathbb{Z}_4$, so we have that there are 9 possible subgroups of $\mathbb{Z}_4 \times \mathbb{Z}_4$. Of those 9 we can't have the subgroup $\{(0, 0)\}$ since it is of order 1, and the subgroup $\{(0, 0), (2, 2)\}$ since it is of order 2. The other 7 subgroups are allowed. They are

   $$\langle(1, 0)\rangle,\ \langle(0, 1)\rangle,\ \langle(1, 1)\rangle,\ \langle(2, 1)\rangle,\ \langle(1, 2)\rangle,\ \langle(3, 1)\rangle,\ \langle(1, 3)\rangle.$$

6. Give an example of an infinite non-commutative group that has exactly 6 elements of finite order.

   Consider the group $\mathbb{Z} \times S_3$. We have shown earlier this semester that S_3 has 6 elements and is noncommutative. This gives that the only elements of finite order are $(0, g)$ where $g \in S_3$.

Chapter 4

Operations, classification, and counting with groups

4.1 Cosets and Lagrange's theorem

Definition 4.1.1 (Coset of H in G)**.** Let G be a group and let H be a nonempty subset of G. For any $a \in G$, the set $\{ah \mid h \in H\}$ is denoted by aH. Similar definitions for Ha and aHa^{-1}.

When H is a subgroup of G, the set aH is called the *left coset* of H in G containing a, whereas Ha is the *right coset*. For these the element a is called the coset representative of aH (or Ha).

Example 4.1.2. Let $G = S_3$ and $H = \{(1), (1,3)\}$. Then the left cosets of H in G are

$$\begin{aligned}(1)H &= H,\\ (12)H &= \{(12), (12)(13)\} = \{(12), (132)\} = (132)H\\ (13)H &= \{(13), (1)\} = H\\ (23)H &= \{(23), (23)(13)\} = \{(23), (123)\} = (123)H.\end{aligned}$$

△

Example 4.1.3. Let $H = \{0, 3, 6\}$ in $\mathbb{Z}_9$ under addition. Then the left cosets of H are

$$\begin{aligned}0H &= \{0, 3, 6\} = 3H = 6H,\\ 1H &= \{1, 4, 7\} = 4H = 7H,\\ 2H &= \{2, 5, 8\} = 5H = 8H.\end{aligned}$$

△

Note from the previous exercises that cosets are not usually subgroups. We also have that $aH = bH$ when $a \neq b$. Finally, we have that aH is not generally equal to Ha, it breaks for noncommutative groups.

Lemma 4.1.4 (Properties of Cosets)**.** *Let H be a subgroup of G, and let a and b belong to G. Then,*

1. $a \in aH$.
2. $aH = H$ *if and only if* $a \in H$.
3. $(ab)H = a(bH)$ *and* $H(ab) = (Ha)b$.
4. $aH = bH$ *if and only if* $a \in bH$.
5. $aH = bH$ *or* $aH \cap bH = \emptyset$.
6. $aH = bH$ *if and only if* $a^{-1}b \in H$.
7. $|aH| = |bH|$.
8. $aH = Ha$ *if and only if* $H = aHa^{-1}$.
9. aH *is a subgroup of* G *if and only if* $a \in H$.

Definition 4.1.5. The *index* of a subgroup H in G is the number of distinct left cosets of H in G. This is denoted by $|G : H|$.

Theorem 4.1.6 (Lagrange's Theorem)**.** *If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. The number of distinct left (right) cosets of H in G is $|G|/|H|$.*

Proof. Let a_1H, a_2H, $\ldots$, a_rH denote the distinct left cosets of H in G. First note that every $a \in G$ belongs to a coset since $a \in aH$ and $aH = a_iH$ for some i. This gives that

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH.$$

By the properties of the cosets we know that they are disjoint, thus

$$|G| = |a_1H| + |a_2H| + \cdots + |a_rH|.$$

Again by the properties of cosets we have $|a_iH| = |H|$ giving that $|G| = r|H|$. □

Corollary 4.1.7. *If G is a finite group and H is a subgroup of G, then $|G : H| = |G|/|H|$.*

Corollary 4.1.8. *In a finite group, the order of each element of the group divides the order of the group.*

Corollary 4.1.9. *A group of prime order is cyclic.*

Corollary 4.1.10. *Let G be a finite group, and let $a \in G$, then $a^{|G|} = e$.*

Corollary 4.1.11. *For every integer a and every prime p, $a^p \bmod p = a \bmod p$.*

Theorem 4.1.12. *For two finite subgroups H and K of a group, define the set*

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

Then $|HK| = |H||K|/|H \cap K|$.

Theorem 4.1.13 (Classification of groups of order $2p$)**.** *Let G be a group of order $2p$, where p is a prime greater than 2. Then G is isomorphic to $\mathbb{Z}_{2p}$ or D_p.*

Example 4.1.14. From the previous theorem, we immediately get that S_3 and $GL(2, \mathbb{Z}_2)$ are isomorphic to D_3. △

In this section we have categorized groups of prime order and of order 2 times a prime. This may make you ask can you characterize all finite groups. The answer is yes. We will revisit this in the final section of this chapter.

4.2 Normal subgroups

Definition 4.2.1 (Normal subgroup)**.** A subgroup H of a group G is called a *normal* subgroup of G if $aH = Ha$ for all $a \in G$. We denote this by $H \triangleleft G$.

Theorem 4.2.2 (Normal subgroup test)**.** *A subgroup H of G is normal if and only if $xHx^{-1} \subseteq H$ for all $x \in G$.*

Proof. If H is normal in G, then for any $x \in G$ and $h \in H$ there is an $h' \in H$ such that $xh = h'x$. Thus $xhx^{-1} = h'$, and therefore $xHx^{-1} \subseteq H$.

Conversely, if $xHx^{-1} \subseteq H$ for all x, then letting $x = a$, we have $aHa^{-1} \subseteq H$ or $aH \subseteq Ha$. On the other hand, letting $x = a^{-1}$, we have $a^{-1}Ha \subseteq H$ or $Ha \subseteq aH$. □

Example 4.2.3. Every subgroup of a commutative group is normal. △

Example 4.2.4. The alternating group A_n of even permutations is a normal subgroup of S_n. △

Example 4.2.5. Let H be a normal subgroup of a group G and K be any subgroup of G. Then

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

is a subgroup of G.

Warning! This only works in general if H is a normal subgroup. △

4.2.1 Exercises

1. Let $H = \{0, \pm 3, \pm 6, \dots\}$. Find all the left cosets of H in $\mathbb{Z}$.
2. Let a and b be elements of a group G and H and K be subgroups of G. If $aH = bK$, prove that $H = K$.
3. Let $H = \{(1), (12)\}$. Is H normal in S_3?
4. Prove that A_n is normal in S_n

4.2.2 Solutions

1. Let $H = \{0, \pm 3, \pm 6, \dots\}$. Find all the left cosets of H in $\mathbb{Z}$.
2. Let a and b be elements of a group G and H and K be subgroups of G. If $aH = bK$, prove that $H = K$.
3. Let $H = \{(1), (12)\}$. Is H normal in S_3?
4. Prove that A_n is normal in S_n

4.3 Quotient groups

Definition 4.3.1. Let $H \triangleleft G$, then the set of left (right) cosets of H in G is a group, called the quotient group of G by H (or commonly the factor group of G by H.

Theorem 4.3.2. *Let G be a group and let H be a normal subgroup of G. The set $G/H = \{aH \mid a \in G\}$ is a group under the operation $(aH)(bH) = abH$.*

Example 4.3.3. Let $4\mathbb{Z} = \{0, \pm 4, \pm 8, \dots\}$. To construct $\mathbb{Z}/4\mathbb{Z}$, we first must determine the left cosets of $4\mathbb{Z}$ in $\mathbb{Z}$. These are

$$\begin{aligned} 0 + 4\mathbb{Z} &= 4\mathbb{Z} \\ 1 + 4\mathbb{Z} &= \{1, 5, 9, \dots; -3, -7, \dots\} \\ 2 + 4\mathbb{Z} &= \{2, 6, 10, \dots; -2, -6, \dots\} \\ 3 + 4\mathbb{Z} &= \{3, 7, 11, \dots; -1, -5, \dots\}. \end{aligned}$$

To get a feel for this group operation we can build the operation table We can

	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$0+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$1+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$
$2+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$
$3+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$

see from this table that $\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$. More generally, if for any $n > 0$ we have $n\mathbb{Z}$, then $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$. △

Information about the factor groups can reveal information about the group. This can be seen in the following 3 theorems.

Theorem 4.3.4. *Let G be a group with center $Z(G)$, if $G/Z(G)$ is cyclic, then G is commutative.*

Proof. Since G being commutative is equivalent to $Z(G) = G$, it suffices to show that the only element of $G/Z(G)$ is the identity coset $Z(G)$. Let $G/Z(G) = \langle gZ(G)\rangle$ and let $a \in G$. Then there exists an integer i such that $aZ(G) =$

$g^iZ(G)$. This gives $a = g^iz$ for some $z \in Z(G)$. Since both g^i and z belong to $C(g)$, so does a. Because a is an arbitrary element of G we know that every element of G commutes with g, so $g \in Z(G)$. Thus $gZ(G) = Z(G)$ is the only element of $G/Z(G)$. □

Theorem 4.3.5. *For any group G, $G/Z(G)$ is isomorphic to $Inn(G)$ (group of inner automorphisms of G).*

Theorem 4.3.6. *Let G be a finite commutative group and let p be a prime that divides the order of G. Then G has an element of order p.*

4.4 Direct sum of groups

Definition 4.4.1. We say that G is the *direct sum of groups* (also known as the *inner direct product* of groups) H and K and we write $G = H + K$ if H and K are normal subgroups of G, $G = HK$ and $H \cap K = \{e\}$.

