Abstract Algebra

Joseph R. Mileti

October 18, 2020

Contents

Chapter 1

Introduction

1.1 Abstraction

Each of the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ (that is, the natural numbers, the integers, the rational numbers, the real numbers, and the complex numbers) come equipped with naturally defined operations of addition and multiplication. When comparing the arithmetic in each of these settings, we see many similarities. For example, regardless of which of these "universes" of numbers we choose to work within, the order in which we add two numbers does not matter. In other words, we always have $a + b = b + a$ for all a and b. There are of course some differences between these worlds as well. In each of the first three sets, there is no number that can be multiplied by itself to produce 2, but such a number does exist in both $\mathbb{R}$ and $\mathbb{C}$.

When thinking about addition and multiplication, we initially gravitate toward working with *numbers*. However, at this point in your mathematical journey, you have seen how to perform these operations on more exotic objects: vectors, polynomials, matrices, functions, etc. In many of these cases, the normal properties of addition and multiplication are still true. For example, essentially all of the basic properties of addition and multiplication carry over to polynomials and functions. However, occasionally the operations of addition and multiplication that one defines fail to have the same properties. The "multiplication" of two vectors in $\mathbb{R}^3$ given by cross product is not commutative, nor is the multiplication of square matrices. When $n \geq 2$, the "multiplication" of two vectors in $\mathbb{R}^n$ given by the dot product takes two vectors and returns an element of $\mathbb{R}$ rather than an element of $\mathbb{R}^n$.

In linear algebra, we learn about *vector spaces*, which form one axiomatic system encapsulating fundamental properties of vector addition and scalar multiplication (i.e. multiplication by real numbers). By taking such an abstract axiomatic approach, we can collectively handle diverse vector spaces, like $\mathbb{R}^n$, polynomials, and continuous functions, all within one framework. In abstract algebra, we will study other axiom systems that capture (occasionally different) properties of addition, multiplication, etc. In other words, we will take some of the essential properties of these operations, codify them as axioms, and then study all occasions where they arise. Of course, we first need to ask the question: What is essential? Where do we draw the line for the properties that we enforce by fiat? A primary goal is to include enough axioms in to force an interesting theory, but keep enough out to leave the theory as general and robust as possible. The delicate balancing act of "interesting" and "general" is no easy task, but centuries of research have isolated a few important collections of axioms as fitting these requirements. Groups, rings, and fields are often viewed as the most central objects, although there are many other examples (such as semigroups, integral domains, etc.). Built upon these in various ways are many other structures, such as vector spaces, modules, and Lie algebras. We will emphasize the "big three", but will also spend a lot of time on integral domains and vector spaces, as well as introduce and explore a few others throughout our study.

Before diving into a study of these strange objects, one may ask "Why do we care?". We'll spend the rest of the sections of this chapter giving motivation, but we first introduce rough descriptions of the types of objects that we will study at a high level so that we can refer to them. Do not worry about the details at this point.

A *group* consists of a set of objects G together with a way of combining two objects to form another object, subject to a few axioms. If we use $\cdot$ to represent the "combination" operation, then the axioms are as follows:

1. *Associativity:* For all $a, b, c \in G$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
2. *Existence of an Identity:* There exists $e \in G$ such that for all $a \in G$, we have $a \cdot e = a$ and $e \cdot a = a$.
3. *Existence of Inverses:* For all $a \in G$, there exists $b \in G$ with $a \cdot b = e$ and $b \cdot a = e$ (where e is the identity described above).

For example, the set $\mathbb{Z}$ under the operation of addition is a group (with $e = 0$), as is $\mathbb{R}\backslash\{0\}$ under the operation of multiplication (with $e = 1$). A more interesting example is the set of all permutations (rearrangements) of a given set A under the natural combining operation that corresponds to permuting one after the other. More formally, the objects are the bijections from the given set A to itself, under the operation of function composition. For example, if $A = \{1, 2, 3\}$ and $f : A \to A$ and $g : A \to A$ are given by

$$\begin{array}{lll} f(1) = 1 & f(2) = 3 & f(3) = 2 \\ g(1) = 3 & g(2) = 1 & g(3) = 2, \end{array}$$

then we combine f and g to form the function $g \circ f : A \to A$ given by

$$(g \circ f)(1) = 3 \qquad (g \circ f)(2) = 2 \qquad (g \circ f)(3) = 1.$$

Taken together, the set of all bijections from A to itself together with function composition is called the *symmetric group*, or *group of all permutations*, of A. Although seemingly abstract, this group has many fascinating properties and interesting applications. For a toy example, consider the Rubik's Cube. If we label the individual squares on each of the faces with numbers from 1 to 54, then a valid transformation of the Rubik's Cube corresponds to a bijection from $\{1, 2, \dots, 54\}$ to itself (notice, however, that some bijections do not correspond to valid transformations of the cube). By understanding the "arithmetic" of the operation of function composition, we gain insight into how to solve the Rubik's Cube with a small number of moves.

A *ring* consists of a set of objects together with *two* ways of combining two objects to form another object, again subject to certain axioms. We call these operations addition and multiplication (even if they are not "natural" versions of addition and multiplication) because the axioms assert that they behave like the usual addition and multiplication operations on the familiar numbers. For example, we have a distributive law that says that $a(b + c) = ab + ac$ for all a, b, c. Each of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ under the usual operations are rings, but $\mathbb{N}$ is not (because it does not have additive inverses). A more exotic ring is the set of all $n \times n$ matrices with real entries under the addition and multiplication rules from linear algebra. Another interesting example is "modular arithmetic", where we work with the set $\{0, 1, 2, \dots, n - 1\}$ and add/multiply as usual, except that we cycle back around when we get a value of n or greater. For instance, consider the case when $n = 5$, where our set is $\{0, 1, 2, 3, 4\}$. To add two elements of this set, we first add them in the usual way, but repeatedly cycle around like a clock in order the find the correct value. In this setting, the sum $2 + 4$ will be 1, because once we hit 5 we cycle to 0, and then the value 6 is one further along. Similarly, we have that $3 \cdot 4$ will be 2 in this ring (because the number 12 cycles through these values twice, and then has 2 left over). We denote these rings by $\mathbb{Z}/n\mathbb{Z}$, and they are examples of finite rings that have many interesting number-theoretic properties.

A *field* is a special kind of ring that satisfies the additional requirement that every nonzero element has a multiplicative inverse (like $1/2$ is a multiplicative inverse for 2). Since elements of $\mathbb{Z}$ do not generally have multiplicative inverses, the ring $\mathbb{Z}$, under the usual operations, is not a field. However, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields under the usual operations, and roughly one thinks of general fields as behaving very much like these examples. It turns out that for primes numbers p, the modular arithmetic ring $\mathbb{Z}/p\mathbb{Z}$ is a fascinating example of a field with finitely many elements.

1.2 Power and Beauty

Throughout our study, we will encounter several exotic mathematical objects and operations. These algebraic structures are often intrinsically fascinating and beautiful, but they also play a fundamental role in understanding many of our typical mathematical objects. Moreover, they have several important applications both to important practical problems and to other areas of science and mathematics.

The complex numbers can be formed by starting with the real numbers, introducing a new number i (unfortunately called "imaginary" for historical reasons - blame Descartes!), proclaiming that $i^2 = -1$, and then closing off under addition and multiplication. Since i^2 is a real number, we can write this set as

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}.$$

Can we extend $\mathbb{C}$ further to include roots of other numbers, perhaps roots of the new numbers like i? Surprisingly, there is not need to do this, because $\mathbb{C}$ already has everything one would want in this regard! For example, one can check that

$$\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \cdot i\right)^2 = i,$$

so i has a square root. Not only is $\mathbb{C}$ closed under taking roots, but in fact *every* nontrivial polynomial with complex coefficients has a root in $\mathbb{C}$! Thus, the complex numbers are not "missing" anything from an algebraic point of view. We call fields with this property *algebraically closed*, and we will eventually prove that $\mathbb{C}$ is such a field.

Although often viewed as a mathematical curiosity to the uninitiated, the complex numbers arose naturally in the history of mathematics by providing ways to solve ordinary problems in mathematics that were inaccessible using standard techniques. In particular, they were surprisingly employed to find *real* roots to cubic polynomials by using the (at the time) mysterious multiplication and root operations on $\mathbb{C}$. Eventually, using complex numbers allowed mathematicians to calculate certain real integrals that resisted solutions arising from the tools of Calculus with real numbers. Complex numbers are now used in an essential way in many areas of science. They unify and simplify many concepts and calculations in electromagnetism and fluid flow. Moreover, they are fundamentally embedded in an essential way within quantum mechanics where "probability amplitudes" are measured using complex numbers rather than nonnegative real numbers. In fact, most of the counterintuitive features of quantum mechanics arise from the fact that "probabilities" are complex-valued.

Even though $\mathbb{C}$ is such a pretty and useful object that has just about everything one could want, that does not mean that we are unable to think about extending it further in different ways. William Hamilton tried to do this by adding something new, let's call it j, and thinking about how to do arithmetic with the set $\{a + bi + cj : a, b, d \in \mathbb{R}\}$. However, he was not able to define things like ij and j^2 in such a way that the arithmetic worked out nicely. One day, he had the inspired idea of going up another dimension and ditching commutativity of multiplication. In the process, he discovered the *quaternions*, which are the set of all "numbers" of the form

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

where $i^2 = j^2 = k^2 = -1$. We also need to explain how to multiply the elements i, j, k together, and this is where things become especially interesting. We multiply them in a cycle so that $ij = k$, $jk = i$ and $ki = j$. However, when we go backwards in the cycle we introduce a negative sign so that $ji = -k$, $kj = -i$, and $ik = -j$. We've lost commutativity of multiplication, but it turns out that $\mathbb{H}$ retains all of the other essential properties, and is an interesting example of a ring that is not a field. Although $\mathbb{H}$ has not found as many applications to science and mathematics as $\mathbb{C}$, it is still useful in some parts of physics and computer graphics to understand rotations in space. From a pure math perspective, by understanding the limitations of $\mathbb{H}$ and what properties fail, we gain a much deeper understanding of the role of commutativity of multiplication in fields like $\mathbb{R}$ and $\mathbb{C}$.

Instead of extending $\mathbb{C}$, we can work inside certain subsets of $\mathbb{C}$. One such example is the set of *Gaussian Integers*, which is

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

At first sight, this world of numbers seems strange. Unlike $\mathbb{C}$, it does not in general have multiplicative inverses. For example, there is no element of $\mathbb{Z}[i]$ that one can multiply $1 + i$ by to obtain 1. However, we'll see that it behaves like the integers $\mathbb{Z}$ in many ways, and moreover that an understanding of its algebraic properties gives us insight into the properties of the normal integers $\mathbb{Z}$. For example, just like how we define primes in the integers, we can define primes in $\mathbb{Z}[i]$ as well as those elements that can not factor in any "nontrivial" ways (there are a few subtleties about how to define nontrivial, but we will sweep them under the rug for now until we study these types of objects in more detail). For example, the number $5 \in \mathbb{Z}$ is certainly prime when viewed as a element of $\mathbb{Z}$. However, it is no longer prime when viewed in the larger ring $\mathbb{Z}[i]$ because we we can factor it as

$$5 = (2 + i)(2 - i).$$

We also have $13 = (3 + 2i)(3 - 2i)$, but 7 does not factor in any nontrivial way, and so is still prime in $\mathbb{Z}[i]$.

How can we tell which primes in $\mathbb{Z}$ stay prime in this new, larger world? Suppose that $p \in \mathbb{Z}$ is a prime which is the sum of two squares of integers. We can then fix $a, b \in \mathbb{Z}$ with $p = a^2 + b^2$. In the Gaussian integers $\mathbb{Z}[i]$ we have

$$p = a^2 + b^2 = (a + bi)(a - bi)$$

so the number p, which is prime in $\mathbb{Z}$, factors in an interesting manner over the larger ring $\mathbb{Z}[i]$. This is precisely what happened with $5 = 2^2 + 1^2$ and $13 = 3^2 + 2^2$ above. Somewhat amazingly, the converse of this result is true as well! In other words, a prime number $p \in \mathbb{Z}$ can be written as the sum of two squares if and only if it is no longer prime in $\mathbb{Z}[i]$. Thus, to solve a basic number theory question about primes, we can instead understand the arithmetic of a larger universe of numbers. We will eventually carry out this vision, and use it to show that an odd prime number $p \in \mathbb{Z}$ can be written as a sum of two squares if and only if it leaves a remainder of 1 when divided by 4. From here, we will be able to determine which integers (not just primes) can written as the sum of two squares.

1.3 Ciphers and Encryption

A *cipher* is a method to encrypt information in order to keep the true contents secret from anyone other than the intended recipient. Ciphers have been used throughout history to protect military communications and other sensitive information, but in the modern information age they are used far more widely. For example, when you send sensitive personal information across the internet (such as credit card information), it is important that nobody eavesdropping along the way can read it.

Suppose that we have some text that we want to scramble in some way. One of the simplest methods one can use to accomplish this task is through a *substitution cipher*. The basic idea is that we replace each letter of a message with another letter. For example, we replace every E with a W, every X with a P, etc. In order for this to work so that one can decode the message, we need to ensure that that we do not use the same code letter for two different ordinary letters, i.e. we can not replace every A with an N and also every B with an N. With this in mind, every substitution cipher is given by a permutation, or rearrangement, of the letters in the set $\{A, B, C, \ldots, Z\}$. In other words, a substitution cipher is really just an element of the symmetric group of $\{A, B, C, \ldots, Z\}$.

Although this cipher might work against a naive and unsophisticated eavesdropper, it is not at all secure. In fact, newspapers and magazines often use them as puzzles. The trick is that in any given language (like English), letters occurs with different frequencies. Thus, given an encoded message of any reasonable length, one can analyze frequencies of letters to obtain the most likely encodings of common letters like E and T. By making such a guess, one can then use that assumption to fill in (the most likely possibilities for) additional letters. Although it's certainly possible to guess incorrectly and result in the need to backtrack, using this method one can almost always decipher the message quite quickly.

In order to combat this simple attack, people developed substitution schemes that change based on the position. For example, we can use five different permutations, and switch between them based on the position of the letter. Thus, the letters in position 1, 6, 11, 16, etc. will all use one permutation, the letters in position 2, 7, 12, 17, etc. will use another, and so on. This approach works better, but it is still susceptible to the same frequency analysis attack if the message is long enough. If the person doing the coding doesn't divulge the number of permutations, or sometimes changes the number, then this adds some security. However, a sophisticated eavesdropper can still break these systems. Also, if the person doing the coding does change the number of permutations, there needs to be some way to communicate this change and the new permutations to the receiver, which can be difficult (after all, if they can arrange this transmission in secret, then why not just that secret means to send the actual message?).

In the previous example, the coding and decoding become unwieldy to carry out by hand if one used more than a few permutations. However, in the 20^{th} century, people created machines to mechanize this process so that the period (or number of steps before returning to the same permutation) was incredibly large. The most famous of these is known as the Enigma machine. Although initially developed for commercial purposes, the German military adopted enhanced versions of these machines to encode and decode military communications. The machines used by the Germans involved 3 or 4 "rotors". With these rotors fixed in a given position, the machine had encoded within it a certain permutation of the letters. However, upon pressing a key to learn the output letter according to that permutation, the machine would also turn (at least) one of the rotors, thus resulting in a new permutation of the letters. The period of a 3-rotor machine is $26^3 = 17,576$, so as long as the messages were less than this length, a permutation would not be repeated in the same message, and hence basic frequency analysis does not work.

If one knew the basic wiring of the rotors and some likely words (and perhaps possible positions of these words) that often occurred in military communications, then one can start to mount an attack on the Enigma machine. To complicate matters, the German military used machines with a manual "plugboard" in order to provide additional letter swaps in a given message. Although this certainly made cryptanalysis more difficult, some group theory facts (about the symmetric groups) played an essential role in the efforts of the Polish and British to decode messages. By the middle of World War II, the British employed group theory, statistical analysis, theoretical weaknesses in the Enigma machine (such as the fact that no letter was ever sent to itself), practical weaknesses in how the Enigma machines were used, specially built machines called "Bombes", along with a lot of hard human work to decode the majority of the German military communications. The resulting intelligence played an enormous role in allied operations and their eventual victory.

Modern day cryptography makes even more essential use of the algebraic objects we will study. One of the most widely used ciphers, known as AES (the "Advanced Encryption Standard") works by performing arithmetic in a field with $2^8 = 256$ many elements. Public-key cryptosystems and key-exchange algorithms like RSA and classical Diffie-Hellman work in the ring $\mathbb{Z}/n\mathbb{Z}$ of modular arithmetic. More sophisticated systems involve exotic finite groups based on certain "elliptic" curves, and these curves themselves are defined over interesting finite fields. We will eventually explain and explore several of these systems once we have developed the mathematical prerequisites.

Chapter 2

The Integers

2.1 Induction and Well-Ordering

We first recall three fundamental and intertwined facts about the natural numbers, namely Induction, Strong Induction, and Well-Ordering on $\mathbb{N}$. We will not attempt to "prove" them formally, nor precisely argue in what sense they are equivalent, because in order to do so in a satisfying manner we would need to clearly state our fundamental assumptions about $\mathbb{N}$. However, in each case, we do give a brief intuitive explanation for why each of these principles is true.

Fact 2.1.1 (Principle of Mathematical Induction on $\mathbb{N}$)**.** *Let $X \subseteq \mathbb{N}$. Suppose that*

- $0 \in X$ *(the* base case*)*
- $n + 1 \in X$ *whenever* $n \in X$ *(the* inductive step*)*

We then have that $X = \mathbb{N}$.

Let's quickly examine why we should believe in the Principle of Induction. Let X be a set of natural numbers that satisfies the two hypotheses. By the first assumption, we know that $0 \in X$. Since $0 \in X$, the second assumption tells us that $1 \in X$. Since $1 \in X$, the second assumption again tells us that $2 \in X$. By repeatedly applying the second assumption in this manner, each particular element of $\mathbb{N}$ is eventually determined to be in X.

In this argument, note that 5 is shown to be an element of X using only the assumption that 4 is an element of X. However, once we've arrived at 5, we've already shown that $0, 1, 2, 3, 4 \in X$, so why shouldn't we be able to make use of all of these assumptions when arguing that $5 \in X$? The answer is that we can, and this version of induction is sometimes called *strong induction*.

Fact 2.1.2 (Principle of Strong Induction on $\mathbb{N}$)**.** *Let $X \subseteq \mathbb{N}$. Suppose that $n \in X$ whenever $k \in X$ for all $k \in \mathbb{N}$ with $k < n$. We then have that $X = \mathbb{N}$.*

Thus, when arguing that $n \in X$, we are allowed to assume that we know all smaller numbers are in X. Notice that with this formulation we can even avoid the base case of checking 0 because of a technicality: If we have the above assumption, then $0 \in X$ because vacuously $k \in X$ whenever $k \in \mathbb{N}$ satisfies $k < 0$, simply because no such k exists. If that twist of logic makes you uncomfortable, feel free to argue a base case of 0 when doing strong induction.

The last of the three fundamental facts looks different from induction, but like induction is based on the concept that natural numbers start with 0 and are built by taking one discrete step at a time forward.

Fact 2.1.3 (Well-Ordering Property of $\mathbb{N}$)**.** *Suppose that $X \subseteq \mathbb{N}$ with $X \neq \emptyset$. There exists $k \in X$ such that $k \leq n$ for all $n \in X$.*

To see intuitively why this is true, suppose that $X \subseteq \mathbb{N}$ with $X \neq \emptyset$. If $0 \in X$, then we can take $k = 0$. Suppose not. If $1 \in X$, then since $1 \leq n$ for all $n \in \mathbb{N}$ with $n \neq 0$, we can take $k = 1$. Continue on. If we keep going until we eventually find $7 \in X$, then we have previously established that $0, 1, 2, 3, 4, 5, 6 \notin X$, so we can take $k = 7$. If we keep going forever consistently finding that each natural number is not in X, then we have determined that $X = \emptyset$, which is a contradiction.

We now give an example of proof by induction. Notice that in this case we start with the base case of 1 rather than 0.

Theorem 2.1.4. *For any $n \in \mathbb{N}^+$, we have*

$$\sum_{k=1}^{n}(2k-1) = n^2,$$

i.e.

$$1 + 3 + 5 + 7 + \cdots + (2n-1) = n^2.$$

Proof. We prove the result by induction. If we want to formally apply the above statement of induction, we are letting

$$X = \{n \in \mathbb{N}^+ : \sum_{k=1}^{n}(2k-1) = n^2\},$$

and using the principle of induction to argue that $X = \mathbb{N}^+$. More formally still if you feel uncomfortable starting with 1 rather than 0, we are letting

$$X = \{0\} \cup \{n \in \mathbb{N}^+ : \sum_{k=1}^{n}(2k-1) = n^2\}$$

and using the principle of induction to argue that $X = \mathbb{N}$, then forgetting about 0 entirely. In the future, we will not bother to make these pedantic diversions to shoehorn our arguments into the technical versions expressed above, but you should know that it is always possible to do so.

- *Base Case:* Suppose that $n = 1$. We have

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

  so the left hand-side is 1. The right-hand side is $1^2 = 1$. Therefore, the result is true when $n = 1$.

- *Inductive Step:* Suppose that for some fixed $n \in \mathbb{N}^+$ we know that

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

  Notice that $2(n+1) - 1 = 2n + 2 - 1 = 2n + 1$, hence

$$\begin{aligned}
\sum_{k=1}^{n+1}(2k-1) &= [\sum_{k=1}^{n}(2k-1)] + [2(n+1)-1] \\
&= [\sum_{k=1}^{n}(2k-1)] + (2n+1) \\
&= n^2 + (2n+1) && \text{(by induction)} \\
&= (n+1)^2
\end{aligned}$$

Since the result holds of 1 and it holds of $n+1$ whenever it holds of n, we conclude that the result holds for all $n \in \mathbb{N}^+$ by induction. $\square$

Before giving another example of a proof by induction, we first introduce some notation.

Definition 2.1.5. *Let $n, k \in \mathbb{N}$ with $k \leq n$. We define*

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$$

In combinatorics, we see that $\binom{n}{k}$ is the number of subsets of an n-element set that have size k. To see why, let's first consider the example where $n = 5$ and $k = 3$. We want to know how many subsets of $\{1, 2, 3, 4, 5\}$ have exactly 3 elements. The intuitive idea is to make 3 choices: First, pick one of the 5 elements to go into our set. Next, put one of the 4 remaining elements to add to it. Finally, finish off the process by picking one of the 3 remaining elements. For example, if we choose the sequence of numbers $1, 3, 5$, then we get the set $\{1, 3, 5\}$. From this reasoning, a natural guess is that there are $5 \cdot 4 \cdot 3$ many subsets with 3 elements. However, a set has neither repetition nor *order*, so a different sequence of choices can produce the same set. For example, picking the sequence $3, 5, 1$ also gives the set $\{1, 3, 5\}$. In fact, we arrive at the set $\{1, 3, 5\}$ in the following six ways:

$$\begin{array}{ccc} 1,3,5 & 1,5,3 & 3,1,5 \\ 3,5,1 & 5,1,3 & 5,3,1 \end{array}$$

In fact, *every* subset of $\{1, 2, 3, 4, 5\}$ with exactly 3 elements arises through 6 different sequences of choices because we can pick those 3 numbers in $3 \cdot 2 \cdot 1 = 6$ many ways. The fact that we count each element 6 times means that the total number of subsets of $\{1, 2, 3, 4, 5\}$ having exactly 3 elements equals

$$\frac{5 \cdot 4 \cdot 3}{3 \cdot 2 \cdot 1} = 10.$$

More generally, to count the number of subsets of an n-element set of size k, we first pick k elements in order without repetition in

$$n \cdot (n-1) \cdot (n-2) \cdots (n-(k-1)) = n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)$$

many ways (notice that we subtract $k-1$ instead of k at the end because we want k terms in the product and we start with $n = n - 0$). Now each particular subset arises from $k \cdot (k-1) \cdot (k-2) \cdots 2 \cdot 1 = k!$ many such choices because we can permute the given k elements in that many ways. Therefore, the number of subsets of an n-element set of size k is

$$\frac{n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)}{k!}$$

which we can rewrite as

$$\frac{n!}{k! \cdot (n-k)!}.$$

The following fundamental result gives a recursive way to calculate $\binom{n}{k}$.

Proposition 2.1.6. *Let $n, k \in \mathbb{N}$ with $k \leq n$. We have*

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}.$$

Proof. One extremely unenlightening proof is to expand out the formula on the right and do terrible algebraic manipulations on it. If you haven't done so, I encourage you to do it. If we believe the combinatorial description of $\binom{n}{k}$, here's a more meaningful combinatorial argument. Let $n, k \in \mathbb{N}$ with $k \leq n$. Consider a set X with $n+1$ many elements. To determine $\binom{n+1}{k+1}$, we need to count the number of subsets of X of size $k+1$. We do this as follows. Fix an arbitrary $a \in X$. Now an arbitrary subset of X of size $k+1$ fits into exactly one of the following types.

- The subset has a as an element. In this case, to completely determine the subset, we need to pick the remaining k elements of the subset from $X \backslash \{a\}$. Since $X \backslash \{a\}$ has n elements, the number of ways to do this is $\binom{n}{k}$.
- The subset does not have a as an element. In this case, to completely determine the subset, we need to pick all $k+1$ elements of the subset from $X \backslash \{a\}$. Since $X \backslash \{a\}$ has n elements, the number of ways to do this is $\binom{n}{k+1}$.

Putting this together, we conclude that the number of subsets of X of size $k+1$ equals $\binom{n}{k} + \binom{n}{k+1}$. □

Using this proposition, together with the fact that

$$\binom{n}{0} = 1 \qquad \text{and} \qquad \binom{n}{n} = 1$$

for all $n \in \mathbb{N}$, we can compute $\binom{n}{k}$ recursively to obtain the following table. The rows are labeled by n and the columns by k. To determine the number that belongs in a given square, we simply add the number above it and the number above and to the left. This table is known as *Pascal's Triangle*:

$\binom{n}{k}$	0	1	2	3	4	5	6	7
0	1	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0
2	1	2	1	0	0	0	0	0
3	1	3	3	1	0	0	0	0
4	1	4	6	4	1	0	0	0
5	1	5	10	10	5	1	0	0
6	1	6	15	20	15	6	1	0
7	1	7	21	35	35	21	7	1

One of the first things to note is that these numbers seem to appear in other places. For example, if $x, y \in \mathbb{R}$, then we have:

- $(x+y)^1 = x + y$.
- $(x+y)^2 = x^2 + 2xy + y^2$.
- $(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$.
- $(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$.

Looking at these, it appears that the coefficients are exactly the corresponding elements of Pascal's Triangle. What is the connection here? Notice that if we do not use commutativity and do not collect like terms, we have

$$\begin{aligned}
(x+y)^2 &= (x+y)(x+y) \\
&= x(x+y) + y(x+y) \\
&= xx + xy + yx + yy,
\end{aligned}$$

and so

$$\begin{aligned}(x+y)^3 &= (x+y)(x+y)^2 \\ &= (x+y)(xx+xy+yx+yy) \\ &= x(xx+xy+yx+yy)+y(xx+xy+yx+yy) \\ &= xxx+xxy+xyx+xyy+yxx+yxy+yyx+yyy.\end{aligned}$$

In other words, it looks like when we fully expand $(x+y)^n$, without using commutativity or collecting x's and y's, that we are getting a sum of all sequences of x's and y's of length n. Thus, if we want to know the coefficient of $x^{n-k}y^k$, then we need only ask how many such sequences have exactly k many y's (or equivalently exactly $n-k$ many x's), and the answer is $\binom{n}{k} = \binom{n}{n-k}$ because we need only pick out the position of the y's (or the x's). More formally, we can prove this by induction.

Theorem 2.1.7 (Binomial Theorem)**.** *Let $x, y \in \mathbb{R}$ and let $n \in \mathbb{N}^+$. We have*

$$\begin{aligned}(x+y)^n &= \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n \\ &= \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k\end{aligned}$$

Proof. We prove the result by induction. The base case when $n = 1$ is trivial. Suppose that we know the result for a given $n \in \mathbb{N}^+$. We have

$$\begin{aligned}(x+y)^{n+1} &= (x+y)\cdot(x+y)^n \\ &= (x+y)\cdot\left(\binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n\right) \\ &= \binom{n}{0}x^{n+1} + \binom{n}{1}x^n y + \binom{n}{2}x^{n-1}y^2 + \cdots + \binom{n}{n-1}x^2y^{n-1} + \binom{n}{n}xy^n \\ &\qquad + \binom{n}{0}x^n y + \binom{n}{1}x^{n-1}y^2 + \cdots + \binom{n}{n-2}x^2y^{n-1} + \binom{n}{n-1}xy^n + \binom{n}{n}y^{n+1} \\ &= x^{n+1} + \left(\binom{n}{1}+\binom{n}{0}\right)\cdot x^n y + \left(\binom{n}{2}+\binom{n}{1}\right)\cdot x^{n-1}y^2 + \cdots + \left(\binom{n}{n}+\binom{n}{n-1}\right)\cdot xy^n + y^{n+1} \\ &= \binom{n+1}{0}x^{n+1} + \binom{n+1}{1}x^n y + \binom{n+1}{2}x^{n-1}y^2 + \cdots + \binom{n+1}{n}xy^n + \binom{n+1}{n+1}y^{n+1}\end{aligned}$$

where we have used the lemma to combine each of the sums to get the last line. $\square$

2.2 Divisibility

Definition 2.2.1. *Let $a, b \in \mathbb{Z}$. We say that a* divides *b, and write $a \mid b$, if there exists $m \in \mathbb{Z}$ with $b = am$.*

For example, we have $2 \mid 6$ because $2 \cdot 3 = 6$ and $-3 \mid 21$ because $-3 \cdot 7 = 21$. We also have that $2 \nmid 5$ since it is "obvious" that no such integer exists. If you are uncomfortable with that (and you should be!), we will give methods to prove such statements in the next couple of sections.

Notice that $a \mid 0$ for every $a \in \mathbb{Z}$ because $a \cdot 0 = 0$ for all $a \in \mathbb{Z}$. In particular, we have $0 \mid 0$ because as noted we have $0 \cdot 0 = 0$. Of course we also have $0 \cdot 3 = 0$ and in fact $0 \cdot m = 0$ for all $m \in \mathbb{Z}$, so every integer serves as a "witness" that $0 \mid 0$. Our definition says nothing about the $m \in \mathbb{Z}$ being unique.

Proposition 2.2.2. *Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.*

Proof. Suppose that $a \mid b$ and $b \mid c$. Since $a \mid b$, we can fix $m \in \mathbb{Z}$ with $b = am$. Since $b \mid c$, we can fix $n \in \mathbb{Z}$ with $c = bn$. Notice that

$$\begin{aligned} c &= bn \\ &= (am)n \\ &= a(mn). \end{aligned}$$

Since $mn \in \mathbb{Z}$, it follows that $a \mid c$. □

Proposition 2.2.3. *Let $a, b, c \in \mathbb{Z}$.*

1. *If $a \mid b$, then $a \mid kb$ for all $k \in \mathbb{Z}$.*
2. *If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.*
3. *If $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for all $m, n \in \mathbb{Z}$.*

Proof.

1. Suppose that $a \mid b$. Let $k \in \mathbb{Z}$ be arbitrary. Since $a \mid b$, we can fix $m \in \mathbb{Z}$ with $b = am$. We then have
$$kb = k(am) = a(mk).$$
Since $mk \in \mathbb{Z}$, it follows that $a \mid kb$.

2. Suppose that $a \mid b$ and $a \mid c$. Since $a \mid b$, we can fix $m \in \mathbb{Z}$ with $b = am$. Since $a \mid c$, we can fix $n \in \mathbb{Z}$ with $c = an$. We then have
$$b + c = am + an = a(m + n).$$
Since $m + n \in \mathbb{Z}$, it follows that $a \mid b + c$.

3. Suppose that $a \mid b$ and $a \mid c$. Let $m, n \in \mathbb{Z}$ be arbitrary. Since $a \mid b$, we conclude from part (1) that $a \mid mb$. Since $a \mid c$, we conclude from part (1) again that $a \mid nc$. Using part (2), it follows that $a \mid (bm + cn)$.

□

Proposition 2.2.4. *Let $a, b \in \mathbb{Z}$. If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.*

Proof. Suppose that $a \mid b$ and $b \neq 0$. Fix $d \in \mathbb{Z}$ with $ad = b$. Since $b \neq 0$, we have $d \neq 0$. Thus, $|d| \geq 1$, and so

$$\begin{aligned} |b| &= |ad| \\ &= |a| \cdot |d| \\ &\geq |a| \cdot 1 \\ &= |a|. \end{aligned}$$

□

Corollary 2.2.5. *Let $a, b \in \mathbb{Z}$. If $a \mid b$ and $b \mid a$, then either $a = b$ or $a = -b$.*

Proof. Suppose that $a \mid b$ and $b \mid a$. Consider the following cases:

- *Case 1:* Suppose that $a \neq 0$ and $b \neq 0$. By the Proposition 2.2.4, we know that both $|a| \leq |b|$ and $|b| \leq |a|$. It follows that $|a| = |b|$, and hence either $a = b$ or $a = -b$.

- *Case 2:* Suppose now that $a = 0$. Since $a \mid b$, we may fix $m \in \mathbb{Z}$ with $b = am$. We then have

$$b = am = 0m = 0$$

as well. Therefore, $a = b$.

- *Case 3:* Suppose finally that $b = 0$. Since $b \mid a$, we may fix $m \in \mathbb{Z}$ with $a = bm$. We then have

$$a = bm = 0m = 0$$

as well. Therefore, $a = b$.

□

Given an integer $a \in \mathbb{Z}$, we introduce the following notation for the set of all divisors of a.

Definition 2.2.6. *Given $a \in \mathbb{Z}$, we let $Div(a) = \{d \in \mathbb{Z} : d \mid a\}$.*

For instance, we have $Div(7) = \{1, -1, 7, -7\}$ (don't forget the negatives!), which we can write more succinctly as $\{\pm 1, \pm 7\}$, while $Div(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$. For a more interesting example, we have $Div(0) = \mathbb{Z}$.

Proposition 2.2.7. *For any $a \in \mathbb{Z}$, we have $Div(a) = Div(-a)$.*

Proof. Exercise. □

2.3 Division with Remainder

The primary goal of this section is to prove the following deeply fundamental result.

Theorem 2.3.1. *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There exist unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$. Uniqueness here means that if $a = q_1 b + r_1$ with $0 \leq r_1 < |b|$ and $a = q_2 b + r_2$ with $0 \leq r_2 < |b|$, then $q_1 = q_2$ and $r_1 = r_2$.*

Here are a bunch of examples illustrating existence:

- If $a = 5$ and $b = 2$, then we have $5 = 2 \cdot 2 + 1$.
- If $a = 135$ and $b = 45$, then we have $135 = 3 \cdot 45 + 0$.
- If $a = 60$ and $b = 9$, then we have $60 = 6 \cdot 9 + 6$.
- If $a = 29$ and $b = -11$, then we have $29 = (-2)(-11) + 7$.
- If $a = -45$ and $b = 7$, then we have $-45 = (-7) \cdot 7 + 4$.
- If $a = -21$ and $b = -4$, then we have $-21 = 6 \cdot (-4) + 3$.

We begin by proving existence via a sequence of lemmas, starting in the case where a, b are natural numbers.

Lemma 2.3.2. *Let $a, b \in \mathbb{N}$ with $b > 0$. There exist $q, r \in \mathbb{N}$ such that $a = qb + r$ and $0 \leq r < b$.*

Proof. Fix $b \in \mathbb{N}$ with $b > 0$. For this fixed b, we prove the existence of q, r for all $a \in \mathbb{N}$ by induction. That is, for this fixed b, we define

$$X = \{a \in \mathbb{N} : \text{ There exist } q, r \in \mathbb{N} \text{ with } a = qb + r\}$$

and show that $X = \mathbb{N}$ by induction.

- *Base Case:* Suppose that $a = 0$. We then have $a = 0 \cdot b + 0$ and clearly $0 < b$, so we may take $q = 0$ and $r = 0$.
- *Inductive Step:* Suppose that we know the result for a given $a \in \mathbb{N}$. Fix $q, r \in \mathbb{Z}$ with $0 \leq r < b$ such that $a = qb + r$. We then have $a + 1 = qb + (r + 1)$. Since $r, b \in \mathbb{N}$ with $r < b$, we know that $r + 1 \leq b$. If $r + 1 < b$, then we are done. Otherwise, we have $r + 1 = b$, hence

$$\begin{aligned} a + 1 &= qb + (r + 1) \\ &= qb + b \\ &= (q + 1)b \\ &= (q + 1)b + 0 \end{aligned}$$

  and so we may take $q + 1$ and 0.

The result follows by induction. □

With this in hand, we now extend to the case where $a \in \mathbb{Z}$.

Lemma 2.3.3. *Let $a, b \in \mathbb{Z}$ with $b > 0$. There exist $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < b$.*

Proof. If $a \geq 0$, we are done by the previous lemma. Suppose that $a < 0$. We then have $-a > 0$, so by the previous lemma we may fix $q, r \in \mathbb{N}$ with $0 \leq r < b$ such that $-a = qb + r$. We then have $a = -(qb + r) = (-q)b + (-r)$. If $r = 0$, then $-r = 0$ and we are done. Otherwise we $0 < r < b$ and

$$\begin{aligned} a &= (-q)b + (-r) \\ &= (-q)b - b + b + (-r) \\ &= (-q - 1)b + (b - r) \end{aligned}$$

Now since $0 < r < b$, we have $0 < b - r < b$, so this gives existence. □

And now we can extend to the case where $b < 0$.

Lemma 2.3.4. *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There exist $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$.*

Proof. If $b > 0$, we are done by the previous lemma. Suppose that $b < 0$. We then have $-b > 0$, so by the previous lemma we can fix $q, r \in \mathbb{N}$ with $0 \leq r < -b$ and $a = q(-b) + r$. We then have $a = (-q)b + r$ and we are done because $|b| = -b$. □

With that sequence of lemmas building to existence now in hand, we finish off the proof of the theorem.

Proof of Theorem 2.3.1. The final lemma above gives us existence. Suppose that $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ and

$$q_1 b + r_1 = a = q_2 b + r_2,$$

where $0 \leq r_1 < |b|$ and $0 \leq r_2 < |b|$. We then have

$$b(q_1 - q_2) = r_2 - r_1,$$

hence $b \mid (r_2 - r_1)$. Now $-|b| < -r_1 \leq 0$, so adding this to $0 \leq r_2 < |b|$, we conclude that

$$-|b| < r_2 - r_1 < |b|,$$

and therefore

$$|r_2 - r_1| < |b|.$$

Now if $r_2 - r_1 \neq 0$, then since $b \mid (r_2 - r_1)$, we can use Proposition 2.2.4 to conclude that $|b| \leq |r_2 - r_1|$, a contradiction. It follows that $r_2 - r_1 = 0$, and hence $r_1 = r_2$. Since

$$q_1 b + r_1 = q_2 b + r_2$$

and $r_1 = r_2$, we conclude that $q_1 b = q_2 b$. Now $b \neq 0$, so we can divide both sides by b to conclude that $q_1 = q_2$. □

Proposition 2.3.5. *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Write $a = qb + r$ for the unique choice of $q, r \in \mathbb{Z}$ with $0 \leq r < |b|$. We then have that $b \mid a$ if and only if $r = 0$.*

Proof. If $r = 0$, then $a = qb + r = bq$, so $b \mid a$. Suppose conversely that $b \mid a$ and fix $m \in \mathbb{Z}$ with $a = bm$. We then have $a = mb + 0$ and $a = qb + r$, so by the uniqueness part of the above theorem, we must have $r = 0$. □

With this proposition in hand, we can now easily verify that $2 \nmid 5$ (the "obvious" fact that we alluded to in the previous section). Simply notice that $5 = 2 \cdot 2 + 1$ and $0 \leq 1 < 2$, so since the unique remainder is $1 \neq 0$, it follows that $2 \nmid 5$.

2.4 Common Divisors, GCDs, and the Euclidean Algorithm

Definition 2.4.1. *Suppose that $a, b \in \mathbb{Z}$. We say that $d \in \mathbb{Z}$ is a* common divisor *of a and b if both $d \mid a$ and $d \mid b$.*

We can write the set of common divisors of a and b as an intersection, i.e. given $a, b \in \mathbb{Z}$, the set of common divisors of a and b is the set $Div(a) \cap Div(b)$. For example, the set of common divisors of 120 and 84 is the set $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$. One way to determine the values in this set is to exhaustively determine each of the sets $Div(120)$ and $Div(84)$, and then comb through them both to find the common elements. However, we will work out a much more efficient way to solve such problems in this section.