The reason this is frequently called the inner direct product of groups, is that we are starting with two subgroups of G, then forming G as an inner product of those groups. Contrast this with our normal product of groups (also called the external product), where we take two, potentially unrelated groups, and use those to form an entirely new group.

Example 4.4.2. Consider the dihedral group of 6 elements, D_6. Let F denote some reflection and let R_k denote a rotation of k degrees. Then

$$D_6 = \{R_0, R_{120}, R_{240}, F, R_{120}F, R_{240}F\} + \{R_0, R_{180}\}.$$

△

Theorem 4.4.3. *If a group G is the internal direct product of a finite number of subgroups $H_1, H_2, \ldots, H_n$, then G is isomorphic to the external direct product of $H_1, \ldots, H_n$.*

Theorem 4.4.4. *Every group of order p^2, where p is a prime, is isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$*

Corollary 4.4.5. *If G is a group of order p^2, where p is a prime, then G is commutative.*

4.4.1 Exercises

1. What is the order of the quotient group $\mathbb{Z}_{60}/\langle 15\rangle$?
2. Explain why a non-commutative group of order 8 cannot be the internal direct product of proper subgroups.
3. Prove that a quotient group of a cyclic group is cyclic.
4. Determine the order of $(\mathbb{Z} + \mathbb{Z})/(\langle 2\rangle + \langle 2\rangle)$. Is this group cyclic?

4.4.2 Solutions

1. What is the order of the quotient group $\mathbb{Z}_{60}/\langle 15\rangle$?

   The order of the quotient group is the number of distinct cosets. First, note that $|\langle 15\rangle| = 4$, now from Lagrange's theorem, we know this to be $60/4 = 15$.

2. Explain why a non-commutative group of order 8 cannot be the internal direct product of proper subgroups.

   Assume for contradiction that the noncommutative group G can be written as the internal direct product of proper subgroups; that is $G = HK$. Now we know that the orders of H and K must be 4 and 2 since they product to order 8. However we have shown that all groups of order 4 or less are commutative. Thus H and K are commutative groups. But from a Theorem today we know that $HK \cong H \times K$ and we have shown that the product of commutative groups is commutative. Thus $HK = G$ is commutative and non-commutative, giving a contradiction.

3. Prove that a quotient group of a cyclic group is cyclic.

4. Determine the order of $(\mathbb{Z} + \mathbb{Z})/(\langle 2\rangle + \langle 2\rangle)$. Is this group cyclic?

4.5 Isomorphism theorems

The following three isomorphism theorem summarize and combine most of the results that we have dealing with isomorphisms, homomorphisms, normal subgroups, product groups, and quotient groups.

Theorem 4.5.1 (First isomorphism theorem)**.** *Let ϕ be a group homomorphism from G to H. Then*

1. *The kernel of ϕ is a normal subgroup of G,*
2. *The image of ϕ is a subgroup of H, and*
3. *The image of ϕ is isomorphic to the quotient group $G/\ker(\phi)$.*

Furthermore, if ϕ is onto, then $H \cong G/\ker(\phi)$.

Corollary 4.5.2. *If ϕ is a homomorphism from a finite group G to H, then $|\phi(G)|$ divides $|G|$ and $|H|$.*

Theorem 4.5.3 (Second isomorphism theorem)**.** *Let G be a group. Let S be a subgroup of G, and let N be a normal subgroup of G. Then*

1. *The product SN is a subgroup of G,*
2. *The subgroup N is a normal subgroup of SN,*
3. *The intersection of $S \cap N$ is a normal subgroup of S, and*

4. *The quotient groups $(SN)/N$ and $S/(S \cap N)$ are isomorphic.*

Theorem 4.5.4 (Third isomorphism theorem)**.** *Let G be a group, and N a normal subgroup of G. Then*

1. *If K is a subgroup of G such that $N \subseteq K \subseteq G$, then G/N has a subgroup isomorphic to K/N.*
2. *Every subgroup of G/N is of the form K/N for some subgroup K of G such that $N \subseteq K \subseteq G$.*
3. *If K is a normal subgroup of G such that $N \subseteq K \subseteq G$, then G/N has a normal subgroup isomorphic to K/N.*
4. *Every normal subgroup of G/N is of the form K/N for some normal subgroup K of G such that $N \subseteq K \subseteq G$.*
5. *If K is a normal subgroup of G such that $N \subseteq K \subseteq G$, then the quotient group $(G/N)/(K/N)$ is isomorphic to G/K.*

Theorem 4.5.5. *Every normal subgroup of a group G is the kernel of a homomorphism of G. In particular, a normal subgroup N is the kernel of the mapping $g \to gN$ from G to G/N.*

4.6 Fundamental theorem of finite commutative groups

Theorem 4.6.1 (Fundamental theorem of finite commutative groups)**.** *Every finite commutative group is a product of cyclic groups of prime-order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.*

The above theorem gives a complete classification of commutative groups. The proof is fairly long and complicated, and so it will not be presented here. Gallian's Abstract algebra book has an excellent break-down of the proof if you are interested.

Corollary 4.6.2. *If m divides the order of a finite commutative group G, then G has a subgroup of order m.*

4.6.1 Exercises

1. Determine all the homeomorphic images of D_4 (the dihedral group) up to isomorphism.
2. Prove that every group of order 77 is cyclic.
3. Suppose that G is a finite group and that $\mathbb{Z}_{10}$ is a homomorphic image of G. What can we say about $|G|$?
4. Suppose that $\mathbb{Z}_{10}$ and $\mathbb{Z}_{15}$ are both homomorphic images of a finite group G. What can we say about $|G|$?
5. Determine all homomorphisms from $\mathbb{Z}$ to S_3.
6. If H and K are normal subgroups of G and $H \cap K = \{e\}$, prove that G is isomorphic to a subgroup of $G/H + G/K$.

4.6.2 Solutions

1.

4.7 Counting with groups

Definition 4.7.1 (Group action)**.** Let G be a group and X is a set, then a (left) group action α of G on X is a function

$$\alpha : G \times X \to X,$$

that satisfies the following two axioms:

1. Identity: $\alpha(e, x) = x$
2. Compatibility: $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$

for all $g, h \in G$ and all $x \in X$.

Using the above definition one may show that an equivalent definition of group action is as a group homomorphism from G into the symmetric group of X.

Definition 4.7.2. Let G be a group acting on a set X. The *orbit* of an element $x \in X$ is the set of elements in X to which x can be moved by the elements of G. Symbolically we write the orbit of x as $G \cdot x$ and can be expressed as

$$G \cdot x = \{g \cdot x : g \in G\}.$$

The set of orbits under the action is denoted X/G.

Theorem 4.7.3. *Let G be a group acting on a set X. The distinct orbits of elements of X form a partition of X.*

Definition 4.7.4 (Stabilizer)**.** Let G be a group acting on X. The *fixed point set* of g in X, denoted X_g, is the set of all $x \in X$ such that $gx = x$.

We can also study the group elements g that fix a given $x \in X$. This turns out to be a subgroup of G called the *stabilizer subgroup*, denoted G_x.

Theorem 4.7.5 (Burnside's Theorem)**.** *If G is a finite group acting on a set X and let $\mathcal{O}(X)$ denote the number of orbits of X. Then*

$$\mathcal{O}(X) = \frac{1}{|G|} \sum_{g \in G} |X_g|$$

4.8 Classification of all finite simple groups

Definition 4.8.1 (Simple group)**.** A simple group is a nontrivial group whose only normal subgroups are the trivial group and the group itself.

Any non-simple group can be broken into smaller groups by using the non-trivial normal subgroup and the quotient group. For finite groups this leads to a unique factorization of groups into a product of simple groups. This is known as the Jordan-Hölder theorem.

Theorem 4.8.2 (Classification of all finite simple groups)**.** *Every finite simple group is isomorphic to one of the following groups:*

- *a member of one of four infinite classes of such, namely:*
  - *the cyclic groups of prime order,*
  - *the alternating groups of degree at least 5,*
  - *the groups of Lie type,*
  - *the derived subgroup of the groups of Lie Type, such as the Tits group*
- *or one of 26 groups called the "sporadic groups"*

This is a monumental result in group theory and was completed only in 2004. It says that any finite group that can be built, must be built from the building blocks given above. This is often regarded as the periodic table of group theory.

Most to all of the Lie type and sporadic groups are out of scope for this class. But it is interesting to highlight the sporadic groups. The 4 other classes are all infinite groups. Which is fairly expected, think of the infinite number of primes needed to give prime factorizations to all positive integers. But there are only a finite number of these sporadic groups. This implies that in 26 instances, there is something special that happens that requires a specific group to fix it. As an interseting note on the sporadic

The final paper solving this problem is over 1000 pages long, and including all the necessary references it is well over 10000 pages long. This proof is also an example of a computer-assisted-proof. That is we were able to reduce the

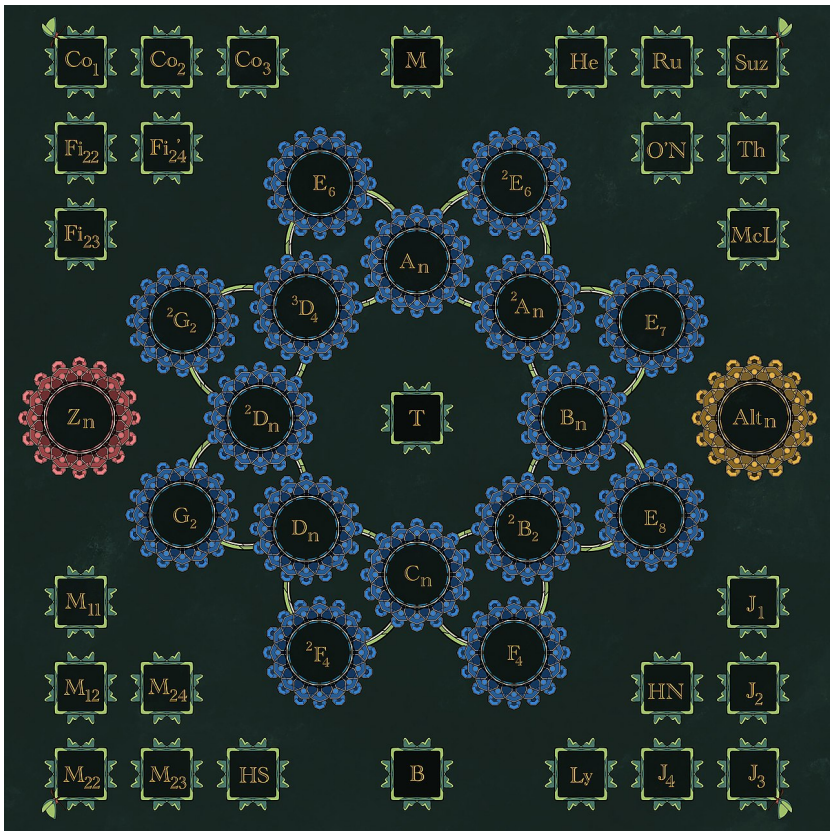


Figure 4.1: Illustration of all fundamental finite simple groups by Mathsies

proof into some finite number of cases, then a computer verified each of these cases were verified.

Computer-assisted-proofs proof are controversial in mathematics because it feels like a breach in understanding. Frequently the ideas in a proof are as important or more important than the statement of the proof itself. Because of this, there is a significant movement within group theorists to write a new proof that does not rely on a computer. This effort, called the second generation, already requires over 5000 pages. Thus, a "simple" proof is unlikely to ever exist.

Chapter 5

Rings and Fields

5.1 Rings and subrings

Definition 5.1.1. A *ring* is a set with two binary operations, addition (denoted by $a + b$) and multiplication (denoted by ab), such that for all $a, b, c \in R$:

1. $a + b = b + a$.
2. $(a + b) + c = a + (b + c)$.
3. There is an additive identity 0; that is $0 + a = a$ for all $a \in R$.
4. There is an element $-a$ in R such that $a + (-a) = 0$.
5. $a(bc) = (ab)c$.
6. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

Another way to view a ring is as an commutative group under addition that also has a binary operation of multiplication, which left and right distribute over addition.

When the operation of multiplication is commutative, we call the ring a *commutative ring*.

Definition 5.1.2. A *unity* (or multiplicative identity) in a ring is a nonzero element that is an identity under multiplication.

Definition 5.1.3. Let R be a commutative ring with an element $a \in R$. If a^{-1} exists, we say that a is a *unit* of R.

Example 5.1.4. The set $\mathbb{Z}$ of integers under ordinary addition and multiplication is a commutative ring with unity 1. The units of $\mathbb{Z}$ are 1 and -1. $\triangle$

Example 5.1.5. The set $\mathbb{Z}[x]$ of all polynomials in the variable x with integer coefficients under ordinary addition and multiplication is a commutative ring with unity $f(x) = 1$. $\triangle$

Example 5.1.6. The set $\mathsf{M}_2(\mathbb{Z})$ of 2x2 matrices with integer entries is a noncommutative ring with unity

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

△

Example 5.1.7. The set $2\mathbb{Z}$ of even integers under ordinary addition and multiplication is a commutative ring without unity. △

Theorem 5.1.8. *Let R be a ring and $a, b, c \in R$, then*

1. $a(0) = 0(a) = 0$.
2. $a(-b) = (-a)b = -(ab)$.
3. $(-a)(-b) = ab$.
4. $a(b - c) = ab - ac$.

If R has a unity element 1, then

5. $(-1)a = -a$.
6. $(-1)(-1) = 1$.

Theorem 5.1.9. *If a ring has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique.*

Definition 5.1.10. A subset S of a ring R is a *subring* of R if S is itself a ring with the operations of R.

Theorem 5.1.11 (Subring test)**.** *A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication. That is if $a, b \in S$, then $a - b$ and ab are in S.*

5.1.1 Exercises

1. Give an example of a finite noncommutative ring.
2. Show that a ring is commutative if it has the property that $ab = ca$ implies $b = c$ when $a \neq 0$.
3. In $\mathbb{Z}_6$ show that $4 \mid 2$ and in $\mathbb{Z}_8$ show that $3 \mid 7$.

5.1.2 Solutions

1. Give an example of a finite noncommutative ring.

   Consider $\mathsf{M}_2(\mathbb{Z}_2)$ (2 by 2 matrices with entries of 0 or 1. The operation is regular matrix addition and multiplication modulo 2.

   Matrix multiplication is not commutative, and the set only contains $2^4 = 16$ elements.

2. Show that a ring is commutative if it has the property that $ab = ca$ implies $b = c$ when $a \neq 0$.

   Let R be a ring with elements x, y, then consider the substitution $a = x$, $b = yx$, and $c = xy$, then we have

   $$xyx = xyx \implies xy = yx.$$

3. In $\mathbb{Z}_6$ show that $4 \mid 2$ and in $\mathbb{Z}_8$ show that $3 \mid 7$.

   For $x \mid y$ with a general, $x, y \in \mathbb{Z}_n$, then we need $y = xk \bmod n$. Thus, we are looking for a k such that $2 = 4k \bmod 6$. We can see that $2(4) = 8$ which modulo 6 gives 2. Hence $4 \mid 2$.

   Similarly, for the second question we have $7 = 3k \bmod 8$ which we can play with the k to find $k = 5$ works.

5.2 Integral domain

The initial idea behind rings was to abstract the integers to allow for further study. This didn't quite work out because general rings are missing three important properties of the integers. The first two are commutativity and the existence of a multiplicative identity. The third property, that we will study in this section, is the cancellation property.

Definition 5.2.1 (Zero divisors)**.** A *zero-divisor* is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.

Definition 5.2.2 (Integral domain)**.** An *integral domain* is a commutative ring with unity and no zero-divisors.

An integral domain gives us that if $ab = 0$, then either $a = 0$ or $b = 0$.

Example 5.2.3. The ring of integers is an integral domain. △

Example 5.2.4. The ring of Gaussian integers, $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ where $i^2 = -1$, is an integral domain. △

Example 5.2.5. The ring, $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is an integral domain. △

Theorem 5.2.6. *Let a, b, c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.*

Definition 5.2.7 (Characteristic of a ring)**.** The *characteristic* of a ring R is the least positive integer n such that $nx = 0$ for all $x \in R$. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by $\text{char}(R)$.

Theorem 5.2.8 (Characteristic of a ring with unity)**.** *Let R be a ring with unity, 1. If 1 has infinite order under addition, then the characteristic of R is 0. If 1 has order n under addition, then the characteristic of R is n.*

Theorem 5.2.9. *The characteristic of an integral domain is* 0 *or prime.*

Proof. By the previous theorem, it suffices to show that if the additive order of 1 is finite, it must be prime. Suppose that 1 has order n and that $n = st$ where $1 \leq s$ and $t \leq n$. Then

$$0 = n \cdot 1 = (st) \cdot (1) = (s \cdot 1)(t \cdot 1).$$

So either $(s \cdot 1) = 0$ or $(t \cdot 1) = 0$. Since n is the least positive integer with the property that $n \cdot 1 = 0$, we must have $s = n$ or $t = n$. Thus n is prime. □

5.3 Ideals

In this section, we will take the idea of normal subgroups and generalize them to rings.

Definition 5.3.1 (Ideal)**.** A subring A of a ring R is called a (two-sided) *ideal* of R if for every $r \in R$ and every $a \in A$ both ra and ar are in A.

An ideal is called *proper* if the subring is a proper subring.

A subring A of a ring R is an ideal of R if A "absorbs" elements from R – that is, if $rA = \{ra \mid a \in A\} \subseteq A$ and $Ar = \{ar \mid a \in A\} \subseteq A$ for all $r \in R$.

Theorem 5.3.2 (Ideal test)**.** *A nonempty subset A of a ring R is an ideal of R if*

1. *$a - b \in A$ whenever $a, b \in A$.*
2. *ra and ar are in A whenever $a \in A$ and $r \in R$.*

Example 5.3.3. For any ring R, $\{0\}$ and R are ideals of R. The ideal $\{0\}$ is called the *trivial* ideal. △

Example 5.3.4. For any positive integer n, the set $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$ is an ideal of $\mathbb{Z}$. △

Example 5.3.5. Let $\mathbb{Z}[x]$ denote the ring of all polynomials with integer coefficients, and let I be the subset of $\mathbb{Z}[x]$ of all polynomials with even constant terms. Then I is an ideal of $\mathbb{Z}[x]$ and $I = \langle x, 2\rangle$. △

Definition 5.3.6 (Principal ideal generated by an element)**.** Let R be a commutative ring with unity and let $a \in R$. The set

$$\langle a\rangle = \{ra \mid r \in R\}$$

is an ideal of, R called the *principal ideal generated by a.*

Definition 5.3.7 (Ideal generated elements)**.** Let R be a commutative ring with unity and let $a_1, a_2, \ldots, a_n \in R$. The set

$$\langle a_1, a_2, \ldots, a_n \rangle = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_i \in R\}$$

is an ideal of, R.