The set of common divisors of 10 and 0 is $\{\pm 1, \pm 2, \pm 5, \pm 10\}$ because $Div(0) = \mathbb{Z}$, and hence the set of common divisors of 10 and 0 is just $Div(10) \cap Div(0) = Div(10) \cap \mathbb{Z} = Div(10)$. In contrast, every element of $\mathbb{Z}$ is a common divisor of 0 and 0, because $Div(0) \cap Div(0) = \mathbb{Z} \cap \mathbb{Z} = \mathbb{Z}$. The following little proposition is fundamental to this entire section.

Proposition 2.4.2. *Suppose that $a, b, q, r \in \mathbb{Z}$ and $a = qb + r$ (we do* not *assume that $0 \leq r < |b|$). We then have $Div(a) \cap Div(b) = Div(b) \cap Div(r)$, i.e.*

$$\{d \in \mathbb{Z} : d \text{ is a common divisor of } a \text{ and } b\} = \{d \in \mathbb{Z} : d \text{ is a common divisor of } b \text{ and } r\}.$$

Proof. We give a double containment proof:

- We first show that $Div(b) \cap Div(r) \subseteq Div(a) \cap Div(b)$. Let $d \in Div(b) \cap Div(r)$ be arbitrary. Since $d \mid b$, $d \mid r$, and

$$\begin{aligned} a &= qb + r \\ &= q \cdot b + 1 \cdot r, \end{aligned}$$

  we may use Proposition 2.2.3 to conclude that $d \mid a$. Therefore, $d \in Div(a) \cap Div(b)$.

- We now show that $Div(a) \cap Div(b) \subseteq Div(b) \cap Div(r)$. Let $d \in Div(a) \cap Div(b)$ be arbitrary. Since $d \mid a$, $d \mid b$, and

$$\begin{aligned} r &= a - qb \\ &= 1 \cdot a + (-q) \cdot b, \end{aligned}$$

  we may use Proposition 2.2.3 to conclude that $d \mid r$. Therefore, $d \in Div(b) \cap Div(r)$.

Since we have shown both containments, we conclude that $Div(a) \cap Div(b) = Div(b) \cap Div(r)$. $\square$

For example, suppose that we are trying to find the set of common divisors of 120 and 84, i.e. we want to understand the elements of the set $Div(120) \cap Div(84)$ (we wrote them above, but now want to justify it). We repeatedly perform division with remainder to reduce the problem as follows:

$$\begin{aligned} 120 &= 1 \cdot 84 + 36 \\ 84 &= 2 \cdot 36 + 12 \\ 36 &= 3 \cdot 12 + 0 \end{aligned}$$

The first line tells us that

$$Div(120) \cap Div(84) = Div(84) \cap Div(36).$$

The next line tells us that

$$Div(84) \cap Div(36) = Div(36) \cap Div(12).$$

The last line tells us that

$$Div(36) \cap Div(12) = Div(12) \cap Div(0).$$

Now $Div(0) = \mathbb{Z}$, so

$$Div(12) \cap Div(0) = Div(12).$$

Putting it all together, we conclude that

$$Div(120) \cap Div(84) = Div(12),$$

which is a more elegant way to determine the set of common divisors of 120 and 84 than the exhaustive process we alluded to above.

The above arguments illustrates the idea behind the following very general and important fact:

Theorem 2.4.3. *For all $a, b \in \mathbb{Z}$, there exists a unique $m \in \mathbb{N}$ such that $Div(a) \cap Div(b) = Div(m)$. In other words, for any $a, b \in \mathbb{Z}$, we can always find a natural number m such that the set of common divisors of a and b equals the set of divisors of m.*

We first sketch the idea of the proof of existence in the case where $a, b \in \mathbb{N}$. If $b = 0$, then since $Div(0) = \mathbb{Z}$, we can simply take $m = a$. Suppose then that $b \neq 0$. Fix $q, r \in \mathbb{N}$ with $a = qb + r$ and $0 \leq r < b$. Now the idea is to assert inductively the existence of an m that works for the pair of numbers (b, r) because this pair is "smaller" than the pair (a, b). The only issue is how to make this intuitive idea of "smaller" precise. There are several ways to do this, but perhaps the most straightforward is to only induct on b. Thus, our base case handles all pairs of form $(a, 0)$. Next, we handle all pairs of the form $(a, 1)$ and in doing this we can use the fact the we know the result for all pairs of the form $(a', 0)$. Notice that we can we even change the value of the first coordinate here, which is why we used the notation a'. Then, we handle all pairs of the form $(a, 2)$ and in doing this we can use the fact that we know the result for all pairs of the form $(a', 0)$ and $(a', 1)$. We now carry out the formal argument.

Proof. We begin by proving existence only in the special case where $a, b \in \mathbb{N}$. We use (strong) induction on b to prove the result. That is, we let

$$X = \{b \in \mathbb{N} : \text{For all } a \in \mathbb{N}, \text{ there exists } m \in \mathbb{N} \text{ with } Div(a) \cap Div(b) = Div(m)\}$$

and prove that $X = \mathbb{N}$ by strong induction.

- *Base Case:* Suppose that $b = 0$. Let $a \in \mathbb{N}$ be arbitrary. We then have that $Div(b) = \mathbb{Z}$, so

  $$Div(a) \cap Div(b) = Div(a) \cap \mathbb{Z} = Div(a),$$

  and hence we may take $m = a$. Since $a \in \mathbb{N}$ was arbitrary, we showed that $0 \in X$.

- *Inductive Step:* Let $b \in \mathbb{N}^+$ be arbitrary, and suppose that we know that the statement is true for all smaller natural numbers. In other words, we are assuming that $c \in X$ whenever $0 \leq c < b$. We prove that $b \in X$. Let $a \in \mathbb{N}$ be arbitrary. From above, we may fix $q, r \in \mathbb{Z}$ with $a = qb + r$ and $0 \leq r < b$. Since $0 \leq r < b$, we know by strong induction that $r \in X$, so we can fix $m \in \mathbb{N}$ with

$$Div(b) \cap Div(r) = Div(m).$$

  By Proposition 2.4.2, we have that $Div(a) \cap Div(b) = Div(b) \cap Div(r)$. Therefore, $Div(a) \cap Div(b) = Div(m)$. Since $a \in \mathbb{N}$ was arbitrary, we showed that $b \in X$.

Therefore, we have shown that $X = \mathbb{N}$, which implies that whenever $a, b \in \mathbb{N}$, there exists $m \in \mathbb{N}$ such that $Div(a) \cap Div(b) = Div(m)$.

To prove the result more generally when $a, b \in \mathbb{Z}$, we use Proposition 2.2.7. So, for example, if $a < 0$ but $b \geq 0$, we can fix $m \in \mathbb{N}$ with $Div(-a) \cap Div(b) = Div(m)$, and then use the fact that $Div(a) = Div(-a)$ to conclude that $Div(a) \cap Div(b) = Div(m)$. A similar argument works if $a \geq 0$ and $b < 0$, or if both $a < 0$ and $b < 0$.

For uniqueness, suppose that $m, n \in \mathbb{N}$ are such that both $Div(a) \cap Div(b) = Div(m)$ and also $Div(a) \cap Div(b) = Div(n)$. We then have that $Div(m) = Div(n)$. Since $m \in Div(m)$ trivially, we have that $m \in Div(n)$, so $m \mid n$. Similarly, we have $n \mid m$. Therefore, by Corollary 2.2.5, either $m = n$ or $m = -n$. Since $m, n \in \mathbb{N}$, we have $m \geq 0$ and $n \geq 0$, so it must be the case that $m = n$. □

With this great result in hand, we now turn our attention to a fundamental concept: greatest common divisors. Given $a, b \in \mathbb{Z}$, one might be tempted to define the greatest common divisor of a and b to be the *largest* natural number that divides both a and b (after all, the name *greatest* surely suggests this!). However, it turns out that this is a poor definition for several reasons:

1. Consider the case $a = 120$ and $b = 84$ from above. We saw that the set of common divisors of 120 and 84 is $Div(120) \cap Div(84) = Div(12)$. Thus, the *largest* natural number that divides both 120 and 84 is 12, but in fact 12 has a much stronger property: every common divisor of 120 and 84 is also a divisor of 12. This stronger property is surprising and much more fundamental that simply being the largest common divisor.

2. The integers have a natural ordering associated with them, but we will eventually (in Chapter 11) want to generalize the idea of a greatest common divisor to settings where there is no analogue of $\leq$.

3. There is one pair of integers where no largest common divisors exists! In the trivial case where $a = 0$ and $b = 0$, then *every* integer is a common divisor of a and b. Although this is a somewhat silly edge case, we would ideally like a definition that handles all cases elegantly.

With all of this background in mind, we now give our formal definition.

Definition 2.4.4. *Let $a, b \in \mathbb{Z}$. We say that an element $m \in \mathbb{Z}$ is a* greatest common divisor *of a and b if all of the following are true:*

- *$m \geq 0$.*
- *m is a common divisor of a and b.*
- *Whenever $d \in \mathbb{Z}$ is a common divisor of a and b, we have $d \mid m$.*

In other words, a greatest common divisor is a nonnegative integer, is a common divisor, and has the property that every common divisors happens to divide it. In terms of point 3 above, it is a straightforward matter to check that 0 is in fact a greatest common divisor of 0 and 0, because every element of $Div(0) \cap Div(0) = \mathbb{Z}$ is a divisor of 0.

Since we require more of a greatest common divisor than just picking the largest, we first need to check that they do indeed exist. However, the next proposition reduces this task to our previous work.

Proposition 2.4.5. *Let $a, b \in \mathbb{Z}$ and let $m \in \mathbb{N}$. The following are equivalent:*

1. *$Div(a) \cap Div(b) = Div(m)$.*
2. *m is a greatest common divisor of a and b.*

Proof. We first prove (1) $\Rightarrow$ (2): Suppose then that $Div(a) \cap (b) = Div(m)$. Since we are assuming that $m \in \mathbb{N}$, we have that $m \geq 0$. Since $m \mid m$, we have $m \in Div(m)$, so $m \in Div(a) \cap Div(b)$, and hence both $m \mid a$ and $m \mid b$. Now let $d \in \mathbb{Z}$ be an arbitrary common divisor of a and b. We then have that both $d \mid a$ and $d \mid b$, so $d \in Div(a) \cap Div(b)$, hence $d \in Div(m)$, and therefore $d \mid m$. Putting it all together, we conclude that m is a greatest common divisor of a and b.

We now prove (2) $\Rightarrow$ (1): Suppose that m is a greatest common divisor of a and b. We need to prove that $Div(a) \cap Div(b) = Div(m)$.

- We first show that $Div(a) \cap Div(b) \subseteq Div(m)$. Let $d \in Div(a) \cap Div(b)$ be arbitrary. We then have both $d \mid a$ and $d \mid b$, so since m is a greatest common divisor of a and b, we conclude that $d \mid m$. Therefore, $d \in Div(m)$.
- We now show that $Div(m) \subseteq Div(a) \cap Div(b)$. Let $d \in Div(m)$ be arbitrary, so $d \mid m$. Now we know that m is a common divisor of a and b, so both $m \mid a$ and $m \mid b$. Using Proposition 2.2.2, we conclude that both $d \mid a$ and $d \mid b$, so $d \in Div(a) \cap Div(b)$.

Since we have shown both $Div(a) \cap Div(b) \subseteq Div(m)$ and $Div(m) \subseteq Div(a) \cap Div(b)$, we conclude that $Div(a) \cap Div(b) \subseteq Div(m)$. □

Corollary 2.4.6. *Every pair of integers $a, b \in \mathbb{Z}$ has a unique greatest common divisor.*

Proof. Immediate from Theorem 2.4.3 and Proposition 2.4.5. □

Definition 2.4.7. *Let $a, b \in \mathbb{Z}$. We let $\gcd(a, b)$ be the unique greatest common divisor of a and b.*

For example we have $\gcd(120, 84) = 12$ and $\gcd(0, 0) = 0$. The following corollary now follows from Proposition 2.4.2.

Corollary 2.4.8. *Suppose that $a, b, q, r \in \mathbb{Z}$ and $a = qb + r$. We have $\gcd(a, b) = \gcd(b, r)$.*

The method of using repeated division and this corollary to reduce the problem of calculating greatest common divisors is known as the *Euclidean Algorithm*. We saw it in action of above with 120 and 84. Here is another example where we are trying to compute $\gcd(525, 182)$. We have:

$$\begin{aligned}
525 &= 2 \cdot 182 + 161 \\
182 &= 1 \cdot 161 + 21 \\
161 &= 7 \cdot 21 + 14 \\
21 &= 1 \cdot 14 + 7 \\
14 &= 2 \cdot 7 + 0,
\end{aligned}$$

so $\gcd(525, 182) = \gcd(7, 0) = 7$.

Let $a, b \in \mathbb{Z}$. Consider the set

$$\{ka + \ell b : k, \ell \in \mathbb{Z}\}.$$

This looks something like the *span* that you saw in Linear Algebra, but here we are only using integer coefficients, so we could describe this as the set of all *integer* combinations of a and b. Notice that if d is a common divisor of a and b, then $d \mid (ka + \ell b)$ for all $k, \ell \in \mathbb{Z}$ by Proposition 2.2.3, and hence d divides every element of this set. Applying this fact in the most interesting case where $d = \gcd(a, b)$ (since all other common divisors of a and b will divide $\gcd(a,b)$), we conclude that every element of $\{ka + \ell b : k, \ell \in \mathbb{Z}\}$ is a multiple of $\gcd(a,b)$. In other words, we have

$$\{ka + \ell b : k, \ell \in \mathbb{Z}\} \subseteq \{n \cdot \gcd(a,b) : n \in \mathbb{Z}\}.$$

What about the reverse containment? In particular, is $\gcd(a,b)$ always an element of $\{ka + \ell b : k, \ell \in \mathbb{Z}\}$? For example, is

$$12 \in \{k \cdot 120 + \ell \cdot 84 : k, \ell \in \mathbb{Z}\}?$$

We can attempt to play around to try to find a suitable value of k and ℓ, but there is a better way. Let's go back and look at the steps of the Euclidean Algorithm:

$$\begin{aligned}
120 &= 1 \cdot 84 + 36 \\
84 &= 2 \cdot 36 + 12 \\
36 &= 3 \cdot 12 + 0
\end{aligned}$$

Notice that the middle line can be manipulated to write 12 as an integer combination of 84 and 36:

$$12 = 1 \cdot 84 + (-2) \cdot 36.$$

With this in hand, we can work our way toward our goal by using the first line, which lets us write 36 as an integer combination of 120 and 84:

$$36 = 1 \cdot 120 + (-1) \cdot 84.$$

Now we can plug this expression of 36 in terms of 120 and 84 into the previous equation:

$$12 = 1 \cdot 84 + (-2) \cdot [1 \cdot 120 + (-1) \cdot 84].$$

From here, we can manipulate this equation (performing only additions and multiplications on the coefficients, not on 84 and 120 themselves!) to obtain

$$12 = (-2) \cdot 120 + 3 \cdot 84.$$

We now generalize this idea and prove that it is always possible to express $\gcd(a,b)$ as an integer combination of a and b. The proof is inductive, and follows a similar strategy to the proof of Theorem 2.4.3. Given $a, b \in \mathbb{N}$, here is the idea. To express $\gcd(a,b)$ as an integer combination of a and b, we first fix $q, r \in \mathbb{N}$ with $a = qb + r$ and $0 \leq r < b$. Now since (b,r) is "smaller" than (a,b), we inductively write $\gcd(b,r)$ as an integer combination of b and r. We then use this combination together with the equation $a = qb + r$ to write $\gcd(a,b)$ as an integer combination of a and b. Notice the similarity to the above argument where we have $120 = 1 \cdot 84 + 36$, and we used a known way to write 12 as an integer combination of 84 and 36 in order to write 12 as an integer combination of 120 and 84.

Theorem 2.4.9. *For all $a, b \in \mathbb{Z}$, there exist $k, \ell \in \mathbb{Z}$ with $\gcd(a,b) = ka + \ell b$.*

Proof. We begin by proving existence in the special case where $a, b \in \mathbb{N}$. We use induction on b to prove the result. That is, we let

$$X = \{b \in \mathbb{N} : \text{For all } a \in \mathbb{N}, \text{ there exist } k, \ell \in \mathbb{Z} \text{ with } \gcd(a,b) = ka + \ell b\}$$

and prove that $X = \mathbb{N}$ by strong induction.

- *Base Case:* Suppose that $b = 0$. Let $a \in \mathbb{N}$ be arbitrary. We then have that

  $$\gcd(a,b) = \gcd(a,0) = a$$

  Since $a = 1 \cdot a + 0 \cdot b$, so we may let $k = 1$ and $\ell = 0$. Since $a \in \mathbb{N}$ was arbitrary, we conclude that $0 \in X$.

- *Inductive Step:* Suppose then that $b \in \mathbb{N}^+$ and we know the result for all smaller nonnegative values. In other words, we are assuming that $c \in X$ whenever $0 \leq c < b$. We prove that $b \in X$. Let $a \in \mathbb{N}$ be arbitrary. From above, we may fix $q, r \in \mathbb{Z}$ with $a = qb + r$ and $0 \leq r < b$. We also know from above that $\gcd(a, b) = \gcd(b, r)$. Since $0 \leq r < b$, we know by strong induction that $r \in X$, hence there exist $k, \ell \in \mathbb{Z}$ with

$$\gcd(b, r) = kb + \ell r.$$

Now $r = a - qb$, so

$$\begin{aligned}\gcd(a, b) &= \gcd(b, r)\\ &= kb + \ell r\\ &= kb + \ell(a - qb)\\ &= kb + \ell a - qb\ell\\ &= \ell a + (k - q\ell)b.\end{aligned}$$

Since $a \in \mathbb{N}$ was arbitrary, we conclude that $b \in X$.

Therefore, we have shown that $X = \mathbb{N}$, which implies that whenever $a, b \in \mathbb{N}$, there exists $k, \ell \in \mathbb{Z}$ with $\gcd(a, b) = ka + \ell b$.

To prove the result more generally when $a, b \in \mathbb{Z}$, we again use Proposition 2.2.7. For example, if $a < 0$ but $b \geq 0$. Let $m = \gcd(a, b)$, so that $Div(m) = Div(a) \cap Div(b)$ by Proposition 2.4.5. Since $Div(-a) = Div(a)$, we also have $Div(m) = Div(-a) \cap Div(b)$, hence $m = \gcd(-a, b)$. Since $-a, b \in \mathbb{N}$, we can fix $k, \ell \in \mathbb{Z}$ with $\gcd(-a, b) = k(-a) + \ell b$. Using the fact that $\gcd(-a, b) = \gcd(a, b)$, we have $\gcd(a, b) = k(-a) + \ell b$, hence $\gcd(a, b) = (-k)a + \ell b$. Since $-k, \ell \in \mathbb{Z}$, we are done. A similar argument works if $a \geq 0$ and $b < 0$, or if both $a < 0$ and $b < 0$. □

Notice the basic structure of the above proof. If $a = qb + r$, and we happen to know $k, \ell \in \mathbb{Z}$ such that

$$\gcd(b, r) = kb + \ell r,$$

then we have

$$\gcd(a, b) = \ell a + (k - q\ell)b.$$

Given $a, b \in \mathbb{Z}$, this argument provides a recursive procedure in order to find an integer combination of a and b that gives $\gcd(a, b)$. Although the recursive procedure can be nicely translated to a computer program, we can carry it out directly by "winding up" the work created from the Euclidean Algorithm. For example, we saw above that $\gcd(525, 182) = 7$ by calculating:

$$\begin{aligned}525 &= 2 \cdot 182 + 161\\ 182 &= 1 \cdot 161 + 21\\ 161 &= 7 \cdot 21 + 14\\ 21 &= 1 \cdot 14 + 7\\ 14 &= 2 \cdot 7 + 0.\end{aligned}$$

We now use these steps in reverse to calculate:

$$\begin{aligned}
7 &= 1 \cdot 7 + 0 \cdot 0 \\
&= 1 \cdot 7 + 0 \cdot (14 - 2 \cdot 7) \\
&= 0 \cdot 14 + 1 \cdot 7 \\
&= 0 \cdot 14 + 1 \cdot (21 - 1 \cdot 14) \\
&= 1 \cdot 21 + (-1) \cdot 14 \\
&= 1 \cdot 21 + (-1) \cdot (161 - 7 \cdot 21) \\
&= (-1) \cdot 161 + 8 \cdot 21 \\
&= (-1) \cdot 161 + 8 \cdot (182 - 1 \cdot 161) \\
&= 8 \cdot 182 + (-9) \cdot 161 \\
&= 8 \cdot 182 + (-9) \cdot (525 - 2 \cdot 182) \\
&= (-9) \cdot 525 + 26 \cdot 182
\end{aligned}$$

This wraps everything up perfectly, but it is easier to simply start at the fifth line.

Now that we've showed that $\gcd(a,b) \in \{ka + \ell b : k, \ell \in \mathbb{Z}\}$ for all $a, b \in \mathbb{Z}$, we can now completely characterize the set of all integer combinations of a and b.

Corollary 2.4.10. *For all $a, b \in \mathbb{Z}$, we have $\{ka + \ell b : k, \ell \in \mathbb{Z}\} = \{n \cdot \gcd(a,b) : n \in \mathbb{Z}\}$.*

Proof. Let $a, b \in \mathbb{Z}$ be arbitrary. Let $m = \gcd(a,b)$. We give a double containment proof:

- $\{ka + \ell b : k, \ell \in \mathbb{Z}\} \subseteq \{nm : n \in \mathbb{Z}\}$: Let $c \in \{ka + \ell b : k, \ell \in \mathbb{Z}\}$ be arbitrary, and fix $k, \ell \in \mathbb{Z}$ with $c = ka + \ell b$. Since $m = \gcd(a,b)$, we have both $m \mid a$ and $m \mid b$. Using Proposition 2.2.3, we conclude that $m \mid c$. Therefore, we can fix $n \in \mathbb{Z}$ with $c = mn$, and hence $c \in \{nm : n \in \mathbb{Z}\}$.

- $\{nm : n \in \mathbb{Z}\} \subseteq \{ka + \ell b : k, \ell \in \mathbb{Z}\}$: Let $c \in \{nm : n \in \mathbb{Z}\}$ be arbitrary, and fix $n \in \mathbb{Z}$ with $c = nm$. Since $m = \gcd(a,b)$, we can use Theorem 2.4.9 to fix $k, \ell \in \mathbb{Z}$ with $m = ka + \ell b$. Multiplying both sides of this equation by n, we have $nm = nka + n\ell b$, so $c = (nk)a + (n\ell)b$. Since $nk, n\ell \in \mathbb{Z}$, it follows that $\{nm : n \in \mathbb{Z}\} \subseteq \{ka + \ell b : k, \ell \in \mathbb{Z}\}$.

Since we have shown both containments, it follows that $\{ka + \ell b : k, \ell \in \mathbb{Z}\} = \{n \cdot \gcd(a,b) : n \in \mathbb{Z}\}$. $\square$

Now that we have proved an interesting theorem about the ability to write $\gcd(a,b)$ as an integer combination of a and b, we turn to an extremely useful consequence of this result. We begin with a definition.

Definition 2.4.11. *Two integers $a, b \in \mathbb{Z}$ are* relatively prime *if* $\gcd(a,b) = 1$.

For example, we have that 40 and 33 are relatively prime, either by exhaustively checking divisors, or using the Euclidean Algorithm:

$$\begin{aligned}
40 &= 1 \cdot 33 + 7 \\
33 &= 4 \cdot 7 + 5 \\
7 &= 1 \cdot 5 + 2 \\
5 &= 2 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0.
\end{aligned}$$

Thus, $\gcd(40, 33) = \gcd(1, 0) = 1$. The following proposition will play an important role in proving the Fundamental Theorem of Arithmetic in the next section.

Proposition 2.4.12. *Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and $\gcd(a,b) = 1$, then $a \mid c$.*

Proof. Since $a \mid bc$, we may fix $n \in \mathbb{Z}$ with $bc = an$. Since $\gcd(a,b) = 1$, we can use Theorem 2.4.9 to fix $k, \ell \in \mathbb{Z}$ with $ak + b\ell = 1$. Multiplying this equation through by c we conclude that $akc + b\ell c = c$, so

$$\begin{aligned} c &= akc + \ell(bc) \\ &= akc + \ell(an) \\ &= a(kc + \ell n). \end{aligned}$$

Since $kc + \ell n \in \mathbb{Z}$, it follows that $a \mid c$. □

Before moving on, we work through another proof of the existence of greatest common divisors, along with the fact that we can write $\gcd(a,b)$ as an integer combination of a and b. This proof also works because of Theorem 2.3.1, but it uses well-ordering and establishes existence without a method of computation. One may ask why we bother with another proof. One answer is that this result is so fundamental and important that two different proofs help to reinforce its value. Another reason is that we will generalize each of these distinct proofs in Chapter 11 to slightly different settings.

Theorem 2.4.13. *Let $a, b \in \mathbb{Z}$ with at least one of a and b nonzero. The set*

$$\{ka + \ell b : k, \ell \in \mathbb{Z}\}$$

has positive elements, and the least positive element is a greatest common divisor of a and b. In particular, for any $a, b \in \mathbb{Z}$, there exist $k, \ell \in \mathbb{Z}$ with $\gcd(a,b) = ka + \ell b$.

Proof. Let

$$S = \{ka + \ell b : k, \ell \in \mathbb{Z}\} \cap \mathbb{N}^+$$

We first claim that $S \neq \emptyset$. If $a > 0$, then $a = 1 \cdot a + 0 \cdot b \in S$. Similarly, if $b > 0$, then $b \in S$. If $a < 0$, then $-a > 0$ and $-a = (-1) \cdot a + 0 \cdot b \in S$. Similarly, if $b < 0$, then $-b \in S$. Since at least one of a and b is nonzero, it follows that $S \neq \emptyset$. By the Well-Ordering property of $\mathbb{N}$, we know that S has a least element. Let $m = \min(S)$. Since $m \in S$, we may fix $k, \ell \in \mathbb{Z}$ with $m = ka + \ell b$. We claim that m is a greatest common divisor of a and b.

First, we need to check that m is a common divisor of a and b. We begin by showing that $m \mid a$. Fix $q, r \in \mathbb{Z}$ with $a = qm + r$ and $0 \leq r < m$. We want to show that $r = 0$. We have

$$\begin{aligned} r &= a - qm \\ &= a - m(ak + b\ell) \\ &= (1 - qk) \cdot a + (-q\ell) \cdot b. \end{aligned}$$

Now if $r > 0$, then we have shown that $r \in S$, which contradicts the choice of m as the least element of S. Hence, we must have $r = 0$, and so $m \mid a$.

We next show that $m \mid b$. Fix $q, r \in \mathbb{Z}$ with $b = qm + r$ and $0 \leq r < m$. We want to show that $r = 0$. We have

$$\begin{aligned} r &= b - qm \\ &= b - q(ak + b\ell) \\ &= (-qk) \cdot a + (1 - q\ell) \cdot b. \end{aligned}$$

Now if $r > 0$, then we have shown that $r \in S$, which contradicts the choice of m as the least element of S. Hence, we must have $r = 0$, and so $m \mid b$.

Finally, we need to check the last condition for m to be the greatest common divisor. Let d be a common divisor of a and b. Since $d \mid a$, $d \mid b$, and $m = ka + \ell b$, we may use Proposition 2.2.3 to conclude that $d \mid m$. □

2.5 Primes and Factorizations in $\mathbb{Z}$

Definition 2.5.1. *An element $p \in \mathbb{Z}$ is prime if $p > 1$ and the only positive divisors of p are 1 and p. If $n \in \mathbb{Z}$ with $n > 1$ is not prime, we say that n is* composite.

We begin with the following simple fact.

Proposition 2.5.2. *Every $n \in \mathbb{N}$ with $n > 1$ is a product of primes.*

Proof. We prove the result by strong induction on $\mathbb{N}$. If $n = 2$, we are done because 2 itself is prime. Suppose that $n > 2$ and we have proven the result for all k with $1 < k < n$. If n is prime, we are done. Suppose that n is not prime and fix a divisor $c \mid n$ with $1 < c < n$. Fix $d \in \mathbb{N}$ with $cd = n$. We then have that $1 < d < n$, so by induction, both c and d are products of primes, say $c = p_1p_2\cdots p_k$ and $d = q_1q_2\cdots q_\ell$ with each p_i and q_j prime. We then have

$$n = cd = p_1p_2\cdots p_kq_1q_2\cdots q_\ell$$

so n is a product of primes. The result follows by induction. □

Corollary 2.5.3. *Every $a \in \mathbb{Z}$ with $a \notin \{-1, 0, 1\}$ is either a product of primes, or -1 times a product of primes.*

Corollary 2.5.4. *Every $a \in \mathbb{Z}$ with $a \notin \{-1, 0, 1\}$ is divisible by at least one prime.*

Proposition 2.5.5. *There are infinitely many primes.*

Proof. We know that 2 is a prime, so there is at least one prime. We will take an arbitrary given finite list of primes and show that there exists a prime which is omitted. Suppose then that $p_1, p_2, \dots, p_k$ is an arbitrary finite list of prime numbers with $k \geq 1$. We show that there exists a prime not in the list. Let

$$n = p_1p_2\cdots p_k + 1$$

We have $n \geq 3$, so by the above corollary we know that n is divisible by some prime q. If $q = p_i$, we would have that $q \mid n$ and also $q \mid p_1p_2\cdots p_k$, so $q \mid (n - p_1p_2\cdots p_k)$. This would imply that $q \mid 1$, so $|q| \leq 1$, a contradiction. Therefore $q \neq p_i$ for all i, and we have succeeded in finding a prime not in the list. □

The next proposition uses our hard work on greatest common divisors. It really is the most useful property of prime numbers. In fact, when we generalize the idea of primes to more exotic and abstract contexts in Chapter 11, we will see this property is really of fundamental importance.

Proposition 2.5.6. *If $p \in \mathbb{Z}$ is prime and $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

Proof. Suppose that $p \mid ab$ and $p \nmid a$. Since $\gcd(a, p)$ divides p and we know that $p \nmid a$, we have $\gcd(a, p) \neq p$. The only other positive divisor of p is 1, so $\gcd(a, p) = 1$. Therefore, by the Proposition 2.4.12, we conclude that $p \mid b$. □

Now that we've handled the product of two numbers, we get the following corollary about finite products by a trivial induction.

Corollary 2.5.7. *If p is prime and $p \mid a_1a_2\cdots a_n$, then $p \mid a_i$ for some i.*

We now have all the tools necessary to provide the uniqueness of prime factorizations.

Theorem 2.5.8 (Fundamental Theorem of Arithmetic)**.** *Every natural number greater than 1 factors uniquely (up to order) into a product of primes. In other words, if $n \geq 2$ and*

$$p_1p_2\cdots p_k = n = q_1q_2\cdots q_\ell$$

with $p_1 \leq p_2 \leq \cdots \leq p_k$ and $q_1 \leq q_2 \leq \cdots \leq q_\ell$ all primes, then $k = \ell$ and $p_i = q_i$ for $1 \leq i \leq k$.

Proof. Existence follows from Proposition 2.5.2. We prove uniqueness by (strong) induction on n. Let $n \in \mathbb{N}$ with $n \geq 2$, and assume that every $m \in \mathbb{N}$ with $2 \leq m < n$ factors uniquely into a product of primes. We prove that n factors uniquely into primes. Let $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_\ell \in \mathbb{N}$ be primes with

$$p_1 p_2 \cdots p_k = n = q_1 q_2 \cdots q_\ell,$$

and where $p_1 \leq p_2 \leq \cdots \leq p_k$ and $q_1 \leq q_2 \leq \cdots \leq q_\ell$. We need to show that $k = \ell$ and that $p_i = q_i$ for all i. We have two cases:

- *Case 1:* Suppose that n is prime. Notice that $p_i \mid n$ for all i and $q_j \mid n$ for all j. Since the only positive divisors of n are 1 and n, and 1 is not prime, we conclude that $p_i = n$ for all i and $q_j = n$ for all j. If $k \geq 2$, then $p_1 p_2 \cdots p_k = n^k > n$, a contradiction, so we must have $k = 1$. Similarly we must have $\ell = 1$.

- *Case 2:* Suppose now that n is composite. We then must have $k \geq 2$ and $\ell \geq 2$. Now $p_1 \mid q_1 q_2 \cdots q_\ell$, so by Corollary 2.5.7, we can fix a j such that $p_1 \mid q_j$. Since q_j is prime and $p_1 \neq 1$, we must have $p_1 = q_j$. Similarly, we must have $q_1 = p_i$ for some i. We then have

  $$p_1 = q_j \geq q_1 = p_i \geq p_1,$$

  hence all inequalities must be equalities, and we conclude that $p_1 = q_1$. Canceling, we conclude that

  $$p_2 \cdots p_k = q_2 \cdots q_\ell,$$

  and this common value is some natural number m with $2 \leq m < n$. By induction, it follows that $k = \ell$ and $p_i = q_i$ for all i with $2 \leq i \leq k$.

□

Given a natural number $n \in \mathbb{N}$ with $n \geq 2$, when we write its prime factorization, we typically group together identical primes and write

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where the p_i are *distinct* primes. We often allow the insertion of "extra" primes in the factorization of n by permitting some α_i to equal to 0. This convention is particularly useful when comparing prime factorization of two numbers so that we can assume that both factorizations have the same primes occurring. It also allows us to write 1 in such a form by choosing all α_i to equal 0. Here is one example.

Proposition 2.5.9. *Suppose that $n, d \in \mathbb{N}^+$. Write the prime factorizations of n and d as*

$$\begin{aligned} n &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \\ d &= p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} \end{aligned}$$

where the p_i are distinct primes, and possibly some α_i and β_j are 0. We then have that $d \mid n$ if and only if $0 \leq \beta_i \leq \alpha_i$ for all i.

Proof. Suppose first that $0 \leq \beta_i \leq \alpha_i$ for all i. We then have that $\alpha_i - \beta_i \geq 0$ for all i, so we may let

$$c = p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \cdots p_k^{\alpha_k - \beta_k} \in \mathbb{Z}.$$

Notice that

$$\begin{aligned} dc &= p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} \cdot p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \cdots p_k^{\alpha_k - \beta_k} \\ &= (p_1^{\beta_1} p_1^{\alpha_1 - \beta_1})(p_2^{\beta_2} p_2^{\alpha_2 - \beta_2}) \cdots (p_k^{\beta_k} p_k^{\alpha_k - \beta_k}) \\ &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \\ &= n, \end{aligned}$$

hence $d \mid n$.

Conversely, suppose that $d \mid n$ and fix $c \in \mathbb{Z}$ with $dc = n$. Notice that $c > 0$ because $d, n > 0$. Now we have $dc = n$, so $c \mid n$. If q is prime and $q \mid c$, then $q \mid n$ by transitivity of divisibility so $q \mid p_i$ for some i by Corollary 2.5.7, and hence $q = p_i$ for some i because each p_i is prime. Thus, we can write the prime factorization of c as

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k},$$

where again we may have some γ_i equal to 0. We then have

$$\begin{aligned} n &= dc \\ &= (p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k})(p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}) \\ &= (p_1^{\beta_1} p_1^{\gamma_1})(p_2^{\beta_2} p_2^{\gamma_2}) \cdots (p_k^{\beta_k} p_k^{\gamma_k}) \\ &= p_1^{\beta_1+\gamma_1} p_2^{\beta_2+\gamma_2} \cdots p_k^{\beta_k+\gamma_k}. \end{aligned}$$

By the Fundamental Theorem of Arithmetic, we have $\beta_i + \gamma_i = \alpha_i$ for all i. Since $\beta_i, \gamma_i, \alpha_i \geq 0$ for all i, we conclude that $\beta_i \leq \alpha_i$ for all i. ☐

Corollary 2.5.10. *Let $a, b \in \mathbb{N}^+$ and write*

$$\begin{aligned} a &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \\ b &= p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} \end{aligned}$$

where the p_i are distinct primes and $\alpha_i, \beta_i \in \mathbb{N}$ for all i. We then have

$$\gcd(a, b) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \cdots p_k^{\min\{\alpha_k,\beta_k\}}.$$

Corollary 2.5.11. *Suppose that $n > 1$ and $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where the p_i are distinct primes. The number of nonnegative divisors of n is*

$$\prod_{i=1}^{k} (\alpha_i + 1),$$

and the number of integers divisors of n is

$$2 \cdot \prod_{i=1}^{k} (\alpha_i + 1).$$

Proof. We know that a nonnegative divisor d of n must factor as

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

where $0 \leq \beta_i \leq \alpha_i$ for all i. Thus, we have $\alpha_i + 1$ many choices for each β_i. Notice that different choices of β_i give rise to different values of d by the Fundamental Theorem of Arithmetic. ☐

Proposition 2.5.12. *Suppose that $m, n \in \mathbb{N}^+$, and write the prime factorization of m as $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where the p_i are distinct primes. We then have that m is an n^{th} power in $\mathbb{N}$ if and only if $n \mid \alpha_i$ for all i.*

Proof. Suppose first that $n \mid \alpha_i$ for all i. For each i, fix β_i such that $\alpha_i = n\beta_i$. Since n and each α_i are nonnegative, it follows that each β_i is also nonnegative. Letting $\ell = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, we then have

$$\ell^n = p_1^{n\beta_1} p_2^{n\beta_2} \cdots p_k^{n\beta_k} = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = m,$$

so m is an n^{th} power in $\mathbb{N}$.

Suppose conversely that m is an n^{th} power in $\mathbb{N}$, and write $m = \ell^n$. Since $m > 1$, we have $\ell > 1$. Write the unique prime factorization of ℓ as

$$\ell = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

We then have

$$m = \ell^n = (p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k})^n = p_1^{n\beta_1} p_2^{n\beta_2} \cdots p_k^{n\beta_k}.$$

By the Fundamental Theorem of Arithmetic, we have $\alpha_i = n\beta_i$ for all i, so $n \mid \alpha_i$ for all i. $\square$

Theorem 2.5.13. *Let $m, n \in \mathbb{N}$ with $m, n \geq 2$. If the unique prime factorization of m does not have the property that every prime exponent is divisible by n, then $\sqrt[n]{m}$ is irrational.*

Proof. We proof the contrapositive. Suppose that $\sqrt[n]{m}$ is rational and write $\sqrt[n]{m} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ with $b \neq 0$. We may assume that $a, b > 0$ because $\sqrt[n]{m} > 0$. We then have

$$\frac{a^n}{b^n} = \left(\frac{a}{b}\right)^n = m$$

hence

$$a^n = b^n m$$

Write a, b, m in their unique prime factorizations as

$$\begin{aligned} a &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \\ b &= p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} \\ m &= p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}, \end{aligned}$$

where the p_i are distinct (and possibly some $\alpha_i, \beta_i, \gamma_i$ are equal to 0). Since $a^n = b^n m$, we have

$$p_1^{n\alpha_1} p_2^{n\alpha_2} \cdots p_k^{n\alpha_k} = p_1^{n\beta_1+\gamma_1} p_2^{n\beta_2+\gamma_2} \cdots p_k^{n\beta_k+\gamma_k}.$$

By the Fundamental Theorem of Arithmetic, we conclude that $n\alpha_i = n\beta_i + \gamma_i$ for all i. Therefore, for each i, we have $\gamma_i = n\alpha_i - n\beta_i = n(\alpha_i - \beta_i)$, and so $n \mid \gamma_i$ for each i. $\square$

Chapter 3

Relations and Functions

3.1 Relations

Definition 3.1.1. *Given two sets A and B, we let $A \times B$ be the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$. We call $A \times B$ the* Cartesian product *of A and B.*

For example, we have

$$\{1, 2, 3\} \times \{6, 8\} = \{(1, 6), (1, 8), (2, 6), (2, 8), (3, 6), (3, 8)\}$$

and

$$\mathbb{N} \times \mathbb{N} = \{(0, 0), (0, 1), (1, 0), (2, 0), \dots, (4, 7), \dots\}.$$

We also use the notation A^2 as shorthand for $A \times A$, so $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ really is the set of points in the plane.

Definition 3.1.2. *Let A and B be sets. A* (binary) relation *between A and B is a subset $R \subseteq A \times B$. If $A = B$, then we call a subset of $A \times A$ a* (binary) relation *on A.*

For example, let $A = \{1, 2, 3\}$ and $B = \{6, 8\}$ as above. Let

$$R = \{(1, 6), (1, 8), (3, 8)\}.$$

We then have that R is a relation between A and B, although certainly not a very interesting one. However, we'll use it to illustrate a few facts. First, in a relation, it's possible for an element of A to be related to multiple elements of B, as in the case for $1 \in A$ in our example R. Also, it's possible that an element of A is related to no elements of B, as in the case of $2 \in A$ in our example R.