Definition 5.3.8 (Sum of ideals)**.** Let I, J be ideals of a ring, the sum of I and J, defined as

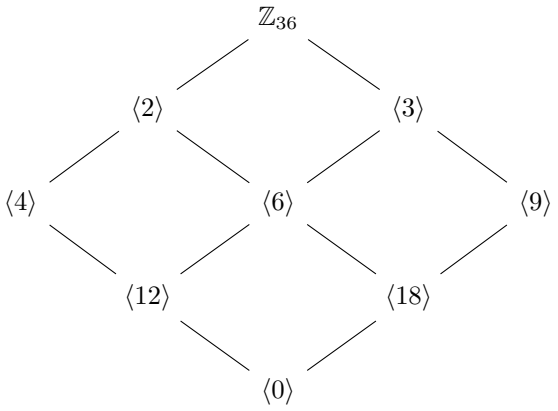
$$I + J = \{a + b \mid a \in I,\ b \in J\},$$

is an ideal.

Definition 5.3.9 (Prime ideal, Maximal ideal)**.** A *prime ideal* A of a commutative ring R is a proper ideal of R such that $a, b \in R$ and $ab \in A$ imply $a \in A$ or $b \in A$. A *maximal* ideal of a commutative ring R is a proper ideal of R such that, whenever B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

Example 5.3.10. Let n be an integer greater than 1. Then, in the ring of integers, the ideal $n\mathbb{Z}$ is prime if and only if n is prime. △

Example 5.3.11. The lattice of ideals, see below, of $\mathbb{Z}_{36}$ shows that $\langle 2 \rangle$ and $\langle 3 \rangle$ are maximal ideals.



△

Example 5.3.12. The ideal $\langle x^2 + 1 \rangle$ is maximal in $\mathbb{R}[x]$. To see this, assume that A is an ideal of $\mathbb{R}[x]$ that properly contains $\langle x^2 + 1 \rangle$. We will prove that $A = \mathbb{R}[x]$ by showing that A contains some nonzero real number c which will give that $A = \mathbb{R}[x]$. To this end, let $f(x) \in A$, but $f(x) \notin \langle x^2 + 1 \rangle$. Then

$$f(x) = q(x)(x^2 + 1) + r(x),$$

where $r(x) \neq 0$ and the degree of $r(x)$ is less than 2. It follows that $r(x) = ax+b$, where a and b are both not 0, and

$$ax + b = r(x) = f(x) - q(x)(x^2 + 1) \in A.$$

Thus,

$$a^2x^2 - b^2 = (ax + b)(ax - b) \in A \quad \text{and} \quad a^2(x^2 + 1) \in A.$$

So,

$$0 \neq a^2 + b^2 = (a^2x^2 + a^2 - a^2x^2 - b^2) \in A.$$

△

5.3.1 Exercises

1. Prove that the ring

$$\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} \mid a, b \in \mathbb{Z}\}$$

is an integral domain. You may assume that it is already a ring.

2. Show that every nonzero element of $\mathbb{Z}_n$ is a unit or a zero-divisor.

3. Give an example of a commutative ring without zero-divisors that is not an integral domain.

4. Find all maximal ideals in

   (a) $\mathbb{Z}_8$.
   (b) $\mathbb{Z}_{12}$.
   (c) $\mathbb{Z}_n$.

5. In the ring of integers, find a positive integer a such that

   (a) $\langle a \rangle = \langle 2 \rangle + \langle 3 \rangle$.
   (b) $\langle a \rangle = \langle 6 \rangle + \langle 8 \rangle$.

6. Prove I from Example 5.3.5 is an ideal. That is, let $\mathbb{Z}[x]$ denote the ring of all polynomials with integer coefficients, and let I be the subset of $\mathbb{Z}[x]$ of all polynomials with even constant terms. Then prove I is an ideal of $\mathbb{Z}[x]$.

5.3.2 Solutions

1. Prove that the ring

$$\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} \mid a, b \in \mathbb{Z}\}$$

is an integral domain. You may assume that it is already a ring.

To prove that the ring is an integral domain we need to show that it is commutative, has a unity, and has no zero-divisors.

For commutative take $a + b\sqrt{p}, c + d\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$, then

$$(a + b\sqrt{p})(c + d\sqrt{p}) = (ac + bdp) + (ad + bc)\sqrt{p} = (c + d\sqrt{p})(a + b\sqrt{p}).$$

For unity we have $1 = 1 + 0\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$.

For no zero divisors, we can treat $\mathbb{Z}[\sqrt{p}]$ as a subset of $\mathbb{R}$. We know that $\mathbb{R}$ has no zero divisors, hence $\mathbb{Z}[\sqrt{p}]$ has no zero divisors.

2. Show that every nonzero element of $\mathbb{Z}_n$ is a unit or a zero-divisor.

   The two facts we will use here is that for an element $a \in \mathbb{Z}_n$, a is a unit if $ab \equiv 1 \bmod n$ for some element $b \in \mathbb{Z}_n$ and a is a zero divisor if $ab \equiv 0 \bmod n$ for some element $b \in \mathbb{Z}_n$.

   With this two facts note that the first one can be rewritten as $\gcd(a, n) = 1$. The second can then be written as $\gcd(a, n) > 1$. That is a is a unit if the greatest common divisor with n is 1, while a is a zero-divisor if the greatest common divisor is greater than 1. Since the greatest common divisor of two numbers is positive, this covers all the cases.

3. Give an example of a commutative ring without zero-divisors that is not an integral domain.

   Consider $2\mathbb{Z} = \{0, \pm 2, \pm 4, \dots\}$. We have that it is commutative, following the integers are commutative. We know that it has no zero divisors since the integers don't have zero divisors. However it is not an integral domain since there is no unity.

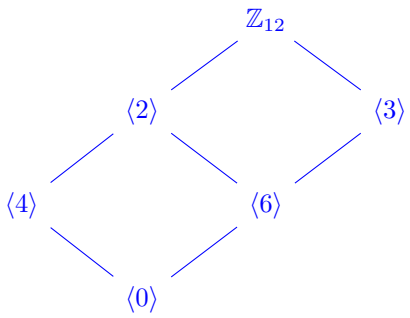
4. Find all maximal ideals in

   (a) $\mathbb{Z}_8$.

   This is similar to one of the examples. The idea is that we can break $\mathbb{Z}_8$ apart into ideals using its factors. So in this case $\langle 4 \rangle$ is one such ideal as well as $\langle 2 \rangle$. We can see that $\langle 2 \rangle$ is maximal, since it is larger than $\langle 4 \rangle$.

   (b) $\mathbb{Z}_{12}$.

   We can make a lattice like in the example giving



   From this we see that $\langle 2 \rangle$ and $\langle 3 \rangle$ are the maximal ideals.

   (c) $\mathbb{Z}_n$.

   The maximal ideals for $\mathbb{Z}_n$ are the primes that factorize n. Note that all the ideals of $\mathbb{Z}_n$ are the prime factors, prime powers, and

combinations of those two. This gives that the maximal case is when we take single primes to generate our ideals.

5. In the ring of integers, find a positive integer a such that

   (a) $\langle a \rangle = \langle 2 \rangle + \langle 3 \rangle$.

   Note first that $\langle 2 \rangle$ contains all even integers, while $\langle 3 \rangle$ contains all multiples of 3. Taking $\langle 2 \rangle + \langle 3 \rangle$ gives linear combinations of those two sets. That is elements are of the form $2x + 3y$. Note that these span the entirety of $\mathbb{Z}$ giving that $a = 1$.

   (b) $\langle a \rangle = \langle 6 \rangle + \langle 8 \rangle$.

   Similar to the previous problem but we now have elements of the form $6x+8y = 2(3x+4y)$. This gives we can reach all even numbers, so $a = 2$.

6. Prove I from Example 5.3.5 is an ideal. That is, let $\mathbb{Z}[x]$ denote the ring of all polynomials with integer coefficients, and let I be the subset of $\mathbb{Z}[x]$ of all polynomials with even constant terms. Then prove I is an ideal of $\mathbb{Z}[x]$.

   To prove that I is an ideal we need to prove that fI and If are subsets of I for all $f \in \mathbb{Z}[x]$. To achomplish this let $g \in I$ and $f \in \mathbb{Z}[x]$ such that

$$f(x) = \sum_{k=0}^{m_1} a_k x^k$$
$$g(x) = \sum_{k=0}^{m_2} 2b_k x^k,$$

   then

$$f(x)g(x) = \sum_{k=0}^{m_3} s_k x^k$$

   where

$$s_j = 2a_j b_0 + 2a_{j-1} b_1 + \cdots + 2a_0 b_j = 2(a_j b_0 + a_{j-1} b_1 + \cdots + a_0 b_j).$$

   Since each term in the product is even we have that $fg \in I$. A similar calculation shows $gf \in I$. Thus I is an ideal of $\mathbb{Z}[x]$.

5.4 Quotient rings

Ideals act as a natural extension of normal subgroups into the ring setting. This raises the question of defining quotient rings as an extension of quotient groups.

Definition 5.4.1 (Quotient ring)**.** Let R be a ring with ideal I, then we define the *quotient ring* R/I whose elements are the cosets, $r+I = \{r+a \mid a \in I\}$, of the ideal I with elements r from R. The operations are defined

$$\begin{aligned}(s+I)+(t+I) &= (s+t)+I\\ (s+I)(t+I) &= (st)+I.\end{aligned}$$

Note that just like with quotient groups we can only define the quotient ring if the subring picked is ideal, if it is just a subring we don't get the ring structure.

Example 5.4.2. Consider $\mathbb{Z}/(4\mathbb{Z}) = \{0+4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\}$. Addition and multiplication of these cosets is then essentially the two operations modulo 4 of the elements out front. △

Example 5.4.3. Consider the factor ring of the Gaussian integers $R = \mathbb{Z}[i]/\langle 2-i\rangle$. What does this ring look like? Or more importantly what do the distinct cosets look like?

First note that all cosets are of the form $a+bi+\langle 2-i\rangle$ where $a, b \in \mathbb{Z}$ and we have that $2-i+\langle 2-i\rangle = 0+\langle 2-i\rangle$ since $2-i \in \langle 2-i\rangle$. This gives us that under this factor ring dealing with the coset representatives we have $2 = i$. So for example

$$3+4i+\langle 2-i\rangle = 3+8+\langle 2-i\rangle = 11+\langle 2-i\rangle.$$

Thus the first reduction is all the distinct cosets can be written in the form $a+\langle 2-i\rangle$. But we can reduce further.

Next look again at $2 = i$, squaring both sides gives $4 = -1 \implies 5 = 0$. Thus from our previous example

$$3+4i+\langle 2-i\rangle = 11+\langle 2-i\rangle = 1+5+5+\langle 2-i\rangle = 1+\langle 2-i\rangle.$$

Thus our distinct cosets are

$$0+\langle 2-i\rangle,\ 1+\langle 2-i\rangle,\ 2+\langle 2-i\rangle,\ 3+\langle 2-i\rangle, \text{ and } 4+\langle 2-i\rangle.$$

Thus this quotient ring is behaving just like $\mathbb{Z}_5$. Once we discuss ring isomorphisms we will be able to prove this. △

Example 5.4.4. Let $\mathbb{R}[x]$ denote the ring of polynomials with real coefficients and let $\langle x^2+1\rangle$ denote the principal ideal generated by x^2+1; that is,

$$\langle x^2+1\rangle = \{f(x)(x^2+1) \mid f(x) \in \mathbb{R}[x]\}.$$

Then

$$\begin{aligned}\mathbb{R}[x]/\langle x^2+1\rangle &= \{g(x)+\langle x^2+1\rangle \mid g(x) \in \mathbb{R}[x]\}\\ &= \{ax+b+\langle x^2+1\rangle \mid a, b \in \mathbb{R}[x]\}.\end{aligned}$$

To see that last step, note that for any polynomial we can use the divison algorithm leaving just the remainder (polynomial of degree 1 or less) as the part not in the ideal.

Thus the distinct cosets of $\mathbb{R}[x]/\langle x^2+1\rangle$ are elements of the form $ax+b$ where $a, b \in \mathbb{R}$. It turns out this field is isomorphic to $\mathbb{C}$. △

Theorem 5.4.5. *Let R be a commutative ring with unity and let I be an ideal of R. Then R/I is an integral domain if and only if I is prime.*

Proof. Suppose that R/A is an integral domain and $ab \in A$. Then $(a+A)(b+A) = ab + A = A$, the zero element of the ring R/A. So, $ab = 0$ which in an integral domain implies $a = 0$ or $b = 0$. Thus either $a + A = A$ or $b + A = A$ giving that A is prime.

For the other direction note that R/A is a commutative ring with unity for any proper ideal A. Thus we need only show that when A is a prime ideal, R/A has no zero divisors. So let A be a prime ideal and let $(a+A)(b+A) = 0+A = A$. Then $ab \in A$ and following A is prime we have that either $a \in A$ or $b \in A$. Thus either $a + A$ or $b + A$ is the zero coset in R/A. □

5.4.1 Exercises

1. Give an example of a commutative ring that has a maximal ideal that is not a prime ideal.

2. In $\mathbb{Z}[x]$, let $I = \{f(x) \in \mathbb{Z}[x] \mid f(0) = 0\}$. Prove that $I = \langle x\rangle$.

3. How many distinct elements are there in $\mathbb{Z}[i]/\langle 3+i\rangle$?

4. How many distinct elements are there in $\mathbb{Z}_5[i]/\langle 1+i\rangle$?

5.4.2 Solutions

1. Give an example of a commutative ring that has a maximal ideal that is not a prime ideal.

   Consider $R = 2\mathbb{Z}$, then $I = 4\mathbb{Z}$ is a maximal ideal that is not prime.

2. In $\mathbb{Z}[x]$, let $I = \{f(x) \in \mathbb{Z}[x] \mid f(0) = 0\}$. Prove that $I = \langle x\rangle$.

   To prove that $I = \langle x\rangle$ we will do a double inclusion proof. To start let $f \in I$, then following the constant term of f is zero we can factor out an x, this gives $f(x) = xg(x)$ for some $g \in \mathbb{Z}[x]$. This gives that $f \in \langle x\rangle$ by definition.

   For the other direction let $f \in \langle x\rangle$, then by definition of the ideal generated by an element, f can be written in the form $xg(x)$ for some $g \in \mathbb{Z}[x]$. But this implies that $f(0) = 0g(0) = 0$. Thus $f \in I$. Since both sets contain each other $I = \langle x\rangle$.

3. How many distinct elements are there in $\mathbb{Z}[i]/\langle 3+i\rangle$?

   We can follow a similar idea to the example. First note that $3+i+\langle 3+i\rangle = 0+\langle 3+i\rangle$. This gives that $3=-i$. With this we only care about cosets of the form $a+\langle 3+i\rangle$, but we can use the identity that $i^2=-1$ with our form of $3=-i$ to get that $9=1 \implies 8=0$. So our distinct elements are 0 through 7 plus $\langle 3+i\rangle$. This gives 8 distinct elements.

4. How many distinct elements are there in $\mathbb{Z}_5[i]/\langle 1+i\rangle$?

   Same as before first we get $1=-i$ and $1=-1 \implies 2=0$. So we have the elements $0+\langle 1+i\rangle$ and $1+\langle 1+i\rangle$. Note that we would now need to check that the restriction of $\mathbb{Z}_5$ has any play here. In this case our elements are already reduced into this, but it may come up for other problems.

5.5 Ring morphisms

Definition 5.5.1. A ring *homomorphism* ϕ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations; that is, for all $a, b \in R$,

$$\phi(a+b)=\phi(a)+\phi(b) \quad \text{and} \quad \phi(ab)=\phi(a)\phi(b).$$

A ring homomorphism that is a bijection is called a *ring isomorphism*.

Example 5.5.2. For any positive integer n, the mapping $k \to k \bmod n$ is a ring homomorphism from $\mathbb{Z}$ onto $\mathbb{Z}_n$. This mapping is called the *natural homomorphism* from $\mathbb{Z}$ to $\mathbb{Z}_n$. △

Example 5.5.3. The mapping $a+bi \to a-bi$ is a ring isomorphism from the complex numbers onto itself. △

Example 5.5.4. Let $\mathbb{R}[x]$ denote the ring of all polynomials with real coefficients. The mapping $f(x) \to f(1)$ is a ring homomorphism from $\mathbb{R}[x]$ onto $\mathbb{R}$. △

Theorem 5.5.5 (Properties of ring homomorphisms)**.** *Let ϕ be a ring homomorphism from a ring R to a ring S. Let A be a subring of R and let B be an ideal of S.*

1. *For any $r \in R$ and any positive integer n, $\phi(nr)=n\phi(r)$ and $\phi(r^n)=(\phi(r))^n$.*
2. *$\phi(A)=\{\phi(A) \mid a \in A\}$ is a subring of S.*
3. *If A is an ideal and ϕ is onto S, then $\phi(A)$ is an ideal.*
4. *$\phi^{-1}(B)=\{r \in R \mid \phi(r) \in B\}$ is an ideal of R.*
5. *If R is commutative, then $\phi(R)$ is commutative.*
6. *If R has a unity 1, $S \neq \{0\}$, and ϕ is onto, then $\phi(1)$ is the unity of S.*

7. *ϕ is an isomorphism if and only if ϕ is onto and $Ker(\phi) = \{r \in R \mid \phi(r) = 0\} = \{0\}$.*

8. *If ϕ is an isomorphism from R onto S, then ϕ^{-1} is an isomorphism from S onto R.*

Theorem 5.5.6 (Kernels are ideals)**.** *Let ϕ be a ring homomorphism from a ring R to a ring S. Then $Ker(\phi) = \{r \in R \mid \phi(r) = 0\}$ is an ideal of R.*

Theorem 5.5.7 (First isomorphism theorem for Rings)**.** *Let ϕ be a ring homomorphism from R to S. Then the mapping from $R/Ker(\phi)$ to $\phi(R)$, given by $r + \ker\phi \to \phi(r)$, is an isomorphism.*

Theorem 5.5.8 (Ideals are kernels)**.** *Every ideal of a ring R is the kernel of a ring homomorphism of R. In particular, an ideal A is the kernel of the mapping $r \to r + A$ from R to R/A.*

Theorem 5.5.9 (Homomorphism from $\mathbb{Z}$ to a ring with unity)**.** *Let R be a ring with unity 1. The mapping $\phi : \mathbb{Z} \to R$ given by $n \to n \cdot 1$ is a ring homomorphism.*

Proof. To be a ring homomorphism we need to preserve both operations. Let ϕ be our mapping and $m, n \in \mathbb{Z}$, then starting with addition we have

$$\phi(m + n) = (m + n) \cdot 1 = m \cdot 1 + n \cdot 1 = \phi(m) + \phi(n).$$

For multiplication we have

$$\phi(mn) = (mn) \cdot 1 = (mn) \cdot ((1)(1)) = (m \cdot 1)(n \cdot 1) = \phi(m)\phi(n).$$

□

Corollary 5.5.10 (A ring with unity contains $\mathbb{Z}_n$ or $\mathbb{Z}$)**.** *If R is a ring with unity and the characteristic of R is $n > 0$, then R contains a subring isomorphic to $\mathbb{Z}_n$. If the characteristic of R is 0, then R contains a subring isomorphic to $\mathbb{Z}$.*

Corollary 5.5.11 ($\mathbb{Z}_m$ is a homomorphism image of $\mathbb{Z}$)**.** *For any positive integer m, the mapping of $\phi : \mathbb{Z} \to \mathbb{Z}_m$ given by $x \to x \bmod m$ is a ring homomorphism.*

5.6 Fields

Definition 5.6.1. A *field* is a commutative ring with unity in which every nonzero element is a unit.