For a geometric example, let A be the set of points in the plane, and let B be the set of lines in the plane. We can then define $R \subseteq A \times B$ to be the set of pairs $(p, L) \in A \times B$ such that p is a point on L.

Here are two examples of binary relations on $\mathbb{Z}$:

- $L = \{(a, b) \in \mathbb{Z}^2 : a < b\}$
- $D = \{(a, b) \in \mathbb{Z}^2 : a \mid b\}$

We have $(4, 7) \in L$ but $(7, 4) \notin L$. Notice that $(5, 5) \notin L$ but $(5, 5) \in D$.

By definition, relations are sets. However, it is typically cumbersome to use set notation to write things like $(1, 6) \in R$. Instead, it usually makes much more sense to use infix notation and write $1R6$. Moreover, we can use better notation for the relation by using a symbol like $\sim$ instead of R. In this case, we would write $1 \sim 6$ instead of $(1, 6) \in \sim$ or $2 \not\sim 8$ instead of $(2, 8) \notin \sim$.

With this new notation, we give a few examples of binary relations on $\mathbb{R}$:

- Given $x, y \in \mathbb{R}$, we let $x \sim y$ if $x^2 + y^2 = 1$.
- Given $x, y \in \mathbb{R}$, we let $x \sim y$ if $x^2 + y^2 \leq 1$.
- Given $x, y \in \mathbb{R}$, we let $x \sim y$ if $x = \sin y$.
- Given $x, y \in \mathbb{R}$, we let $x \sim y$ if $y = \sin x$.

Again, notice from these examples that given $x \in \mathbb{R}$, there might be 0, 1, 2, or even infinitely many $y \in \mathbb{R}$ with $x \sim y$.

If we let A be the set of all finite sequences of 0's and 1's, then the following are binary relations on A:

- Given $\sigma, \tau \in A$, we let $\sigma \sim \tau$ if σ and τ have the same number of 1's.
- Given $\sigma, \tau \in A$, we let $\sigma \sim \tau$ if σ occurs as a consecutive subsequence of τ (for example, we have $010 \sim 001101011$ because 010 appears in positions 5-6-7 of 001101011).

For a final example, let A be the set consisting of the 50 states. Let R be the subset of $A \times A$ consisting of those pairs of states that have a common letter in the second position of their postal codes. For example, we have (Iowa,California) $\in R$ and and (Iowa, Virginia) $\in R$ because the postal codes of these sets are IA, CA, VA. We also have (Minnesota, Tennessee) $\in R$ because the corresponding postal codes are MN and TN. Now (Texas, Texas) $\in R$, but there is no $a \in A$ with $a \neq$ Texas such that (Texas, a) $\in R$, because no other state has X as the second letter of its postal code. Texas stands alone.

3.2 Equivalence Relations

Definition 3.2.1. *An* equivalence relation *on a set A is a binary relation $\sim$ on A having the following three properties:*

- *$\sim$ is reflexive: $a \sim a$ for all $a \in A$.*
- *$\sim$ is symmetric: Whenever $a, b \in A$ satisfy $a \sim b$, we have $b \sim a$.*
- *$\sim$ is transitive: Whenever $a, b, c \in A$ satisfy $a \sim b$ and $b \sim c$, we have $a \sim c$.*

Consider the binary relation $\sim$ on $\mathbb{Z}$ where $a \sim b$ means that $a \leq b$. Notice that $\sim$ is reflexive because $a \leq a$ for all $a \in \mathbb{Z}$. Also, $\sim$ is transitive because if $a \leq b$ and $b \leq c$, then $a \leq c$. However, $\sim$ is not symmetric because $3 \sim 4$ but $4 \not\sim 3$. Thus, although $\sim$ satisfies two out of the three requirements, it is not an equivalence relation.

A simple example of an equivalence relation is where $A = \mathbb{R}$ and $a \sim b$ means that $|a| = |b|$. In this case, it is straightforward to check that $\sim$ is an equivalence relation. We now move on to some more interesting examples which we treat more carefully.

Example 3.2.2. *Let A be the set of all $n \times n$ matrices with real entries. Let $M \sim N$ mean that there exists an invertible $n \times n$ matrix P such that $M = PNP^{-1}$. We then have that $\sim$ is an equivalence relation on A.*

Proof. We need to check the three properties:

- Reflexive: Let $M \in A$. The $n \times n$ identity matrix I is invertible and satisfies $I^{-1} = I$, so we have $M = IMI^{-1}$. Therefore, $\sim$ is reflexive.
- Symmetric: Let $M, N \in A$ with $M \sim N$. Fix an $n \times n$ invertible matrix P with $M = PNP^{-1}$. Multiplying on the left by P^{-1} we get $P^{-1}M = NP^{-1}$, and now multiplying on the right by P we conclude that $P^{-1}MP = N$. We know from linear algebra that P^{-1} is also invertible and $(P^{-1})^{-1} = P$, so $N = P^{-1}M(P^{-1})^{-1}$ and hence $N \sim M$.

- Transitive: Let $L, M, N \in A$ with $L \sim M$ and $M \sim N$. Since $L \sim M$, we may fix a $n \times n$ invertible matrix P with $L = PMP^{-1}$. Since $M \sim N$, we may fix a $n \times n$ invertible matrix Q with $M = QNQ^{-1}$. We then have
$$L = PMP^{-1} = P(QNQ^{-1})P^{-1} = (PQ)N(Q^{-1}P^{-1})$$
Now by linear algebra, we know that the product of two invertible matrices is invertible, so PQ is invertible and furthermore we know that $(PQ)^{-1} = Q^{-1}P^{-1}$. Therefore, we have
$$L = (PQ)N(PQ)^{-1}$$
so $L \sim N$.

Putting it all together, we conclude that $\sim$ is an equivalence relation on A. ☐

Example 3.2.3. *Let A be the set $\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$, i.e. A is the set of all pairs $(a, b) \in \mathbb{Z}^2$ with $b \neq 0$. Define a relation $\sim$ on A as follows. Given $a, b, c, d \in \mathbb{Z}$ with $b, d \neq 0$, we let $(a, b) \sim (c, d)$ mean $ad = bc$. We then have that $\sim$ is an equivalence relation on A.*

Proof. We check the three properties:

- Reflexive: Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Since $ab = ba$, it follows that $(a, b) \sim (a, b)$.
- Symmetric: Let $a, b, c, d \in \mathbb{Z}$ with $b, d \neq 0$, and $(a, b) \sim (c, d)$. We then have that $ad = bc$. From this, we conclude that $cb = da$ so $(c, d) \sim (a, b)$.
- Transitive: Let $a, b, c, d, e, f \in \mathbb{Z}$ with $b, d, f \neq 0$ where $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. We then have that $ad = bc$ and $cf = de$. Multiplying the first equation by f we see that $adf = bcf$. Multiplying the second equation by b gives $bcf = bde$. Therefore, we know that $adf = bde$. Now $d \neq 0$ by assumption, so we may cancel it to conclude that $af = be$. It follows that $(a, b) \sim (e, f)$

Therefore, $\sim$ is an equivalence relation on A. ☐

Let's analyze the above situation more carefully. We have $(1, 2) \sim (2, 4)$, $(1, 2) \sim (4, 8)$, $(1, 2) \sim (-5, -10)$, etc. If we think of (a, b) as representing the fraction $\frac{a}{b}$, then the relation $(a, b) \sim (c, d)$ is saying exactly that the fractions $\frac{a}{b}$ and $\frac{c}{d}$ are equal. You may never have thought about equality of fractions as the result of imposing an equivalence relation on pairs of integers, but that is exactly what it is. We will be more precise about this below.

The next example is an important example in geometry. We introduce it now, and will return to it later.

Example 3.2.4. *Let A be the set $\mathbb{R}^2\backslash\{(0, 0)\}$. Define a relation $\sim$ on A by letting $(x_1, y_1) \sim (x_2, y_2)$ if there exists a real number $\lambda \neq 0$ with $(x_1, y_1) = (\lambda x_2, \lambda y_2)$. We then have that $\sim$ is an equivalence relation on A.*

Proof. We check the three properties.

- Reflexive: Let $(x, y) \in \mathbb{R}^2\backslash\{(0, 0)\}$ we have $(x, y) \sim (x, y)$ because using $\lambda = 1$ we see that $(x, y) = (1 \cdot x, 1 \cdot y)$. Therefore, $\sim$ is reflexive.
- Symmetric: Suppose now that $(x_1, y_1) \sim (x_2, y_2)$, and fix a real number $\lambda \neq 0$ such that $(x_1, y_1) = (\lambda x_2, \lambda y_1)$. We then have that $x_1 = \lambda x_2$ and $y_1 = \lambda y_2$, so $x_2 = \frac{1}{\lambda} \cdot x_1$ and $y_2 = \frac{1}{\lambda} \cdot y_1$ (notice that we are using $\lambda \neq 0$ so we can divide by it). Hence $(x_2, y_2) = (\frac{1}{\lambda} \cdot x_2, \frac{1}{\lambda} \cdot y_2)$, and so $(x_2, y_2) \sim (x_1, y_1)$. Therefore, $\sim$ is symmetric.
- Transitive: Suppose that $(x_1, y_1) \sim (x_2, y_2)$ and $(x_2, y_2) \sim (x_3, y_3)$. Fix a real number $\lambda \neq 0$ with $(x_1, y_1) = (\lambda x_2, \lambda y_2)$, and also fix a real number $\mu \neq 0$ with $(x_2, y_2) = (\mu x_3, \mu y_3)$. We then have that $(x_1, y_1) = ((\lambda\mu)x_3, (\lambda\mu)y_3)$. Since both $\lambda \neq 0$ and $\mu \neq 0$, notice that $\lambda\mu \neq 0$ as well, so $(x_1, y_1) \sim (x_3, y_3)$. Therefore, $\sim$ is transitive.

It follows that $\sim$ is an equivalence relation on A. $\square$

Definition 3.2.5. *Let $\sim$ be an equivalence relation on a set A. Given $a \in A$, we let*

$$\overline{a} = \{b \in A : a \sim b\}.$$

The set $\overline{a}$ is called the equivalence class *of a.*

Some sources use the notation $[a]$ instead of $\overline{a}$. This notation helps emphasize that the equivalence class of a is a *subset* of A rather than an element of A. However, it is cumbersome notation when we begin working with equivalence classes. We will stick with our notation, although it might take a little time to get used to. Notice that by the reflexive property of $\sim$, we have that $a \in \overline{a}$ for all $a \in A$.

For example, let's return to where A is the set consisting of the 50 states and R is the subset of $A \times A$ consisting of those pairs of states whose second letter of their postal codes are equal. It's straightforward to show that R is an equivalence relation on A. We have

$$\overline{\text{Iowa}} = \{\text{California}, \text{Georgia}, \text{Iowa}, \text{Louisiana}, \text{Massachusetts}, \text{Pennsylvania}, \text{Virginia}, \text{Washington}\},$$

while

$$\overline{\text{Minnesota}} = \{\text{Indiana}, \text{Minnesota}, \text{Tennessee}\}$$

and

$$\overline{\text{Texas}} = \{\text{Texas}\}.$$

Notice that each of these are sets, even in the case of $\overline{\text{Texas}}$.

For another example, suppose we are working as above with $A = \mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ where $(a, b) \sim (c, d)$ means that $ad = bc$. As discussed above, some elements of $\overline{(1, 2)}$ are $(1, 2)$, $(2, 4)$, $(4, 8)$, $(-5, -10)$, etc. So

$$\overline{(1, 2)} = \{(1, 2), (2, 4), (4, 8), (-5, -10), \dots\}.$$

Again, I want to emphasize that $\overline{(a, b)}$ is a subset of A.

The following proposition is hugely fundamental. It says that if two equivalence classes overlap, then they must in fact be equal. In other words, if $\sim$ is an equivalence on A, then the equivalence classes *partition* the set A into pieces.

Proposition 3.2.6. *Let $\sim$ be an equivalence relation on a set A and let $a, b \in A$. If $\overline{a} \cap \overline{b} \neq \emptyset$, then $\overline{a} = \overline{b}$.*

Proof. Suppose that $\overline{a} \cap \overline{b} \neq \emptyset$. Since this set is nonempty, we can fix some $c \in \overline{a} \cap \overline{b}$. We then have $a \sim c$ and $b \sim c$. By symmetry, we know that $c \sim b$, and using transitivity we get that $a \sim b$. Using symmetry again, we conclude that $b \sim a$. We now show that $\overline{a} = \overline{b}$ by showing each containment:

- We first show that $\overline{a} \subseteq \overline{b}$. Let $x \in \overline{a}$. We then have that $a \sim x$. Since $b \sim a$, we can use transitivity to conclude that $b \sim x$, hence $x \in \overline{b}$.
- We next show that $\overline{b} \subseteq \overline{a}$. Let $x \in \overline{b}$. We then have that $b \sim x$. Since $a \sim b$, we can use transitivity to conclude that $a \sim x$, hence $x \in \overline{a}$.

Putting this together, we get that $\overline{a} = \overline{b}$. $\square$

With that proposition in hand, we are ready for the foundational theorem about equivalence relations.

Theorem 3.2.7. *Let $\sim$ be an equivalence relation on a set A and let $a, b \in A$.*

1. *$a \sim b$ if and only if $\overline{a} = \overline{b}$.*
2. *$a \not\sim b$ if and only if $\overline{a} \cap \overline{b} = \emptyset$.*

Proof.

1. Suppose first that $a \sim b$. We then have that $b \in \overline{a}$. Now we know that $b \sim b$ because $\sim$ is reflexive, so $b \in \overline{b}$. Thus, $b \in \overline{a} \cap \overline{b}$, so $\overline{a} \cap \overline{b} \neq \emptyset$. Using Proposition 3.2.6, we conclude that $\overline{a} = \overline{b}$.

   Suppose conversely that $\overline{a} = \overline{b}$. Since $b \sim b$ because $\sim$ is reflexive, we have that $b \in \overline{b}$. Therefore, $b \in \overline{a}$ and hence $a \sim b$.

2. Suppose that $a \not\sim b$. Since we just proved (1), it follows that $\overline{a} \neq \overline{b}$, so by Proposition 3.2.6 we must have $\overline{a} \cap \overline{b} = \emptyset$.

   Suppose conversely that $\overline{a} \cap \overline{b} = \emptyset$. We then have $\overline{a} \neq \overline{b}$ (because $a \in \overline{a}$ so $\overline{a} \neq \emptyset$), so $a \not\sim b$ by part (1).

□

Therefore, given an equivalence relation $\sim$ on a set A, the equivalence classes partition A into pieces. Working out the details in our postal code example, one can show that $\sim$ has 1 equivalence class of size 8 (namely $\overline{\text{Iowa}}$, which is the same set as $\overline{\text{California}}$ and 6 others), 3 equivalence classes of size 4, 4 equivalence classes of size 3, 7 equivalence classes of size 2, and 4 equivalence classes of size 1.

Let's revisit the example of $A = \mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ where $(a, b) \sim (c, d)$ means $ad = bc$. The equivalence class of $(1, 2)$, namely the set $\overline{(1, 2)}$ is the set of all pairs of integers which are ways of representing the fraction $\frac{1}{2}$. In fact, this is how once can "construct" the rational numbers from the integers. We simply *define* the rational numbers to be the set of equivalence classes of A under $\sim$. In other words, we let

$$\frac{a}{b} = \overline{(a, b)}.$$

So when we write something like

$$\frac{1}{2} = \frac{4}{8},$$

we are simply saying that

$$\overline{(1, 2)} = \overline{(4, 8)},$$

which is true because $(1, 2) \sim (4, 8)$.

Example 3.2.8. *Recall the example above where $A = \mathbb{R}^2\backslash\{(0, 0)\}$ and where $(x_1, y_1) \sim (x_2, y_2)$ means that there exists a real number $\lambda \neq 0$ with $(x_1, y_1) = (\lambda x_2, \lambda y_2)$. The equivalence classes of $\sim$ are the lines through the origin (omitting the origin itself).*

Proof. Our first claim is that every point of A is equivalent to exactly one of the following points:

- $(0, 1)$
- $(1, m)$ for some $m \in \mathbb{R}$.

We first show that every point is equivalent to at least one of the above points. Suppose that $(x, y) \in A$ so $(x, y) \neq (0, 0)$. If $x = 0$, then we must have $y \neq 0$, so $(x, y) \sim (0, 1)$ via $\lambda = y$. Now if $x \neq 0$, then $(x, y) \sim (1, \frac{y}{x})$ via $\lambda = x$. This gives existence.

To show uniqueness, it suffices to show that no two of the above points are equivalent to each other because we already know that $\sim$ is an equivalence relation. Suppose that $m \in \mathbb{R}$ and that $(0, 1) \sim (1, m)$. Fix $\lambda \in \mathbb{R}$ with $\lambda \neq 0$ such that $(0, 1) = (\lambda 1, \lambda m)$. Looking at the first coordinate, we conclude that $\lambda = 0$, a contradiction. Therefore, $(0, 1)$ is not equivalent to any point of the second type. Suppose now that $m, n \in \mathbb{R}$ with $(1, m) \sim (1, n)$. Fix $\lambda \in \mathbb{R}$ with $\lambda \neq 0$ such that $(1, m) = (\lambda 1, \lambda n)$. Looking at first coordinates, we must have $\lambda = 1$, so examining second coordinates gives $m = \lambda n = n$. Therefore $(1, m) \not\sim (1, n)$ whenever $m \neq n$. This finishes the claim.

Now we examine the equivalence classes of each of the above points. We first handle $\overline{(0,1)}$ and claim that it equals the set of points in A on the line $x = 0$. Notice first that if $(x,y) \in \overline{(0,1)}$, then $(0,1) \sim (x,y)$, so fixing $\lambda \neq 0$ with $(0,1) = (\lambda x, \lambda y)$ we conclude that $\lambda x = 0$ and hence $x = 0$. Thus, every element of $\overline{(0,1)}$ is indeed on the line $x = 0$. Now taking an arbitrary point on the line $x = 0$, say $(0,y)$ with $y \neq 0$, we simply notice that $(0,1) \sim (0,y)$ via $\lambda = \frac{1}{y}$. Hence, every point on the line $x = 0$ is an element of $\overline{(0,1)}$.

Finally we fix $m \in \mathbb{R}$ and claim that $\overline{(1,m)}$ is the set of points in A on the line $y = mx$. Notice first that if $(x,y) \in \overline{(1,m)}$, then $(1,m) \sim (x,y)$, hence $(x,y) \sim (1,m)$. Fix $\lambda \neq 0$ with $(x,y) = (\lambda 1, \lambda m)$. We then have $x = \lambda$ by looking at first coordinates, so $y = \lambda m = mx$ by looking at second coordinates. Thus, every element of $\overline{(1,m)}$ lies on the line $y = mx$. Now take an arbitrary point in A on the line $y = mx$, say (x, mx). We then have that $x \neq 0$ because $(0,0) \notin A$. Thus $(1,m) \sim (x, mx)$ via $\lambda = x$. Hence, every point on the line $y = mx$ is an element of $\overline{(1,m)}$. $\square$

The set of equivalence classes of $\sim$ in the previous example is known as the *projective real line*.

3.3 Functions

Intuitively, given two sets A and B, a function $f \colon A \to B$ is a input-output "mechanism" that produces a *unique* output $b \in B$ for any given input $a \in A$. Up through calculus, the vast majority of functions that we encounter are given by simple formulas, so this "mechanism" was typically interpreted in an algorithmic and computational sense. However, some functions such as $f(x) = \sin x$, $f(x) = \ln x$, or integral functions like $f(x) = \int_a^x g(t)\,dt$ (given a continuous function $g(t)$ and a fixed $a \in \mathbb{R}$) were defined in more interesting ways where it was not at all obvious how to compute them. We are now in a position to define functions as relations that satisfy a certain property. Thinking about functions from this more abstract point of view eliminates the vague "mechanism" concept because they will simply be certain types of sets. With this perspective, we'll see that functions can be defined in any way that a set can be defined. This approach both clarifies the concept of a function as well as providing us with some much needed flexibility in defining functions in more interesting ways.

Definition 3.3.1. *Let A and B be sets. A* function *from A to B is a subset f of $A \times B$ with the property that for all $a \in A$, there exists a unique $b \in B$ with $(a,b) \in f$. Also, instead of writing "f is a function from A to B", we typically use the shorthand notation "$f \colon A \to B$".*

For example, let $A = \{2,3,5,7\}$ and let $B = \mathbb{N} = \{0,1,2,3,4,\dots\}$. An example of a function $f \colon A \to B$ is the set
$$f = \{(2,71), (3,4), (5,9382), (7,4)\}.$$
Notice that in the definition of a function from A to B, we know that for every $a \in A$, there is a unique $b \in B$ such that $(a,b) \in f$. However, as this example shows, it may not be the case that for every $b \in B$, there is a unique $a \in A$ with $(a,b) \in f$. Be careful with the order of quantifiers!

We can also convert the typical way of defining a function into this formal set theoretic way. For example, consider the function $f \colon \mathbb{R} \to \mathbb{R}$ by letting $f(x) = x^2$. We can instead define f by the set
$$\{(x,y) \in \mathbb{R} \times \mathbb{R} : y = x^2\},$$
or parametrically as
$$\{(x,x^2) : x \in \mathbb{R}\}.$$
One side effect of our definition of a function is that we immediately obtain a nice definition for when two functions $f \colon A \to B$ and $g \colon A \to B$ are equal because we have defined when two sets are equal. Given two function $f \colon A \to B$ and $g \colon A \to B$, if we unwrap our definition of set equality, we see that $f = g$ exactly when f and g have the same elements, which is precisely the same thing as saying that $f(a) = g(a)$ for all $a \in A$.

In particular, the *manner* in which we describe functions does not matter so long as the functions behave the same on all inputs. For example, if we define $f\colon \mathbb{R} \to \mathbb{R}$ and $g\colon \mathbb{R} \to \mathbb{R}$ by letting $f(x) = \sin^2 x + \cos^2 x$ and $g(x) = 1$, then we have that $f = g$ because $f(x) = g(x)$ for all $x \in \mathbb{R}$.

Thinking of functions as special types of sets is helpful to clarify definitions, but is often awkward to work with in practice. For example, writing $(2, 71) \in f$ to mean that f sends 2 to 71 quickly becomes annoying. Thus, we introduce some new notation matching up with our old experience with functions.

Notation 3.3.2. *Let A and B be sets. If $f\colon A \to B$ and $a \in A$, we write $f(a)$ to mean the unique $b \in B$ such that $(a, b) \in f$.*

For instance, in the above example of f, we can instead write

$$f(2) = 71, \qquad f(3) = 4, \qquad f(5) = 9382, \qquad \text{and} \qquad f(7) = 4.$$

Definition 3.3.3. *Let $f\colon A \to B$ be a function.*

- *We call A the* domain *of f.*
- *We call B the* codomain *of f.*
- *We define $range(f) = \{b \in B : \text{There exists } a \in A \text{ with } f(a) = b\}$.*

Notice that given a function $f\colon A \to B$, we have $\text{range}(f) \subseteq B$, but it is possible that $\text{range}(f) \neq B$. For example, in the above case, we have that the codomain of f is $\mathbb{N}$, but $\text{range}(f) = \{4, 71, 9382\}$. In general, given a function $f\colon A \to B$, it may be very difficult to determine $\text{range}(f)$ because we may need to search through all $a \in A$.

For an interesting example of a function with a mysterious looking range, fix $n \in \mathbb{N}^+$ and define $f\colon \{0, 1, 2, \dots, n-1\} \to \{0, 1, 2, \dots, n-1\}$ by letting $f(a)$ be the remainder when dividing a^2 by n. For example, if $n = 10$, then we have

$$\begin{array}{lllll} f(0) = 0 & f(1) = 1 & f(2) = 4 & f(3) = 9 & f(4) = 6 \\ f(5) = 5 & f(6) = 6 & f(7) = 9 & f(8) = 4 & f(9) = 1. \end{array}$$

Thus, for $n = 10$, we have $\text{range}(f) = \{0, 1, 4, 5, 6, 9\}$. This simple but strange looking function has many interesting properties, and we will explore it some in Chapter **??**. Given a reasonably large number $n \in \mathbb{N}$, it looks potentially difficult to determine whether an element is in $\text{range}(f)$ because we might need to search through a huge number of inputs to see if a given output actually occurs. If n is prime, then it turns out that there are much faster ways to determine if a given element is in $\text{range}(f)$ (see Chapter **??**). However, it is widely believed (although we do not currently have a proof!) that there is no efficient method to do this when n is the product of two large primes, and this is the basis for some cryptosystems (Goldwasser-Micali) and pseudo-random number generators (Blum-Blum-Shub).

Definition 3.3.4. *Suppose that $f\colon A \to B$ and $g\colon B \to C$ are functions. The* composition *of g and f, denoted $g \circ f$, is the function $g \circ f\colon A \to C$ defined by letting $(g \circ f)(a) = g(f(a))$ for all $a \in A$.*

Instead of defining $g \circ f$ in function language, one can also define function composition directly in terms of the sets f and g. Suppose that $f\colon A \to B$ and $g\colon B \to C$ are functions. Define a new set

$$R = \{(a, c) \in A \times C : \text{There exists } b \in B \text{ with } (a, b) \in f \text{ and } (b, c) \in g\}.$$

Now R is a relation, and one can check that it is a function (using the assumption that f and g are both functions). We define $g \circ f$ to be this set.

Notice that in general we have $f \circ g \neq g \circ f$ even when both are defined! If $f\colon \mathbb{R} \to \mathbb{R}$ is $f(x) = x+1$ and $g\colon \mathbb{R} \to \mathbb{R}$ is $g(x) = x^2$, then

$$\begin{aligned}(f \circ g)(x) &= f(g(x)) \\ &= f(x^2) \\ &= x^2 + 1,\end{aligned}$$

while

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) \\ &= g(x+1) \\ &= (x+1)^2 \\ &= x^2 + 2x + 1.\end{aligned}$$

Notice then that $(f \circ g)(1) = 1^2 + 1 = 2$ while $(g \circ f)(1) = 1^2 + 2 \cdot 1 + 1 = 4$. Since we have found one example of an $x \in \mathbb{R}$ with $(f \circ g)(x) \neq (f \circ g)(x)$, we conclude that $f \circ g \neq g \circ f$. It does not matter that there do exist some values of x with $(f \circ g)(x) = (f \circ g)(x)$ (for example, this is true when $x = 0$). Remember that two functions are equal precisely when they agree on *all* inputs, so to show that the two functions are not equal it suffices to find just one value where they disagree.

Proposition 3.3.5. *Let A, B, C, D be sets. Suppose that $f\colon A \to B$, that $g\colon B \to C$, and that $h\colon C \to D$ are functions. We then have that $(h \circ g) \circ f = h \circ (g \circ f)$. Stated more simply, function composition is associative whenever it is defined.*

Proof. Let $a \in A$ be arbitrary. We then have

$$\begin{aligned}((h \circ g) \circ f)(a) &= (h \circ g)(f(a)) \\ &= h(g(f(a))) \\ &= h((g \circ f)(a)) \\ &= (h \circ (g \circ f))(a).\end{aligned}$$

Therefore $((h \circ g) \circ f)(a) = (h \circ (g \circ f))(a)$ for all $a \in A$. It follows that $(h \circ g) \circ f = h \circ (g \circ f)$. □

Definition 3.3.6. *Let A be a set. The function $id_A\colon A \to A$ defined by $id_A(a) = a$ for all $a \in A$ is called the* identity function *on A.*

The identity function does leave other functions alone when we compose with it. However, we have to be careful that we compose with the identity function on the correct set and the correct side.

Proposition 3.3.7. *For any function $f\colon A \to B$, we have $f \circ id_A = f$ and $id_B \circ f = f$.*

Proof. Let $f\colon A \to B$. For any $a \in A$, we have

$$(f \circ id_A)(a) = f(id_A(a)) = f(a).$$

Since $a \in A$ was arbitrary, it follows that $f \circ id_A = f$. For any $b \in B$, we have

$$(id_B \circ f)(a) = id_B(f(a)) = f(a),$$

because $f(a)$ is some element in B. Since $b \in B$ was arbitrary, it follows that $id_B \circ f = f$. □

3.4 Injections, Surjections, and Inverses

Recall the following fundamental definitions.

Definition 3.4.1. *Let $f\colon A \to B$ be a function.*

- *We say that f is injective (or one-to-one) if whenever $a_1, a_2 \in A$ and $f(a_1) = f(a_2)$, we have $a_1 = a_2$.*
- *We say that f is surjective (or onto) if for all $b \in B$ there exists $a \in A$ such that $f(a) = b$. In other words, f is surjective if $range(f) = B$.*
- *We say that f is bijective if f is both injective and surjective.*

An equivalent condition for f to be injective is obtained by simply taking the contrapositive, i.e. $f\colon A \to B$ is injective if and only if whenever $a_1 \neq a_2$, we have $f(a_1) \neq f(a_2)$. Stated in more colloquial language, f is injective if every element of B is hit by at most one element of A via f. In this manner, f is surjective if every element of B is hit by at least one element of a via f, and f is bijective if every element of B is hit by exactly one element of A via f.

For example, consider the function $f\colon \mathbb{N} \to \mathbb{N}$ defined by letting $f(n)$ be the number of nonnegative divisors of n. Notice that f is not injective because $f(3) = 2 = f(5)$ but of course $3 \neq 5$. On the other hand, f is surjective, because given any $n \in \mathbb{N}^+$, we have $f(2^{n-1}) = n$ (by Corollary 2.5.11).

If we want to prove that a function $f\colon A \to B$ is injective, it is usually better to use our official definition than the contrapositive one with negations. Thus, we want to start by assuming that we are given arbitrary $a_1, a_2 \in A$ that satisfy $f(a_1) = f(a_2)$, and using this assumption we want to prove that $a_1 = a_2$. The reason why this approach is often preferable is because it is typically easier to work with and manipulate a statement involving equality than it is to derive statements from a non-equality.

Proposition 3.4.2. *Suppose that $f\colon A \to B$ and $g\colon B \to C$ are both functions.*

1. *If both f and g are injective, then $g \circ f$ is injective.*
2. *If both f and g are surjective, then $g \circ f$ is surjective.*
3. *If both f and g are bijective, then $g \circ f$ is bijective.*

Proof.

1. Suppose that $a_1, a_2 \in A$ satisfy $(g \circ f)(a_1) = (g \circ f)(a_2)$. We then have that $g(f(a_1)) = g(f(a_2))$. Using the fact that g is injective, we conclude that $f(a_1) = f(a_2)$. Now using the fact that f is injective, it follows that $a_1 = a_2$. Therefore, $g \circ f$ is injective.
2. Let $c \in C$. Since $g\colon B \to C$ is surjective, we may fix $b \in B$ with $g(b) = c$. Since $f\colon A \to B$ is surjective, we may fix $a \in A$ with $f(a) = b$. We then have
$$(g \circ f)(a) = g(f(a)) = g(b) = c$$
Therefore, $g \circ f$ is surjective.
3. This follows from combining 1 and 2.

□

Definition 3.4.3. *Let $f\colon A \to B$ be a function.*

- *A* left inverse *of f is a function $g\colon B \to A$ such that $g \circ f = id_A$.*

- *A* right inverse *of f is a function $g\colon B \to A$ such that $f \circ g = id_B$.*
- *An* inverse *of f is a function $g\colon B \to A$ that is* both *a left inverse and a right inverse of f simultaneously, i.e. a function $g\colon B \to A$ such that both $g \circ f = id_A$ and $f \circ g = id_B$.*

For an example, let $A = \{1, 2, 3\}$ and $B = \{5, 6, 7, 8\}$, and consider the function $f\colon A \to B$ defined as follows:

$$f(1) = 7 \qquad f(2) = 5 \qquad f(3) = 8.$$

As a set, we can write $f = \{(1, 7), (2, 5), (3, 8)\}$. Notice that f is injective but not surjective because $6 \notin \text{range}(f)$. Does f have a left inverse or a right inverse? A guess would be to define $g\colon B \to A$ as follows:

$$g(5) = 2 \qquad g(6) = \,? \qquad g(7) = 1 \qquad g(8) = 3.$$

Notice that it is unclear how to define $g(6)$ because 6 is not hit by f. Suppose that we pick a random $c \in A$ and let $g(6) = c$. We have the following:

$$\begin{array}{rcccl} g(f(1)) & = & g(7) & = & 1 \\ g(f(2)) & = & g(5) & = & 2 \\ g(f(3)) & = & g(8) & = & 3. \end{array}$$

Thus, we have $g(f(a)) = a$ for all $a \in A$, so $g \circ f = id_A$ regardless of how we choose to define $g(6)$. We have shown that f has a left inverse (in fact, we have shown that f has at least 3 left inverses because we have 3 choices for $g(6)$). Notice that the value of $g(6)$ never came up in the above calculation because $6 \notin \text{range}(f)$. What happens when we look at $f \circ g$? Ignoring 6 for the moment, we have the following:

$$\begin{array}{rcccl} f(g(5)) & = & f(2) & = & 5 \\ f(g(7)) & = & f(1) & = & 7 \\ f(g(8)) & = & f(3) & = & 8. \end{array}$$

Thus, we have $f(g(b)) = b$ for all $b \in \{5, 7, 8\}$. However, notice that no matter how we choose $c \in A$ to define $g(6) = c$, it doesn't work. For example, if we let $g(6) = 1$, then $f(g(6)) = f(1) = 7$. You can work through the other two possibilities directly, but notice that no matter how we choose c, we will have $f(g(c)) \in \text{range}(f)$, and hence $f(g(c)) \neq 6$ because $6 \notin \text{range}(f)$. In other words, it appears that f does not have a right inverse. Furthermore, this problem seems to arise whenever we have a function that is not surjective.

Let's see an example where f is not injective. Let $A = \{1, 2, 3\}$ and $B = \{5, 6\}$, and consider the function $f\colon A \to B$ defined as follows:

$$f(1) = 5 \qquad f(2) = 6 \qquad f(3) = 5.$$

As a set, we can write $f = \{(1, 5), (2, 6), (3, 5)\}$. Notice that f is surjective but not injective (since $f(1) = f(3)$ but $1 \neq 3$). Does f have a left inverse or a right inverse? The guess would be to define $g\colon B \to A$ by letting $g(6) = 2$, but it's unclear how to define $g(5)$. Should we let $g(5) = 1$ or should we let $g(5) = 3$? Suppose that we choose $g\colon B \to A$ as follows:

$$g(5) = 1 \qquad g(6) = 2.$$

Let's first look at $f \circ g$. We have the following:

$$\begin{array}{rcccl} f(g(5)) & = & f(1) & = & 5 \\ f(g(6)) & = & f(2) & = & 6. \end{array}$$

We have shown that $f(g(b)) = b$ for all $b \in B$, so $f \circ g = id_B$. Now if we instead choose $g(5) = 3$, then we would have

$$\begin{array}{rcrcl} f(g(5)) & = & f(3) & = & 5 \\ f(g(6)) & = & f(2) & = & 6, \end{array}$$

which also works. Thus, we have shown that f has a right inverse, and in fact it has at least 2 right inverses. What happens if we look at $g \circ f$ for these functions g? If we define $g(5) = 1$, then we have

$$g(f(3)) \quad = \quad g(5) \quad = \quad 1,$$

which does not work. Alternatively, if we define $g(5) = 3$, then we have

$$g(f(1)) \quad = \quad g(5) \quad = \quad 3,$$

which does not work either. It seems that no matter how we choose $g(5)$, we will obtain the wrong result on some input to $g \circ f$. In other words, it appears that f does not have a left inverse. Furthermore, this problem seems to arise whenever we have a function that is not injective.

With these examples in hand, we are ready to classify when a function has an inverse in terms of injectivity and surjectivity.

Proposition 3.4.4. *Let $f\colon A \to B$ be a function.*

1. *f is injective if and only f has a left inverse.*
2. *f is surjective if and only f has a right inverse.*
3. *f is bijective if and only if f has an inverse.*

Proof.

1. Suppose first that f has a left inverse, and fix a function $g\colon B \to A$ with $g \circ f = id_A$. Suppose that $a_1, a_2 \in A$ satisfy $f(a_1) = f(a_2)$. Applying the function g to both sides we see that $g(f(a_1)) = g(f(a_2))$, and hence $(g \circ f)(a_1) = (g \circ f)(a_2)$. We now have

$$\begin{aligned} a_1 &= id_A(a_1) \\ &= (g \circ f)(a_1) \\ &= (g \circ f)(a_2) \\ &= id_A(a_2) \\ &= a_2, \end{aligned}$$

   so $a_1 = a_2$. It follows that f is injective.

   Suppose conversely that f is injective. If $A = \emptyset$, then $f = \emptyset$, and we are done by letting $g = \emptyset$ (if the empty set as a function annoys you, just ignore this case). Let's assume then that $A \neq \emptyset$ and fix $a_0 \in A$. We now define a function $g\colon B \to A$ as follows. Given $b \in B$, here is how we define $g(b)$:

   - If $b \in \text{range}(f)$, then there exists a unique $a \in A$ with $f(a) = b$ (because f is injective), and we let $g(b) = a$ for this unique choice.
   - If $b \notin \text{range}(f)$, then we let $g(b) = a_0$.

   This completes the definition of $g\colon B \to A$. In terms of sets, g is obtained from f by flipping all of the pairs, and adding (b, a_0) for all $b \notin \text{range}(f)$. We need to check that $g \circ f = id_A$. Let $a \in A$ be arbitrary. We then have that $f(a) \in B$, and furthermore $f(a) \in \text{range}(f)$ trivially. Therefore, in the definition of g on the input $f(a)$, we defined $g(f(a)) = a$, so $(g \circ f)(a) = id_A(a)$. Since $a \in A$ was arbitrary, it follows that $g \circ f = id_A$. Therefore, f has a left inverse.

2. Suppose first that f has a right inverse, and fix a function $g\colon B \to A$ with $f \circ g = id_B$. Let $b \in B$ be arbitrary. We then have that
$$\begin{aligned} b &= id_B(b) \\ &= (f \circ g)(b) \\ &= f(g(b)), \end{aligned}$$
hence there exists $a \in A$ with $f(a) = b$, namely $a = g(b)$. Since $b \in B$ was arbitrary, it follows that f is surjective.

   Suppose conversely that f is surjective. We define $g\colon B \to A$ as follows. For every $b \in B$, we know that there exists (possibly many) $a \in A$ with $f(a) = b$ because f is surjective. Given $b \in B$, we then define $g(b) = a$ for some (any) $a \in A$ for which $f(a) = b$. Now given any $b \in B$, notice that $g(b)$ satisfies $f(g(b)) = b$ by definition of g, so $(f \circ g)(b) = b = id_B(b)$. Since $b \in B$ was arbitrary, it follows that $f \circ g = id_B$.

3. The right-to-left direction is immediate from parts (1) and (2). For the left-to-right direction, we need only note that if f is a bijection, then the function g defined in the left-to-right direction in the proof of (1) equals the function g defined in the left-to-right direction in the proof of (2).

□

Finally, we prove a few results about inverses that only make use of identity functions and the associatively of function composition.

Proposition 3.4.5. *Let $f\colon A \to B$ be a function. If $g\colon B \to A$ is a left inverse of f and $h\colon B \to A$ is a right inverse of f, then $g = h$.*

Proof. By definition, we have that that $g \circ f = id_A$ and $f \circ h = id_B$. The key function to consider is the composition $(g \circ f) \circ h = g \circ (f \circ h)$ (notice that these are equal by Proposition 3.3.5). We have
$$\begin{aligned} g &= g \circ id_B \\ &= g \circ (f \circ h) \\ &= (g \circ f) \circ h && \text{(by Proposition 3.3.5)} \\ &= id_A \circ h \\ &= h. \end{aligned}$$
Therefore, we conclude that $g = h$. □

Corollary 3.4.6. *If $f\colon A \to B$ is a function, then there exists at most one function $g\colon B \to A$ that is an inverse of f.*

Proof. Suppose that $g\colon B \to A$ and $h\colon B \to A$ are both inverses of f. In particular, we then have that g is a left inverse of f and h is a right inverse of f. Therefore, $g = h$ by Proposition 3.4.5. □

Corollary 3.4.7. *Let $f\colon A \to B$ be a function.*

1. *If f has a left inverse, then f has at most one right inverse.*
2. *If f has a right inverse, then f has at most one left inverse.*

Proof. Suppose that f has a left inverse, and fix such a left inverse $g\colon B \to A$. Suppose that $h_1\colon B \to A$ and $h_2\colon B \to A$ are both right inverse of f. Using Proposition 3.4.5, we conclude that $g = h_1$ and $g = h_2$. Therefore, $h_1 = h_2$.

The proof of the second result is completely analogous. □

Notice that it is possible for a function to have many left inverses, but this result says that that f must fail to have a right inverse in this case. This is exactly what happened in one of the above examples.