Theorem 5.6.2. *A finite integral domain is a field.*

Corollary 5.6.3. *For every prime p, $\mathbb{Z}_p$, is a field.*

Example 5.6.4. Let

$$\begin{aligned}\mathbb{Z}_3[i] &= \{a + bi \mid a, b \in \mathbb{Z}_3\} \\ &= \{0, i, 2i, 1, 1 + i, 1 + 2i, 2, 2 + i, 2 + 2i\}.\end{aligned}$$

Where the addition and multiplication operations are as they are for complex numbers mod 3. In particular note that $-1 = 2$. With these operations $\mathbb{Z}_3[i]$ forms a field with 9 elements. △

Example 5.6.5. The real numbers with regular addition and multiplication form a field. △

5.7 Vector spaces

Definition 5.7.1 (Vector space)**.** A set V is said to be a vector space over a field F if V is a commutative group under addition and, if for each $a \in F$ and $v \in V$, there is an element $av \in V$ such that the following conditions hold for all $a, b \in F$ and all $u, v \in V$.

1. $a(v + u) = av + au$
2. $(a + b)v = av + bv$
3. $a(bv) = (ab)v$
4. $1v = v$.

The elements in V are called vectors while the elements from F are called scalars.

Example 5.7.2. The set

$$\mathbb{R}^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in \mathbb{R}\}$$

is a vector space over $\mathbb{R}$. Where the operations are elementwise addition and scalar multiplication. △

Example 5.7.3. The set $\mathsf{M}_2(\mathbb{Q})$ of 2 by 2 matrices with entries from $\mathbb{Q}$ is a vector space over $\mathbb{Q}$. The operations are

$$\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} + \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} = \begin{bmatrix} a_1 + b_1 & a_2 + b_2 \\ a_3 + b_3 & a_4 + b_4 \end{bmatrix}$$

and

$$b \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} = \begin{bmatrix} ba_1 & ba_2 \\ ba_3 & ba_4 \end{bmatrix}.$$

△

Example 5.7.4. The set $\mathbb{Z}_p[x]$ of polynomials with coefficients from $\mathbb{Z}_p$ is a vector space over $\mathbb{Z}_p$, where p is a prime.

More generally, if F is a field and $F[x]$ are the polynomials with coefficients from F, then $F[x]$ is a vector space. △

Definition 5.7.5 (Subspace)**.** Let V be a vector space over a field F and let U be a subset of V. We say that U is a *subspace* of V if U is also a vector space over F under the operations of V.

Definition 5.7.6 (Linear independence)**.** A set S of vectors is said to be *linearly dependet* over the field F if there are vectors $v_1, \dots v_n$ from S and elements $a_1, \dots a_n$ from F, not all zero, such that $a_1v_1 + \cdots + a_nv_n = 0$.

If a set of vectors is not linearly dependent, then we say they are *linearly independent*.

Definition 5.7.7 (Basis)**.** Let V be a vector space over F. A subset B of V is called a basis for V if B is linearly independent over F and every element of V is a linear combination of elements of B.

5.7.1 Exercises

1. Show that the correspondence $x \to 5x$ from $\mathbb{Z}_5$ to $\mathbb{Z}_{10}$ does not preserve addition.
2. Show that the correspondence $x \to 3x$ from $\mathbb{Z}_4$ to $\mathbb{Z}_{12}$ does not preserve multiplication.
3. Prove that every ring homomorphism ϕ from $\mathbb{Z}_n$ to itself has the form $\phi(x) = ax$, where $a^2 = a$.
4. Determine whether or not the set
$$\left\{ \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \right\}$$
is linearly independent over $\mathbb{Z}_5$.
5. Let $V = \mathbb{R}^3$, determine if the following are a subspace of V.
   (a) $W = \{(a, b, c) \in V \mid a^2 + b^2 = c^2\}$.
   (b) $W = \{(a, b, c) \in V \mid a + b = c\}$.

5.7.2 Solutions

1. Show that the correspondence $x \to 5x$ from $\mathbb{Z}_5$ to $\mathbb{Z}_{10}$ does not preserve addition.

   Take
$$\phi(2) + \phi(3) = 5(2) + 5(3) = 10 + 15 = 5 \neq 0 = \phi(2 + 3) = \phi(0).$$

2. Show that the correspondence $x \to 3x$ from $\mathbb{Z}_4$ to $\mathbb{Z}_{12}$ does not preserve multiplication.

   Consider $x = 3$ and $y = 3$

   $$\phi(3(3)) = \phi(1) = 3 \neq 9 = \phi(3)\phi(3).$$

3. Prove that every ring homomorphism ϕ from $\mathbb{Z}_n$ to itself has the form $\phi(x) = ax$, where $a^2 = a$.

   First note that $\phi(x) = \phi(x \cdot 1) = x\phi(1)$. Let $a = \phi(1)$, now we need to show $a = a^2$. For this take

   $$a = \phi(1) = \phi(1(1)) = \phi(1)\phi(1) = a^2.$$

4. Determine whether or not the set

   $$\left\{ \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \right\}$$

   is linearly independent over $\mathbb{Z}_5$.

   To determine if these vectors are linerly independent we can setup the following equation

   $$a \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} + b \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix} + c \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2a + c & a + b + c \\ a + b + c & 2b + c \end{bmatrix}.$$

   Thus for this to be zero we need

   $$2a + c = 0, \ a + b + c = 0, \text{ and } 2b + c = 0.$$

   With this we can see that $a = b$ and $-2b = c$. Thus if we take $a = 1$, $b = 1$, and $c = -2$, then we get zero. Since these are not all zero, we have that the system is linearly dependent.

5. Let $V = \mathbb{R}^3$, determine if the following are a subspace of V.

   (a) $W = \{a, b, c\} \in V \mid a^2 + b^2 = c^2\}$.
   Not a subspace, consider $(1, 1, 2) \in W$, but $2(1, 1, 2) \notin W$.

   (b) $W = \{(a, b, c) \in V \mid a + b = c\}$.

5.8 Polynomial rings

Definition 5.8.1 (Ring of polynomials)**.** Let R be a commutative ring. The set of formal symbols

$$R[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in R, \ n \text{ is a nonnegative integer}\}.$$

is called the *ring of polynomials* over R in the indeterminant x.

Two elements

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

and

$$b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

of $R[x]$ are considered equal if and only if $a_i = b_i$ for all nonnegative integers i.

Theorem 5.8.2. *If D is an integral domain, then $D[x]$ is an integral domain.*

We care about integral domains because they behave like the integers. Now that we have that $D[x]$ is an integral domain whenever D is an integral domain, we can start to take tools that we fequently use on the integers and extend them to polynomials.

Theorem 5.8.3 (Division Algorithm for a polynomial over a field)**.** *Let F be a field and let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exists unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$ and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.*

Example 5.8.4. Consider $f(x) = 3x^4 + x^3 + 2x^2 + 1$ and $g(x) = x^2 + 4x + 2$ where $f(x)$ and $g(x)$ belong to $\mathbb{Z}_5[x]$. We can apply the division algorithm to get

$$3x^4 + x^3 + 2x^2 + 1 = (x^2 + 4x + 2)(3x^2 + 4x) + 2x + 1.$$

△

Corollary 5.8.5 (Remainder theorem)**.** *Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.*

Corollary 5.8.6 (Factor theorem)**.** *Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then a is a zero of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.*

Theorem 5.8.7. *A polynomial of degree n over a field has at most n zeros, counting multiplicity.*

Theorem 5.8.8. *Let F be a field. Then $F[x]$ is a principal ideal domain.*

Theorem 5.8.9. *Let F be a field, I a nonzero ideal in $F[x]$, and $g(x)$ an element of $F[x]$. Then, $I = \langle g(x) \rangle$ if and only if $g(x)$ is a nonzero polynomial of minimum degree in I.*

Example 5.8.10. Consider the homomorphism ϕ from $\mathbb{R}[x]$ onto $\mathbb{C}$ given by $f(x) \to f(i)$. Then $x^2 + 1 \in \ker \phi$ and is clearly a polynomial of minimum degree in $\ker \phi$. Thus, $\ker \phi = \langle x^2 + 1 \rangle$ and $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ is isomorphic to $\mathbb{C}$. △

5.9 Factorization of polynomials

Definition 5.9.1. Let D be an integral domain. A polynomial $f(x)$ from $D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be *irreducible* over D if, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$, with $g(x)$ and $h(x)$ from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$.

A nonzero, nonunit element of $D[x]$ that is not irreducible over D is called *reducible*.

Example 5.9.2. The polynomial $f(x) = 2x^2 + 4$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{Z}$, since $2x^2 + 4 = 2(x^2 + 2)$ and neither 2 nor $x^2 + 2$ is a unit in $\mathbb{Z}[x]$.

The polynomial f is irreducible over $\mathbb{R}$ but reducible over $\mathbb{C}$. It is irreducible over $\mathbb{R}$ for the same reason it is irreducible over $\mathbb{Q}$, but when we move to $\mathbb{C}$ we can factor it as $f(x) = (x - i\sqrt{2})(x + i\sqrt{2})$ △

Theorem 5.9.3. *Let F be a field. If $f(x) \in F[x]$ and $\deg f(x)$ is 2 or 3, then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.*

Definition 5.9.4 (Primitive polynomial)**.** A *primitive polynomial* is an element of $\mathbb{Z}[x]$ where the greatest common divisor of the coefficients of the polynomial is 1.

Lemma 5.9.5 (Gauss's lemma)**.** *The product of two primitive polynomials is primitive.*

Theorem 5.9.6. *Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.*

Theorem 5.9.7. *Let F be a field and let $p(x) \in F[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in $F[x]$ if and only if $p(x)$ is irreducible over F.*

Corollary 5.9.8. *Let F be a field and $p(x)$ be an irreducible polynomial over F. Then $F[x]/\langle p(x) \rangle$ is a field.*

Corollary 5.9.9. *Let F be a field and let $p(x), a(x), b(x) \in F[x]$. If $p(x)$ is irreducible over F and $p(x)|a(x)b(x)$, then $p(x)|a(x)$ or $p(x)|b(x)$.*

The above corollary gives us a way to factor polynomials. A consequence that we don't have time to get to is that under certain conditions we can factor polynomials uniquely into a product of irreducible components. You may recognize doing this when we write a polynomial as a product of its roots, since those are exactly its irreducible pieces in $\mathbb{C}[x]$.