3.5 Defining Functions on Equivalence Classes

Suppose that $\sim$ is an equivalence relation on the set A. When we look at the equivalence classes of A, we know that we have shattered the set A into pieces. Just as in the case where we constructed the rationals, we often want to form a new set which consists of the equivalence classes themselves. Thus, the elements of this new set are themselves sets. Here is the formal definition.

Definition 3.5.1. *Let A be a set and let $\sim$ be an equivalence relation on A. The set whose elements are the equivalence classes of A under $\sim$ is called the* quotient *of A by $\sim$ and is denoted $A/\sim$.*

Thus, if let $A = \mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ where $(a,b) \sim (c,d)$ means $ad = bc$, then the set of all rationals is the quotient $A/\sim$. Letting $Q = A/\sim$, we then have that the *set* $\overline{(a,b)}$ is an *element* of Q for every choice of $a, b \in \mathbb{Z}$ with $b \neq 0$. This quotient construction is extremely general, and we will see that it will play a fundamental role in our studies. Before we delve into our first main example of modular arithmetic in the next section, we first address an important and subtle question.

To begin, notice that a given element of Q (namely a rational) is *represented* by many different pairs of integers. After all, we have

$$\frac{1}{2} = \overline{(1,2)} = \overline{(2,4)} = \overline{(-5,-10)} = \dots$$

Suppose that we want to define a function whose domain is Q. For example, we want to define a function $f\colon Q \to \mathbb{Z}$. Now we can try to write down something like:

$$f(\overline{(a,b)}) = a.$$

Intuitively, we are trying to define $f\colon Q \to \mathbb{Z}$ by letting $f(\frac{a}{b}) = a$. From a naive glance, this might look perfectly reasonable. However, there is a real problem arising from the fact that elements of Q have many representations. On the one hand, we should have

$$f(\overline{(1,2)}) = 1,$$

and on the other hand we should have

$$f(\overline{(2,4)}) = 2.$$

But we know that $\overline{(1,2)} = \overline{(2,4)}$, which contradicts the very definition of a function (after all, a function must have a unique output for any given input, but our description has imposed multiple different outputs for the same input). Thus, if we want to define a function on Q, we need to check that our definition does not depend on our choice of representatives.

For a positive example, consider the projective real line P. That is, let $A = \mathbb{R}^2\backslash\{(0,0)\}$ where $(x_1,y_1) \sim (x_2,y_2)$ means there there exists a real number $\lambda \neq 0$ such that $(x_1,y_1) = (\lambda x_2, \lambda y_2)$. We then have have that $P = A/\sim$. Consider trying to define the function $g\colon P \to \mathbb{R}$ by

$$g(\overline{(x,y)}) = \frac{5xy}{x^2+y^2}.$$

First we check a technicality: If $\overline{(x,y)} \in P$, then $(x,y) \neq (0,0)$, so $x^2+y^2 \neq 0$, and hence the domain of g really is all of P. Now we claim that g "makes sense", i.e. that it actually is a function. To see this, we take two elements (x_1,y_1) and (x_2,y_2) with $\overline{(x_1,y_1)} = \overline{(x_2,y_2)}$, and check that $g(\overline{(x_1,y_1)}) = g(\overline{(x_2,y_2)})$. In other words, we check that our definition of g does not actually depend on our choice of representative. Suppose then that $\overline{(x_1,y_1)} = \overline{(x_2,y_2)}$. We then have $(x_1,y_1) \sim (x_2,y_2)$, so we may fix $\lambda \neq 0$ with $(x_1,y_1) = (\lambda x_2, \lambda y_2)$.

Now

$$\begin{aligned}
g(\overline{(x_1,y_1)}) &= \frac{5x_1y_1}{x_1^2+y_1^2} \\
&= \frac{5(\lambda x_2)(\lambda y_2)}{(\lambda x_2)^2+(\lambda y_2)^2} \\
&= \frac{5\lambda^2 x_2y_2}{\lambda^2x_2^2+\lambda^2y_2^2} \\
&= \frac{\lambda^2\cdot 5x_2y_2}{\lambda^2\cdot(x_2^2+y_2^2)} \\
&= \frac{5x_2y_2}{x_2^2+y_2^2} \\
&= g(\overline{(x_2,y_2)}).
\end{aligned}$$

Hence, g does indeed make sense as a function on P.

Now technically we are being sloppy above when we start by defining a "function", and then only check after the fact that the definition makes sense and actually results in an honest function. However, this shortcut is completely standard. The process of checking that a "function" $f\colon A/\sim\ \to X$ defined via representatives of equivalence classes is independent of the actual representatives chosen, and so actually makes sense, is called checking that f is *well-defined*.

For a final example, let's consider a function from a quotient to another quotient. Going back to Q, we define a function $f\colon Q\to Q$ as follows:

$$f(\overline{(a,b)}) = \overline{(a^2+3b^2,2b^2)}.$$

We claim that this function is well-defined on Q. Intuitively, we want to define the following function on fractions:

$$f\left(\frac{a}{b}\right) = \frac{a^2+3b^2}{2b^2}.$$

Let's check that it does indeed make sense. Suppose that $a,b,c,d\in\mathbb{Z}$ with $b,d\neq 0$ and we have $\overline{(a,b)}=\overline{(c,d)}$, i.e. that $(a,b)\sim(c,d)$. We need to show that $f(\overline{(a,b)})=f(\overline{(c,d)})$, i.e. that $\overline{(a^2+3b^2,2b^2)}=\overline{(c^2+3d^2,2d^2)}$ or equivalently that $(a^2+3b^2,2b^2)\sim(c^2+3d^2,2d^2)$. Since we are assuming that $(a,b)\sim(c,d)$, we know that $ad=bc$. Hence

$$\begin{aligned}
(a^2+3b^2)\cdot 2d^2 &= 2a^2d^2+6b^2d^2 \\
&= 2(ad)^2+6b^2d^2 \\
&= 2(bc)^2+6b^2d^2 \\
&= 2b^2c^2+6b^2d^2 \\
&= 2b^2\cdot(c^2+3d^2).
\end{aligned}$$

Therefore, $(a^2+3b^2,2b^2)\sim(c^2+3d^2,2d^2)$, which is to say that $f(\overline{(a,b)})=f(\overline{(c,d)})$. It follows that f is well-defined on Q.

3.6 Modular Arithmetic

Definition 3.6.1. *Let $n\in\mathbb{N}^+$. We define a relation $\equiv_n$ on $\mathbb{Z}$ by letting $a\equiv_n b$ mean that $n\mid(a-b)$. When $a\equiv_n b$ we say that a is congruent to b modulo n.*

Proposition 3.6.2. *Let $n \in \mathbb{N}^+$. The relation $\equiv_n$ is an equivalence relation on $\mathbb{Z}$.*

Proof. We need to check the three properties.

- Reflexive: Let $a \in \mathbb{Z}$. Since $a - a = 0$ and $n \mid 0$, we have that $n \mid (a - a)$, hence $a \equiv_n a$.
- Symmetric: Let $a, b \in \mathbb{Z}$ with $a \equiv_n b$. We then have that $n \mid (a - b)$. Thus $n \mid (-1)(a - b)$ by Proposition 2.2.3, which says that $n \mid (b - a)$, and so $b \equiv_n a$.
- Transitive: Let $a, b, c \in \mathbb{Z}$ with $a \equiv_n b$ and $b \equiv_n c$. We then have that $n \mid (a - b)$ and $n \mid (b - c)$. Using Proposition 2.2.3, it follows that $n \mid [(a - b) + (b - c)]$, which is to say that $n \mid (a - c)$. Therefore, $a \equiv_n c$.

Putting it all together, we conclude that $\equiv_n$ is an equivalence relation on $\mathbb{Z}$. □

By our general theory about equivalence relations, we know that $\equiv_n$ partitions $\mathbb{Z}$ into equivalence classes. We next determine the number of such equivalence classes.

Proposition 3.6.3. *Let $n \in \mathbb{N}^+$ and let $a \in \mathbb{Z}$. There exists a unique $b \in \{0, 1, \dots, n - 1\}$ such that $a \equiv_n b$. In fact, if we write $a = qn + r$ for the unique choice of $q, r \in \mathbb{Z}$ with $0 \leq r < n$, then $b = r$.*

Proof. As in the statement, fix $q, r \in \mathbb{Z}$ with $a = qn + r$ and $0 \leq r < n$. We then have $a - r = nq$, so $n \mid (a - r)$. It follows that $a \equiv_n r$, so we have proven existence.

Suppose now that $b \in \{0, 1, \dots, n - 1\}$ and $a \equiv_n b$. We then have that $n \mid (a - b)$, so we may fix $k \in \mathbb{Z}$ with $nk = a - b$. This gives $a = kn + b$. Since $0 \leq b < n$, we may use the uniqueness part of Theorem 2.3.1 to conclude that $k = q$ (which is unnecessary) and also that $b = r$. This proves uniqueness. □

Therefore, the quotient $\mathbb{Z}/\equiv_n$ has n elements, and we can obtain unique representatives for these equivalence classes by taking the representatives from the set $\{0, 1, \dots, n - 1\}$. For example, if $n = 5$, we have that $\mathbb{Z}/\equiv_n$ consists of the following five sets.

- $\overline{0} = \{\dots, -10, -5, 0, 5, 10, \dots\}$.
- $\overline{1} = \{\dots, -9, -4, 1, 6, 11, \dots\}$.
- $\overline{2} = \{\dots, -8, -3, 2, 7, 12, \dots\}$.
- $\overline{3} = \{\dots, -7, -2, 3, 8, 13, \dots\}$.
- $\overline{4} = \{\dots, -6, -1, 4, 9, 14, \dots\}$.

Now that we've used $\equiv_n$ to break $\mathbb{Z}$ up into n pieces, our next goal is to show how to add and multiply elements of this quotient. The idea is to define addition/multiplication of elements of $\mathbb{Z}/\equiv_n$ by simply adding/multiplying representatives. In other words, we would like to define

$$\overline{a} + \overline{b} = \overline{a + b} \qquad \text{and} \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Of course, whenever we define functions on equivalence classes via representatives, we need to be careful to ensure that our function is well-defined, i.e. that it does not depend of the choice of representatives. That is the content of the next result.

Proposition 3.6.4. *Suppose that $a, b, c, d \in \mathbb{Z}$ with $a \equiv_n c$ and $b \equiv_n d$. We then have the following:*

1. $a + b \equiv_n c + d$.
2. $ab \equiv_n cd$.

Proof. Since $a \equiv_n c$ and $b \equiv_n d$, we have $n \mid (a - c)$ and $n \mid (b - d)$.

1. Notice that
$$(a + b) - (c + d) = (a - c) + (b - d).$$
Since $n \mid (a - c)$ and $n \mid (b - d)$, it follows that $n \mid [(a - c) + (b - d)]$ and so $n \mid [(a + b) - (c + d)]$. Therefore, $a + b \equiv_n c + d$.

2. Notice that
$$\begin{aligned} ab - cd &= ab - bc + bc - cd \\ &= (a - c) \cdot b + (b - d) \cdot c. \end{aligned}$$
Since $n \mid (a - c)$ and $n \mid (b - d)$, it follows that $n \mid [(a - c) \cdot b + (b - d) \cdot c]$ and so $n \mid (ab - cd)$. Therefore, $ab \equiv_n cd$.

$\square$

In this section, we've used the notation $a \equiv_n b$ to denote the relation because it fits in with our general infix notation. However, for both historical reasons and because the subscript can be annoying, one typically uses the following notation.

Notation 3.6.5. *Given $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}^+$, we write $a \equiv b \pmod{n}$ to mean that $a \equiv_n b$..*

Chapter 4

Introduction to Groups

4.1 Definitions

We briefly introduced the concept of a group in Chapter 1, and we now embark on a detailed study of these objects. As mentioned, groups are algebraic objects with just one operation. We choose to start with them in order to get practice with rigor and abstraction in as simple a setting as possible. Also, it turns out that groups appear across all areas of mathematics in many different guises.

Definition 4.1.1. *Let X be a set. A* binary operation *on X is a function $f\colon X^2 \to X$.*

In other words, a binary operation on a set X is a rule which tells us how to "put together" any two elements of X. For example, the function $f\colon \mathbb{R}^2 \to \mathbb{R}$ defined by $f(x,y) = x^2e^y$ is a binary operation on $\mathbb{R}$. Notice that a binary operation must be defined for *all* pairs of elements from X, and it must return an element of X. The function $f(x,y) = \frac{x}{y-1}$ is not a binary operation on $\mathbb{R}$ because it is not defined for any point of the form $(x,1)$. The function $f\colon \mathbb{Z}^2 \to \mathbb{R}$ defined by $f(x,y) = \sin(xy)$ is defined on all of $\mathbb{Z}^2$, but it is not a binary operation on $\mathbb{Z}$ because although some values of f are integers (like $f(0,0) = 1$), not all outputs are integers even when we provide integer inputs (for example, $f(1,1) = \sin 1$ is not an integer). Also, the dot product is not a binary operation on $\mathbb{R}^3$ because given two element of $\mathbb{R}^3$, it returns an element of $\mathbb{R}$ (rather than an element of $\mathbb{R}^3$).

Instead of using the standard function notation for binary operations, one typically uses something called infix notation. For example, when we add two numbers, we write $x + y$ rather the far more cumbersome $+(x,y)$. For the binary operation involved with groups, we will follow this infix notation.

Definition 4.1.2. *A* group *is a set G equipped with a binary operation $\cdot$ and an element $e \in G$ such that:*

1. *(Associativity) For all $a,b,c \in G$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*
2. *(Identity) For all $a \in G$, we have $a \cdot e = a$ and $e \cdot a = a$.*
3. *(Inverses) For all $a \in G$, there exists $b \in G$ with $a \cdot b = e$ and $b \cdot a = e$.*

In the abstract definition of a group, we have chosen to use the symbol $\cdot$ for the binary operation. This symbol may look like the "multiplication" symbol, but the operation need not be the usual multiplication in any sense. In fact, the $\cdot$ operation may be addition, exponentiation, or some bizarre and unnatural operation we never thought of before.

Notice that any description of a group needs to provide three things: a set G, a binary operation $\cdot$ on G (i.e. function from G^2 to G), and a particular element $e \in G$. Absolutely any such choice of set, function, and element can conceivably comprise a group. To check whether this is indeed the case, we need only check whether the above three properties are true of that fixed choice.

Here are a few examples of groups (in most cases we do not verify all of the properties here, but we will do so later):

1. $(\mathbb{Z}, +, 0)$ is a group, as are $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$, and $(\mathbb{C}, +, 0)$.
2. $(\mathbb{Q}\backslash\{0\}, \cdot, 1)$ is a group. We need to omit 0 because it has no multiplicative inverse. Notice that the product of two nonzero elements of $\mathbb{Q}$ is nonzero, so $\cdot$ really is a binary operation on $\mathbb{Q}\backslash\{0\}$.
3. The set of invertible 2×2 matrices over $\mathbb{R}$ with matrix multiplication and identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. In order to verify that multiplication is a binary operation on these matrices, it is important to note that the product of two invertible matrices is itself invertible, and that the inverse of an invertible matrix is itself invertible. These are fundamental facts from linear algebra, but will also follow from our results in Section 4.3.
4. $(\{1, -1, i, -i\}, \cdot, 1)$ is a group where $\cdot$ is multiplication of complex numbers.
5. $(\{T, F\}, \oplus, F)$ where $\oplus$ is "exclusive or" on T (interpreted as "true") and F (interpreted as "false"). Thus, we have $T \oplus T = F$, $T \oplus F = T$, $F \oplus T = T$, and $F \oplus F = F$.
6. Fix $n \in \mathbb{N}^+$ and let $\{0, 1\}^n$ be the set of all sequences of 0's and 1's of length n. If we let $\oplus$ be the bitwise "exclusive or" operation (interpreting 1 as true and 0 as false), then $(\{0, 1\}^n, \oplus, 0^n)$ is a group. Notice that when $n = 1$, and we interpret 0 as false and 1 as true, then this example looks just like the previous one.

In contrast, here are some examples of sets with binary operations that do *not* form groups:

1. $(\mathbb{Z}, -, 0)$ is not a group. Notice that $-$ is not associative because $(3 - 2) - 1 = 1 - 1 = 0$ but $3 - (2 - 1) = 3 - 1 = 2$. Also, 0 is not an identity because although $a - 0 = a$ for all $a \in \mathbb{Z}$, we have $0 - 1 = -1 \neq 1$.
2. Let S be the set of all odd elements of $\mathbb{Z}$, with the additional inclusion of 0, i.e. $S = \{0\} \cup \{n \in \mathbb{Z} : n \text{ is odd}\}$. Then $(S, +, 0)$ is not a group. Notice that $+$ is associative, that 0 is an identity, and that inverses exist. However, $+$ is not a binary operation on S because $1 + 3 = 4 \notin S$. In other words, S is not *closed* under $+$.
3. $(\mathbb{Q}, \cdot, 1)$ is not a group because 0 has no inverse.

Returning to the examples of groups above, notice that the group operation is commutative in all the examples except for (3). To see that the operation in (3) is not commutative, simply notice that each of the matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

are invertible (they both have determinant 1), but

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

while

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Thus, there are groups in which the group operation $\cdot$ is not commutative. The special groups that satisfy this additional fundamental property are named after Niels Abel.

Definition 4.1.3. *A group* $(G, \cdot, e)$ *is* abelian *if* $\cdot$ *is commutative, i.e. if* $a \cdot b = b \cdot a$ *for all* $a, b \in G$. *A group that is not abelian is called* nonabelian.

We will see many examples of nonabelian groups in time.

Notice that for a group G, there is no requirement at all that the set G or the operation $\cdot$ are in any way "natural" or "reasonable". For example, suppose that we work with the set $G = \{3, \aleph, @\}$ with operation $\cdot$ defined by the following table.

$\cdot$	3	$\aleph$	@
3	@	3	$\aleph$
$\aleph$	3	$\aleph$	@
@	$\aleph$	@	3

Interpret the above table as follows. To determine $a \cdot b$, go to the row corresponding to a and the column corresponding to b, and $a \cdot b$ will be the corresponding entry. For example, in order to compute $3 \cdot @$, we go to the row labeled 3 and column labeled @, which tells us that $3 \cdot @ = \aleph$. We can indeed check that this does form a group with identity element $\aleph$. However, this is a painful check because there are 27 choices of triples for which we need to verify associativity. This table view of a group G described above is called the *Cayley table* of G.

Here is another example of a group using the set $G = \{1, 2, 3, 4, 5, 6\}$ with operation $*$ defined by the following Cayley table:

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

It is straightforward to check that 1 is an identity for G and that every element has an inverse. However, as above, I very strongly advise against checking associativity directly. We will see later how to build many new groups and verify associativity without directly trying all possible triples. Notice that this last group is an example of a finite nonabelian group because $2 * 3 = 6$ while $3 * 2 = 5$.

4.2 Basic Properties, Notation, and Conventions

First, notice that in the definition of a group, we merely stated that there exists an identity element. There was no comment on how many such elements there might be. We begin by proving that there is only one such element in every group.

Proposition 4.2.1. *Let* $(G, \cdot, e)$ *be a group. There exists a unique identity element in* G, *i.e. if* $d \in G$ *has the property that* $a \cdot d = a$ *and* $d \cdot a = a$ *for all* $a \in G$, *then* $d = e$.

Proof. Let $d \in G$ be an arbitrary identity element, i.e. suppose that $a \cdot d = a$ and $d \cdot a = a$ for all $a \in G$. The key element to consider is $d \cdot e$. On the one hand, we know that $d \cdot e = d$ because e is an identity element. On the other hand, we have $d \cdot e = e$ because d is an identity element. Therefore, $d = d \cdot e = e$, so $d = e$. $\square$

We now move on to a similar question about inverses. The axioms only state the existence of an inverse for every given element, but we now prove uniqueness as well.

Proposition 4.2.2. *Let $(G, \cdot, e)$ be a group. For each $a \in G$, there exists a unique $b \in G$ such that $a \cdot b = e$ and $b \cdot a = e$.*

Proof. Let $a \in G$. By the group axioms, we know that there exists an inverse of a. Suppose that b and c both work as inverses, i.e. that $a \cdot b = e = b \cdot a$ and $a \cdot c = e = c \cdot a$. The crucial element to think about is $(b \cdot a) \cdot c = b \cdot (a \cdot c)$. We have

$$\begin{aligned} b &= b \cdot e \\ &= b \cdot (a \cdot c) \\ &= (b \cdot a) \cdot c \\ &= e \cdot c \\ &= c, \end{aligned}$$

hence $b = c$. $\square$

Definition 4.2.3. *Let $(G, \cdot, e)$ be a group. Given an element $a \in G$, we let a^{-1} denote the unique element such that $a \cdot a^{-1} = e$ and $a^{-1} \cdot a = e$.*

Proposition 4.2.4. *Let $(G, \cdot, e)$ be a group and let $a, d \in G$.*

1. *There exists a unique element $x \in G$ such that $a \cdot x = d$, namely $x = a^{-1} \cdot d$.*
2. *There exists a unique element $x \in G$ such that $x \cdot a = d$, namely $x = d \cdot a^{-1}$.*

Proof. We prove (1) and leave (2) as an exercise (it is completely analogous). Notice that $x = a^{-1} \cdot d$ works because

$$\begin{aligned} a \cdot (a^{-1} \cdot d) &= (a \cdot a^{-1}) \cdot d \\ &= e \cdot d \\ &= d. \end{aligned}$$

Suppose now that $x \in G$ satisfies $a \cdot x = d$. We then have that

$$\begin{aligned} x &= e \cdot x \\ &= (a^{-1} \cdot a) \cdot x \\ &= a^{-1} \cdot (a \cdot x) \\ &= a^{-1} \cdot d. \end{aligned}$$

Here's an alternate presentation of the latter part (it is the exact same proof, just with more words and a little more motivation). Suppose that $x \in G$ satisfies $a \cdot x = d$. We then have that $a^{-1} \cdot (a \cdot x) = a^{-1} \cdot d$. By associatively, the left-hand side is $(a^{-1} \cdot a) \cdot x$, which is $e \cdot x$, with equals x. Therefore, $x = a^{-1} \cdot b$. $\square$

Corollary 4.2.5 (Cancellation Laws)**.** *Let $(G, \cdot, e)$ be a group and let $a, b, c \in G$.*

1. *If $a \cdot b = a \cdot c$, then $b = c$.*
2. *If $b \cdot a = c \cdot a$, then $b = c$.*

Proof. Suppose that $a \cdot b = a \cdot c$. Letting d equal this common value, it follows from the uniqueness part of Proposition 4.2.4 that $b = c$. Alternatively, multiply both sides on the left by a^{-1} and use associativity. Part (2) is completely analogous. $\square$

In terms of the Cayley table of a group G, Proposition 4.2.4 says that every element of a group appears exactly once in each row of the table, and exactly once in each column of the table. In fancy terminology, the Cayley table of a group is a Latin square.

Proposition 4.2.6. *Let $(G, \cdot, e)$ be a group and let $a \in G$. We have $(a^{-1})^{-1} = a$.*

Proof. By definition we have $a \cdot a^{-1} = e = a^{-1} \cdot a$. Thus, a satisfies the requirement to be the inverse of a^{-1}. In other words, $(a^{-1})^{-1} = a$. □

Proposition 4.2.7. *Let $(G, \cdot, e)$ be a group and let $a, b \in G$. We have $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.*

Proof. We have

$$\begin{aligned}(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) &= ((a \cdot b) \cdot b^{-1}) \cdot a^{-1} \\ &= (a \cdot (b \cdot b^{-1})) \cdot a^{-1} \\ &= (a \cdot e) \cdot a^{-1} \\ &= a \cdot a^{-1} \\ &= e.\end{aligned}$$

and similarly $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e$. Therefore, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. □

We now establish some notation. First, we often just say "Let G be a group" rather than the more precise "Let $(G, \cdot, e)$ be a group". In other words, we typically do not explicitly mention the binary operation and will just write $\cdot$ afterward if we feel the need to use it. The identity element is unique as shown in Proposition 4.2.1, so we do not feel the need to be so explicit about it and will just call it e later if we need to refer to it. If some confusion may arise (for example, there are several natural binary operations on the given set), then we will need to be explicit.

Let G be a group. If $a, b \in G$, we typically write ab rather than explicitly writing the binary operation in $a \cdot b$. Of course, sometimes it makes sense to insert the dot. For example, if G contains the integers 2 and 4 and 24, writing 24 would certainly be confusing. Also, if the group operation is standard addition or some other operation with a conventional symbol, we will switch up and use that symbol to avoid confusion. However, when there is no confusion, and when we are dealing with an abstract group without explicit mention of what the operation actually is, we will tend to omit it.

With this convention in hand, associativity tells us that $(ab)c = a(bc)$ for all $a, b, c \in G$. Now using associativity repeatedly we obtain what can be called "generalized associativity". For example, suppose that G is a group and $a, b, c, d \in G$. We then have that $(ab)(cd) = (a(bc))d$ because we can use associativity twice as follows:

$$\begin{aligned}(ab)(cd) &= ((ab)c)d \\ &= (a(bc))d.\end{aligned}$$

In general, such rearrangements are always possible by iteratively moving the parentheses around as long as the order of the elements doesn't change. In other words, no matter how we insert parentheses in $abcd$ so that it makes sense, we always obtain the same result. For a sequence of 4 elements it is straightforward to try them all, and for 5 elements it is tedious but feasible. However, it is true no matter how long the sequence is. A proof of this general fact requires a careful definition of what a "permissible insertion of parentheses" means, and at this level such an involved tangent is more distracting from our primary aims than it is enlightening. We will simply take the result as true.

Keep in mind that the order of the elements occurring does matter. There is no reason at all to think that $abcd$ equals $dacb$ unless the group is abelian. However, if G is abelian, then upon any insertion of parentheses into these expressions so that they make sense, they will evaluate to the same value. Thus, assuming that G is commutative, we obtain a kind of "generalized commutativity" just like we have a "generalized associativity".

At the moment, we only have a few examples of groups. We know that the usual sets of numbers under addition like $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$, and $(\mathbb{C}, +, 0)$ are groups. We listed a few other examples above, such as $(\mathbb{Q}\backslash\{0\}, \cdot, 1)$, $(\mathbb{R}\backslash\{0\}, \cdot, 1)$, and the invertible 2×2 matrices under multiplication with the usual $n \times n$ identity matrix. In these last few examples, we needed to "throw away" some elements from the natural set in order to satisfy the inverse requirement, and in the next section we outline this construction in general.

4.3 Building Groups From Associative Operations

When constructing new groups from scratch, the most difficult property to verify is the associative property of the binary operation. In the next few sections, we will construct some fundamental groups using some known associative operations. However, even if we have a known associative operation with a natural identity element, we may not always have inverses. In the rest of this section, we show that in such a situation, if we restrict down to the "invertible" elements, then we indeed do have a group.

Definition 4.3.1. *Let $\cdot$ be a binary operation on a set A that is associative and has an identity element e. Given $a \in A$, we say that a is* invertible *if there exists $b \in A$ with both $ab = e$ and $ba = e$. In this case, we say that b is an* inverse *for a.*

Proposition 4.3.2. *Let $\cdot$ be a binary operation on a set A that is associative and has an identity element e. We then have that each $a \in A$ has at most one inverse.*

Proof. The proof is completely analogous to the proof for functions and the uniqueness part of Proposition 4.2.2. Let $a \in A$ and suppose that b and c are both inverses for a. We then have that

$$\begin{aligned} b &= be \\ &= b(ac) \\ &= (ba)c \\ &= ec \\ &= c, \end{aligned}$$

so $b = c$. □

Notation 4.3.3. *Let $\cdot$ be a binary operation on a set A that is associative and has an identity element e. If $a \in A$ is invertible, then we denote its unique inverse by a^{-1}.*

Proposition 4.3.4. *Let $\cdot$ be a binary operation on a set A that is associative and has an identity element e.*

1. *e is an invertible element with $e^{-1} = e$.*
2. *If a and b are both invertible, then ab is invertible and $(ab)^{-1} = b^{-1}a^{-1}$.*
3. *If a is invertible, then a^{-1} is invertible and $(a^{-1})^{-1} = a$.*

Proof.

1. Since $ee = e$ because e is an identity element, we see immediately that e is invertible and $e^{-1} = e$.
2. Suppose that $a, b \in A$ are both invertible. We then have that

$$\begin{aligned} abb^{-1}a^{-1} &= aea^{-1} \\ &= aa^{-1} \\ &= e, \end{aligned}$$

and also

$$\begin{aligned} b^{-1}a^{-1}ab &= beb^{-1} \\ &= bb^{-1} \\ &= e. \end{aligned}$$

It follows that ab is invertible and $(ab)^{-1} = b^{-1}a^{-1}$.

3. Suppose that $a \in A$ is invertible. By definition, we then have that both $aa^{-1} = e$ and also that $a^{-1}a = e$. Looking at these equations, we see that a satisfies the definition of being an inverse for a^{-1}. Therefore, a^{-1} is invertible and $(a^{-1})^{-1} = a$.

□

Corollary 4.3.5. *Let $\cdot$ be a binary operation on a set A that is associative and has an identity element e. Let B be the set of all invertible elements of A. We then have that $\cdot$ is a binary operation on B and that $(B, \cdot, e)$ is a group. Furthermore, if $\cdot$ is commutative on A, then $(B, \cdot, e)$ is an abelian group.*

Proof. By Proposition 4.3.4, we know that if $b_1, b_2 \in B$, then $b_1 b_2 \in B$, and hence $\cdot$ is a binary operation on B. Proposition 4.3.4 also tells us that $e \in B$. Furthermore, since e is an identity for A, and $B \subseteq A$, it follows that e is an identity element for B. Now $\cdot$ is an associative operation on A and $B \subseteq A$, so it follows that $\cdot$ is an associative operation on B. Finally, if $b \in B$, then Proposition 4.3.4 tells us that $b^{-1} \in B$ as well, so b does have an inverse in B. Putting this all together, we conclude that $(B, \cdot, e)$ is a group. For the final statement, simply notice that if $\cdot$ is an commutative operation on A, then since $B \subseteq A$ it follows that $\cdot$ is a commutative operation on B. □

One special case of this construction is that $(\mathbb{Q}\backslash\{0\}, \cdot, 1)$, $(\mathbb{R}\backslash\{0\}, \cdot, 1)$, and $(\mathbb{C}\backslash\{0\}, \cdot, 1)$ are all abelian groups. In each case, multiplication is an associative and commutative operation on the whole set, and 1 is an identity element. Furthermore, in each case, every element but 0 is invertible. Thus, Corollary 4.3.5 says that each of these are abelian groups.

Another associative operation that we know is the multiplication of matrices. Of course, the set of all $n \times n$ matrices does not form a group because some matrices do not have inverses. However, if we restrict down to just the invertible matrices, then Corollary 4.3.5 tells us that we do indeed obtain a group.

Definition 4.3.6. *Let $n \in \mathbb{N}^+$. The set of all $n \times n$ invertible matrices with real entries forms a group under matrix multiplication, with identity element equal to the $n \times n$ identity matrix with 1's on the diagonal and 0's everywhere else. We denote this group by $GL_n(\mathbb{R})$ and call it the* general linear group *of degree n over $\mathbb{R}$.*

Notice that $GL_1(\mathbb{R})$ is really just the group $(\mathbb{R}\backslash\{0\}, \cdot, 1)$. However, for each $n \geq 2$, the group $GL_n(\mathbb{R})$ is nonabelian, so we have an infinite family of such groups (it is worthwhile to explicitly construct two $n \times n$ invertible matrices that do not commute with each other).

Moreover, it also possible to allow entries of the matrices to come from a place other than $\mathbb{R}$. For example, we can consider matrices with entries from $\mathbb{C}$. In this case, matrix multiplication is still associative, and the the usual identity matrix is still an identity element. Thus, we can define the following group:

Definition 4.3.7. *Let $n \in \mathbb{N}^+$. The set of all $n \times n$ invertible matrices with complex entries forms a group under matrix multiplication, with identity element equal to the $n \times n$ identity matrix with 1's on the diagonal and 0's everywhere else). We denote this group by $GL_n(\mathbb{C})$ and call it the* general linear group *of degree n over $\mathbb{C}$.*

As we will see in Chapter 9, we can even generalize this matrix construction to other "rings" other than $\mathbb{R}$ and $\mathbb{C}$.

4.4 The Groups $\mathbb{Z}/n\mathbb{Z}$ and $U(\mathbb{Z}/n\mathbb{Z})$

Most of the examples of groups that we have seen thus far have infinitely many elements. However, some examples, like $(\{T, F\}, \oplus, F)$ have only finitely many. We introduce the following definition.

Definition 4.4.1. *Let G be a group. If G is a finite set, then the order of G, denoted $|G|$, is the number of elements in G. If G is infinite, we simply write $|G| = \infty$.*

For example, if G is the group $(\{T, F\}, \oplus, F)$, then $|G| = 2$. On the other, if G is any of the groups $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$ under addition, then $|G| = \infty$. In this section, we construct two very important families of finite groups.

Proposition 4.4.2. *Let $n \in \mathbb{N}^+$ and let $G = \mathbb{Z}/\equiv_n$, i.e. the elements of G are the equivalence classes of $\mathbb{Z}$ under the equivalence relation $\equiv_n$. Define a binary operation $+$ on G by letting $\overline{a} + \overline{b} = \overline{a + b}$. We then have that $(G, +, \overline{0})$ is an abelian group.*

Proof. We have already shown in Proposition 3.6.4 that $+$ is well-defined on G. With that in hand, the definition makes it immediate that $+$ is a binary operation on G. We now check the axioms for an abelian group.

- Associative: For any $a, b, c \in \mathbb{Z}$ we have

$$\begin{aligned}
(\overline{a} + \overline{b}) + \overline{c} &= (\overline{a + b}) + \overline{c} \\
&= \overline{(a + b) + c} \\
&= \overline{a + (b + c)} && \text{(since } + \text{ is associative on } \mathbb{Z}) \\
&= \overline{a} + \overline{b + c} \\
&= \overline{a} + (\overline{b} + \overline{c}),
\end{aligned}$$

  so $+$ is associative on G.

- Identity: For any $a \in \mathbb{Z}$ we have
$$\overline{a} + \overline{0} = \overline{a + 0} = \overline{a}$$
  and
$$\overline{0} + \overline{a} = \overline{0 + a} = \overline{a}.$$

- Inverses: For any $a \in \mathbb{Z}$ we have
$$\overline{a} + \overline{-a} = \overline{a + (-a)} = \overline{0}$$
  and
$$\overline{-a} + \overline{a} = \overline{(-a) + a} = \overline{0}.$$

- Commutative: For any $a, b \in \mathbb{Z}$ we have

$$\begin{aligned}
\overline{a} + \overline{b} &= \overline{a + b} \\
&= \overline{b + a} && \text{(since } + \text{ is commutative on } \mathbb{Z}) \\
&= \overline{b} + \overline{a},
\end{aligned}$$

  so $+$ is commutative on G.

Therefore, $(G, +, \overline{0})$ is an abelian group. $\square$

Definition 4.4.3. *Let $n \in \mathbb{N}^+$. We denote the above abelian group by $\mathbb{Z}/n\mathbb{Z}$. We call the group "$\mathbb{Z}$ mod $n\mathbb{Z}$".*

This notation is unmotivated at the moment, but will make sense when we discuss quotient groups (and be consistent with the more general notation we establish there). Using Proposition 3.6.3, we have that

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$$

and that $\overline{k} \neq \overline{\ell}$ whenever $0 \leq k < \ell < n$ by It follows that $|\mathbb{Z}/n\mathbb{Z}| = n$ for all $n \in \mathbb{N}^+$, and so we have shown that there exists an abelian group of every finite order.

Let's examine one example in detail. Consider $\mathbb{Z}/5\mathbb{Z}$. As we just mentioned, the equivalence classes $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$ and $\overline{4}$ are all distinct and give all elements of $\mathbb{Z}/5\mathbb{Z}$. By definition, we have $\overline{3} + \overline{4} = \overline{7}$. This is perfectly correct, but 7 is not one of the special representatives we chose above. Since $\overline{7} = \overline{2}$, we can also write $\overline{3}+\overline{4} = \overline{2}$ and now we have removed mention of all representatives other than the chosen ones. Working it all out with only those representatives, we get the following Cayley table for $\mathbb{Z}/5\mathbb{Z}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

We also showed in Proposition 3.6.4 that multiplication is well-defined on the quotient. Now it is straightforward to mimic the above arguments to show that multiplication is both associative and commutative, and that $\overline{1}$ is an identity. However, it seems unlikely that we always have inverses because $\mathbb{Z}$ itself fails to have multiplicative inverses for all elements other than ± 1. But let's look at what happens in the case $n = 5$. For example, we have $\overline{4} \cdot \overline{4} = \overline{16} = \overline{1}$, so in particular $\overline{4}$ does have a multiplicative inverse. Working out the computations, we get the following table.

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Examining the table, we are pleasantly surprised that every element other that $\overline{0}$ does have a multiplicative inverse! In hindsight, there was no hope of $\overline{0}$ having a multiplicative inverse because $\overline{0} \cdot \overline{a} = \overline{0 \cdot a} = \overline{0} \neq \overline{1}$ for all $a \in \mathbb{Z}$. With this one example we might have the innocent hope that we always get multiplicative inverses for elements other $\overline{0}$ when we change n. Let's dash those hopes now by looking at the case when $n = 6$.

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Looking at the table, we see that only $\overline{1}$ and $\overline{5}$ have multiplicative inverses. There are other curiosities as well. For example, we can have two nonzero elements whose product is zero as shown by $\overline{3} \cdot \overline{4} = \overline{0}$. This is an interesting fact, and will return to such considerations when we get to ring theory. However, let's get to our primary concern of forming a group under multiplication. Since $\cdot$ is an associative and commutative operation on $\mathbb{Z}/n\mathbb{Z}$ with identity element $\overline{1}$, Corollary 4.3.5 tells us that we can form an abelian group by trimming down to those elements that do have inverses. To get a better handle on what elements will be in this group, we use the following fact.

Proposition 4.4.4. *Let $n \in \mathbb{N}^+$ and let $a \in \mathbb{Z}$. The following are equivalent.*

1. *There exists $c \in \mathbb{Z}$ with $ac \equiv 1 \pmod{n}$.*
2. $\gcd(a, n) = 1$.

Proof.

- (1) $\Rightarrow$ (2): Assume that (1) is true. Fix $c \in \mathbb{Z}$ with $ac \equiv 1 \pmod{n}$. We then have $n \mid (ac - 1)$, so we may fix $k \in \mathbb{Z}$ with $nk = ac - 1$. Rearranging, we see that $ac + n(-k) = 1$. Since $\gcd(a, n)$ divides both a and n, we may use Proposition 2.2.3 to conclude that $\gcd(a, n)$ divides $ac + n(-k)$, and hence $\gcd(a, n) \mid 1$. Now we know that $\gcd(a, n) \geq 0$ by definition, and $\gcd(a, n) \neq 0$ because $n \neq 0$, so we conclude that $\gcd(a, n) = 1$.
- (2) $\Rightarrow$ (1): Suppose that $\gcd(a, n) = 1$. Using Theorem 2.4.9, we can fix $k, \ell \in \mathbb{Z}$ with $ak + n\ell = 1$. Rearranging gives $n(-\ell) = ak - 1$, so $n \mid (ak - 1)$. It follows that $ak \equiv 1 \pmod{n}$, so we can choose $c = k$.

□

Thus, when $n = 6$, the fundamental reason why $\overline{1}$ and $\overline{5}$ have multiplicative inverses is that $\gcd(1, 6) = 1 = \gcd(5, 6)$. In the case of $n = 5$, the reason why every element other than $\overline{0}$ had a multiplicative inverse is because every positive number less than 5 is relatively prime with 5, which is essentially just saying that 5 is prime. Notice that the above argument can be turned into an explicit algorithm for finding such a c as follows. Given $n \in \mathbb{N}^+$ and $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, use the Euclidean algorithm to produce $k, \ell \in \mathbb{Z}$ with $ak + n\ell = 1$. As the argument shows, we can then choose $c = k$.

As a consequence of the above result and the fact that multiplication is well-defined (Proposition 3.6.4), we see that if $a \equiv b \pmod{n}$, then $\gcd(a, n) = 1$ if and only if $\gcd(b, n) = 1$. Of course we could have proved this without this result: Suppose that $a \equiv b \pmod{n}$. We then have that $n \mid (a - b)$, so we may fix $k \in \mathbb{Z}$ with $nk = a - b$. This gives $a = kn + b$ so $\gcd(a, n) = \gcd(b, n)$ by Corollary 2.4.8.

Now that we know which elements have multiplicative inverses, if we trim down to these elements then we obtain an abelian group.

Proposition 4.4.5. *Let $n \in \mathbb{N}^+$ and let $G = \mathbb{Z}/\equiv_n$, i.e. G the elements of G are the equivalence classes of $\mathbb{Z}$ under the equivalence relation $\equiv_n$. Let U be the following subset of G:*

$$U = \{\overline{a} : a \in \mathbb{Z} \text{ and } \gcd(a, n) = 1\}.$$

Define a binary operation $\cdot$ on U by letting $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. We then have that $(U, \cdot, \overline{1})$ is an abelian group.

Proof. Since $\cdot$ is an associative and commutative operation on $\mathbb{Z}/n\mathbb{Z}$ with identity element $\overline{1}$, this follows immediately from Corollary 4.3.5 and Proposition 4.4.4. □

Definition 4.4.6. *Let $n \in \mathbb{N}^+$. We denote the above abelian group by $U(\mathbb{Z}/n\mathbb{Z})$.*

Again, this notation may seems a bit odd, but we will come back and explain it in context when we get to ring theory (the U is short for *units*, which are special elements of a ring). To see some examples of Cayley tables of these groups, here is the Cayley table of $U(\mathbb{Z}/5\mathbb{Z})$:

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

and here is the Cayley table of $U(\mathbb{Z}/6\mathbb{Z})$:

$\cdot$	$\overline{1}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{1}$

Finally, we give the Cayley table of $U(\mathbb{Z}/8\mathbb{Z})$ because we will return to this group later as an important example:

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{7}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{7}$	$\overline{1}$	$\overline{3}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$

Definition 4.4.7. *We define a function $\varphi\colon \mathbb{N}^+ \to \mathbb{N}^+$ as follows. For each $n \in \mathbb{N}^+$, we let*

$$\varphi(n) = |\{a \in \{0, 1, 2, \dots, n-1\} : \gcd(a, n) = 1\}|.$$

The function φ is called the Euler φ-function or Euler totient function.

Directly from our definition of $U(\mathbb{Z}/n\mathbb{Z})$, we see that $|U(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$ for all $n \in \mathbb{N}^+$. Calculating $\varphi(n)$ is a nontrivial task, although it is straightforward if we know the prime factorization of n (see Chapter **??**). Notice that $\varphi(p) = p - 1$ for all primes p, so $|U(\mathbb{Z}/p\mathbb{Z})| = p - 1$ for all primes p.

4.5 The Symmetric Groups

Using all of our hard work in Chapter 3, we can now construct a group whose elements are *functions*. The key fact is that function composition is an associative operation by Proposition 3.3.5, so we can think about using it as a group operation. However, there are a couple of things to consider. First if $f\colon A \to B$ and $g\colon B \to C$ are functions, then $g \circ f$ makes sense, but $f \circ g$ likely doesn't make sense unless $A = C$. Even more importantly, $f \circ f$ doesn't make sense unless $A = B$. Thus, if we want to make sure that composition always works, we should stick only to those functions that are from a given set A to itself. With this in mind, let's consider the set S of all functions $f\colon A \to A$. We now have that composition is an associative operation on S, and furthermore id_A serves as an identity element. Of course, not all elements of S have an inverse, but we do know from Proposition 3.4.4 that an element $f \in S$ has an inverse if and only if f is a bijection. With that in mind, we can use Corollary 4.3.5 to form a group.

Definition 4.5.1. *Let A be a set. A* permutation *of A is a bijection $f\colon A \to A$. Rather than use the standard symbols $f, g, h, \dots$ employed for general functions, we typically employ letters late in the greek alphabet, like $\sigma, \tau, \pi, \mu, \dots$ for permutations.*

Definition 4.5.2. *Let A be a set. The set of all permutations of A together with the operation of function composition is a group called the* symmetric group *on A. We denote this group by S_A. If we're given $n \in \mathbb{N}^+$, we simply write S_n rather than $S_{\{1,2,\dots,n\}}$.*

Remember that elements of S_A are *functions* and the operation is *composition*. It's exciting to have built such an interesting group, but working with functions as group elements takes some getting used to. For an example, suppose that $A = \{1, 2, 3, 4, 5, 6\}$. To define a permutation $\sigma\colon A \to A$, we need to say what σ does on each element of A, which can do this by a simple list. Define $\sigma\colon A \to A$ as follows.

- $\sigma(1) = 5$.
- $\sigma(2) = 6$.
- $\sigma(3) = 3$.
- $\sigma(4) = 1$.
- $\sigma(5) = 4$.
- $\sigma(6) = 2$.

We then have that $\sigma\colon A \to A$ is a permutation (note every element of A is hit by exactly one element). Now it's unnecessarily cumbersome to write out the value of $\sigma(k)$ on each k in a bulleted list like this. Instead, we can use the slightly more compact notation:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 1 & 4 & 2 \end{pmatrix}.$$

Interpret the above matrix by taking the top row as the inputs and each number below as the corresponding output. Let's throw another permutation $\tau \in S_6$ into the mix. Define

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 6 & 2 & 4 \end{pmatrix}.$$

Let's compute $\sigma \circ \tau$. Remember that function composition happens from right to left. That is, the composition $\sigma \circ \tau$ is obtained by performing τ first and following after by performing σ. For example, we have

$$(\sigma \circ \tau)(2) = \sigma(\tau(2)) = \sigma(1) = 5.$$

Working through the 6 inputs, we obtain:

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 2 & 6 & 1 \end{pmatrix}.$$

On the other hand, we have

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 3 & 6 & 1 \end{pmatrix}.$$

Notice that $\sigma \circ \tau \neq \tau \circ \sigma$. We have just shown that S_6 is a nonabelian group. Let's determine just how large these groups are.

Proposition 4.5.3. *If $|A| = n$, then $|S_A| = n!$. In particular, $|S_n| = n!$ for all $n \in \mathbb{N}^+$.*

Proof. We count the number of elements of the set S_A by constructing all possible permutations $\sigma\colon A \to A$ via a sequence of choices. To construct such a permutation, we can first determine the value $\sigma(1)$. Since no numbers have been claimed, we have n possibilities for this value because we can choose any element of A. Now we move on to determine the value $\sigma(2)$. Notice that we can make $\sigma(2)$ any value in A *except* for the chosen value of $\sigma(1)$ (because we need to ensure that σ is an injection). Thus, we have $n-1$ many possibilities. Now to determine the value of $\sigma(3)$, we can choose any value in A other than $\sigma(1)$ and $\sigma(2)$ because those have already been claimed, so we have $n-2$ many choices. In general, when trying to define $\sigma(k+1)$, we have already claimed k necessarily distinct elements of A, so we have exactly $n-k$ possibly choices for the value. Thus, the number of permutations of A equals

$$n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 = n!$$

□

Let's return to our element σ in S_6:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 1 & 4 & 2 \end{pmatrix}.$$

This method of representing σ is reasonably compact, but it hides the fundamental structure of what is happening. For example, it takes a few steps to "see" what the inverse of σ is, and it is unclear what happens when we compose σ with itself repeatedly. We now develop another method for representing a permutation on A called *cycle notation*. The basic idea is to take an element of A and follow its path through σ. For example, let's start with 1. We have $\sigma(1) = 5$. Now instead of moving on to deal with 2, let's continue this thread and determine the value $\sigma(5)$. Looking above, we see that $\sigma(5) = 4$. If we continue on this path to investigate 4, we see that $\sigma(4) = 1$, and we have found a "cycle" $1 \to 5 \to 4 \to 1$ hidden inside σ. We will denote this cycle with the notation $(1\ 5\ 4)$. Now that those numbers are taken care of, we start again with the smallest number not yet claimed, which in this case is 2. We have $\sigma(2) = 6$ and following up gives $\sigma(6) = 2$. Thus, we have found the cycle $2 \to 6 \to 2$ and we denote this by $(2\ 6)$. We have now claimed all numbers other than 3, and when we investigate 3 we see that $\sigma(3) = 3$, so we form the sad lonely cycle (3). Putting this all together, we write σ in cycle notation as

$$\sigma = (1\ 5\ 4)(2\ 6)(3).$$

One might wonder whether we ever get "stuck" when trying to build these cycles. What would happen if we follow 1 and we repeat a number before coming back to 1? For example, what if we see $1 \to 3 \to 6 \to 2 \to 6$? Don't fear because this can never happen. The only way the example above could crop up is if the purported permutation sent both 3 and 2 to 6, which would violate the fact that the purported permutation is injective. Also, if we finish a few cycles and start up a new one, then it is not possible that our new cycle has any elements in common with previous ones. For example, if we already have the cycle $1 \to 3 \to 2 \to 1$ and we start with 4, we can't find $4 \to 5 \to 3$ because then both 1 and 5 would map to 3.

Our conclusion is that this process of writing down a permutation in cycle notation never gets stuck and results in writing the given permutation as a product of disjoint cycles. Working through the same process with the permutation

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 6 & 2 & 4 \end{pmatrix},$$

we see that in cycle notation we have

$$\tau = (1\ 3\ 5\ 2)(4\ 6).$$

Now we can determine $\sigma \circ \tau$ in cycle notation directly from the cycle notations of σ and τ. For example, suppose we want to calculate the following:

$$(1\ 2\ 4)(3\ 6)(5) \circ (1\ 6\ 2)(3\ 5\ 4).$$

We want to determine the cycle notation of the resulting function, so we first need to determine where it sends 1. Again, function composition happens from right to left. Looking at the function represented on the right, we see the cycle containing 1 is (1 6 2), so the right function sends 1 to 6. We then go to the function on the left and see where it sends 6. The cycle containing 6 there is (3 6), so it takes 6 and sends it to 3. It follows that the composition sends 1 to 3. Thus, our result starts out as

$$(1\ 3.$$

Now we need to see what happens to 3. The function on the right sends 3 to 5, and the function on the left takes 5 and leave it alone, so we have

$$(1\ 3\ 5.$$

When we move on to see what happens to 5, we notice that the right function sends it to 4 and then the left function takes 4 to 1. Since 1 is the first element the cycle we started, we now close the loop and have

$$(1\ 3\ 5).$$

We now pick up the least element not in the cycle and continue. Working it out, we end with:

$$(1\ 2\ 4)(3\ 6)(5) \circ (1\ 6\ 2)(3\ 5\ 4) = (1\ 3\ 5)(2)(4\ 6).$$

Finally, we make our notation a bit more compact with a few conventions. First, we simply omit any cycles of length 1, so we just write (1 2 4)(3 6) instead of (1 2 4)(3 6)(5). Of course, this requires an understanding of which n we are using to avoid ambiguity as the notation (1 2 4)(3 6) doesn't specify whether we are viewing is as an element of S_6 or S_8 (in the latter case, the corresponding function fixes both 7 and 8). Also, as with most group operations, we simply omit the $\circ$ when composing functions. Thus, we would write the above as:

$$(1\ 2\ 4)(3\ 6)(1\ 6\ 2)(3\ 5\ 4) = (1\ 3\ 5)(2)(4\ 6).$$

Now there is potential for some conflict here. Looking at the first two cycles above, we meant to think of (1 2 4)(3 6) as one particular function on $\{1, 2, 3, 4, 5, 6\}$, but by omitting the group operation it could also be interpreted as $(1\ 2\ 4) \circ (3\ 6)$. Fortunately, these are exactly the same function because the cycles are disjoint. Thus, there is no ambiguity.

Let's work out everything about S_3. First, we know that $|S_3| = 3! = 6$. Working through the possibilities, we determine that

$$S_3 = \{id, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

so S_3 has the identity function, three 2-cycles, and two 3-cycles. Here is the Cayley table of S_3:

$\circ$	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
id	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	id	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	id	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	id	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	id
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	id	(1 2 3)

Notice that S_3 is a nonabelian group with 6 elements. In fact, it is the smallest possible nonabelian group, as we shall see later.

We end this section with two straightforward but important results.

Proposition 4.5.4. *Disjoint cycles commutes. That is, if A is a set and $a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_\ell \in A$ are all distinct, then*

$$(a_1\ a_2\ \cdots\ a_k)(b_1\ b_2\ \cdots\ b_\ell) = (b_1\ b_2\ \cdots\ b_\ell)(a_1\ a_2\ \cdots\ a_k).$$

Proof. Simply work through where each a_i and b_j are sent on each side. Since $a_i \neq b_j$ for all i and j, each a_i is fixed by the cycle containing the b_j's and vice versa. Furthermore, if $c \in A$ is such that $c \neq a_i$ and $c \neq b_j$ for all i and j, then both cycles fix c, so both sides fix c. □

Proposition 4.5.5. *Let A be a set and let $a_1, a_2, \dots, a_k \in A$ be distinct. Let $\sigma = (a_1\ a_2\ \cdots\ a_k)$. We then have that*

$$\begin{aligned}\sigma^{-1} &= (a_k\ a_{k-1}\ \cdots\ a_2\ a_1) \\ &= (a_1\ a_k\ a_{k-1}\ \cdots\ a_2)\end{aligned}$$

Proof. Let $\tau = (a_1\ a_k\ a_{k-1}\ \cdots\ a_2)$. For any i with $1 \leq i \leq k-1$, we have

$$(\tau \circ \sigma)(a_i) = \tau(\sigma(a_i)) = \tau(a_{i+1}) = a_i$$

and also

$$(\tau \circ \sigma)(a_k) = \tau(\sigma(a_k)) = \tau(a_1) = a_k$$

Furthermore, for any i with $2 \leq i \leq k$, we have

$$(\sigma \circ \tau)(a_1) = \sigma(\tau(a_1)) = \sigma(a_k) = a_1$$

and also

$$(\sigma \circ \tau)(a_i) = \sigma(\tau(a_i)) = \sigma(a_{i-1}) = a_i$$

Finally, if $c \in A$ is such that $c \neq a_i$ for all i, then

$$(\tau \circ \sigma)(c) = \tau(\sigma(c)) = \tau(c) = c$$

and

$$(\sigma \circ \tau)(c) = \sigma(\tau(c)) = \sigma(c) = c$$

Since $\sigma \circ \tau$ and $\tau \circ \sigma$ have the same output for every element of A, we conclude that $\sigma \circ \tau = \tau \circ \sigma$. □

4.6 Orders of Elements

Definition 4.6.1. *Let G be a group and let $a \in G$. For each $n \in \mathbb{N}^+$, we define*

$$a^n = aaa \cdots a,$$

where there are n total a's in the above product. If we want to be more formal, we define a^n recursively by letting $a^1 = a$ and $a^{n+1} = a^n a$ for all $n \in \mathbb{N}^+$. We also define

$$a^0 = e.$$

Finally, we extend the notation a^n for $n \in \mathbb{Z}$ as follows. If $n < 0$, we let

$$a^n = (a^{-1})^{|n|}.$$

In other words, if $n < 0$, we let

$$a^n = a^{-1}a^{-1}a^{-1} \cdots a^{-1},$$

where there are $|n|$ total (a^{-1})'s in the above product.

Let G be a group and let $a \in G$. Notice that

$$a^3a^2 = (aaa)(aa) = aaaaa = a^5,$$

and

$$(a^3)^2 = a^3a^3 = (aaa)(aaa) = aaaaaa = a^6.$$

For other examples, notice that

$$a^5a^{-2} = (aaaaa)(a^{-1}a^{-1}) = aaaaaa^{-1}a^{-1} = aaaaa^{-1} = aaa = a^3,$$

and

$$(a^4)^{-1} = (aaaa)^{-1} = a^{-1}a^{-1}a^{-1}a^{-1} = (a^{-1})^4 = a^{-4}.$$

In general, we have the following. A precise proof would involve induction using the formal recursive definition of a^n given above. However, just like the above discussion, these special cases explain where they come from and such a formal argument adds little enlightenment so will be omitted.

Proposition 4.6.2. *Let G be a group. Let $a \in G$ and let $m, n \in \mathbb{Z}$. We have*

1. $a^{m+n} = a^m a^n$.
2. $a^{mn} = (a^m)^n$.

In some particular groups, this notation is very confusing if used in practice. For example, when working in the group $(\mathbb{Z}, +, 0)$, we would have $2^4 = 2 + 2 + 2 + 2 = 8$ because the operation is addition rather than multiplication. However, with the standard operation of exponentiation on $\mathbb{Z}$ we have $2^4 = 16$. Make sure to understand what operation is in use whenever we use that notation a^n in a given group. It might be better to use a different notation if confusion can arise.

Definition 4.6.3. *Let G be a group and let $a \in G$. We define the* order *of a as follows. Let*

$$S = \{n \in \mathbb{N}^+ : a^n = e\}.$$

If $S \neq \emptyset$, we let $|a| = \min(S)$ (which exists by well-ordering), and if $S = \emptyset$, we define $|a| = \infty$. In other words, $|a|$ is the least positive n such that $a^n = e$, provided such an n exists.

The reason why we choose to overload the word *order* for two apparently very different concepts (when applied to a group versus when applied to an element of a group) will be explained in the next chapter on subgroups.

Example 4.6.4. *Here are some examples of computing orders of elements in a group.*

- *In any group G, we have $|e| = 1$.*
- *In the group $(\mathbb{Z}, +)$, we have $|0| = 1$ as noted, but $|n| = \infty$ for all $n \neq 0$.*
- *In the group $\mathbb{Z}/n\mathbb{Z}$, we have $|\overline{1}| = n$.*
- *In the group $\mathbb{Z}/12\mathbb{Z}$, we have $|\overline{9}| = 4$ because*

$$\overline{9}^2 = \overline{9} + \overline{9} = \overline{18} = \overline{6} \qquad \overline{9}^3 = \overline{9} + \overline{9} + \overline{9} = \overline{27} = \overline{3} \qquad \overline{9}^4 = \overline{9} + \overline{9} + \overline{9} + \overline{9} = \overline{36} = \overline{0}$$

- *In the group $U(\mathbb{Z}/7\mathbb{Z})$ we have $|\overline{4}| = 3$ because*

$$\overline{4}^2 = \overline{4} \cdot \overline{4} = \overline{16} = \overline{2} \qquad \overline{4}^3 = \overline{4} \cdot \overline{4} \cdot \overline{4} = \overline{64} = \overline{1}$$

The order of an element $a \in G$ is the *least* positive $m \in \mathbb{Z}$ with $a^m = e$. There may be many other larger positive powers of a that give the identity, or even negative powers that do. For example, consider $\overline{1} \in \mathbb{Z}/2\mathbb{Z}$. We have $|\overline{1}| = 2$, but $\overline{1}^4 = \overline{0}$, $\overline{1}^6 = \overline{0}$, and $\overline{1}^{-14} = \overline{0}$. In general, given the order of an element, we can characterize all powers of that element which give the identity as follows.

Proposition 4.6.5. *Let G be a group and let $a \in G$.*

1. *Suppose that $|a| = m \in \mathbb{N}^+$. For any $n \in \mathbb{Z}$, we have $a^n = e$ if and only if $m \mid n$.*
2. *Suppose that $|a| = \infty$. For any $n \in \mathbb{Z}$, we have $a^n = e$ if and only if $n = 0$.*

Proof. We first prove (1). Let $m = |a|$ and notice that $m > 0$. We then have in particular that $a^m = e$. Suppose first that $n \in \mathbb{Z}$ is such that $m \mid n$. Fix $k \in \mathbb{Z}$ with $n = mk$ We then have

$$\begin{aligned} a^n &= a^{mk} \\ &= (a^m)^k \\ &= e^k \\ &= e, \end{aligned}$$

so $a^n = e$. Suppose conversely that $n \in \mathbb{Z}$ and that $a^n = e$. Since $m > 0$, we may write $n = qm + r$ where $0 \leq r < m$. We then have

$$\begin{aligned} e &= a^n \\ &= a^{qm+r} \\ &= a^{qm}a^r \\ &= (a^m)^q a^r \\ &= e^q a^r \\ &= a^r. \end{aligned}$$

Now by definition we know that m is the least positive power of a which gives the identity. Therefore, since $0 \leq r < m$ and $a^r = e$, we must have that $r = 0$. It follows that $n = qm$ so $m \mid n$.

We now prove (2). Suppose that $|a| = \infty$. If $n = 0$, then we have $a^n = a^0 = e$. If $n > 0$, then we have $a^n \neq e$ because by definition no positive power of a equals the identity. Suppose then that $n < 0$ and that $a^n = e$. We then have

$$e = e^{-1} = (a^n)^{-1} = a^{-n}.$$

Now $-n > 0$ because $n < 0$, but this is a contradiction because no positive power of a gives the identity. It follows that if $n < 0$, then $a^n \neq e$. Therefore, $a^n = e$ if and only if $n = 0$. $\square$

Next, we work to understand the orders of elements in symmetric groups. Recall that elements of a symmetric group are *functions*, and the identity element is the identity function, which is the function that fixes each point in the set. Thus, if we are working in S_7 and are looking at the cycle $(2\ 7\ 5\ 4)$, then we are talking about a function that sends 2 to 7, sends 7 to 5, sends 5 to 4, sends 4 to 2, and fixes each of 1, 3, and 6.

Proposition 4.6.6. *Let A be a set and let $a_1, a_2, \dots, a_k \in A$ be distinct. Let $\sigma = (a_1\ a_2\ \cdots\ a_k) \in S_A$. We then have that $|\sigma| = k$. In other words, the order of a cycle is its length.*

Proof. Given any m with $1 \leq m < k$, we have $\sigma^m(a_1) = a_{m+1} \neq a_1$, so $\sigma^m \neq id$. It follows that $|\sigma| \geq k$. Now for each i with $1 \leq i \leq k$, we have $\sigma^k(a_i) = a_i$, so σ^k fixes each a_i. Since σ fixes all other elements of A, it follows that σ^k fixes all other elements of A. Therefore, $\sigma^k = id$, and we have shown that $|\sigma| = k$. $\square$

On the homework, you developed the basic theory of least common multiples. We now show how they come up when computing the order of elements in a symmetric group.

Proposition 4.6.7. *Let A be a set and let $\sigma \in S_A$. We then have that $|\sigma|$ is the least common multiple of the cycle lengths occurring in the cycle notation of σ.*

Proof. Suppose that $\sigma = \tau_1\tau_2 \cdots \tau_\ell$ where the τ_i are disjoint cycles. For each i, let $m_i = |\tau_i|$ and notice $|\tau_i| = m_i$ from Proposition 4.6.6. Since disjoint cycles commute by Proposition 4.5.4, for any $n \in \mathbb{N}^+$ we have

$$\sigma^n = \tau_1^n\tau_2^n \cdots \tau_\ell^n.$$

Now if $m_i \mid n$ for each i, then $\tau_i^n = id$ for each i by Proposition 4.6.5, so $\sigma^n = id$. Conversely, suppose that $n \in \mathbb{N}^+$ is such that there exists i with $m_i \nmid n$. We then have that $\tau_i^n \neq id$ by Proposition 4.6.5, so we may fix $a \in A$ with $\tau_i^n(a) \neq a$. Now both a and $\tau_i^n(a)$ are fixed by each τ_j with $j \neq i$ (because the cycles are disjoint). Therefore $\sigma^n(a) = \tau_i^n(a) \neq a$, and hence $\sigma^n \neq id$.

It follows that $\sigma^n = id$ if and only if $m_i \mid n$ for each i. Since $|\sigma|$ is the least $n \in \mathbb{N}^+$ with $\sigma^n = id$, it follows that $|\sigma|$ is the least $n \in \mathbb{N}^+$ satisfying $m_i \mid n$ for each i, which is to say that $|\sigma|$ is the least common multiple of the m_i. $\square$

Suppose now that we have an element a of a group G and we know its order. How do we compute the orders of the powers of a? For an example, consider $\overline{3} \in \mathbb{Z}/30\mathbb{Z}$. It is straightforward to check that $|\overline{3}| = 10$. Let's look at the orders of some powers of $\overline{3}$. Now $\overline{3}^2 = \overline{6}$ and a simple check shows that $|\overline{6}| = 5$ so $|\overline{3}^2| = 5$. Now consider $\overline{3}^3 = \overline{9}$. We have $\overline{9}^2 = \overline{18}$, then $\overline{9}^3 = \overline{27}$, and then $\overline{9}^4 = \overline{36} = \overline{6}$. Since 30 is not a multiple of 9 we see that we "cycle around" and it is not quite as clear when we will hit $\overline{0}$ as we continue. However, if we keep at it, we will find that $|\overline{3}^3| = 10$. If we keep calculating away, we will find that $|\overline{3}^4| = 5$ and $|\overline{3}^5| = 2$. We would like to have a better way to determine these values without resorting to tedious calculations, and that is what the next proposition supplies.

Proposition 4.6.8. *Let G be a group and let $a \in G$.*

1. *Suppose that $|a| = m \in \mathbb{N}^+$. For any $n \in \mathbb{Z}$, we have*
$$|a^n| = \frac{m}{\gcd(m, n)}.$$

2. *Suppose that $|a| = \infty$. We have $|a^n| = \infty$ for all $n \in \mathbb{Z}\backslash\{0\}$.*

Proof. We first prove (1). Fix $n \in \mathbb{Z}$ and let $d = \gcd(m, n)$. Since d is a common divisor of m and n, we may fix $s, t \in \mathbb{Z}$ with $m = ds$ and $n = dt$. Notice that $s > 0$ because both $m > 0$ and $d > 0$. With this notation, we need to show that $|a^n| = s$.

Notice that

$$\begin{aligned} (a^n)^s &= a^{ns} \\ &= a^{dts} \\ &= a^{mt} \\ &= (a^m)^t \\ &= e^t \\ &= e. \end{aligned}$$

Thus, s is a positive power of a^n which gives the identity, and so $|a^n| \leq s$.

Suppose now that $k \in \mathbb{N}^+$ with $(a^n)^k = e$. We need to show that $s \leq k$. We have $a^{nk} = e$, so by Proposition 4.6.5, we know that $m \mid nk$. Fix $\ell \in \mathbb{Z}$ with $m\ell = nk$. We then have that $ds\ell = dtk$, so canceling $d > 0$ we conclude that $s\ell = tk$, and hence $s \mid tk$. Now $\gcd(s,t) = 1$ (a good exercise), so using Proposition 2.4.12, we conclude that $s \mid k$. Since $s, k > 0$, it follows that $s \leq k$.

Therefore, s is the least positive value of k such that $(a^n)^k = e$, and so we conclude that $|a^n| = s$.

We now prove (2). Suppose that $n \in \mathbb{Z}\backslash\{0\}$. Let $k \in \mathbb{N}^+$. We then have $(a^n)^k = a^{nk}$. Now $nk \neq 0$ because $n \neq 0$ and $k > 0$, hence $(a^n)^k = a^{nk} \neq 0$ by the previous proposition. Therefore, $(a^n)^k \neq 0$ for all $k \in \mathbb{N}^+$ and hence $|a^n| = \infty$. □

Corollary 4.6.9. *Let $n \in \mathbb{N}^+$ and let $k \in \mathbb{Z}$. In the group $\mathbb{Z}/n\mathbb{Z}$, we have*

$$|\overline{k}| = \frac{n}{\gcd(k,n)}$$

Proof. Working in the group $\mathbb{Z}/n\mathbb{Z}$, we know that $|\overline{1}| = n$. Now $\overline{k} = \overline{1}^k$, so the result follows from the previous proposition. □

Given a group G, we can form the set $\{|a| : a \in G\}$. Now if every element of G has finite order, then this set is a nonempty subset of $\mathbb{N}^+$. What kinds of subsets of $\mathbb{N}^+$ can we obtain in this way? For example, if $G = \mathbb{Z}/10\mathbb{Z}$, this the corresponding set of orders of elements is $\{1, 2, 5, 10\}$, while if $G = S_3$, then the corresponding set of orders of elements is $\{1, 2, 3\}$. The next result shows that this set is closed downwards under divisibility, i.e. if m is in this set, then every positive divisor of m is in this set.

Proposition 4.6.10. *Let G be a group, and let $d, m \in \mathbb{N}^+$ with $d \mid m$. If G has an element of order m, then G has an element of order d.*

Proof. Suppose that G has an element of order m, and fix $a \in G$ with $|a| = m$. Since $d \mid m$, we can fix $k \in \mathbb{Z}$ with $kd = m$. Now we are assuming that $d, m \in \mathbb{N}^+$, so it follows that $k \in \mathbb{N}^+$ as well. Since $m = kd + 0$, Corollary 2.4.8 implies that $\gcd(m,k) = \gcd(k,0) = k$. Using Proposition 4.6.8, we have

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

Thus a^k is an element of G with order d. □

We'll have much more to say about the orders of elements in a group G in Chapter 5.

4.7 Direct Products

We give a construction for putting groups together.

Definition 4.7.1. *Suppose that $(G_i, \star_i)$ for $1 \leq i \leq n$ are all groups. Consider the Cartesian product of the sets $G_1, G_2, \dots, G_n$, i.e.*

$$G_1 \times G_2 \times \cdots \times G_n = \{(a_1, a_2, \dots, a_n) : a_i \in G_i \text{ for } 1 \leq i \leq n\}$$

Define an operation $\cdot$ on $G_1 \times G_2 \times \cdots \times G_n$ by letting

$$(a_1, a_2, \dots, a_n) \cdot (b_1, b_2, \dots, b_n) = (a_1 \star_1 b_1, a_2 \star_2 b_2, \dots, a_n \star_n b_n)$$

Then $(G_1 \times G_2 \times \cdots \times G_n, \cdot)$ is a group which is called the (external) direct product *of $G_1, G_2, \dots, G_n$.*

We first verify the claim that $(G_1 \times G_2 \times \cdots \times G_n, \cdot)$ is a group.

Proposition 4.7.2. *Suppose that $(G_i, \star_i)$ for $1 \leq i \leq n$ are all groups. The direct product defined above is a group with the following properties:*

- *The identity is $(e_1, e_2, \dots, e_n)$ where e_i is the unique identity of G_i.*
- *Given $a_i \in G_i$ for all i, we have*
$$(a_1, a_2, \dots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \dots, a_n^{-1}).$$
where a_i^{-1} is the inverse of a_i in the group G_i.
- $|G_1 \times G_2 \times \cdots \times G_n| = \prod_{i=1}^{n} |G_i|$, *i.e. the order of the direct product of the G_i is the product of the orders of the G_i.*

Proof. We first check that $\cdot$ is associative. Suppose that $a_i, b_i, c_i \in G_i$ for $1 \leq i \leq n$. We have

$$\begin{aligned}
((a_1, a_2, \dots, a_n) \cdot (b_1, b_2, \dots, b_n)) \cdot (c_1, c_2, \dots, c_n) &= (a_1 \star_1 b_1, a_2 \star_2 b_2, \dots, a_n \star_n b_n) \cdot (c_1, c_2, \dots, c_n) \\
&= ((a_1 \star_1 b_1) \star_1 c_1, (a_2 \star_2 b_2) \star_2 c_2, \dots, (a_n \star_n b_n) \star_n c_n) \\
&= (a_1 \star_1 (b_1 \star_1 c_1), a_2 \star_2 (b_2 \star_2 c_2), \dots, a_n \star_n (b_n \star_n c_n)) \\
&= (a_1, a_2, \dots, a_n) \cdot (b_1 \star_1 c_1, b_2 \star_2 c_2, \dots, b_n \star_n c_n) \\
&= (a_1, a_2, \dots, a_n) \cdot ((b_1, b_2, \dots, b_n) \cdot (c_1, c_2, \dots, c_n)).
\end{aligned}$$

Let e_i be the identity of G_i. We now check that $(e_1, e_2, \dots, e_n)$ is an identity of the direct product. Let $a_i \in G_i$ for all i. We have

$$\begin{aligned}
(a_1, a_2, \dots, a_n) \cdot (e_1, e_2, \dots, e_n) &= (a_1 \star_1 e_1, a_2 \star_2 e_2, \dots, a_n \star_n e_n) \\
&= (a_1, a_2, \dots, a_n)
\end{aligned}$$

and

$$\begin{aligned}
(e_1, e_2, \dots, e_n) \cdot (a_1, a_2, \dots, a_n) &= (e_1 \star_1 a_1, e_2 \star_2 a_2, \dots, e_n \star_n a_n) \\
&= (a_1, a_2, \dots, a_n)
\end{aligned}$$

hence $(e_1, e_2, \dots, e_n)$ is an identity for the direct product.

We finally check the claim about inverses inverses. Let $a_i \in G_i$ for $1 \leq i \leq n$. For each i, let a_i^{-1} be the inverse of a_i in G_i. We then have

$$\begin{aligned}
(a_1, a_2, \dots, a_n) \cdot (a_1^{-1}, a_2^{-1}, \dots, a_n^{-1}) &= (a_1 \star_1 a_1^{-1}, a_2 \star_2 a_2^{-1}, \dots, a_n \star_n a_n^{-1}) \\
&= (e_1, e_2, \dots, e_n)
\end{aligned}$$

and

$$\begin{aligned}
(a_1^{-1}, a_2^{-1}, \dots, a_n^{-1}) \cdot (a_1, a_2, \dots, a_n) &= (a_1^{-1} \star_1 a_1, a_2^{-1} \star_2 a_2, \dots, a_n^{-1} \star_n a_n) \\
&= (e_1, e_2, \dots, e_n)
\end{aligned}$$

hence $(a_1^{-1}, a_2^{-1}, \dots, a_n^{-1})$ is an inverse of $(a_1, a_2, \dots, a_n)$.

Finally, since there are $|G_1|$ elements to put in the first coordinate of the n-tuple, $|G_2|$ elements to put in the second coordinates, etc., it follows that

$$|G_1 \times G_2 \times \cdots \times G_n| = \prod_{i=1}^{n} |G_i|.$$

$\square$

For example, consider the group $G = S_3 \times \mathbb{Z}$ (where we are considering $\mathbb{Z}$ as a group under addition). Elements of G are ordered pairs (σ, n) where $\sigma \in S_3$ and $n \in \mathbb{Z}$. For example, $((1\ 2), 8)$, $(id, -6)$, and $((1\ 3\ 2), 42)$ are all elements of G. The group operation on G is obtained by working in each coordinate separately and performing the corresponding group operation there. For example, we have

$$((1\ 2), 8) \cdot ((1\ 3\ 2), 42) = ((1\ 2) \circ (1\ 3\ 2), 8 + 42) = ((1\ 3), 50).$$

Notice that the direct product puts two groups together in a manner that makes them completely ignore each other. Each coordinate goes about doing its business without interacting with the others at all.

Proposition 4.7.3. *The group $G_1 \times G_2 \times \cdots \times G_n$ is abelian if and only if each G_i is abelian.*

Proof. For each i, let $\star_i$ be the group of operation of G_i.

Suppose first that each G_i is abelian. Suppose that $a_i, b_i \in G_i$ for $1 \leq i \leq n$. We then have

$$\begin{aligned}(a_1, a_2, \dots, a_n) \cdot (b_1, b_2, \dots, b_n) &= (a_1 \star_1 b_1, a_2 \star_2 b_2, \dots, a_n \star_n b_n) \\ &= (b_1 \star_1 a_1, b_2 \star_2 a_2, \dots, b_n \star_n a_n) \\ &= (b_1, b_2, \dots, b_n) \cdot (a_1, a_2, \dots, a_n).\end{aligned}$$

Therefore, $G_1 \times G_2 \times \cdots \times G_n$ is abelian.

Suppose conversely that $G_1 \times G_2 \times \cdots \times G_n$ is abelian. Fix i with $1 \leq i \leq n$. Suppose that $a_i, b_i \in G_i$. Consider the elements $(e_1, \dots, e_{i-1}, a_i, e_i, \dots, e_n)$ and $(e_1, \dots, e_{i-1}, b_i, e_i, \dots, e_n)$ in $G_1 \times G_2 \times \cdots \times G_n$. Using the fact that the direction product is abelian, we see that

$$\begin{aligned}&(e_1, \dots, e_{i-1}, a_i \star_i b_i, e_{i+1}, \dots, e_n) \\ &\qquad = (e_1 \star_1 e_1, \dots, e_{i-1} \star_{i-1} e_{i-1}, a_i \star_i b_i, e_{i+1} \star_{i+1} e_{i+1}, \dots, e_n \star_n e_n) \\ &\qquad = (e_1, \dots, e_{i-1}, a_i, e_{i+1}, \dots, e_n) \cdot (e_1, \dots, e_{i-1}, b_i, e_{i+1}, \dots, e_n) \\ &\qquad = (e_1, \dots, e_{i-1}, b_i, e_{i+1}, \dots, e_n) \cdot (e_1, \dots, e_{i-1}, a_i, e_{i+1}, \dots, e_n) \\ &\qquad = (e_1 \star_1 e_1, \dots, e_{i-1} \star_{i-1} e_{i-1}, b_i \star_i a_i, e_{i+1} \star_{i+1} e_{i+1}, \dots, e_n \star_n e_n) \\ &\qquad = (e_1, \dots, e_{i-1}, b_i \star_i a_i, e_{i+1}, \dots, e_n).\end{aligned}$$

Comparing the i^{th} coordinates of the first and last tuple, we conclude that $a_i \star_i b_i = b_i \star_i a_i$. Therefore, G_i is abelian. $\square$

We can build all sorts of groups with this construction. For example $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is an abelian group of order 4 with elements

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}$$

In this group, the element $(\overline{0}, \overline{0})$ is the identity and all other elements have order 2. We can also use this construction to build nonabelian groups of various orders. For example $S_3 \times \mathbb{Z}/2\mathbb{Z}$ is a nonabelian group of order 12.

Proposition 4.7.4. *Let $G_1, G_2, \dots, G_n$ be groups. Let $a_i \in G_i$ for $1 \leq i \leq n$. The order of the element $(a_1, a_2, \dots, a_n) \in G_1 \times G_2 \times \cdots \times G_n$ is the least common multiple of the orders of the a_i's in G_i.*

Proof. For each i, let $m_i = |a_i|$, so m_i is the order of a_i in the group G_i. Now since the group operation in the direct product works in each coordinate separately, a simple induction shows that

$$(a_1, a_2, \dots, a_n)^k = (a_1^k, a_2^k, \dots, a_n^k)$$

for all $k \in \mathbb{N}^+$. Now if $m_i \mid k$ for each i, then $a_i^k = e_i$ for each i, so

$$(a_1, a_2, \dots, a_n)^k = (a_1^k, a_2^k, \dots, a_n^k) = (e_1, e_2, \dots, e_n)$$

Conversely, suppose that $k \in \mathbb{N}^+$ is such that there exists i with $m_i \nmid k$. For such an i, we then have that $a_i^k \neq e_i$ by Proposition 4.6.5, so

$$(a_1, a_2, \ldots, a_n)^k = (a_1^k, a_2^k, \ldots, a_n^k) \neq (e_1, e_2, \ldots, e_n)$$

It follows that $(a_1, a_2, \ldots, a_n)^k = (e_1, e_2, \ldots, e_n)$ if and only if $m_i \mid k$ for all i. Since $|(a_1, a_2, \ldots, a_n)|$ is the least $k \in \mathbb{N}^+$ with $(a_1, a_2, \ldots, a_n)^k = (e_1, e_2, \ldots, e_n)$, it follows that $|(a_1, a_2, \ldots, a_n)|$ is the least $k \in \mathbb{N}^+$ satisfying $m_i \mid k$ for all i, which is to say that $|(a_1, a_2, \ldots, a_n)|$ is the least common multiple of the m_i. $\square$

For example, suppose that we are working in the group $S_4 \times \mathbb{Z}/42\mathbb{Z}$ and we consider the element $((1\ 4\ 2\ 3), \overline{7})$. Since $|(1\ 4\ 2\ 3)| = 4$ in S_4 and $|\overline{7}| = 6$ in $\mathbb{Z}/42\mathbb{Z}$, it follows that the order of $((1\ 4\ 2\ 3), \overline{7})$ in $S_4 \times \mathbb{Z}/42\mathbb{Z}$ equals $\text{lcm}(4, 6) = 12$.

For another example, the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is an abelian group of order 8 in which every nonidentity element has order 2. Generalizing this construction by taking n copies of $\mathbb{Z}/2\mathbb{Z}$, we see how to construct an abelian group of order 2^n in which every nonidentity element has order 2.

Chapter 5

Subgroups and Cosets

5.1 Subgroups

If we have a group, we can consider subsets of G which also happen to be a group under the same operation. If we take a subset of a group and restrict the group operation to that subset, we trivially have the operation is associative on H because it is associative on G. The only issues are whether the operation remains a binary operation on H (it could conceivably combine two elements of H and return an element not in H), whether the identity is there, and whether the inverse of every element of H is also in H. This gives the following definition.