5.9.1 Exercises

1. How many zeros does $x^2 + 7$ have in $\mathbb{Z}_8$?
2. Let $f(x) = 5x^4 + 3x^3 + 1$ and $g(x) = 3x^2 + 2x + 1$ in $\mathbb{Z}_7[x]$. Determine the quotient and remainder of dividing $f(x)$ by $g(x)$.
3. Are there any non-constant polynomials in $\mathbb{Z}[x]$ that have a multiplicative inverse? What about for $\mathbb{Z}_p[x]$ when p is prime?
4. Let $f(x) \in \mathbb{R}[x]$. Suppose that $f(a) = 0$, but $f'(a) \neq 0$, where $f'(x)$ is the derivative of $f(x)$. Show that a is a zero of $f(x)$ of multiplicity 1.
5. Construct a field of order 25.
6. Show that $x^3 + x^2 + x + 1$ is reducible over $\mathbb{Q}$.

5.9.2 Solutions

1. How many zeros does $x^2 + 7$ have in $\mathbb{Z}_8$?

   Since we are in a finite ring we can just check all the options, this gives that $1, 3, 5, 7$ are all zeros.

   Note that this does not cause problems for our theorem that says a degree n polynomial can have at most n zeros since that is only for fields and $\mathbb{Z}_8$ is not a field.

2. Let $f(x) = 5x^4 + 3x^3 + 1$ and $g(x) = 3x^2 + 2x + 1$ in $\mathbb{Z}_7[x]$. Determine the quotient and remainder of dividing $f(x)$ by $g(x)$.

3. Are there any non-constant polynomials in $\mathbb{Z}[x]$ that have a multiplicative inverse? What about for $\mathbb{Z}_p[x]$?

   No, when you multiply two polynomials from $\mathbb{Z}[x]$ of degree greater than 0 together the resulting degree is the sum of the two polynomials degree. This gives that only constant polynomials can have inverses, and for $\mathbb{Z}[x]$ this means only $1, -1$ have inverses.

   For $\mathbb{Z}_p[x]$ the answer is still no. $\mathbb{Z}_p$ is a field and so the same property as above holds where the product of two polynomials gives the sum of their degrees.

4. Let $f(x) \in \mathbb{R}[x]$. Suppose that $f(a) = 0$, but $f'(a) \neq 0$, where $f'(x)$ is the derivative of $f(x)$. Show that a is a zero of $f(x)$ of multiplicity 1.

   If $f(a) = 0$, then we can factor f into $f(x) = (x - a)^m g(x)$. The goal is to now show that $m = 0$. To do this take the derivative of f which gives

   $$f'(x) = m(x - a)^{m-1} g(x) + (x - a)^m g'(x).$$

   Now $f'(a) = m(0)^{m-1} g(a) + 0^m g'(a)$, thus if $m \neq 1$, then we would have that $f'(a) = 0$.

5. Construct a field of order 25.

   Let

   $$\mathbb{Z}_5[i] = \{a + bi \mid a, b \in \mathbb{Z}_5\}.$$

   Where the addition and multiplication operations are as they are for complex numbers mod 5. In particular note that $-1 = 4$. With these operations $\mathbb{Z}_5[i]$ forms a field with 25 elements.

6. Show that $x^3 + x^2 + x + 1$ is reducible over $\mathbb{Q}$.

   This polynomial is reducible since we can factor it into $(x + 1)(x^2 + 1)$.

Chapter 6

Applications of rings and fields

6.1 Insolvability of the quintic

Question 6.1.1. What are the roots to $f(x) = x^2 + 4x - 5$?

We can fairly easily solve this by either visually factoring or plugging this into the quadratic formula. Which gives

$$x = -5 \quad \text{and} \quad x = 1.$$

Theorem 6.1.2. *Given a polynomial $ax^2 + bx + c$, the roots are*

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

This formula has been known for thousands of years. We can extend this formula to both cubic and quartic equations. Their formulas are too long and complicated to give here, but as a partial example the equation

$$x^3 + bx + c = 0$$

has the three solutions

$$\begin{gathered} A + B, \\ -\frac{A+B}{2} + \sqrt{-3}\left(\frac{A-B}{2}\right) \\ -\frac{A+B}{2} - \sqrt{-3}\left(\frac{A-B}{2}\right) \end{gathered}$$

where

$$A = \left(\frac{-c}{2} + \sqrt{\frac{b^3}{27} + \frac{c^2}{4}}\right)^{1/3} \quad \text{and} \quad B = \left(\frac{-c}{2} - \sqrt{\frac{b^3}{27} + \frac{c^2}{4}}\right)^{1/3}.$$

The general formula's for the cubic and quartic were both developed in the 16th century. Finding them caused a major stir in the math community at the time and there was a massive push for a more general formula, or algorithmic process that would give the roots.

However, Abel and Galois showed the following theorem.

Theorem 6.1.3 (Insolvability of the quintic)**.** *Let*

$$f(x) = a_1x^5 + a_2x^4 + a_3x^3 + a_4x^2 + a_5x + a_6,$$

then there is no general formula for the roots of f using addition, subtraction, multiplication, division, roots, and powers.

The proof of this can be reached in a second course on abstract algebra if Galois theory is the focus. For the class we will attempt to reach a sketch of the proof.

Definition 6.1.4. A field E is an *extension field* of a field F if $F \subseteq E$ and the operations of F are those of E restricted to F.

Theorem 6.1.5 (Fundamental theorem of field theory)**.** *Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there is an extension field E of F in which $f(x)$ has a zero.*

Example 6.1.6. Let $f(x) = x^2 + 1 \in \mathbb{Q}[x]$. Then we can build the extension field $E[x] = (\mathbb{Q}[x]/\langle x^2 + 1\rangle)[x]$. Note that in $E[x]$ we have

$$f(x + \langle x^2 + 1\rangle) = (x + \langle x^2 + 1\rangle)^2 + 1 = x^2 + 1\langle x^2 + 1\rangle = 0 + \langle x^2 + 1\rangle.$$

Thus with this we have constructed a field that contains the rational numbers and a zero for the polynomial $x^2 + 1$ by using only rational numbers. △

For a field F, the notation $F(a_1, a_2, \ldots, a_n)$ means the smallest field extension of F that contains $a_1, \ldots, a_n$.

Definition 6.1.7. Let E be an extension field of F and let $f(x) \in F[x]$ with degree at least 1. We say that $f(x)$ *splits* in E if there are elements $a \in F$ and $a_1, \ldots, a_n \in E$ such that

$$f(x) = a(x - a_1)(x - a_2)\ldots(x - a_n).$$

We call E a *splitting field* for $f(x)$ over F if

$$E = F(a_1, \ldots, a_n).$$

The important idea with the splitting field is that for a given f, within E f can be written as a product of linera factors in E.

Theorem 6.1.8. *Let F be a field and let $f(x)$ be a nonconstant element of $F[x]$. Then there exists a a splitting field E for $f(x)$ over F.*

Definition 6.1.9 (Solvable by Radicals)**.** Let F be a field, and let $f(x) \in F[x]$. We say that $f(x)$ is *solvable by radicals* over F if $f(x)$ splits in some extension $F(a_1, a_2, \ldots, a_n)$ of F and there exist positive integers $k_1, \ldots, k_n$ such that $a_1^{k_1} \in F$ and $a_i^{k_i} \in F(a_1, \ldots, a_{a_{i-1}})$ for $i = 2, \ldots, n$.

Example 6.1.10. Let $\omega = \sqrt{2}/2 + i\sqrt{2}/2$. Then $x^8 - 3$ splits in $Q(\omega, (3)^{1/8})$ since $\omega^8 \in \mathbb{Q}$, and $(3^{1/8})^8 \in \mathbb{Q}$. Thus, $x^8 - 3$ is solvable by radicals over $\mathbb{Q}$. In particular, they are

$$\pm(3^{1/8}),\ \pm(3^{1/8})\sqrt{-1},\ \pm(3^{1/8})\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{-1}\sqrt{2}}{2}\right),\ \pm(3^{1/8})\left(\frac{\sqrt{2}}{2} - \frac{\sqrt{-1}\sqrt{2}}{2}\right).$$

△

Thus, the question of can I solve this polynomial by radicals, can be turned into a question about field extensions.

Next we will bring it into a question of groups. But we need a couple more tools.

Definition 6.1.11. Let E be an extension field of the field F. An *automorphism* of E is a ring isomorphism from E onto E.

The *Galois group* of E over F, $\mathrm{Gal}(E/F)$, is the set of all automorphism of E that take every element of F to itself.

Example 6.1.12. Consider the extension $\mathbb{Q}(\sqrt{2})$ of $\mathbb{Q}$, the possible automorphisms that fix $\mathbb{Q}$ are completely determined by where $\sqrt{2}$ gets mapped. Thus, if ϕ is an automorphism of $\mathbb{Q}(\sqrt{2})$, then

$$2 = \phi(2) = \phi(\sqrt{2}\sqrt{2}) = (\phi(\sqrt{2}))^2,$$

giving that $\phi(\sqrt{2}) = \pm 2$. This shows that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ has two elements, the identity mapping ($\phi(\sqrt{2}) = \sqrt{2}$) and the mapping that send $a + b\sqrt{2}$ to $a - b\sqrt{2}$. △

Theorem 6.1.13 (Fundamental Theorem of Galois theory)**.** *Let F be a field of characteristic 0 or a finite field. If E is the splitting field over F for some polynomial in $F[x]$, then the mapping from the set of subfields of E containing F to the set of subgroups of $Gal(E/F)$ given by $K \to Gal(E/K)$ is a one-to-one correspondence.*

The above theorem gives us the tool to convert the problem into group theory. That is, if we want to show the quintic can't exist we first use the solvable by radicals definition to ask is there a field extension that the polynomial splits over. Then we use the fundamental theorem of Galois theory to say finding the splitting field is the same as finding a Galois group. Before we get to our main punchline we need one last piece of notation.