Definition 5.1.1. *Let G be a group and let $H \subseteq G$. We say that H is a* subgroup *of G if*

1. *$e \in H$ (H contains the identity of G).*
2. *$ab \in H$ whenever $a \in H$ and $b \in H$ (H is closed under the group operation).*
3. *$a^{-1} \in H$ whenever $a \in H$ (H is closed under inverses).*

Example 5.1.2. *Here are some examples of subgroups.*

- *For any group G, we always have two trivial examples of subgroups. Namely G is always a subgroup of itself, and $\{e\}$ is always a subgroup of G.*
- *$\mathbb{Z}$ is a subgroup of $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$. This follows because $0 \in \mathbb{Z}$, the sum of two integers is an integer, and the additive inverse of an integer is an integer.*
- *The set $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$. This follows from the fact that $0 = 2 \cdot 0 \in 2\mathbb{Z}$, that $2m + 2n = 2(m + n)$ so the sum of two evens is even, and that $-(2n) = 2(-n)$ so the the additive inverse of an even number is even.*
- *The set $H = \{\overline{0}, \overline{3}\}$ is a subgroup of $\mathbb{Z}/6\mathbb{Z}$. To check that H is a subgroup, we need to check the three conditions. We have $\overline{0} \in H$, so H contains the identity. Also $\overline{0}^{-1} = \overline{0} \in H$ and $\overline{3}^{-1} = \overline{3} \in H$, so the inverse of each element of H lies in H. Finally, to check that H is closed under the group operation, we simply have to check the four possibilities. For example, we have $\overline{3} + \overline{3} = \overline{6} = \overline{0} \in H$. The other 3 possible sums are even easier.*

Example 5.1.3. *Let $G = (\mathbb{Z}, +)$. Here are some examples of subsets of $\mathbb{Z}$ which are* **not** *subgroups of G.*

- *The set $H = \{2n + 1 : n \in \mathbb{Z}\}$ is not a subgroup of G because $0 \notin H$.*

- *The set* $H = \{0\} \cup \{2n+1 : n \in \mathbb{Z}\}$ *is not a subgroup of* G *because even though it contains* 0 *and is closed under inverses, it is not closed under the group operation. For example,* $1 \in H$ *and* $3 \in H$*, but* $1 + 3 \notin H$*.*

- *The set* $\mathbb{N}$ *is not a subgroup of* G *because even though it contains* 0 *and is closed under the group operation, it is not closed under inverses. For example,* $1 \in H$ *but* $-1 \notin H$

Now it is possible that a subset of a group G forms a group under a completely different binary operation that the one used in G, but whenever we talk about a subgroup H of G we only think of restricting the group operation of G down to H. For example, let $G = (\mathbb{Q}, +)$. The set $H = \mathbb{Q}\backslash\{0\}$ is *not* a subgroup of G (since it does not contain the identity) even though H can be made into a group with the completely different operation of multiplication. When we consider a subset H of a group G, we only call it a subgroup of G if it is a group with respect to the exact same binary operation.

Proposition 5.1.4. *Let* $n \in \mathbb{N}^+$*. The set* $H = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\}$ *is a subgroup of* $GL_n(\mathbb{R})$*.*

Proof. Letting I_n be the $n \times n$ identity matrix (which is the identity of $GL_n(\mathbb{R})$), we have that $\det(I_n) = 1$ so $I_n \in H$. Suppose that $M, N \in H$ so $\det(M) = 1 = \det(N)$. We then have

$$\det(MN) = \det(M) \cdot \det(N) = 1 \cdot 1 = 1$$

so $MN \in H$. Suppose finally that $M \in H$. We have $MM^{-1} = I_n$, so $\det(MM^{-1}) = \det(I_n) = 1$, hence $\det(M) \cdot \det(M^{-1}) = 1$. Since $M \in H$ we have $\det(M) = 1$, hence $\det(M^{-1}) = 1$. It follows that $M^{-1} \in H$. We have checked the three properties of a subgroup, so H is a subgroup of G. □

Definition 5.1.5. *Let* $n \in \mathbb{N}^+$*. We let* $SL_n(\mathbb{R})$ *be the above subgroup of* $GL_n(\mathbb{R})$*. That is,*

$$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\}$$

The group $SL_n(\mathbb{R})$ *is called the* special linear group *of degree* n*.*

The following proposition occasionally makes the process of checking whether a subset of a group is indeed a subgroup a bit easier.

Proposition 5.1.6. *Let* G *be a group and let* $H \subseteq G$*. The following are equivalent:*

- H *is a subgroup of* G
- $H \neq \emptyset$ *and* $ab^{-1} \in H$ *whenever* $a, b \in H$*.*

Proof. Suppose first that H is a subgroup of G. By definition, we must have $e \in H$, so $H \neq \emptyset$. Suppose that $a, b \in H$. Since H is a subgroup and $b \in H$, we must have $b^{-1} \in H$. Now using the fact that $a \in H$ and $b^{-1} \in H$, together with the second part of the definition of a subgroup, it follows that $ab^{-1} \in H$.

Now suppose conversely that $H \neq \emptyset$ and $ab^{-1} \in H$ whenever $a, b \in H$. We need to check the three defining characteristics of a subgroup. Since $H \neq \emptyset$, we may fix $c \in H$. Using our condition and the fact that $c \in H$, it follows that $e = cc^{-1} \in H$, so we have checked the first property. Now using the fact that $e \in H$, given any $a \in H$ we have $a^{-1} = ea^{-1} \in H$ by our condition, so we have checked the third property. Suppose now that $a, b \in H$. From what we just showed, we know that $b^{-1} \in H$. Therefore, using our condition, we conclude that $ab = a(b^{-1})^{-1} \in H$, so we have verified the second property. We have shown that all 3 properties hold for H, so H is a subgroup of G. □

We end with an important fact.

Proposition 5.1.7. *Let* G *be a group. If* H *and* K *are both subgroups of* G*, then* $H \cap K$ *is a subgroup of* G*.*

Proof. We check the three properties for the subset $H \cap K$:

- First notice that since both H and K are subgroups of G, we have that $e \in H$ and $e \in K$. Therefore, $e \in H \cap K$.
- Suppose that $a, b \in H \cap K$. We then have that both $a \in H$ and $b \in H$, so $ab \in H$ because H is a subgroup of G. We also have that both $a \in K$ and $b \in K$, so $ab \in K$ because K is a subgroup of G. Therefore, $ab \in H \cap K$. Since $a, b \in H \cap K$ were arbitrary, it follows that $H \cap K$ is closed under the group operation.
- Suppose that $a \in H \cap K$. We then have that $a \in H$, so $a^{-1} \in H$ because H is a subgroup of G. We also have that $a \in K$, so $a^{-1} \in K$ because K is a subgroup of G. Therefore, $a^{-1} \in H \cap K$. Since $a \in H \cap K$ was arbitrary, it follows that $H \cap K$ is closed under inverses.

Therefore, $H \cap K$ is a subgroup of G. □

5.2 Generating Subgroups

Let G be a group and let $c \in G$. Suppose that we want to form the smallest subgroup of G containing the element c. If H is any such subgroup, then we certainly need to have $c^2 = c \cdot c \in H$. Since we must have $c^2 \in H$, it then follows that $c^3 = c^2 \cdot c \in H$. In this way, we see that $c^n \in H$ for any $n \in \mathbb{N}^+$. Now we also need to have $e \in H$, and since $e = c^0$, we conclude that $c^n \in H$ for all $n \in \mathbb{N}$. Furthermore, H needs to be closed under inverses, so $c^{-1} \in H$ and in fact $c^{-n} = (c^n)^{-1} \in H$ for all $n \in \mathbb{N}^+$. Putting it all together, we see that $c^n \in H$ for all $n \in \mathbb{Z}$.

Definition 5.2.1. *Let G be a group and let $c \in G$. We define*

$$\langle c \rangle = \{c^n : n \in \mathbb{Z}\}.$$

The set $\langle c \rangle$ is called the subgroup of G generated by c.

The next proposition explains our choice of definition for $\langle c \rangle$. Namely, the set $\langle c \rangle$ is the smallest subgroup of G containing c as an element.

Proposition 5.2.2. *Let G be a group and let $c \in G$. Let $H = \langle c \rangle = \{c^n : n \in \mathbb{Z}\}$.*

1. *H is a subgroup of G with $c \in H$.*
2. *If K is a subgroup of G with $c \in K$, then $H \subseteq K$.*

Proof. We first prove (1). We check that three properties.

- Notice that $e = c^0 \in H$.
- Suppose that $a, b \in H$. Fix $m, n \in \mathbb{Z}$ with $a = c^m$ and $b = c^n$. We then have

  $$ab = c^m c^n = c^{m+n}$$

  so $ab \in H$ because $m + n \in \mathbb{Z}$.
- Suppose that $a \in H$. Fix $m \in \mathbb{Z}$ with $a = c^m$. We then have

  $$a^{-1} = (c^m)^{-1} = c^{-m}$$

  so $a^{-1} \in H$ because $-m \in \mathbb{Z}$.

Therefore, H is a subgroup of G.

We now prove (2). Suppose that K is a subgroup of G with $c \in K$. We first prove by induction on $n \in \mathbb{N}^+$ that $c^n \in K$. We clearly have $c^1 = c \in K$ by assumption. Suppose that $n \in \mathbb{N}^+$ and we know that $c^n \in K$. Since $c^n \in K$ and $c \in K$, and K is a subgroup of G, it follows that $c^{n+1} = c^n c \in K$. Therefore, by induction, we know that $c^n \in K$ for all $n \in \mathbb{N}^+$. Now $c^0 = e \in K$ because K is a subgroup of G, so $c^n \in K$ for all $n \in \mathbb{N}$. Finally, if $n \in \mathbb{Z}$ with $n < 0$, then $c^{-n} \in K$ because $-n \in \mathbb{N}^+$ and hence $c^n = (c^{-n})^{-1} \in K$ because inverses of elements of K must be in K. Therefore, $c^n \in K$ for all $n \in \mathbb{Z}$, which is to say that $H \subseteq K$. $\square$

For example, suppose that we are working with the group $G = \mathbb{Z}$ under addition. Since the group operation is addition, given $c, n \in \mathbb{Z}$, we have that c^n (under the general group theory definition) equals nc (under the usual definition of multiplication). Therefore,

$$\langle c \rangle = \{nc : n \in \mathbb{Z}\},$$

so $\langle c \rangle$ is the set of all multiples of c.

For another example, let $G = \mathbb{Z}/5\mathbb{Z}$ and consider $H = \langle \overline{3} \rangle$. We certainly must have $\overline{0} = \overline{3}^0 \in H$ and also $\overline{3} \in H$. Notice then that $\overline{3} + \overline{3} = \overline{6} = \overline{1} \in H$. From here, we conclude that $\overline{1} + \overline{3} = \overline{4} \in H$ (this is $\overline{3}^3$ in group theory notation), and from this we conclude that $\overline{4} + \overline{3} = \overline{7} = \overline{2} \in H$. Putting it all together, it follows that $\{\overline{0}, \overline{3}, \overline{1}, \overline{4}, \overline{2}\} \subseteq H$ and hence $H = \mathbb{Z}/5\mathbb{Z}$. Notice that we were able to stop once we computed $\overline{3}^n$ for n with $0 \leq n \leq 4$ because we've exhausted all of H. Now if we add $\overline{3}$ again we end up with $\overline{2} + \overline{3} = \overline{0}$, so we've come back around to the identity. If we continue, we see that we will cycle through these values repeatedly.

This next proposition explains this "cycling" phenomenon more fully, and also finally justifies our overloading of the word *order*. Given a group G and an element $c \in G$, it says that $|c|$ (the order of c as an element of G) equals $|\langle c \rangle|$ (the number of elements in the subgroup of G generated by c).

Proposition 5.2.3. *Suppose that G is a group and that $c \in G$. Let $H = \langle c \rangle$.*

1. *Suppose that $|c| = m \in \mathbb{N}^+$. We then have that $H = \{c^i : 0 \leq i < m\} = \{e, c, c^2, \ldots, c^{m-1}\}$ and $c^k \neq c^\ell$ whenever $0 \leq k < \ell < m$. Thus, $|H| = m$.*

2. *Suppose that $|c| = \infty$. We then have that $c^k \neq c^\ell$ whenever $k, \ell \in \mathbb{Z}$ with $k < \ell$, so $|H| = \infty$*

In particular, we have $|c| = |\langle c \rangle|$.

Proof. We first prove (1). By definition we have $H = \{c^n : n \in \mathbb{Z}\}$, so we trivially have that

$$\{c^i : 0 \leq i < m\} \subseteq H.$$

Now let $n \in \mathbb{Z}$. Write $n = qm + r$ where $0 \leq r < m$. We then have

$$c^n = c^{qm+r} = (c^m)^q c^r = e^1 c^r = c^r$$

so $c^n = c^r \in \{c^i : 0 \leq i < m\}$. Therefore, $H \subseteq \{c^i : 0 \leq i < m\}$ and combining this with the reverse inclusion above we conclude that $H = \{c^i : 0 \leq i < m\}$.

Suppose now that $0 \leq k < \ell < m$. Assume for the sake of obtaining a contradiction that $c^k = c^\ell$. Multiplying both sides by c^{-k} on the right, we see that $c^k c^{-k} = c^\ell c^{-k}$, hence

$$e = c^0 = c^{k-k} = c^k c^{-k} = c^\ell c^{-k} = c^{\ell-k}$$

Now we have $0 \leq k < \ell < m$, so $0 < \ell - k < m$. This contradicts the assumption that $m = |c|$ is the least positive power of c giving the identity. Hence, we must have $c^k \neq c^\ell$.

We now prove (2). Suppose that $k, \ell \in \mathbb{Z}$ with $k < \ell$. Assume that $c^k = c^\ell$. As in part 1 we can multiply both sides on the right by c^{-k} to conclude that $c^{\ell-k} = e$. Now $\ell - k > 0$, so this contradicts the assumption that $|c| = \infty$. Therefore, we must have $c^k \neq c^\ell$. $\square$

Corollary 5.2.4. *If G is a finite group, then every element of G has finite order. Moreover, for each $a \in G$, we have $|a| \leq |G|$.*

Proof. Let $a \in G$. We then have that $\langle a \rangle \subseteq G$, so $|\langle a \rangle| \leq |G|$. Since $|a| = |\langle a \rangle|$ by Proposition 5.2.3, we conclude that that $|a| \leq |G|$. $\square$

In fact, much more is true. We will see as a consequence of Lagrange's Theorem that the order of every element of a finite group G is actually a divisor of $|G|$.

Definition 5.2.5. *A group G is* cyclic *if there exists $c \in G$ such that $G = \langle c \rangle$. An element $c \in G$ with $G = \langle c \rangle$ is called a* generator *of G.*

For example, for each $n \in \mathbb{N}^+$, the group $\mathbb{Z}/n\mathbb{Z}$ is cyclic because $\overline{1}$ is a generator (since $\overline{1}^k = \overline{k}$ for all k). Also, $\mathbb{Z}$ is cyclic because 1 is a generator (remember than $\langle c \rangle$ is the set of all powers of c, both positive and negative). In general, a cyclic group has many generators. For example, -1 is a generator of $\mathbb{Z}$, and $\overline{3}$ is a generator of $\mathbb{Z}/5\mathbb{Z}$ as we saw above.

Proposition 5.2.6. *Let G be a finite group with $|G| = n$. An element $c \in G$ is a generator of G if and only if $|c| = n$. In particular, G is cyclic if and only if it has an element of order n.*

Proof. Suppose first that c is a generator of G so that $G = \langle c \rangle$. We know from above that $|c| = |\langle c \rangle|$, so $|c| = |G| = n$. Suppose conversely that $|c| = n$. We then know that $|\langle c \rangle| = n$. Since $\langle c \rangle \subseteq G$ and each has n elements, we must have that $G = \langle c \rangle$. $\square$

For an example of a noncyclic group, consider S_3. The order of each element of S_3 is either 1, 2, or 3, so S_3 has no element of order 6. Thus, S_3 has no generators, and so S_3 is not cyclic. We could also conclude that S_3 is not cyclic by using the following result.

Proposition 5.2.7. *All cyclic groups are abelian.*

Proof. Suppose that G is a cyclic group and fix $c \in G$ with $G = \langle c \rangle$. Let $a, b \in G$. Since $G = \langle c \rangle$, we may fix $m, n \in \mathbb{Z}$ with $a = c^m$ and $b = c^n$. We then have

$$\begin{aligned} ab &= c^m c^n \\ &= c^{m+n} \\ &= c^{n+m} \\ &= c^n c^m \\ &= ba. \end{aligned}$$

Therefore, $ab = ba$ for all $a, b \in G$, so G is abelian. $\square$

The converse of the preceding proposition is false. In other words, there exist abelian groups which are not cyclic. For example, consider the group $U(\mathbb{Z}/8\mathbb{Z})$. We have $U(\mathbb{Z}/8\mathbb{Z}) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$, so $|U(\mathbb{Z}/8\mathbb{Z})| = 4$, but every nonidentity element has order 2 (as can be seen by examining the Cayley table at the end of Section 4.4). Alternatively, the abelian group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has order 4 but every nonidentity element has order 2. For an infinite example, the infinite abelian group $(\mathbb{Q}, +)$ is also not cyclic: We clearly have $\langle 0 \rangle \neq \mathbb{Q}$, and if $q \neq 0$, then $\frac{q}{2} \notin \{nq : n \in \mathbb{Z}\} = \langle q \rangle$.

Suppose that G is a group. We have seen how to take an element $c \in G$ and form the smallest subgroup of G containing c by simply taking the set $\{c^n : n \in \mathbb{Z}\}$. Suppose now that we have many elements of G and we want to form the smallest subgroup of G which contains them. For definiteness now, suppose that we have $c, d \in G$. How would we construct the smallest possible subgroup of G containing both c and d, which we denote by $\langle c, d \rangle$? A natural guess would be

$$\{c^m d^n : m, n \in \mathbb{Z}\},$$

but unless G is abelian there is no reason to think that this set is closed under multiplication. For example, we must have $cdc \in \langle c, d\rangle$, but it doesn't obviously appear there. Whatever $\langle c, d\rangle$ is, it must contain the following elements:

$$cdcdcdc \qquad c^{-1}dc^{-1}d^{-1}c \qquad c^3d^6c^{-2}d^7.$$

If we generate with 3 elements (instead of two), it gets even more complicated because we can alternate the 3 elements in such sequences without such a repetitive pattern. If we have infinitely many elements, it gets even worse. Since the explicit descriptions of the subgroups they generate are messy, we define the subgroup generated by an arbitrary set in a much less explicit manner. The key idea comes from Proposition 5.2.2, which says that $\langle c\rangle$ is the "smallest" subgroup of G containing c as an element. Here, "smallest" does not mean the least number of elements, but instead means the subgroup that is a subset of all other subgroups containing the elements in question.

Proposition 5.2.8. *Let G be a group and let $A \subseteq G$. There exists a subgroup H of G with the following properties:*

- *$A \subseteq H$.*
- *Whenever K is a subgroup of G with the property that $A \subseteq K$, we have $H \subseteq K$.*

Furthermore, the subgroup H is unique (i.e. if both H_1 and H_2 have the above properties, then $H_1 = H_2$).

Proof. The idea is to intersect all of the subgroups of G that contain A, and argue that the result is a subgroup. Since there might be infinitely many such subgroups, we can not simply appeal to Proposition 5.1.7. However, our argument is very similar.

We first prove existence. Notice that there is at least one subgroup of G containing A, namely G itself. Define

$$H = \{a \in G : a \in K \text{ for all subgroups } K \text{ of } G \text{ such that } A \subseteq K\}$$

Notice we certainly have $A \subseteq H$ by definition. Moreover, if K is a subgroup of G with the property that $A \subseteq K$, then we have $H \subseteq K$ by definition of H. We now show that H is indeed a subgroup of G.

- Since $e \in K$ for every subgroup K of G with $A \subseteq K$, we have $e \in H$.
- Let $a, b \in H$. For any subgroup K of G such that $A \subseteq K$, we must have both $a, b \in K$ by definition of H, hence $ab \in K$ because K is a subgroup. Since this is true for all such K, we conclude that $ab \in H$ by definition of H.
- Let $a \in H$. For any subgroup K of G such that $A \subseteq K$, we must have both $a \in K$ by definition of H, hence $a^{-1} \in K$ because K is a subgroup. Since this is true for all such K, we conclude that $a^{-1} \in H$ by definition of H.

Combining these three, we conclude that H is a subgroup of G. This finishes the proof of existence.

Finally, suppose that H_1 and H_2 both have the above properties. Since H_2 is a subgroup of G with $A \subseteq H_2$, we know that $H_1 \subseteq H_2$. Similarly, since H_1 is a subgroup of G with $A \subseteq H_1$, we know that $H_2 \subseteq H_1$. Therefore, $H_1 = H_2$. □

Definition 5.2.9. *Let G be a group and let $A \subseteq G$. We define $\langle A\rangle$ to be the unique subgroup H of G given by Proposition 5.2.8. If $A = \{a_1, a_2, \dots, a_n\}$, we write $\langle a_1, a_2, \dots, a_n\rangle$ rather than $\langle \{a_1, a_2, \dots, a_n\}\rangle$.*

For example, consider the group $G = S_3$, and let $H = \langle (1\ 2), (1\ 2\ 3)\rangle$. We know that H is a subgroup of G, so $id \in H$. Furthermore, we must have $(1\ 3\ 2) = (1\ 2\ 3)(1\ 2\ 3) \in H$. We also must have

$$(1\ 3) = (1\ 2\ 3)(1\ 2) \in H$$

and

$$(2\ 3) = (1\ 2)(1\ 2\ 3) \in H.$$

Therefore, $H = S_3$, i.e. $\langle (1\ 2), (1\ 2\ 3)\rangle = S_3$.

On the other hand, working in S_3, we have $\langle (1\ 2\ 3), (1\ 3\ 2)\rangle = \{id, (1\ 2\ 3), (1\ 3\ 2)\}$. This follows from the fact that $\{id, (1\ 2\ 3), (1\ 3\ 2)\}$ is a subgroup (which one can check directly, or by simply noticing that it equals $\langle (1\ 2\ 3)\rangle$), containing the given set.

Definition 5.2.10. *Let A be a set. A* transposition *is an element of S_A whose cycle notation equals $(a\ b)$ with $a \neq b$. In other words, a transposition is a bijection which flips two elements of A and leaves all other elements of A fixed.*

Proposition 5.2.11. *Let $n \in \mathbb{N}^+$. Every element of S_n can be written as a product of transpositions. Thus, if $T \subseteq S_n$ is the set of all transpositions, then $\langle T\rangle = S_n$.*

Proof. We've seen that every permutation can we written as a product of disjoint cycles, so it suffices to show that every cycle can be written as a product of transpositions. If $a_1, a_2, \dots, a_k \in \{1, 2, \dots, n\}$ are distinct, we have

$$(a_1\ a_2\ a_3\ \cdots\ a_{k-1}\ a_k) = (a_1\ a_k)(a_1\ a_{k-1})\cdots(a_1\ a_3)(a_1\ a_2).$$

The result follows. $\square$

To illustrate the above construction in a special case, we have

$$(1\ 7\ 2\ 5)(3\ 9)(4\ 8\ 6) = (1\ 5)(1\ 2)(1\ 7)(3\ 9)(4\ 6)(4\ 8).$$

5.3 The Alternating Groups

At the end of the previous section, we showed that every element of S_n can be written as a product of transpositions, and in fact we showed explicitly how to construct this product from a description of an element of S_n as a product of cycles. However, this decomposition is far from unique and in fact it is even possible the change the number of transpositions. For example, following our description, we have

$$(1\ 2\ 3) = (1\ 3)(1\ 2).$$

However, we can also write

$$(1\ 2\ 3) = (1\ 3)(2\ 3)(1\ 2)(1\ 3).$$

Although we can change the number and order of transpositions, it is a somewhat surprising fact that we can not change the parity of the number of transpositions. That is, it is impossible to find a $\sigma \in S_n$ which we can write simultaneously as a product of an even number of transpositions and also as a product of an odd number of transpositions. To build up to this important fact, we introduce a new and interesting concept.

Definition 5.3.1. *Let $\sigma \in S_n$. An* inversion *of σ is an ordered pair (i, j) with $i < j$ but $\sigma(i) > \sigma(j)$. We let $Inv(\sigma)$ be the set of all inversions of σ.*

For example, let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 4 & 6 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 2 & 4 & 6 \end{pmatrix} \qquad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 5 & 1 & 6 \end{pmatrix}$$

In cycle notation, these are

$$\sigma = (1\ 3\ 2)(4\ 5)(6) \qquad \tau = (1\ 3\ 5\ 4\ 2)(6) \qquad \pi = (1\ 3\ 2\ 4\ 5)(6)$$

Although it's not immediately obvious, notice that τ and π are obtained by swapping just two elements in the bottom row of σ. More formally, they are obtained by composing with a transposition first, and we have $\sigma = \tau \circ (3\ 4)$ and $\sigma = \pi \circ (2\ 5)$. We now examine the inversions in each of these permutations. Notice that it is typically easier to determine these in first representations rather than in cycle notation:

$$\begin{aligned}
Inv(\sigma) &= \{(1,2),(1,3),(4,5)\} \\
Inv(\tau) &= \{(1,2),(1,4),(3,4),(3,5)\} \\
Inv(\pi) &= \{(1,3),(1,5),(2,3),(2,5),(3,5),(4,5)\}
\end{aligned}$$

From this example, it may seem puzzling to see how the inversions are related. However, there is something quite interesting that is happening. Let's examine the relationship between $Inv(\sigma)$ and $Inv(\tau)$. By swapping the third and fourth positions in the second row, the inversion $(1,3)$ in σ became the inversion $(1,4)$ in τ, and the inversion $(4,5)$ in σ became the inversion $(3,5)$ in τ, so those match up. However, we added a new inversion by this swap, because although originally we had $\sigma(3) < \sigma(4)$, the swapping made $\tau(3) > \tau(4)$. This accounts for the one additional inversion in τ. If instead we had $\sigma(3) > \sigma(4)$, then this swap would have lost an inversion. However, in either case, this example illustrates that a swapping of two adjacent numbers either increases or decreases the number of inversions by 1.

Lemma 5.3.2. *Suppose $\sigma \in S_n$. If μ is a transposition consisting of two adjacent numbers, say $\mu = (k\ k{+}1)$, then $|Inv(\sigma)|$ and $|Inv(\sigma \circ \mu)|$ differ by* 1.

Proof. Notice that if $i, j \notin \{k, k+1\}$, then

$$(i,j) \in Inv(\sigma) \Longleftrightarrow (i,j) \in Inv(\sigma \circ \mu)$$

because μ fixes both i and j. Now since $\mu(k) = k+1$, $\mu(k+1) = k$, and μ fixes all other numbers, given any i with $i < k$, we have each of the following:

$$\begin{aligned}
(i,k) \in Inv(\sigma) &\Longleftrightarrow (i,k+1) \in Inv(\sigma \circ \mu) \\
(i,k+1) \in Inv(\sigma) &\Longleftrightarrow (i,k) \in Inv(\sigma \circ \mu).
\end{aligned}$$

Similarly, given any j with $j > k+1$, we have each of the following:

$$\begin{aligned}
(k,j) \in Inv(\sigma) &\Longleftrightarrow (k+1,j) \in Inv(\sigma \circ \mu) \\
(k+1,j) \in Inv(\sigma) &\Longleftrightarrow (k,j) \in Inv(\sigma \circ \mu).
\end{aligned}$$

The final thing to notice is that

$$(k,k+1) \in Inv(\sigma) \Longleftrightarrow (k,k+1) \notin Inv(\sigma \circ \mu),$$

because if $\sigma(k) > \sigma(k{+}1)$ then $(\sigma{\circ}\mu)(k) < (\sigma{\circ}\mu)(k{+}1)$, while if $\sigma(k) < \sigma(k{+}1)$ then $(\sigma{\circ}\mu)(k) > (\sigma{\circ}\mu)(k{+}1)$. Since we have a bijection between $Inv(\sigma) \backslash \{(k,k+1)\}$ and $Inv(\sigma \circ \mu) \backslash \{(k,k+1)\}$, while $(k,k+1)$ is in exactly one of the sets $Inv(\sigma)$ and $Inv(\sigma \circ \mu)$, it follows that $|Inv(\sigma)|$ and $|Inv(\sigma \circ \mu)|$ differ by 1. $\square$

A similar analysis is more difficult to perform on π because the swapping involved two non-adjacent numbers. As a result, elements in the middle had slightly more complicated interactions, and the above example shows that a swap of this type can sizably increase the number of inversions. Although it is possible to handle it directly, the key idea is to realize we can perform this swap through a sequence of adjacent swaps. This leads to the following result.

Corollary 5.3.3. *Suppose $\sigma \in S_n$. If μ is a transposition, then $|Inv(\sigma)| \not\equiv |Inv(\sigma \circ \mu)| \pmod 2$, i.e. the parity of the number of inversions of σ does not equal the parity of the number of inversions of $\sigma \circ \mu$.*

Proof. Let μ be a transposition, and write $\mu = (k\ \ell)$ where $k < \ell$. The key fact is that we can write $(k\ \ell)$ as a composition of $2(\ell - k) - 1$ many adjacent transposition in succession. In other words, we have

$$(k\ \ell) = (k\ k+1) \circ (k+1\ k+2) \circ \cdots \circ (\ell-2\ \ell-1) \circ (\ell-1\ \ell) \circ (\ell-2\ \ell-1) \cdots \circ (k+1\ k+2) \circ (k\ k+1).$$

Thus, the number of inversions of $\sigma \circ \mu$ equals the number of inversions of

$$\sigma \circ (k\ k+1) \circ (k+1\ k+2) \circ \cdots \circ (\ell-2\ \ell-1) \circ (\ell-1\ \ell) \circ (\ell-2\ \ell-1) \cdots \circ (k+1\ k+2) \circ (k\ k+1).$$

Using associativity, we can handle each of these in succession, and use Lemma 5.3.2 to conclude that each changes the number of inversion by 1 (either increasing or decreasing it). Since there are an odd number of adjacent transpositions, the result follows. □

Definition 5.3.4. *Let $n \in \mathbb{N}^+$. We define a function $\varepsilon \colon S_n \to \{1, -1\}$ by letting $\varepsilon(\sigma) = (-1)^{|Inv(\sigma)|}$, i.e.*

$$\varepsilon(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ has an even number of inversions} \\ -1 & \text{if } \sigma \text{ has an odd number of inversions.} \end{cases}$$

The value $\varepsilon(\sigma)$ is called the sign *of σ.*

Proposition 5.3.5. *Let $n \in \mathbb{N}^+$.*

- *$\varepsilon(id) = 1$.*
- *If $\sigma \in S_n$ can be written as a product of an even number of transpositions (not necessarily disjoint), then $\varepsilon(\sigma) = 1$.*
- *If $\sigma \in S_n$ can be written as a product of an odd number of transpositions (not necessarily disjoint), then $\varepsilon(\sigma) = -1$.*

Proof. The first of these is immediate because $|Inv(id)| = 0$. Suppose that $\sigma = \mu_1\mu_2 \cdots \mu_m$ where the μ_i are transpositions. In order to use the above results, we then write

$$\sigma = id \circ \mu_1 \circ \mu_2 \circ \cdots \circ \mu_m$$

Now $|Inv(id)| = 0$, so using Corollary 5.3.3 repeatedly, we conclude that $|Inv(id \circ \mu_1)|$ is odd, and then $|Inv(id \circ \mu_1 \circ \mu_2)|$ is even, etc. In general, a straightforward induction on k shows that

$$|Inv(id \circ \mu_1 \circ \mu_2 \cdots \circ \mu_k)|$$

is odd if k is odd, and is even if k is even. Thus, if m is even, then $\varepsilon(\sigma) = 1$, and if m is odd, then $\varepsilon(\sigma) = -1$. □

Corollary 5.3.6. *It is impossible for a permutation to be written as both a product of an even number of transpositions and as a product of an odd number of transpositions.*

Proof. If we could write a permutation in both ways, then both $\varepsilon(\sigma) = 1$ and $\varepsilon(\sigma) = -1$, a contradiction. □

Definition 5.3.7. *Let $n \in \mathbb{N}^+$ and let $\sigma \in S_n$. If $\varepsilon(\sigma) = 1$, then we say that σ is an* even *permutation. If $\varepsilon(\sigma) = -1$, then we say that σ is an* odd *permutation.*

Proposition 5.3.8. *Let $n \in \mathbb{N}^+$. For all $\sigma, \tau \in S_n$, we have $\varepsilon(\sigma\tau) = \varepsilon(\sigma) \cdot \varepsilon(\tau)$.*

Proof. If either $\sigma = id$ or $\tau = id$, this is immediate from the fact that $\varepsilon(id) = 1$. We now handle the various cases:

- If σ and τ can both be written as a product of an even number of transpositions, then $\sigma\tau$ can also be written as a product of an even number of transpositions, so we have $\varepsilon(\sigma) = 1$, $\varepsilon(\tau) = 1$, and $\varepsilon(\sigma\tau) = 1$ by Proposition 5.3.5.
- If σ and τ can both be written as a product of an odd number of transpositions, then $\sigma\tau$ can be written as a product of an even number of transpositions, so we have $\varepsilon(\sigma) = -1$, $\varepsilon(\tau) = -1$, and $\varepsilon(\sigma\tau) = 1$ by Proposition 5.3.5.
- If σ can be written as a product of an even number of transpositions, and τ can be written as a product of an odd number of transpositions, then $\sigma\tau$ can be written as a product of an odd number of transpositions, so we have $\varepsilon(\sigma) = 1$, $\varepsilon(\tau) = -1$, and $\varepsilon(\sigma\tau) = -1$ by Proposition 5.3.5.
- If σ can be written as a product of an odd number of transpositions, and τ can be written as a product of an even number of transpositions, then $\sigma\tau$ can be written as a product of an odd number of transpositions, so we have $\varepsilon(\sigma) = -1$, $\varepsilon(\tau) = 1$, and $\varepsilon(\sigma\tau) = -1$ by Proposition 5.3.5.

Therefore, in all cases, we have $\varepsilon(\sigma\tau) = \varepsilon(\sigma) \cdot \varepsilon(\tau)$. □

Proposition 5.3.9. *Let $n \in \mathbb{N}^+$. Suppose that $\sigma \in S_n$ is a k-cycle.*

- *If k is an even number, then σ is an odd permutation, i.e. $\varepsilon(\sigma) = -1$.*
- *If k is an odd number, then σ is an even permutation, i.e. $\varepsilon(\sigma) = 1$.*

Proof. Write $\sigma = (a_1\ a_2\ a_3\ \cdots\ a_{k-1}\ a_k)$ where the a_i are distinct. As above, we have

$$\sigma = (a_1\ a_k)(a_1\ a_{k-1}) \cdots (a_1\ a_3)(a_1\ a_2)$$

Thus, σ is the product of $k-1$ many transpositions. If k is an even number, then $k-1$ is an odd number, and hence σ is an odd permutation. If k is an odd number, then $k-1$ is an even number, and hence σ is an even permutation. □

Using Proposition 5.3.8 and Proposition 5.3.9, we can now easily compute the sign of any permutation once we've written it in cycle notation. For example, suppose that

$$\sigma = (1\ 9\ 2\ 6\ 4\ 11)(3\ 8\ 5)(7\ 10).$$

We then have

$$\begin{aligned} \varepsilon(\sigma) &= \varepsilon((1\ 9\ 2\ 6\ 4\ 11)) \cdot \varepsilon((3\ 8\ 5)) \cdot \varepsilon((7\ 10)) \\ &= (-1) \cdot 1 \cdot (-1) \\ &= 1, \end{aligned}$$

so σ is an even permutation.

Proposition 5.3.10. *Let $n \in \mathbb{N}^+$ and define*

$$A_n = \{\sigma \in S_n : \varepsilon(\sigma) = 1\}.$$

We then have that A_n is a subgroup of S_n.

Proof. We have $\varepsilon(id) = (-1)^0 = 1$, so $id \in A_n$. Suppose that $\sigma, \tau \in A_n$ so that $\varepsilon(\sigma) = 1 = \varepsilon(\tau)$. we then have

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma) \cdot \varepsilon(\tau) = 1 \cdot 1 = 1,$$

so $\sigma\tau \in A_n$. Finally, suppose that $\sigma \in A_n$. We then have $\sigma\sigma^{-1} = id$ so

$$\begin{aligned} 1 &= \varepsilon(id) \\ &= \varepsilon(\sigma\sigma^{-1}) \\ &= \varepsilon(\sigma) \cdot \varepsilon(\sigma^{-1}) \\ &= 1 \cdot \varepsilon(\sigma^{-1}) \\ &= \varepsilon(\sigma^{-1}), \end{aligned}$$

so $\sigma^{-1} \in A_n$. □

Definition 5.3.11. *The subgroup $A_n = \{\sigma \in S_n : \varepsilon(\sigma) = 1\}$ of S_n is called the* alternating group *of degree n.*

Let's take a look at a few small examples. We trivially have $A_1 = \{id\}$, and we also have $A_2 = \{id\}$ because $(1\ 2)$ is an odd permutation. The group S_3 has 6 elements: the identity, three 2-cycles, and two 3-cycles, so $A_3 = \{id, (1\ 2\ 3), (1\ 3\ 2)\}$. When we examine S_4, we see that it contains the following:

- The identity.
- Six 4-cycles.
- Eight 3-cycles.
- Six 2-cycles.
- Three elements that are the product of two disjoint 2-cycles.

Now of these, A_4 consists of the identity, the eight 3-cycles, and the three products of two disjoint 2-cycles, so $|A_4| = 12$. In general, we have the following.

Proposition 5.3.12. *For any $n \geq 2$, we have $|A_n| = \frac{n!}{2}$.*

Proof. Define a function $f \colon A_n \to S_n$ by letting $f(\sigma) = \sigma(1\ 2)$. We first claim that f is injective. To see this, suppose that $\sigma, \tau \in A_n$ and that $f(\sigma) = f(\tau)$. We then have $\sigma(1\ 2) = \tau(1\ 2)$. Multiplying on the right by $(1\ 2)$, we conclude that $\sigma = \tau$. Therefore, f is injective.

We next claim that $\text{range}(f) = S_n \backslash A_n$. Suppose first that $\sigma \in A_n$. We then have $\varepsilon(\sigma) = 1$, so

$$\varepsilon(f(\sigma)) = \varepsilon(\sigma(1\ 2)) = \varepsilon(\sigma) \cdot \varepsilon((1\ 2)) = 1 \cdot (-1) = -1$$

so $f(\sigma) \in S_n \backslash A_n$. Conversely, suppose that $\tau \in S_n \backslash A_n$ so that $\varepsilon(\tau) = -1$. We then have

$$\varepsilon(\tau(1\ 2)) = \varepsilon(\tau) \cdot \varepsilon((1\ 2)) = (-1) \cdot (-1) = 1$$

so $\tau(1\ 2) \in A_n$. Now

$$f(\tau(1\ 2)) = \tau(1\ 2)(1\ 2) = \tau$$

so $\tau \in \text{range}(f)$. It follows that $\text{range}(f) = S_n \backslash A_n$. Therefore, f maps A_n bijectively onto $S_n \backslash A_n$ and hence $|A_n| = |S_n \backslash A_n|$. Since S_n is the disjoint union of these two sets and $|S_n| = n!$, it follows that $|A_n| = \frac{n!}{2}$. □

5.4 The Dihedral Groups

We now define another subgroup of S_n which has a very geometric flavor. By way of motivation, consider a regular n-gon, i.e. a convex polygon with n edges in which all edges have the same length and all interior angles are congruent. Now we want to consider the symmetries of this polygon obtained by rigid motions. That is, we want to think about all results obtained by picking up the polygon, moving it around in space, and then placing it back down so that it looks exactly the same. For example, one possibility is that we rotate the polygon around the center by $360/n$ degrees. We can also flip the polygon over across an imaginary line through the center so long as we take vertices to vertices.

To put these geometric ideas in more algebraic terms, first label the vertices clockwise with the number $1, 2, 3, \dots, n$. Now a symmetry of the polygon will move vertices to vertices, so will correspond to a bijection of $\{1, 2, 3, \dots, n\}$, i.e. an element of S_n. For example, the permutation $(1\ 2\ 3\ \cdots\ n)$ corresponds to rotation by $360/n$ degrees because it sends vertex 1 to the position originally occupied by vertex 2, sends vertex 2 to the position originally occupied by vertex 3, etc.

Definition 5.4.1. *Fix $n \geq 3$. We define the following elements of S_n:*

- $r = (1\ 2\ 3\ \cdots\ n)$.
- $s = (2\ n)(3\ n-1)(4\ n-2)\cdots$. *More formally:*
  - *If $n = 2k$ where $k \in \mathbb{N}^+$, let $s = (2\ n)(3\ n-1)(4\ n-2)\cdots(k\ k+2)$.*
  - *If $n = 2k+1$ where $k \in \mathbb{N}^+$, let $s = (2\ n)(3\ n-1)(4\ n-2)\cdots(k+1\ k+2)$.*

Thus, r corresponds to clockwise rotation by $360/n$ degrees (as describe above), and s corresponds to flipping the polygon across the line through the vertex 1 and the center. Now given two symmetries of the polygon, we can do one followed by the other to get another symmetry. In other words, the composition of two symmetries is a symmetry. We can also reverse any rigid motion, so the inverse of a symmetry is a symmetry. Finally, the identity function is a trivial symmetry, so the set of all symmetries of the regular n-gon forms a subgroup of S_n.

Definition 5.4.2. *Let $n \geq 3$. With the notation of r and s as above, we define $D_n = \langle r, s\rangle$, i.e. D_n is the smallest subgroup of S_n containing both r and s. The group D_n is called the* dihedral group *of degree n.*

In other words, we simply *define* D_n to be every symmetry we can obtain through a simple rotation and a simple flip. This is a nice precise algebraic description. Since the collection of symmetries is closed under composition and inverses, every element of D_n is indeed a rigid symmetry of the n-gon. We will explain below (after we develop a bit of theory) why every such symmetry of a regular n-gon is given by an element of D_n.

As an example, the following is an element of D_n.

$$r^7 s^5 r^{-4} s^{-4} r s^{-3} r^{14}.$$

We would like to find a way to simplify such expressions, and the next proposition is the primary tool that we will need.

Proposition 5.4.3. *Let $n \geq 3$. We have the following*

1. $|r| = n$.
2. $|s| = 2$.
3. $sr = r^{-1}s = r^{n-1}s$.
4. *For all $k \in \mathbb{N}^+$, we have $sr^k = r^{-k}s$.*

Proof. We have $|r| = n$ because r is an n-cycle and $|s| = 2$ because s is a product of disjoint 2-cycles. We now check that $sr = r^{-1}s$. First notice that

$$r^{-1} = (n \;\; n-1 \;\; \cdots \;\; 3 \;\; 2 \;\; 1) = (1 \;\; n \;\; n-1 \;\; \cdots \;\; 3 \;\; 2).$$

Suppose first that $n = 2k$ where $k \in \mathbb{N}^+$. We then have

$$\begin{aligned} sr &= (2 \;\; n)(3 \;\; n-1)(4 \;\; n-2) \cdots (k \;\; k+2)(1 \;\; 2 \;\; 3 \;\; \cdots \;\; n) \\ &= (1 \;\; n)(2 \;\; n-1)(3 \;\; n-2) \cdots (k \;\; k+1), \end{aligned}$$

and

$$\begin{aligned} r^{-1}s &= (n \;\; n-1 \;\; \cdots \;\; 3 \;\; 2 \;\; 1)(2 \;\; n)(3 \;\; n-1)(4 \;\; n-2) \cdots (k \;\; k+2) \\ &= (1 \;\; n)(2 \;\; n-1)(3 \;\; n-2) \cdots (k \;\; k+1). \end{aligned}$$

so $sr = r^{-1}s$. Suppose now that $n = 2k+1$ where $k \in \mathbb{N}^+$. We then have

$$\begin{aligned} sr &= (2 \;\; n)(3 \;\; n-1)(4 \;\; n-2) \cdots (k+1 \;\; k+2)(1 \;\; 2 \;\; 3 \;\; \cdots \;\; n) \\ &= (1 \;\; n)(2 \;\; n-1)(3 \;\; n-2) \cdots (k \;\; k+2), \end{aligned}$$

and

$$\begin{aligned} r^{-1}s &= (n \;\; n-1 \;\; \cdots \;\; 3 \;\; 2 \;\; 1)(2 \;\; n)(3 \;\; n-1)(4 \;\; n-2) \cdots (k+1 \;\; k+2) \\ &= (1 \;\; n)(2 \;\; n-1)(3 \;\; n-2) \cdots (k \;\; k+2), \end{aligned}$$

so $sr = r^{-1}s$. Thus, $sr = r^{-1}s$ in all cases. Since we know that $|r| = n$, we have $rr^{n-1} = e$ and $r^{n-1}r = e$, so $r^{-1} = r^{n-1}$. It follows that $r^{-1}s = r^{n-1}s$.

The last statement now follows by induction from the third. □

We now give an example of how to use this proposition to simplify the above expression in the case $n = 5$. We have

$$\begin{aligned} r^7s^5r^{-4}s^{-4}rs^{-3}r^{14} &= r^2srrsr^4 && \text{(using } |r| = 5 \text{ and } |s| = 2\text{)} \\ &= r^2sr^2sr^4 \\ &= r^2sr^2r^{-4}s \\ &= r^2sr^{-2}s \\ &= r^2sr^3s \\ &= r^2r^{-3}ss \\ &= r^{-1}s^2 \\ &= r^4. \end{aligned}$$

Theorem 5.4.4. *Let $n \geq 3$.*

1. *$D_n = \{r^is^k : 0 \leq i \leq n-1, 0 \leq k \leq 1\}$.*
2. *If $r^is^k = r^js^\ell$ with $0 \leq i, j \leq n-1$ and $0 \leq k, \ell \leq 1$, then $i = j$ and $k = \ell$.*

In particular, we have $|D_n| = 2n$.

Proof. Using the fundamental relations that $|r| = n$, that $|s| = 2$, and that $sr^k = r^{-k}s$ for all $k \in \mathbb{N}^+$, the above argument shows that any product of r, s, and their inverses equals $r^i s^k$ for some i, k with $0 \leq i \leq n-1$ and $0 \leq k \leq 1$. To be more precise, one can use the above relations to show that the set

$$\{r^i s^k : 0 \leq i \leq n-1, 0 \leq k \leq 1\}$$

is closed under multiplication and under inverses, so it equals D_n. I will leave such a check for you if you would like to work through it. This gives part 1.

Suppose now that $r^i s^k = r^j s^\ell$ with $0 \leq i, j \leq n-1$ and $0 \leq k, \ell \leq 1$. Multiplying on the left by r^{-j} and on the right by s^{-k}, we see that

$$r^{i-j} = s^{\ell-k}.$$

Suppose for the sake of obtaining a contradiction that $k \neq \ell$. Since $k, \ell \in \{0, 1\}$, we must have $\ell - k \in \{-1, 1\}$, so as $s^{-1} = s$ it follows that $r^{i-j} = s^{\ell-k} = s$. Now we have $s(1) = 1$, so we must have $r^{i-j}(1) = 1$ as well. This implies that $n \mid (i-j)$, so as $-n < i-j < n$, we conclude that $i - j = 0$. Thus $r^{i-j} = e$, and we conclude that $s = e$, a contradiction. Therefore, we must have $k = \ell$. It follows that $s^{\ell-k} = s^0 = e$, so $r^{i-j} = e$. Using the fact that $|r| = n$ now, we see that $n \mid (i-j)$, and as above this implies that $i - j = 0$ so $i = j$. □

Corollary 5.4.5. *Let $n \geq 3$. We then have that D_n is a nonabelian group with $|D_n| = 2n$.*

Proof. We claim that $rs \neq sr$. Suppose instead that $rs = sr$. Since we know that $sr = r^{-1}s$, it follows that $rs = r^{-1}s$. Canceling the s on the right, we see that $r = r^{-1}$. Multiplying on the left by r we see that $r^2 = e$, but this is a contradiction because $|r| = n \geq 3$. Therefore, $rs \neq sr$ and hence D_n is nonabelian. Now by the previous theorem we know that

$$D_n = \{r^i s^k : 0 \leq i \leq n-1, 0 \leq k \leq 1\}$$

and by the second part of the theorem that the $2n$ elements described in the set are distinct. □

We now come back around to giving a geometric justification for why the elements of D_n exactly correspond to the symmetries of the regular n-gon. We have described why every element of D_n does indeed give a symmetry (because both r and s do, and the set of symmetries must be closed under composition and inversion), so we need only understand why all possible symmetries of the regular n-gon arise from an element of D_n. To determine a symmetry, we first need to send the vertex labeled by 1 to another vertex. We have n possible choices for where to send it, and suppose we send it to the original position of vertex k. Once we have sent vertex 1 to the position of vertex k, we now need to determine were the vertex 2 is sent. Now vertex 2 must go to one of the vertices adjacent to k, so we only have 2 choices for where to send it. Finally, once we've determined these two vertices (where vertex 1 and vertex 2 go), the rest of the n-gon is determined because we have completely determined where an entire edge goes. Thus, there are a total of $n \cdot 2 = 2n$ many possible symmetries. Since $|D_n| = 2n$, it follows that all symmetries are given by elements of D_n.

Finally notice that $D_3 = S_3$ simply because D_3 is a subgroup of S_3 and $|D_3| = 6 = |S_3|$. In other words, any permutation of the vertices of an equilateral triangle is obtainable via a rigid motion of the triangle. However, if $n \geq 4$, then $|D_n|$ is much smaller than $|S_n|$ as most permutations of the vertices of a regular n-gon can not be obtained from a rigid motion.

We end with the Cayley table of D_4:

$\circ$	e	r	r^2	r^3	s	rs	r^2s	r^3s
e	e	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	e	rs	r^2s	r^3s	s
r^2	r^2	r^3	e	r	r^2s	r^3s	s	rs
r^3	r^3	e	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	e	r^3	r^2	r
rs	rs	s	r^3s	r^2s	r	e	r^3	r^2
r^2s	r^2s	rs	s	r^3s	r^2	r	e	r^3
r^3s	r^3s	r^2s	rs	s	r^3	r^2	r	e

5.5 The Quaternion Group

Consider the following three 2×2 matrices over $\mathbb{C}$:

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \qquad C = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

For A, we have

$$A^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I.$$

For B, we have

$$B^2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I.$$

For C, we have

$$C^2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I.$$

Since

$$A^2 = B^2 = C^2 = -I,$$

it follows that

$$A^4 = B^4 = C^4 = I.$$

Thus, each of A, B, and C have order at most 4. One can check that none of them have order 3 (either directly, using general results on powers giving the identity, or using the fact that otherwise $A^3 = I = A^4$, so $A = I$, a contradiction). In particular, each of these matrices is an element of $GL_2(\mathbb{C})$ because $A \cdot A^3 = I = A^3 \cdot A$ (and similarly for B and C).

We have

$$AB = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = C,$$

and

$$BA = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = -C.$$

We also have

$$CA = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = B,$$

and

$$AC = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = -B.$$

Finally, we have

$$BC = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = A,$$

and

$$CB = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -A.$$

Thus, if we are working with $GL_2(\mathbb{C})$, then

$$\langle A, B, C \rangle = \{I, -I, A, -A, B, -B, C, -C\}.$$

This subgroup of 8 elements is called the *quaternion group*. However, just like in the situation for D_n, we typically give these elements other names and forgot that they are matrices (just as we often forgot that the elements of D_n are really elements of S_n).

Definition 5.5.1. *The* quaternion group *is the group on the set* $\{1, -1, i, -i, j, -j, k, -k\}$ *where we define the group operation on* $\{i, j, k\}^2$ *as*

$$\begin{array}{ccc} i^2 = -1 & j^2 = -1 & k^2 = -1 \\ ij = k & jk = i & ki = j \\ ji = -k & kj = -i & ik = -j, \end{array}$$

and all other multiplications in the natural way. We denote this group by Q_8.

For example, we have $(-k)(-j) = -(-(kj)) = kj = -i$.

5.6 The Center of a Group

Definition 5.6.1. *Given a group* G*, we let* $Z(G) = \{a \in G : ag = ga \text{ for all } g \in G\}$*, i.e.* $Z(G)$ *is the set of elements of* G *that commute with every element of* G*. We call* $Z(G)$ *the* center *of* G*.*

Proposition 5.6.2. *For any group* G*, we have that* $Z(G)$ *is a subgroup of* G*.*

Proof. We check the three conditions.

- First notice that for any $b \in G$ we have
$$eg = g = ge$$
directly from the identity axiom, hence $e \in Z(G)$.

- Suppose that $a, b \in Z(G)$. Let $g \in G$ be arbitrary. We then have
$$\begin{aligned} g(ab) &= (ga)b && \text{(by associativity)} \\ &= (ag)b && \text{(since } a \in Z(G)\text{)} \\ &= a(gb) && \text{(by associativity)} \\ &= a(bg) && \text{(since } y \in Z(G)\text{)} \\ &= (ab)g && \text{(by associativity).} \end{aligned}$$
Since $g \in G$ was arbitrary, we conclude that $g(ab) = (ab)g$ for all $g \in G$, so $ab \in Z(G)$. Thus, $Z(G)$ is closed under multiplication.

- Suppose that $a \in Z(G)$. Let $g \in G$ be arbitrary. Since $a \in Z(G)$, we have
$$ga = ag.$$
Multiplying on the left by a^{-1} we conclude that
$$a^{-1}ga = a^{-1}ag,$$
so
$$a^{-1}ga = g.$$
Now multiplying this equation on the right by a^{-1} gives
$$a^{-1}gaa^{-1} = ga^{-1},$$
so
$$a^{-1}g = ga^{-1}.$$
Since $g \in G$ was arbitrary, we conclude that $ga^{-1} = a^{-1}g$ for all $g \in G$, so $a^{-1} \in Z(G)$. Thus, $Z(G)$ is closed under inverses.

Combining the above three facts, we conclude that $Z(G)$ is a subgroup of G. □

We now calculate $Z(G)$ for many of the groups G that we have encountered:

- First notice that if G is an abelian group, then we trivially have that $Z(G) = G$. In particular, we have $Z(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ and $Z(U(\mathbb{Z}/n\mathbb{Z})) = U(\mathbb{Z}/n\mathbb{Z})$ for all $n \in \mathbb{N}^+$.

- On the homework, we proved that if $n \geq 3$ and $\sigma \in S_n \backslash \{id\}$. then there exists $\tau \in S_n$ with $\sigma\tau \neq \tau\sigma$, so $\sigma \notin Z(S_n)$. Since the identity of a group is always in the center, it follows that $Z(S_n) = \{id\}$ for all $n \geq 3$. Notice that we also have $Z(S_1) = \{id\}$ trivially, but $Z(S_2) = \{id, (1\ 2)\} = S_2$.

- If $n \geq 4$, then $Z(A_n) = \{id\}$. Suppose that $\sigma \in A_n$ with $\sigma \neq id$. We have that $\sigma \colon \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ is a bijection which is not the identity map. Thus, we may fix $i \in \{1, 2, \dots, n\}$ with $\sigma(i) \neq i$, say $\sigma(i) = j$. Since $n \geq 4$, we may fix $k, \ell \in \{1, 2, \dots, n\} \backslash \{i, j\}$ with $k \neq \ell$. Define $\tau \colon \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ by
$$\tau(m) = \begin{cases} k & \text{if } m = j \\ \ell & \text{if } m = k \\ j & \text{if } m = \ell \\ m & \text{otherwise} \end{cases}$$
In other words, $\tau = (j\ k\ \ell)$ in cycle notation. Notice that $\tau \in A_n$, that
$$(\tau \circ \sigma)(i) = \tau(\sigma(i)) = \tau(j) = k$$
and that
$$(\sigma \circ \tau)(i) = \sigma(\tau(i)) = \sigma(i) = j.$$
Since $j \neq k$, we have shown that the functions $\sigma \circ \tau$ and $\tau \circ \sigma$ disagree on i, and hence are distinct functions. In other words, in A_n we have $\sigma\tau \neq \tau\sigma$. Thus, $Z(A_n) = \{id\}$ if $n \geq 4$.

  Notice that $A_1 = \{id\}$ and $A_2 = \{id\}$, so we also have $Z(A_n) = \{id\}$ trivially when $n \leq 2$. However, when $n = 3$, we have that $A_3 = \{id, (1\ 2\ 3), (1\ 3\ 2)\} = \langle (1\ 2\ 3) \rangle$ is cyclic and hence abelian, so $Z(A_3) = A_3$.

- We have $Z(Q_8) = \{1, -1\}$. We trivially have that $1 \in Z(Q_8)$, and showing that $-1 \in Z(Q_8)$ is simply a matter of checking the various possibilities. Now $i \notin Z(Q_8)$ because $ij = k$ but $ji = -k$, and $-i \notin Z(Q_8)$ because $(-i)j = -k$ and $j(-i) = k$. Similar arguments show that the other four elements are not in $Z(Q_8)$ either.

- We claim that
$$Z(GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} : r \in \mathbb{R}\backslash\{0\} \right\}$$
To see this, first notice that if $r \in \mathbb{R}\backslash\{0\}$, then
$$\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \in GL_n(\mathbb{R})$$
because
$$\begin{pmatrix} \frac{1}{r} & 0 \\ 0 & \frac{1}{r} \end{pmatrix}$$
is an inverse. Now for any matrix
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$$
we have
$$\begin{aligned} \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} ra & rb \\ rc & rd \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \end{aligned}$$
Therefore
$$\left\{ \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} : r \in \mathbb{R}\backslash\{0\} \right\} \subseteq Z(GL_2(\mathbb{R}))$$
Suppose now that $A \in Z(GL_2(\mathbb{R}))$, i.e. that $AB = BA$ for all $B \in GL_2(\mathbb{R})$. Write
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
Using our hypothesis in the special case where
$$B = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$$
(which is easily seen to be invertible), we obtain
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
Multiplying out these matrices we see that
$$\begin{pmatrix} 2a & b \\ 2c & d \end{pmatrix} = \begin{pmatrix} 2a & 2b \\ c & d \end{pmatrix}$$
Thus, $b = 2b$ and $c = 2c$, which tells us that $b = 0$ and $c = 0$. It follows that
$$A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

Now using our hypothesis in the special case where

$$B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

(which is easily seen to be invertible), we obtain

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

Multiplying out these matrices we see that

$$\begin{pmatrix} 0 & a \\ d & 0 \end{pmatrix} = \begin{pmatrix} 0 & d \\ a & 0 \end{pmatrix}$$

Therefore $a = d$, and we conclude that

$$A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

completing our proof.

- Generalizing the above example, one can show that

$$Z(GL_n(\mathbb{R})) = \{r \cdot I_n : r \in \mathbb{R}\backslash\{0\}\}$$

where I_n is the $n \times n$ identity matrix.

On the homework, you will calculate $Z(D_n)$.

5.7 Cosets

Suppose that G is a group and that H is a subgroup of G. The idea we want to explore is how to collapse the elements of H by considering them all to be "trivial" like the identity e. If we want this idea to work, we would then want to identify two elements $a, b \in G$ if we can get from one to the other via multiplication by a "trivial" element. In other words, we want to identify elements a and b if there exists $h \in H$ with $ah = b$.

For example, suppose that G is the group $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ under addition (so $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$) and that $H = \{(0, b) : b \in \mathbb{R}\}$ is the y-axis. Notice that H is subgroup of G. We want to consider everything on the y-axis, that is every pair of the form $(0, b)$, as trivial. Now if we want the y-axis to be considered "trivial", then we would want to consider two points to be the "same" if we can get from one to the other by adding an element of the y-axis. Thus, we would want to identify (a_1, b_1) with (a_2, b_2) if and only if $a_1 = a_2$, because then we can add the "trivial" point $(0, b_2 - b_1)$ to (a_1, b_1) to get (a_2, b_2).

Let's move on to the group $G = \mathbb{Z}$. Let $n \in \mathbb{N}^+$ and consider $H = \langle n \rangle = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. In this situation, we want to consider all multiples of n to be "equal" to 0, and in general we want to consider $a, b \in \mathbb{Z}$ to be equal if we can add some multiple of n to a in order to obtain b. In other words, we want to identify a and b if and only if there exists $k \in \mathbb{Z}$ with $a + kn = b$. Working it out, we want to identify a and b if and only if $b - a$ is a multiple of n, i.e. if and only if $a \equiv b \pmod{n}$. Thus, in the special case of the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$, we recover the fundamental ideas of modular arithmetic and our eventual definition of $\mathbb{Z}/n\mathbb{Z}$.

Left Cosets

Definition 5.7.1. *Let G be a group and let H be a subgroup of G. We define a relation $\sim_H$ on G by letting $a \sim_H b$ mean that there exists $h \in H$ with $ah = b$.*

Proposition 5.7.2. *Let G be a group and let H be a subgroup of G. The relation $\sim_H$ is an equivalence relation on G.*

Proof. We check the three properties.

- Reflexive: Let $a \in G$. We have that $ae = a$ and we know that $e \in H$ because H is a subgroup of G, so $a \sim_H a$.
- Symmetric: Let $a, b \in G$ with $a \sim_H b$. Fix $h \in H$ with $ah = b$. Multiplying on the right by h^{-1}, we see that $a = bh^{-1}$, so $bh^{-1} = a$. Now $h^{-1} \in H$ because H is a subgroup of G, so $b \sim_H a$.
- Transitive: Let $a, b, c \in G$ with $a \sim_H b$ and $b \sim_H c$. Fix $h_1, h_2 \in H$ with $ah_1 = b$ and $bh_2 = c$. We then have
$$a(h_1h_2) = (ah_1)h_2 = bh_2 = c.$$
Now $h_1h_2 \in H$ because H is a subgroup of G, so $a \sim_H c$.

Therefore, $\sim_H$ is an equivalence relation on G. □

The next proposition is a useful little rephrasing of when $a \sim_H b$.

Proposition 5.7.3. *Let G be a group and let H be a subgroup of G. Given $a, b \in G$, we have $a \sim_H b$ if and only if $a^{-1}b \in H$.*

Proof. Suppose first that $a, b \in G$ satisfy $a \sim_H b$. Fix $h \in H$ with $ah = b$. Multiplying on the left by a^{-1}, we conclude that $h = a^{-1}b$, so $a^{-1}b = h \in H$.

Suppose conversely that $a^{-1}b \in H$. Since
$$a(a^{-1}b) = (aa^{-1})b = eb = b,$$
it follows that $a \sim_H b$. □

Definition 5.7.4. *Let G be a group and let H be a subgroup of G. Under the equivalence relation $\sim_H$, we have*
$$\begin{aligned}\overline{a} &= \{b \in G : a \sim_H b\} \\ &= \{b \in G : \text{ There exists } h \in H \text{ with } b = ah\} \\ &= \{ah : h \in H\} \\ &= aH.\end{aligned}$$
These equivalence classes are called left cosets *of H in G.*

Since the left cosets of H in G are the equivalence classes of the equivalence relation $\sim_H$, all of our theory about equivalence relations apply. For example, if two left cosets of H in G intersect nontrivially, then they are in fact equal. Also, as is the case for general equivalence relations, the left cosets of H in G partition G into pieces. Using Proposition 5.7.3, we obtain the following fundamental way of determining when two left cosets are equal:
$$aH = bH \iff a^{-1}b \in H \iff b^{-1}a \in H.$$
Let's work through an example.

Example 5.7.5. *Let $G = S_3$ and let $H = \langle (1\ 2) \rangle = \{id, (1\ 2)\}$. Determine the left cosets of H in G.*

Proof. The left cosets are the sets σH for $\sigma \in G$. For example, we have the left coset

$$idH = \{id \circ id, id \circ (1\ 2)\} = \{id, (1\ 2)\}.$$

We can also consider the left coset

$$(1\ 2)H = \{id \circ (1\ 2), (1\ 2) \circ (1\ 2)\} = \{(1\ 2), id\} = \{id, (1\ 2)\}.$$

Thus, the two left cosets idH and $(1\ 2)H$ are equal. This should not be surprising because

$$id^{-1} \circ (1\ 2) = id \circ (1\ 2) = (1\ 2) \in H.$$

Alternatively, we can simply note that $(1\ 2) \in idH$ and $(1\ 2) \in (1\ 2)H$, so since the left cosets idH and $(1\ 2)H$ intersect nontrivially, we know immediately that they must be equal. Working through all the examples, we compute σH for each of the six $\sigma \in S_3$:

1. $idH = (1\ 2)H = \{id, (1\ 2)\}$.
2. $(1\ 3)H = (1\ 2\ 3)H = \{(1\ 3), (1\ 2\ 3)\}$.
3. $(2\ 3)H = (1\ 3\ 2)H = \{(2\ 3), (1\ 3\ 2)\}$.

Thus, there are 3 distinct left cosets of H in G. $\square$

Intuitively, if H is a subgroup of G, then a left coset aH is simply a "translation" of the subgroup H within G using the element $a \in G$. In the above example, $(1\ 3)H$ is simply the "shift" of the subgroup H using $(1\ 3)$ because we obtain it by hitting every element of H on the left by $(1\ 3)$.

To see this geometrically, consider again the group $G = \mathbb{R}^2$ under addition with subgroup

$$H = \{(0, b) : b \in \mathbb{R}\}$$

equal to the y-axis (or equivalently the line $x = 0$). Since the operation in G is $+$, we will denote the left coset of $(a, b) \in G$ by $(a, b) + H$ (rather than $(a, b)H$). Let's consider the left coset $(3, 0) + H$. We have

$$\begin{aligned} (3, 0) + H &= \{(3, 0) + (0, b) : b \in \mathbb{R}\} \\ &= \{(3, b) : b \in \mathbb{R}\}, \end{aligned}$$

so $(3, 0) + H$ is the line $x = 3$. Thus, the left coset $(3, 0) + H$ is the translation of the line $x = 0$. Let's now consider the coset $(3, 5) + H$. We have

$$\begin{aligned} (3, 5) + H &= \{(3, 5) + (0, b) : b \in \mathbb{R}\} \\ &= \{(3, 5 + b) : b \in \mathbb{R}\} \\ &= \{(3, c) : c \in \mathbb{R}\} \\ &= (3, 0) + H. \end{aligned}$$

Notice that we could have obtained this with less work by noting that the inverse of $(3, 5)$ in G is $(-3, -5)$ and $(-3, -5) + (3, 0) = (0, -5) \in H$, hence $(3, 5) + H = (3, 0) + H$. Therefore, the left coset $(3, 5) + H$ also gives the line $x = 3$. Notice that every element of H when hit by $(3, 5)$ translates right 3 and shifts up 5, but as a set this latter shift of 5 is washed away.

Finally, let's consider $G = \mathbb{Z}$ (under addition) and $H = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ where $n \in \mathbb{N}^+$. Notice that given $a, b \in \mathbb{Z}$, we have

$$\begin{aligned}
a \sim_{n\mathbb{Z}} b &\iff \text{There exists } h \in n\mathbb{Z} \text{ with } a + h = b \\
&\iff \text{There exists } k \in \mathbb{Z} \text{ with } a + nk = b \\
&\iff \text{There exists } k \in \mathbb{Z} \text{ with } nk = b - a \\
&\iff n \mid (b - a) \\
&\iff b \equiv a \pmod{n} \\
&\iff a \equiv b \pmod{n}.
\end{aligned}$$

Therefore the two relations $\sim_{n\mathbb{Z}}$ and $\equiv_n$ are precisely the same, and we have recovered congruence modulo n as a special case of our general construction. Since the relations are the same, they have the same equivalence classes. Hence, the equivalence class of a under the equivalence relation $\equiv_n$, which in the past we denoted by $\overline{a}$, equals the equivalence class of a under the equivalence relation $\sim_{n\mathbb{Z}}$, which is the left coset $a + n\mathbb{Z}$.

Right Cosets

In the previous section, we defined $a \sim_H b$ to mean that there exists $h \in H$ with $ah = b$. Thus, we considered two elements of G to be equivalent if we could get from a to b through multiplication by an element of H on the right of a. In particular, with this definition, we saw that when we consider $G = S_3$ and $H = \langle(1\ 2)\rangle$, we have $(1\ 3) \sim_H (1\ 2\ 3)$ because $(1\ 3)(1\ 2) = (1\ 2\ 3)$.

What happens if we switch things up? For the rest of this section, completely ignore the definition of $\sim_H$ defined above because we will redefine it on the other side now.

Definition 5.7.6. *Let G be a group and let H be a subgroup of G. We define a relation $\sim_H$ on G by letting $a \sim_H b$ mean that there exists $h \in H$ with $ha = b$.*

The following results are proved exactly as above just working on the other side.

Proposition 5.7.7. *Let G be a group and let H be a subgroup of G. The relation $\sim_H$ is an equivalence relation on G.*

Proposition 5.7.8. *Let G be a group and let H be a subgroup of G. Given $a, b \in G$, we have $a \sim_H b$ if and only if $ab^{-1} \in H$.*

Now it would be nice if this new equivalence relation was the same as the original equivalence relation. Too bad. In general, they are different! For example, with this new equivalence relation, we do **not** have $(1\ 3) \sim_H (1\ 2\ 3)$ because $id \circ (1\ 3) = (1\ 3)$ and $(1\ 2)(1\ 3) = (1\ 3\ 2)$. Now that we know that the two relations differ in general, we should think about the equivalence classes of this new equivalence relation.

Definition 5.7.9. *Let G be a group and let H be a subgroup of G. Under the equivalence relation $\sim_H$, we have*

$$\begin{aligned}
\overline{a} &= \{b \in G : a \sim_H b\} \\
&= \{b \in G : \textit{ There exists } h \in H \textit{ with } b = ha\} \\
&= \{ha : h \in H\} \\
&= Ha.
\end{aligned}$$

These equivalence classes are called right cosets *of H in G.*

Let's work out the right cosets of our previous example.

Example 5.7.10. *Let $G = S_3$ and let $H = \langle (1\ 2) \rangle = \{id, (1\ 2)\}$. Determine the right cosets of H in G.*

Proof. Working them all out, we obtain the following right cosets:

- $Hid = H(1\ 2) = \{id, (1\ 2)\}$.
- $H(1\ 3) = H(1\ 3\ 2) = \{(1\ 3), (1\ 3\ 2)\}$.
- $H(2\ 3) = H(1\ 2\ 3) = \{(2\ 3), (1\ 2\ 3)\}$.

Thus, there are 3 distinct right cosets of H in G. □

Notice that although we obtained both 3 left cosets and 3 right cosets, these cosets were different. In particular, we have $(1\ 3)H \neq H(1\ 3)$. In other words, it is not true in general that the left coset aH equals the right coset Ha. Notice that this is fundamentally an issue because S_3 is nonabelian. If we were working in an abelian group G with a subgroup H of G, then $ah = ha$ for all $h \in H$, so $aH = Ha$.

As in the left coset section, using Proposition 5.7.8, we have the following fundamental way of determining when two left cosets are equal:

$$Ha = Hb \Longleftrightarrow ab^{-1} \in H \Longleftrightarrow ba^{-1} \in H$$

Index of a Subgroup

As we saw in the previous sections, it is not in general true that left cosets are right cosets and vice versa. However, in the one example we saw above, we at least had the same number of left cosets as we had right cosets. This is a general and important fact, which we now establish.

First, let's once again state the fundamental way to tell when two left cosets are equal and when two right cosets are equal:

$$aH = bH \Longleftrightarrow a^{-1}b \in H \Longleftrightarrow b^{-1}a \in H$$

and

$$Ha = Hb \Longleftrightarrow ab^{-1} \in H \Longleftrightarrow ba^{-1} \in H.$$

Suppose now that G is a group and that H is a subgroup of G. Let $\mathcal{L}_H$ be the set of left cosets of H in G and let $\mathcal{R}_H$ be the set of right cosets of H in G. We will show that $|\mathcal{L}_H| = |\mathcal{R}_H|$ by defining a bijection $f\colon \mathcal{L}_H \to \mathcal{R}_H$. Now the natural idea is to define f by letting $f(aH) = Ha$. However, we need to be very careful. Recall that the left cosets of H in G are the equivalence classes of a certain equivalence relation. By "defining" f as above we are giving a definition based on particular representatives of these equivalence classes, and it may be possible that $aH = bH$ but $Ha \neq Hb$. In other words, we must determine whether f is well-defined.

In fact, in general the above f is not well-defined. Consider our standard example of $G = S_3$ and $H = \langle (1\ 2) \rangle$. Checking our above computations, we have $(1\ 3)H = (1\ 2\ 3)H$ but $H(1\ 3) \neq H(1\ 2\ 3)$. Therefore, in this particular case, that choice of f is not well-defined. We need to define f differently to make it well-defined in general, and the following lemma is the key to do so.

Lemma 5.7.11. *Let H be a subgroup of G and let $a, b \in G$. The following are equivalent.*

1. $aH = bH$.
2. $Ha^{-1} = Hb^{-1}$.

Proof. Suppose that $aH = bH$. We then have that $a^{-1}b \in H$ so using the fact that $(b^{-1})^{-1} = b$, we see that $a^{-1}(b^{-1})^{-1} \in H$. It follows that $Ha^{-1} = Hb^{-1}$.

Suppose conversely that $Ha^{-1} = Hb^{-1}$. We then have that $a^{-1}(b^{-1})^{-1} \in H$ so using the fact that $(b^{-1})^{-1} = b$, we see that $a^{-1}b \in H$. It follows that $aH = bH$. □

We can now prove our result.

Proposition 5.7.12. *Let G be a group and let H be a subgroup of G. Let $\mathcal{L}_H$ be the set of left cosets of H in G and let $\mathcal{R}_H$ be the set of right cosets of H in G. Define $f \colon \mathcal{L}_H \to \mathcal{R}_H$ by letting $f(aH) = Ha^{-1}$. We then have that f is a well-defined bijection from $\mathcal{L}_H$ onto $\mathcal{R}_H$. In particular, $|\mathcal{L}_H| = |\mathcal{R}_H|$.*

Proof. Notice that f is well-defined by the above lemma because if $aH = bH$, then

$$f(aH) = Ha^{-1} = Hb^{-1} = f(bH).$$

We next check that f is injective. Suppose that $f(aH) = f(bH)$, so that $Ha^{-1} = Hb^{-1}$. By the other direction of the lemma, we have that $aH = bH$. Therefore, f is injective.

Finally, we need to check that f is surjective. Fix an element of $\mathcal{R}_H$, say Hb. We then have that $b^{-1}H \in \mathcal{L}_H$ and

$$f(b^{-1}H) = H(b^{-1})^{-1} = Hb.$$

Hence, $\text{range}(f) = \mathcal{R}_H$, so f is surjective.

Putting it all together, we conclude that f is a well-defined bijection from $\mathcal{L}_H$ onto $\mathcal{R}_H$. □

Definition 5.7.13. *Let G be a group and let H be a subgroup of G. We define $[G : H]$ to be the number of left cosets of H in G (or equivalently the number of right cosets of H in G). That is, $[G : H]$ is the number of equivalence classes of G under the equivalence relation $\sim_H$. If there are infinitely many left cosets (or equivalently infinitely many right cosets), we write $[G : H] = \infty$. We call $[G : H]$ the* index *of H in G.*

For example, we saw above that $[S_3 : \langle (1\ 2) \rangle] = 3$. For any $n \in \mathbb{N}^+$, we have $[\mathbb{Z} : n\mathbb{Z}] = n$ because the left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}$.

5.8 Lagrange's Theorem

We are now in position to prove one of the most fundamental theorems about finite groups. We start with a proposition.

Proposition 5.8.1. *Let G be a group and let H be a subgroup of G. Let $a \in G$. Define a function $f \colon H \to aH$ by letting $f(h) = ah$. We then have that f is a bijection, so $|H| = |aH|$. In other words, all left cosets of H in G have the same size.*

Proof. Notice that f is surjective because if $b \in aH$, then we may fix $h \in H$ with $b = ah$, and notice that $f(h) = ah = b$, so $b \in \text{range}(f)$. Suppose that $h_1, h_2 \in H$ and that $f(h_1) = f(h_2)$. We then have that $ah_1 = ah_2$, so by canceling the a's on the left (i.e. multiplying on the left by a^{-1}), we conclude that $h_1 = h_2$. Therefore, f is injective. Putting this together with the fact that f is surjective, we conclude that f is a bijection. The result follows. □

Theorem 5.8.2 (Lagrange's Theorem)**.** *Let G be a finite group and let H be a subgroup of G. We have*

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

In particular, $|H|$ divides $|G|$ and

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

Proof. The previous proposition shows that the $[G : H]$ many left cosets of H in G each have cardinality $|H|$. Since G is partitioned into $[G : H]$ many sets each of size $|H|$, we conclude that $|G| = [G : H] \cdot |H|$. □

For example, instead of finding all of the left cosets of $\langle(1\ 2)\rangle$ in S_3 to determine that $[S_3 : \langle(1\ 2)\rangle] = 3$, we could have simply calculated

$$[S_3 : \langle(1\ 2)\rangle] = \frac{|S_3|}{|\langle(1\ 2)\rangle|} = \frac{6}{2} = 3.$$

Notice the assumption in Lagrange's Theorem that G is finite. It makes no sense to calculate $[\mathbb{Z} : n\mathbb{Z}]$ in this manner (if you try to write $\frac{\infty}{\infty}$ you will make me very angry). We end this section with several simple consequences of Lagrange's Theorem.

Corollary 5.8.3. *Let G be a finite group. Let K be a subgroup of G and let H be a subgroup of K. We then have*

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

Proof. Since G is finite (and hence trivially both H and K are finite) we may use Lagrange's Theorem to note that

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

□

Corollary 5.8.4. *Let G be a finite group and let $a \in G$. We then have that $|a|$ divides $|G|$.*

Proof. Let $H = \langle a \rangle$. By Proposition 5.2.3, we know that H is a subgroup of G and $|a| = |H|$. Therefore, by Lagrange's Theorem, we may conclude that $|a|$ divides $|G|$. □

Corollary 5.8.5. *Let G be a finite group. We then have that $a^{|G|} = e$ for all $a \in G$.*

Proof. Let $m = |a|$. By the previous corollary, we know that $m \mid |G|$. Therefore, by Proposition 4.6.5, it follows that $a^{|G|} = e$. □

Theorem 5.8.6. *Every group of prime order is cyclic (so in particular every group of prime order is abelian). In fact, if G is a group of prime order, then every nonidentity element is a generator of G.*

Proof. Let $p = |G|$ be the prime order of G. Suppose that $c \in G$ with $c \neq e$. We know that $|c|$ divides p, so as p is prime we must have that either $|c| = 1$ or $|c| = p$. Since $c \neq e$, we must have $|c| = p$. By Proposition 5.2.6, we conclude that c is a generator of G. Hence, every nonidentity element of G is a generator of G. □

Theorem 5.8.7 (Euler's Theorem)**.** *Let $n \in \mathbb{N}^+$ and let $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. We then have $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Proof. We apply Corollary 5.8.5 to the group $U(\mathbb{Z}/n\mathbb{Z})$. Since $\gcd(a, n) = 1$, we have that $\overline{a} \in U(\mathbb{Z}/n\mathbb{Z})$. Since $|U(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$, Corollary 5.8.5 tells us that $\overline{a}^{\varphi(n)} = \overline{1}$. Therefore, $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

Corollary 5.8.8 (Fermat's Little Theorem)**.** *Let $p \in \mathbb{N}^+$ be prime.*

1. *If $a \in \mathbb{Z}$ with $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*
2. *If $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$.*

Proof. We first prove 1. Suppose that $a \in \mathbb{Z}$ with $p \nmid a$. We then have that $\gcd(a, p) = 1$ (because $\gcd(a, p)$ divides p, so it must be either 1 or p, but it can not be p since $p \nmid a$). Now using the fact that $\varphi(p) = p - 1$, we conclude from Euler's Theorem that $a^{p-1} \equiv 1 \pmod{p}$.

We next prove 2. Suppose that $a \in \mathbb{Z}$. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$ by part 1, so multiplying both sides by a gives $a^p \equiv a \pmod{p}$. Now if $p \mid a$, then we trivially have $p \mid a^p$ as well, so $p \mid (a^p - a)$ and hence $a^p \equiv a \pmod{p}$. □

Chapter 6

Quotients and Homomorphisms

6.1 Quotients of Abelian Groups

The quotient construction is one of the most subtle but important constructions in group theory (and algebra more generally). As suggested by the name, the quotient should somehow be "smaller" than G. Given a group G together with a subgroup H, the idea is to build a new group G/H that is obtained by "trivializing" H. We already know that we obtain an equivalence relation $\sim_H$ from H that breaks up the group G into cosets. The fundamental idea is to make a new group whose elements are these cosets. However, the first question we need to ask ourselves is whether we will use left cosets or right cosets (i.e. which version of $\sim_H$ will we work with). To avoid this issue, and to focus on the key elements of the construction first, we will begin by assuming that our group is abelian so that there is no worry about which side we work on. As we will see, this abelian assumption helps immensely in other ways as well.

Suppose then that G is an abelian group and that H is a subgroup of G. We let G/H be the set of all (left) cosets of H in G, so elements of G/H are of the form aH for some $a \in G$. In the language established when discussing equivalence relations, we are looking at the set $G/{\sim_H}$, but we simplify the notation and just write G/H. Now that we have decided what the elements of G/H are, we need to define the operation. How should we define the product of aH and bH? The natural idea is simply to define $(aH) \cdot (bH) = (ab)H$. That is, given the two cosets aH and bH, take the product ab in G and form its coset. Alarm bells should immediately go off in your head and you should be asking: Is this well-defined? After all, a coset has many different representatives. What if $aH = cH$ and $bH = dH$? On the one hand, the product should be $(ab)H$ and on the other the product should be $(cd)H$. Are these necessarily the same? Recall that we are dealing with equivalence classes so $aH = bH$ if and only if $a \sim_H b$. The next proposition says that everything is indeed well-defined in the abelian case we are currently considering.