Definition 6.1.14 (Solvable group)**.** We say that a group G is *solvable* if G has a series of subgroups

$$\{e\} = H_0 \subset H_1 \subset H_2 \subset \cdots \subset H_k = G,$$

where, for each $0 \leq i < k$, H_i is normal in H_{i+1} and H_{i+1}/H_i is commutative.

Theorem 6.1.15 (Solvable by radical if and only if solvable group)**.** *Let F be a field of characteristic 0 and let $f(x) \in F[x]$, then $f(x)$ is solvable by radicals if and only if Gal(E/F) is solvable where E is the splitting field for f over F.*

With the above Theorem, you can show that a general quintic polynomial does not yield a solvable Galois group. This result also highlights the power of group theory. Not only did we show that this one thing is impossible, we gave a general method for determining when it is possible over any type of field. Hence, in pursuit of the solution to this specific problem, mathematicians were able to prove a much broader question.

To end this section, we give an explicit example of such a polynomial.

Example 6.1.16. Consider $g(x) = 3x^5 - 15x + 5$. You can easily show that the three real roots of g lie in the region between $[-2, 2]$ and numerical computation shows that they are approximately

$$0.33, \ -1.57, \text{ and } \ 1.4,$$

but there is no way to express these roots using radicals and elements in $\mathbb{Q}$. $\triangle$

6.2 Nonnegative matrices and Algebraic geometry

For our second application I want to highlight algebraic geometry, to further motivate this I will take it as an application to the nonnegative inverse eigenvalue problem (NIEP).

6.2.1 NIEP

Definition 6.2.1. Let $A \in \mathsf{M}_n(\mathbb{R})$ (a real coefficient n by n matrix), then we say that A is nonnegative, denoted $A \geq 0$ if it is entrywise nonnegative.

Question 6.2.2 (NIEP)**.** Give necessary and sufficient conditions for a list of complex numbers to be the spectrum (eigenvalues) of a nonnegative matrix.

Note that this is an inverse problem, so we are starting with the eigenvalues and trying to build matrices with certain properties (in this case nonnegative). This makes the problem substantially harder, since many matrices may have the same eigenvalues.

This question is very open and has only been solved for $n \leq 4$ with the solution of $n = 4$ being complicated enough that it is still an active area of research to simplify it.

To make this easier, we will instead focus on a subproblem.

Question 6.2.3. Give necessary and sufficient conditions for a list of real numbers to be the spectrum (eigenvalues) of a nonnegative symmetric matrix.

This is again only been solved for $n \leq 4$, but the solution for $n = 4$ is now only $1 + x + y + z \geq 0$ where the list of real numbers is $(1, x, y, z)$ with $-1 \leq z \leq y \leq x \leq 1$.

Before we jump into the algebraic geometry, I want to highlight some things about eigenvalues of matrices.

Recall the following definitions

Definition 6.2.4. Let $A \in \mathsf{M}_n(\mathbb{R})$, then the *characteristic polynomial* of A is

$$p_A(t) = \det(tI - A).$$

The *eigenvalues* of A are then the roots of $p_A(t)$.

With the above definition and what we learned from the Galois theory, you may be confused, if the problem is asking to solve for the roots of polynomials of degree greater than 5, then aren't we stuck?

This is where the algebraic geometry comes in, but first we need a couple of tools.

Definition 6.2.5. The kth elementary symmetric function of n complex numbers $\sigma = (\lambda_1, \lambda_2, \ldots, \lambda_n)$, for $k \leq n$ is

$$S_k(\sigma) = \sum_{1 \leq i_1 < \cdots < i_k \leq n} \prod_{j=1}^{k} \lambda_{i_j}.$$

For $n = 2$ the elementary symmetric functions are

$$\begin{aligned} S_1(\lambda_1, \lambda_2) &= \lambda_1 + \lambda_2 \\ S_2(\lambda_1, \lambda_2) &= \lambda_1 \lambda_2 \end{aligned}$$

For $n = 3$ the elementary symmetric functions are

$$\begin{aligned} S_1(\lambda_1, \lambda_2, \lambda_3) &= \lambda_1 + \lambda_2 + \lambda_3 \\ S_2(\lambda_1, \lambda_2, \lambda_3) &= \lambda_1 \lambda_2 + \lambda_1 \lambda_3 + \lambda_2 \lambda_3 \\ S_3(\lambda_1, \lambda_2, \lambda_3) &= \lambda_1 \lambda_2 \lambda_3 \end{aligned}$$

Definition 6.2.6. A minor of a matrix A is the determinant of sub matrix of A. A minor is called principal if the picked rows and columns of the submatrix are the same.

Definition 6.2.7. For a given matrix A, denote $E_k(A)$ to be the sums of the principal minors of size k of A.

These definitions lead to the powerful result.

Theorem 6.2.8. *For a given matrix A let*

$$p_A(t) = t^n + (-1)a_1 t^{n-1} + \cdots + (-1)^{n-1} a_{n-1} t + (-1)^n a_n$$

be its characteristic polynomial, then

$$a_k = E_k(A) = S_k(\sigma(A)).$$

This theorem gives us a way of relating the entries of the matrix directly to the eigenvalues, through a system of multivariable polynomial equations. The question is then, what does the restriction of nonnegativity do to the eigenvalues.

Definition 6.2.9. A **semi-algebraic set** is a subset of R^n of the form

$$\bigcup_{i=1}^{s} \bigcap_{j=1}^{r_i} \{x \in R^n \mid f_{i,j} *_{i,j} 0\},$$

where $f_{i,j} \in R[X_1, \ldots, X_n]$ and $*_{i,j}$ is either $>$, $\geq$, or $=$, for $i = 1, \ldots, s$ and $j = 1, \ldots, r_i$.

A **basic closed semi-algebraic** subset of R^n is a set of the form

$$\{x \in R^n \mid f_1(x) \geq 0, \ldots, f_s(x) \geq 0\},$$

where $f_1, \ldots, f_s \in R[X_1, \ldots, X_n]$.

A **basic open semi-algebraic** subset of R^n is a set of the form

$$\{x \in R^n \mid f_1(x) > 0, \ldots, f_s(x) > 0\},$$

where $f_1, \ldots, f_s \in R[X_1, \ldots, X_n]$.

Theorem 6.2.10. *Let $A \subset R^n$ be an open (resp. closed) semi-algebraic set. Then A is a finite union of basic open (resp. basic closed) semi-algebraic sets.*

Semi-algebraic sets are useful on their own as sets whose boundaries are defined by polynomial equations, but one of their main strengths is their stability through several types of natural operations. Most notably is if you project off a variable of a semi-algebraic set, the resulting set is still semi-algebraic. This result is given below.

Definition 6.2.11. Given a semi-algebraic set

$$S = \{(x, y) \in R^n \times R : \Phi(x, y)\}$$

where $\Phi(x, y)$ is some finite union and intersection of polynomial inequalities. The projection, $\pi : R^n \times R \to R^n$, of S is defined by

$$\pi(S) = \{x \in R^n : \exists y \ \Phi(x, y)\}.$$

The projection of a variable in a semi-algebraic set moves that variable from a free variable to a quantified variable. The following theorem, originally given by Tarski and Seidenberg in [**tarski1998**] and in [**seidenberg1954**], guarantees that the projected set is still semi-algebraic and the process of removing the quantifier from a system of polynomial inequalities is known as quantifier elimination.

Theorem 6.2.12 (Tarski-Seidenberg theorem)**.** *Let R be a real-closed field, let $\pi : R^n \times R^m \to R^n$ be the projection map, and let S be a semi-algebraic set in $R^n \times R^m$. Then $\pi(S)$ is a semi-algebraic set in R^n.*

6.3 Hilbert's Nullstellensatz

Theorem 6.3.1 (Hilbert's Nullstellensatz)**.** *Let k be a field with algebraic closure K, consider the polynomial ring $k[x_1, \ldots, x_n]$ and let I be an ideal in this ring. Define the set $V(I)$ to be all tuples in K^n such that $f(x) = 0$ for all f in I.*

Let $p \in F[x_1, \ldots, x_n]$ such that $p(x) = 0$ for all $x \in V(I)$, then there exists a natural number r such that $p^r \in I$.

Corollary 6.3.2 (Weak Nullstellensatz)**.** *The ideal $I \subseteq k[x_1, \ldots, x_n]$ contains 1 if and only if the polynomials in I do not have any common zeros in K^n.*

These two theorems form the basis for algebraic geometry. They give a direct connection between the algebraic object of the ideal, and the geometric object of roots of polynomials. Using these tools as a basis there has been a lot of reserach into the connections between algebra and geometry.

Example 6.3.3. Consider the system of polynomial equations

$$f(x, y) = x^2 + y^2 - 1$$
$$g(x, y) = x^2 + y^2 - 2.$$

We can tell directly that there are no points in $\mathbb{C}^2$ such that $f(x, y) = g(x, y) = 0$. However the Nullstellensatz gives the algorithm and the proof. We construct the ideal $\langle f(x, y), g(x, y) \rangle$, then we attempt to construct 1. To do this take $f(x, y) - g(x, y) = 1$. Thus f and g share no common zeros. This process can be done for any set of equations in any dimension. △