Proposition 6.1.1. *Let G be an abelian group and let H be a subgroup of G. Suppose that $a \sim_H c$ and $b \sim_H d$. We then have that $ab \sim_H cd$.*

Proof. Fix $h, k \in H$ such that $ah = c$ and $bk = d$. We then have that

$$cd = ahbk = abhk.$$

Now $hk \in H$ because H is a subgroup of G. Since $cd = ab \cdot hk$, it follows that $ab \sim_H cd$. $\square$

Notice how fundamentally we used the fact that G was abelian in this proof to write $hb = bh$. Overcoming this apparent stumbling block will be our primary focus when we get to nonabelian groups.

For example, suppose that $G = \mathbb{R}^2$ and $H = \{(0, b) : b \in \mathbb{R}\}$ is the y-axis. Again, we will write $(a, b) + H$ for the left coset of H In G. The elements of the quotient group G/H are the left cosets of H in G, which we know are the set of vertical lines in the plane. Let's examine how we add two elements of G/H. The definition says that we add left cosets by finding representatives of those cosets, adding those representatives, and then taking the left coset of the result. In other words, to add two vertical lines, we pick points on the lines, add those points, and output the line containing the result. For example, we add the cosets $(3,2)+H$ and $(4,-7)+H$ by computing $(3,2)+(4,-7)=(7,-5)$ and outputting the corresponding coset $(7,-5)+H$. In other words, we have

$$((3,2)+H)+((4,-7)+H)=(7,-5)+H.$$

Now we could have chosen different representatives of those two cosets. For example, we have $(3,2)+H=(3,16)+H$ (after all both are on the line $x=3$) and $(4,-7)+H=(4,1)+H$, and if we calculate the sum using these representatives we see that

$$((3,16)+H)+((4,1)+H)=(7,17)+H.$$

Now although the elements of G given by $(7,-5)$ and $(7,17)$ are different, the cosets $(7,-5)+H$ and $(7,17)+H$ are equal because $(7,-5)\sim_H(7,17)$.

We are now ready to formally define the quotient of an abelian group G by a subgroup H. We verify that the given definition really is a group in the proposition immediately after the definition.

Definition 6.1.2. *Let G be an abelian group and let H be a subgroup of G. We define a new group, called the* quotient *of G by H and denoted G/H, by letting the elements be the left cosets of H in G (i.e. the equivalence classes of G under $\sim_H$), and defining the binary operation $aH\cdot bH=(ab)H$. The identity is eH (where e is the identity of G) and the inverse of aH is $a^{-1}H$.*

Proposition 6.1.3. *Let G be an abelian group and let H be a subgroup of G. The set G/H with the operation just defined is indeed a group with $|G/H|=[G:H]$. Furthermore, it is an abelian group.*

Proof. We verified that the operation $aH\cdot bH=(ab)H$ is well-defined in Proposition 6.1.1. With that in hand, we just need to check the group axioms.

We first check that the $\cdot$ is an associative operation on G/H. For any $a,b,c\in G$ we have

$$\begin{aligned}(aH\cdot bH)\cdot cH&=(ab)H\cdot cH\\&=((ab)c)H\\&=(a(bc))H&&\text{(since }\cdot\text{ is associative on }G)\\&=aH\cdot(bc)H\\&=aH\cdot(bH\cdot cH).\end{aligned}$$

We next check that eH is an identity. For any $a\in G$ we have

$$aH\cdot eH=(ae)H=aH$$

and

$$eH\cdot aH=(ea)H=aH.$$

For inverses, notice that given any $a\in G$, we have

$$aH\cdot a^{-1}H=(aa^{-1})H=eH$$

and

$$a^{-1}H\cdot aH=(a^{-1}a)H=eH.$$

Thus, G/H is indeed a group, and it has order $[G : H]$ because the elements are the left cosets of H in G. Finally, we verify that G/H is abelian by noting that for any $a, b \in G$, we have

$$\begin{aligned} aH \cdot bH &= (ab)H \\ &= (ba)H && \text{(since } G \text{ is abelian)} \\ &= bH \cdot aH. \end{aligned}$$

□

Here is another example. Suppose that $G = U(\mathbb{Z}/18\mathbb{Z})$ and let $H = \langle 17 \rangle = \{\overline{1}, \overline{17}\}$. We then have that the left cosets of H in G are:

- $\overline{1}H = \overline{17}H = \{\overline{1}, \overline{17}\}$.
- $\overline{5}H = \overline{13}H = \{\overline{5}, \overline{13}\}$.
- $\overline{7}H = \overline{11}H = \{\overline{7}, \overline{11}\}$.

Therefore, $|G/H| = 3$. To multiply two cosets, we choose representatives and multiply. For example, we could calculate

$$\overline{5}H \cdot \overline{7}H = (\overline{5} \cdot \overline{7})H = \overline{17}H.$$

We can multiply the exact same two cosets using different representatives. For example, we have $\overline{7}H = \overline{11}H$, so we could calculate

$$\overline{5}H \cdot \overline{11}H = (\overline{5} \cdot \overline{11})H = \overline{1}H.$$

Notice that we obtained the same answer since $\overline{1}H = \overline{17}H$. Now there is no canonical choice of representatives for the various cosets, so if you want to give each element of G/H a unique "name", then you simply have to pick which representative of each coset you will use. We will choose (somewhat arbitrarily) to view G/H as the following:

$$G/H = \{\overline{1}H, \overline{5}H, \overline{7}H\}.$$

Here is the Cayley table of G/H using these choices of representatives.

$\cdot$	$\overline{1}H$	$\overline{5}H$	$\overline{7}H$
$\overline{1}H$	$\overline{1}H$	$\overline{5}H$	$\overline{7}H$
$\overline{5}H$	$\overline{5}H$	$\overline{7}H$	$\overline{1}H$
$\overline{7}H$	$\overline{7}H$	$\overline{1}H$	$\overline{5}H$

Again, notice that using the definition we have $\overline{5}H \cdot \overline{7}H = \overline{17}H$, but since $\overline{17}$ was not one of our chosen representatives and $\overline{17}H = \overline{1}H$ where $\overline{1}$ is one of our chosen representatives, we used $\overline{5}H \cdot \overline{7}H = \overline{1}H$ in the above table.

Finally, let us take a moment to realize that we have been dealing with quotient groups all along when working with $\mathbb{Z}/n\mathbb{Z}$. This group is exactly the quotient of the group $G = \mathbb{Z}$ under addition by the subgroup $H = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. Recall from Section 5.7 that given $a, b \in \mathbb{Z}$, we have

$$a \sim_{n\mathbb{Z}} b \Longleftrightarrow a \equiv b \pmod{n}$$

so the left cosets of $n\mathbb{Z}$ are precisely the equivalence classes of $\equiv_n$. Stated in symbols, if $\overline{a}$ is the equivalence class of a under $\equiv_n$, then $\overline{a} = a + n\mathbb{Z}$ (we are again using $+$ in left cosets because that is the operation in $\mathbb{Z}$). Furthermore, our definition of the operation in $\mathbb{Z}/n\mathbb{Z}$ was given by

$$\overline{a} + \overline{b} = \overline{a + b}.$$

However, in terms of cosets, this simply says

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z},$$

which is exactly our definition of the operation in the quotient $\mathbb{Z}/n\mathbb{Z}$. Therefore, the group $\mathbb{Z}/n\mathbb{Z}$ is precisely the quotient of the group $\mathbb{Z}$ by the subgroup $n\mathbb{Z}$, which is the reason why we have used that notation all along.

6.2 Normal Subgroups and Quotient Groups

In discussing quotients of abelian groups, we used the abelian property in two places. The first place was to avoid choosing whether we were dealing with left cosets or right cosets (since they will be the same whenever G is abelian). The second place we used commutativity was in checking that the group operation on the quotient was well-defined. Now the first choice of left/right cosets doesn't seem so hard to overcome because we can simply choose one. For the moment, say we choose to work with left cosets. However, the well-defined issue looks like it might be hard to overcome because we used commutativity in what appears to be a very central manner. Let us recall our proof. We had a subgroup H of an abelian group G, and we were assuming $a \sim_H c$ and $b \sim_H d$. We then fixed $h, k \in H$ with $ah = c$ and $bk = d$ and observed that

$$cd = ahbk = abhk,$$

hence $ab \sim_H cd$ because $hk \in H$. Notice the key use of commutativity to write $hb = bh$. In fact, we can easily see that the operation is not always well-defined if G is nonabelian. Consider our usual example of $G = S_3$ with $H = \langle(1\ 2)\rangle = \{id, (1\ 2)\}$. We computed the left cosets in Section 5.7:

- $idH = (1\ 2)H = \{id, (1\ 2)\}$.
- $(1\ 3)H = (1\ 2\ 3)H = \{(1\ 3), (1\ 2\ 3)\}$.
- $(2\ 3)H = (1\ 3\ 2)H = \{(2\ 3), (1\ 3\ 2)\}$.

Thus, we have $id \sim_H (1\ 2)$ and $(1\ 3) \sim_H (1\ 2\ 3)$. Now $id(1\ 3) = (1\ 3)$ and $(1\ 2)(1\ 2\ 3) = (2\ 3)$, but a quick look at the left cosets shows that $(1\ 3) \not\sim_H (2\ 3)$. Hence

$$id(1\ 3) \not\sim_H (1\ 2)(1\ 2\ 3).$$

In other words, the operation $\sigma H \cdot \tau H = (\sigma\tau)H$ is not well-defined because on the one hand we would have

$$idH \cdot (1\ 3)H = (1\ 3)H,$$

and on the other hand

$$(1\ 2)H \cdot (1\ 2\ 3)H = (2\ 3)H,$$

which contradicts the definition of a function since $(1\ 3)H \neq (2\ 3)H$.

With the use of commutativity so essential in our well-defined proof and a general counterexample in hand, it might appear that we have little hope in dealing with nonabelian groups. We just showed that we have no hope for an arbitrary subgroup H of G, but maybe we get by with some special subgroups. Recall again our proof that used

$$cd = ahbk = abhk.$$

We do really need to get b next to a, and with a little thought, we can find some wiggle room. For example, one way we could get by is if $H \subseteq Z(G)$. Under this assumption, the elements of H commute with everything in G, so the above argument still works. This suffices, but it is very restrictive. We can make things work with even less. Suppose that we weaken the assumption that H commutes with all elements of G to the following:

For all $g \in G$ and all $h \in H$, there exists $\ell \in H$ with $hg = g\ell$.

In other words, we do not need to be able to move b past h in a manner which does not disturb h at all, but instead we could get by with moving b past h in a manner which changes h to perhaps a different element of H.

It turns out that the above condition on a subgroup H of a group G is equivalent to many other fundamental concepts. First, we introduce the following definition.

Definition 6.2.1. *Let G be a group and let H be a subgroup of G. Given $g \in G$, we define*

$$gHg^{-1} = \{ghg^{-1} : g \in G, h \in H\}.$$

Proposition 6.2.2. *Let G be a group and let H be a subgroup of G. The following are equivalent:*

1. *For all $g \in G$ and all $h \in H$, there exists $\ell \in H$ with $hg = g\ell$.*
2. *For all $g \in G$ and all $h \in H$, there exists $\ell \in H$ with $gh = \ell g$.*
3. *$g^{-1}hg \in H$ for all $g \in G$ and all $h \in H$.*
4. *$ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$.*
5. *$gHg^{-1} \subseteq H$ for all $g \in G$.*
6. *$gHg^{-1} = H$ for all $g \in G$.*
7. *$Hg \subseteq gH$ for all $g \in G$.*
8. *$gH \subseteq Hg$ for all $g \in G$.*
9. *$gH = Hg$ for all $g \in G$.*

Proof.

- (1) $\Rightarrow$ (2): Suppose that we know (1). Let $g \in G$ and let $h \in H$. Applying (1) with $g^{-1} \in G$ and $h \in H$, we may fix $\ell \in H$ with $hg^{-1} = g^{-1}\ell$. Multiplying on the left by g we see that $ghg^{-1} = \ell$, and then multiplying on the right by g we conclude that $gh = \ell g$.

- (2) $\Rightarrow$ (1): Suppose that we know (2). Let $g \in G$ and let $h \in H$. Applying (2) with $g^{-1} \in G$ and $h \in H$, we may fix $\ell \in H$ with $g^{-1}h = \ell g^{-1}$. Multiplying on the right by g we see that $g^{-1}hg = \ell$, and then multiplying on the left by g we conclude that $hg = g\ell$.

- (1) $\Rightarrow$ (3): Suppose that we know (1). Let $g \in G$ and let $h \in H$. By (1), we may fix $\ell \in H$ with $hg = g\ell$. Multiplying on the left by g^{-1}, we see that $g^{-1}hg = \ell \in H$. Since $g \in G$ and $h \in H$ were arbitrary, we conclude that $g^{-1}hg \in H$ for all $g \in G$ and all $h \in H$.

- (3) $\Rightarrow$ (1): Suppose that we know (3). Let $g \in G$ and let $h \in H$. Now

  $$hg = ehg = (gg^{-1})hg = g(g^{-1}hg)$$

  and by (3) we know that $g^{-1}hg \in H$. Thus we have (1).

- (2) $\Leftrightarrow$ (4): This follows in exactly that same manner as (1) $\Leftrightarrow$ (3).

- (4) $\Leftrightarrow$ (5): These two are simply restatements of each other.

- (5) $\Rightarrow$ (6): Suppose we know (5). To prove (6), we need only prove that $H \subseteq gHg^{-1}$ for all $g \in G$ (since the reverse containment is given to us). Let $g \in G$ and let $h \in H$. By (5) applied to g^{-1}, we see that $g^{-1}H(g^{-1})^{-1} \subseteq H$, hence $g^{-1}Hg \subseteq H$ and in particular we conclude that $g^{-1}hg \in H$. Since

$$h = ehe = (gg^{-1})h(gg^{-1}) = g(g^{-1}hg)g^{-1}$$

  and $g^{-1}hg \in H$, we see that $h \in gHg^{-1}$. Since $g \in G$ and $h \in H$ were arbitrary, it follows that $H \subseteq gHg^{-1}$ for all $g \in G$.

- (6) $\Rightarrow$ (5): This is trivial.
- (1) $\Leftrightarrow$ (7): These two are simply restatements of each other.
- (2) $\Leftrightarrow$ (8): These two are simply restatements of each other.
- (9) $\Rightarrow$ (8): This is trivial.
- (7) $\Rightarrow$ (9): Suppose that we know (7). Since (7) $\Rightarrow$ (1) $\Rightarrow$ (2) $\Rightarrow$ (8), it follows that we know (8) as well. Putting (7) and (8) together, we conclude (9).

$\square$

As the Proposition shows, the condition we are seeking to ensure that multiplication of left cosets is well-defined is equivalent to the condition that the left cosets of H in G are equal to the right cosets of H in G. Thus, by adopting that condition we automatically get rid of the other problematic question of which side to work on. This condition is shaping up to be so useful that we given the subgroups which satisfy it a special name.

Definition 6.2.3. *Let G be a group and let H be a subgroup of G. We say that H is a* normal subgroup *of G if $gHg^{-1} \subseteq H$ for all $g \in G$ (or equivalently any of properties in the previous proposition hold).*

Our entire goal in defining and exploring the concept of a normal subgroup H of a group G was to allow us to prove that multiplication of left cosets via representatives is well-defined. It turns out that this condition is precisely equivalent to this operation being well-defined.

Proposition 6.2.4. *Let G be an group and let H be a subgroup of G. The following are equivalent:*

1. *H is a normal subgroup of G.*
2. *Whenever $a, b, c, d \in G$ with $a \sim_H c$ and $b \sim_H d$, we have $ab \sim_H cd$. (Here, $\sim_H$ is the equivalence relation corresponding to left cosets.)*

Proof. We first prove that (1) $\Rightarrow$ (2). Suppose that $a, b, c, d \in G$ with $a \sim_H c$ and $b \sim_H d$. Fix $h, k \in H$ such that $ah = c$ and $bk = d$. Since H is a normal subgroup of G, we may fix $\ell \in H$ with $hb = b\ell$. We then have that

$$cd = ahbk = ab\ell k.$$

Now $\ell k \in H$ because H is a subgroup of G. Since $cd = ab \cdot \ell k$, it follows that $ab \sim_H cd$.

We now prove that (2) $\Rightarrow$ (1). Assume (2). We prove that H is a normal subgroup of G by showing that $g^{-1}hg \in H$ for all $g \in G$ and $h \in H$. Let $g \in G$ and let $h \in H$. Notice that we have $e \sim_H h$ because $eh = h$ and $g \sim_H g$ because $ge = g$. Since we are assuming (2), it follows that $eg \sim_H hg$ and hence $g \sim_H hg$. Fix $k \in H$ with $gk = hg$. Multiplying on the left by g^{-1} we get $k = g^{-1}hg$ so $g^{-1}hg \in H$. The result follows. $\square$

For example, $A_3 = \langle (1\ 2\ 3) \rangle$ is a normal subgroup of S_3. To show this, we can directly compute the cosets (although we will see a faster method soon). The left cosets of A_3 in S_3 are:

- $idA_3 = (1\ 2\ 3)A_3 = (1\ 3\ 2)A_3 = \{id, (1\ 2\ 3), (1\ 3\ 2)\}$.

- $(1\ 2)A_3 = (1\ 3)A_3 = (2\ 3)A_3 = \{(1\ 2), (1\ 3), (2\ 3)\}$.

The right cosets of A_3 in S_3 are:

- $A_3 id = A_3(1\ 2\ 3) = A_3(1\ 3\ 2) = \{id, (1\ 2\ 3), (1\ 3\ 2)\}$.
- $A_3(1\ 2) = A_3(1\ 3) = A_3(2\ 3) = \{(1\ 2), (1\ 3), (2\ 3)\}$.

Thus, $\sigma A_3 = A_3\sigma$ for all $\sigma \in S_3$ and hence A_3 is a normal subgroup of S_3.

Proposition 6.2.5. *Let G be a group and let H be a subgroup of G. If $H \subseteq Z(G)$, then H is a normal subgroup of G.*

Proof. For any $g \in G$ and $h \in H$, we have $hg = gh$ because $h \in Z(G)$. Therefore, H is a normal subgroup of G by Condition 1 above. □

Proposition 6.2.6. *Let G be a group and let H be a subgroup of G. If $[G : H] = 2$, then H is a normal subgroup of G.*

Proof. Since $[G : H] = 2$, we know that there are exactly two distinct left cosets of H in G and exactly two distinct right cosets of H in G. One left coset of H in G is $eH = H$. Since the left cosets partition G and there are only two of them, it must be the case that the other left coset of H in G is the set $G\backslash H$ (that is the set G with the set H removed). Similarly, one right coset of H in G is $He = H$. Since the right cosets partition G and there are only two of them, it must be the case that the other right coset of H in G is the set $G\backslash H$.

To show that H is a normal subgroup of G, we know that it suffices to show that $gH = Hg$ for all $g \in G$ (by Proposition 6.2.2). Let $g \in G$ be arbitrary. We have two cases.

- Suppose that $g \in H$. We then have that $g \in gH$ and $g \in eH$, so $gH \cap eH \neq \emptyset$ and hence $gH = eH = H$. We also have that $g \in Hg$ and $g \in He$, so $Hg \cap He \neq \emptyset$ and hence $Hg = He = H$. Therefore $gH = H = Hg$.
- Suppose that $g \notin H$. We then have $g \notin eH$, so $gH \neq eH$, and hence we must have $gH = G\backslash H$ (because it is the only other left coset). We also have $g \notin He$, so $Hg \neq He$, and hence $Hg = G\backslash H$. Therefore $gH = G\backslash H = Hg$.

Thus, for any $g \in G$, we have $gH = Hg$. It follows that H is a normal subgroup of G. □

Since $[S_3 : A_3] = 2$, this proposition gives a different way to prove that A_3 is a normal subgroup of S_3 without doing all of the calculations we did above. In fact, we get the following.

Corollary 6.2.7. *A_n is a normal subgroup of S_n for all $n \in \mathbb{N}^+$.*

Proof. This is trivial if $n = 1$. When $n \geq 2$, we have

$$\begin{aligned} [S_n : A_n] &= \frac{|S_n|}{|A_n|} \\ &= \frac{n!}{n!/2} && \text{(by Proposition 5.3.12)} \\ &= 2, \end{aligned}$$

so A_n is a normal subgroup of S_n by Proposition 6.2.6. □

Corollary 6.2.8. *For any $n \geq 3$, the subgroup $H = \langle r \rangle$ is a normal subgroup of D_n.*

Proof. We have $|H| = |r| = n$ and $|D_n| = 2n$, so again this follows from Proposition 6.2.6. □

We are now in a position to define the quotient of a (possibly nonabelian) group G by a normal subgroup H. As in the abelian case, we verify that the definition really is a group immediately afterwards.

Definition 6.2.9. *Let G be an group and let H be a normal subgroup of G. We define a new group, called the* quotient *of G by H and denoted G/H, by letting the elements be the left cosets of H in G (i.e. the equivalence classes of G under $\sim_H$), and defining the binary operation $aH \cdot bH = (ab)H$. The identity is eH (where e is the identity of G) and the inverse of aH is $a^{-1}H$.*

Proposition 6.2.10. *Let G be a group and let H be a normal subgroup of G. The set G/H with the operation just defined is indeed a group with $|G/H| = [G : H]$.*

Proof. We verified that the operation $aH \cdot bH = (ab)H$ is well-defined in Proposition 6.2.4. With that in hand, we just need to check the group axioms.

We first check that $\cdot$ is an associative operation on G/H. For any $a, b, c \in G$ we have

$$\begin{aligned}
(aH \cdot bH) \cdot cH &= (ab)H \cdot cH \\
&= ((ab)c)H \\
&= (a(bc))H && \text{(since } \cdot \text{ is associative on } G\text{)} \\
&= aH \cdot (bc)H \\
&= aH \cdot (bH \cdot cH).
\end{aligned}$$

We next check that eH is an identity. For any $a \in G$ we have

$$aH \cdot eH = (ae)H = aH$$

and

$$eH \cdot aH = (ea)H = aH.$$

For inverses, notice that given any $a \in G$, we have

$$aH \cdot a^{-1}H = (aa^{-1})H = eH$$

and

$$a^{-1}H \cdot aH = (a^{-1}a)H = eH.$$

Thus, G/H is indeed a group, and it has order $[G : H]$ because the elements are the left cosets of H in G. □

For example, suppose that $G = D_4$ and $H = Z(G) = \{e, r^2\}$. We know from Proposition 6.2.5 that H is a normal subgroup of G. The left cosets (and hence right cosets because H is normal in G) of H in G are:

- $eH = r^2H = \{e, r^2\}$.
- $rH = r^3H = \{r, r^3\}$.
- $sH = r^2sH = \{s, r^2s\}$.
- $rsH = r^3sH = \{rs, r^3s\}$.

As usual, there are no "best" choices of representatives for these cosets when we consider G/H. We choose to take

$$G/H = \{eH, rH, sH, rsH\}.$$

The Cayley table of G/H using these representatives is:

$\cdot$	eH	rH	sH	rsH
eH	eH	rH	sH	rsH
rH	rH	eH	rsH	sH
sH	sH	rsH	eH	rH
rsH	rsH	sH	rH	eH

Notice that we had to switch to our "chosen" representatives several times when constructing this table. For example, we have

$$rH \cdot rH = r^2H = eH,$$

and

$$sH \cdot rH = srH = r^{-1}sH = r^3sH = rsH.$$

Examining the table, we see a few interesting facts. The group G/H is abelian even though G is not abelian. Furthermore, every nonidentity element of G/H has order 2 even though r itself has order 4. We next see how the order of an element in the quotient relates to the order of the representative in the original group.

Proposition 6.2.11. *Let G be a group and let H be a normal subgroup of G. Suppose that $a \in G$ has finite order. The order of aH (in the group G/H) is finite and divides the order of a (in the group G).*

Proof. Let $n = |a|$ (in the group G). We have $a^n = e$, so

$$(aH)^n = a^nH = eH.$$

Now eH is the identity of G/H, so we have found some power of the element aH which gives the identity in G/H. Thus, aH has finite order. Let $m = |aH|$ (in the group G/H). Since we checked that n is a power of aH giving the identity, it follow from Proposition 4.6.5 that $m \mid n$. ☐

It is possible that $|aH|$ is strictly smaller than $|a|$. In the above example of D_4, we have $|r| = 4$ but $|rH| = 2$. Notice however that $2 \mid 4$ as the previous proposition proves must be the case.

We now show how it is possible to prove theorems about groups using quotients and induction. The general idea is as follows. Given a group G, proper subgroups of G and nontrivial quotients of G (that is by normal subgroups other than $\{e\}$ and G) are "smaller" than G. So the idea is to prove a result about finite groups by using induction on the order of the group. By the inductive hypothesis, we know information about the proper subgroups and nontrivial quotients, so the hope is to piece together that information to prove the result about G. We give an example of this technique by proving the following theorem.

Theorem 6.2.12. *Let $p \in \mathbb{N}^+$ be prime. If G is a finite abelian group with $p \mid |G|$, then G has an element of order p.*

Proof. The proof is by (strong) induction on $|G|$. If $|G| = 1$, then the result is trivial because $p \nmid 1$ (if you don't like this vacuous base case, simply note the if $|G| = p$, then every nonidentity element of G has order p by Lagrange's Theorem). Suppose then that G is a finite group with $p \mid |G|$, and suppose that the result is true for all groups K satisfying $p \mid |K|$ and $|K| < |G|$. Fix $a \in G$ with $a \neq e$, and let $H = \langle a \rangle$. We then have that H is a normal subgroup of G because G is abelian. We now have two cases:

- *Case 1:* Suppose that $p \mid |a|$. By Proposition 4.6.10, G has an element of order p.
- *Case 2:* Suppose that $p \nmid |a|$. We have

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

so $|G| = |H| \cdot |G/H|$. Since $p \mid |G|$ and $p \nmid |H|$ (because $|H| = |a|$), it follows that $p \mid |G/H|$. Now $|G/H| < |G|$ because $|H| > 1$, so by induction there exists an element $bH \in G/H$ with $|bH| = p$. By Proposition 6.2.11, we may conclude that $p \mid |b|$. Therefore, by Proposition 4.6.10, G has an element of order p.

In either case, we have concluded that G has an element of order p. The result follows by induction. $\square$

Notice where we used the two fundamental assumptions that p is prime and that G is abelian. For the prime assumption, we used the key fact that if $p \mid ab$, then either $p \mid a$ or $p \mid b$. In fact, the result is not true if we omit the assumption that p is prime. The abelian group $U(\mathbb{Z}/8\mathbb{Z})$ has order 4 but it has no element of order 4.

We made use of the abelian assumption to get that H was a normal subgroup of G without any work. In general, with a little massaging, we could slightly alter the above proof as long as we could assume that every group has some normal subgroup other than the two trivial normal subgroups $\{e\}$ and G (because this would allow us to either use induction on H or on G/H). Unfortunately, it is not in general true that every group always has such a normal subgroup. Those that do not are given a name.

Definition 6.2.13. *A group G is* simple *if $|G| \neq 1$ and the only normal subgroups of G are $\{e\}$ and G.*

A simple group is a group that we are unable to "break up" into a smaller normal subgroup H and corresponding smaller quotient G/H. They are the "atoms" of the groups and are analogous to the primes. In fact, every group G that has prime order is simple for the trivial reason that the only subgroups of such a G are $\{e\}$ and all of G by Lagrange's Theorem. It turns out that these are the only simple abelian groups (see homework). Now if these were the only simple groups at all, there would not be much of problem because they are quite easy to get a handle on. However, there are infinitely many finite simple nonabelian groups. For example, we will see later that A_n is a simple group for all $n \geq 5$. The existence of these groups is a serious obstruction to any inductive proof for all groups in the above style. Nonetheless, the above theorem is true for all groups (including nonabelian ones), and the result is known as Cauchy's Theorem. We will prove it later (see Theorem 8.3.7) using more advanced tools, but we will start that proof knowing that we have already handled the abelian case.

6.3 Isomorphisms

Definitions and Examples

We have developed several ways to construct groups. We started with well-known groups like $\mathbb{Z}$, $\mathbb{Q}$ and $GL_n(\mathbb{R})$. From there, we introduced the groups $\mathbb{Z}/n\mathbb{Z}$ and $U(\mathbb{Z}/n\mathbb{Z})$. After that, we developed our first family of nonabelian groups in the symmetric groups S_n. With those in hand, we obtained many other groups as subgroups of these, such as $SL_n(\mathbb{R})$, A_n, and D_n. Finally, we built new groups from all of these using direct products and quotients.

With such a rich supply on groups now, it is time to realize that some of these groups are essentially the "same". For example, let $G = \mathbb{Z}/2\mathbb{Z}$, let $H = S_2$, and let K be the group $(\{T, F\}, \oplus)$ where $\oplus$ is "exclusive or" discussed in the first section. Here are the Cayley tables of these groups:

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\circ$	id	$(1\ 2)$
id	id	$(1\ 2)$
$(1\ 2)$	$(1\ 2)$	id

$\oplus$	F	T
F	F	T
T	T	F

Now of course these groups are different because the sets are completely different. The elements of G are equivalence classes and thus subsets of $\mathbb{Z}$, the elements of H are permutations of the set $\{1, 2\}$ (and hence are actually functions), and the elements of K are T and F. Furthermore the operations themselves have little in common since in G we have addition of cosets via representatives, in H we have function composition, and in K we have this funny logic operation. However, despite all these differences, a glance at the above tables tells us that there is a deeper "sameness" to them. For G and H, if we pair off $\overline{0}$ with id and pair off $\overline{1}$ and $(1\ 2)$, then we have provided a kind of "rosetta stone" for translating between the groups. This is formalized with the following definition.

Definition 6.3.1. *Let $(G, \cdot)$ and $(H, \star)$ be groups. An* isomorphism *from G to H is a function $\varphi\colon G \to H$ such that*

1. *φ is a bijection.*
2. *$\varphi(a \cdot b) = \varphi(a) \star \varphi(b)$ for all $a, b \in G$. In shorthand, φ preserves the group operation.*

Thus, an isomorphism $\varphi\colon G \to H$ is a pairing of elements of G with elements of H (that is the bijection part) in such a way that we can either operate on the G side first and then walk over to H, or equivalently can walk over to H with our elements first and then operate on that side. In our case of $G = \mathbb{Z}/2\mathbb{Z}$ and $H = S_2$, we define $\varphi\colon G \to H$ by letting $\varphi(\overline{0}) = id$ and $\varphi(\overline{1}) = (1\ 2)$. Clearly, φ is a bijection. Now we have to check four pairs to check the second property. We have

- $\varphi(\overline{0} + \overline{0}) = \varphi(\overline{0}) = id$ and $\varphi(\overline{0}) + \varphi(\overline{0}) = id \circ id = id$.
- $\varphi(\overline{0} + \overline{1}) = \varphi(\overline{1}) = (1\ 2)$ and $\varphi(\overline{0}) + \varphi(\overline{1}) = id \circ (1\ 2) = (1\ 2)$.
- $\varphi(\overline{1} + \overline{0}) = \varphi(\overline{1}) = (1\ 2)$ and $\varphi(\overline{1}) + \varphi(\overline{0}) = (1\ 2) \circ id = (1\ 2)$.
- $\varphi(\overline{1} + \overline{1}) = \varphi(\overline{0}) = id$ and $\varphi(\overline{1}) + \varphi(\overline{1}) = (1\ 2) \circ (1\ 2) = id$.

Therefore, $\varphi(a + b) = \varphi(a) \circ \varphi(b)$ for all $a, b \in \mathbb{Z}/2\mathbb{Z}$. Since we already noted that φ is a bijection, it follows that φ is an isomorphism. All of these checks are just really implicit in the above table. The bijection $\varphi\colon G \to H$ we defined pairs off $\overline{0}$ with id and pairs off $\overline{1}$ with $(1\ 2)$. Since this aligning of elements carries the table of G to the table of H as seen in the above tables, φ is an isomorphism.

Notice if instead we define $\psi\colon G \to H$ by letting $\psi(\overline{0}) = (1\ 2)$ and $\psi(\overline{1}) = id$, then ψ is not an isomorphism. To see this, we just need to find a counterexample to the second property. We have

$$\psi(\overline{0} + \overline{0}) = \psi(\overline{0}) = (1\ 2),$$

and

$$\psi(\overline{0}) + \psi(\overline{0}) = (1\ 2) \circ (1\ 2) = id,$$

so

$$\psi(\overline{0} + \overline{0}) \neq \psi(\overline{0}) + \psi(\overline{0}).$$

Essentially we are writing the Cayley tables as:

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\circ$	$(1\ 2)$	id
$(1\ 2)$	id	$(1\ 2)$
id	$(1\ 2)$	id

and noting that ψ does not carry the table of G to the table of H (as can be seen in the $(1, 1)$ entry). Thus, even if one bijection is an isomorphism, there may be other bijections which are not. We make the following definition.

Definition 6.3.2. *Let G and H be groups. We say that G and H are* isomorphic*, and write $G \cong H$, if there exists an isomorphism $\varphi\colon G \to H$.*

In colloquial language, two groups G and H are isomorphic exactly when there is *some* way to pair off elements of G with H which maps the Cayley table of G onto the Cayley table of H. For example, we have $U(\mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ via the bijection

$$\varphi(\overline{1}) = (\overline{0}, \overline{0}), \qquad \varphi(\overline{3}) = (\overline{0}, \overline{1}), \qquad \varphi(\overline{5}) = (\overline{1}, \overline{0}), \qquad \text{and} \qquad \varphi(\overline{7}) = (\overline{1}, \overline{1}),$$

as shown by the following tables:

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{7}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{7}$	$\overline{1}$	$\overline{3}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$

$+$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$
$(\overline{1},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$
$(\overline{1},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$

Furthermore, looking back at Section 4.1, we see that the strange group $G = \{3, \aleph, @\}$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ as the following ordering of elements of shows:

$\cdot$	3	$\aleph$	@
3	@	3	$\aleph$
$\aleph$	3	$\aleph$	@
@	$\aleph$	@	3

$+$	$\overline{1}$	$\overline{0}$	$\overline{2}$
$\overline{1}$	$\overline{2}$	$\overline{1}$	$\overline{0}$
$\overline{0}$	$\overline{1}$	$\overline{0}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Also, the 6 element group at the very end of Section 4.1 is isomorphic to S_3:

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

$\circ$	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
id	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	id	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	id	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	id	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	id
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	id	(1 2 3)

The property of being isomorphic has the following basic properties. Roughly, we are saying that isomorphism is an equivalence relation on the set of all groups. Formally, there are technical problems talking about "the set of all groups" (some collections are simply too big to be sets), but let's not dwell on those details here.

Proposition 6.3.3.

1. *For any group G, the function $id_G \colon G \to G$ is an isomorphism, so $G \cong G$.*
2. *If $\varphi \colon G \to H$ is an isomorphism, then $\varphi^{-1} \colon H \to G$ is an isomorphism. In particular, if $G \cong H$, then $H \cong G$.*
3. *If $\varphi \colon G \to H$ and $\psi \colon H \to K$ are isomorphisms, then $\psi \circ \varphi \colon G \to K$ is an isomorphism. In particular, if $G \cong H$ and $H \cong K$, then $G \cong K$.*

Proof.

1. Let $(G, \cdot)$ be a group. The function $id_G \colon G \to G$ is a bijection, and for any $a, b \in G$ we have
$$id_G(a \cdot b) = a \cdot b = id_G(a) \cdot id_G(b).$$
so $id_G \colon G \to G$ is an isomorphism.
2. Let $\cdot$ be the group operation in G and let $\star$ be the group operation in H. Since $\varphi \colon G \to H$ is a bijection, we know that it has an inverse $\varphi^{-1} \colon H \to G$ which is also a bijection (because φ^{-1} has an inverse, namely φ). We need only check the second property. Let $c, d \in H$. Since φ is a bijection, it is a surjection, so we may fix $a, b \in G$ with $\varphi(a) = c$ and $\varphi(b) = d$. By definition of φ^{-1}, we then have $\varphi^{-1}(c) = a$ and $\varphi^{-1}(d) = b$. Now
$$\varphi(a \cdot b) = \varphi(a) \star \varphi(b) = c \star d,$$

so by definition of φ^{-1} we also have $\varphi^{-1}(c \star d) = a \cdot b$. Therefore,

$$\varphi^{-1}(c \star d) = a \cdot b.$$

Putting this information together we see that

$$\varphi^{-1}(c \star d) = a \cdot b = \varphi^{-1}(c) \cdot \varphi^{-1}(d).$$

Since $c, d \in H$ were arbitrary, the second property holds. Therefore, $\varphi^{-1} \colon H \to G$ is an isomorphism.

3. Let $\cdot$ be the group operation in G, let $\star$ be the group operation in H, and let $*$ be the group operation in K. Since the composition of bijections is a bijection, it follows that $\psi \circ \varphi \colon G \to K$ is a bijection. For any $a, b \in G$, we have

$$\begin{aligned}(\psi \circ \varphi)(a \cdot b) &= \psi(\varphi(a \cdot b)) \\ &= \psi(\varphi(a) \star \varphi(b)) && \text{(because } \varphi \text{ is an isomorphism)} \\ &= \psi(\varphi(a)) * \psi(\varphi(b)) && \text{(because } \psi \text{ is an isomorphism)} \\ &= (\psi \circ \varphi)(a) * (\psi \circ \varphi)(b).\end{aligned}$$

Therefore, $\psi \circ \phi \colon G \to K$ is an isomorphism.

□

It quickly becomes tiresome to consistently use different notation for the operation in G and the operation in H, so we will stop doing it unless absolutely necessary. Thus, we will write

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b),$$

where you need to keep in mind that the $\cdot$ on the left is the group operation in G and the $\cdot$ on the right is the group operation in H.

Proposition 6.3.4. *Let $\varphi \colon G \to H$ be an isomorphism. We have the following:*

1. $\varphi(e_G) = e_H$.
2. $\varphi(a^{-1}) = \varphi(a)^{-1}$ *for all* $a \in G$.
3. $\varphi(a^n) = \varphi(a)^n$ *for all* $a \in G$ *and all* $n \in \mathbb{Z}$.

Proof.

1. We have
$$\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G),$$
hence
$$e_H \cdot \varphi(e_G) = \varphi(e_G) \cdot \varphi(e_G).$$
Using the cancellation law, it follows that $\varphi(e_G) = e_H$.

2. Let $a \in G$. We have
$$\varphi(a) \cdot \varphi(a^{-1}) = \varphi(a \cdot a^{-1}) = \varphi(e_G) = e_H$$
and
$$\varphi(a^{-1}) \cdot \varphi(a) = \varphi(a^{-1} \cdot a) = \varphi(e_G) = e_H.$$
Therefore, $\varphi(a^{-1}) = \varphi(a)^{-1}$.

3. For $n = 0$, this says that $\varphi(e_G) = e_H$, which is true by part 1. The case $n = 1$ is trivial, and the case $n = -1$ is part 2. We first prove the result for all $n \in \mathbb{N}^+$ by induction. We already noticed that $n = 1$ is trivial. Suppose that $n \in \mathbb{N}^+$ is such that $\varphi(a^n) = \varphi(a)^n$ for all $a \in G$. For any $a \in G$ we have
$$\begin{aligned}\varphi(a^{n+1}) &= \varphi(a^n \cdot a) \\ &= \varphi(a^n) \cdot \varphi(a) && \text{(since } \varphi \text{ is an isomorphism)} \\ &= \varphi(a)^n \cdot \varphi(a) && \text{(by induction)} \\ &= \varphi(a)^{n+1}.\end{aligned}$$
Thus, the result holds for $n + 1$. Therefore, the result is true for all $n \in \mathbb{N}^+$ by induction. We finally handle $n \in \mathbb{Z}$ with $n < 0$. For any $a \in G$ we have
$$\begin{aligned}\varphi(a^n) &= \varphi((a^{-1})^{-n}) \\ &= \varphi(a^{-1})^{-n} && \text{(since } -n > 0) \\ &= (\varphi(a)^{-1})^{-n} && \text{(by part 2)} \\ &= \varphi(a)^n.\end{aligned}$$
Thus, the result is true for all $n \in \mathbb{Z}$.

□

Theorem 6.3.5. *Let G be a cyclic group.*

1. *If $|G| = \infty$, then $G \cong \mathbb{Z}$.*
2. *If $|G| = n$, then $G \cong \mathbb{Z}/n\mathbb{Z}$.*

Proof.

1. Suppose that $|G| = \infty$. Since G is cyclic, we may fix $c \in G$ with $G = \langle c \rangle$. Since $|G| = \infty$, it follows that $|c| = \infty$. Define $\varphi \colon \mathbb{Z} \to G$ by letting $\varphi(n) = c^n$. Notice that φ is surjective because $G = \langle c \rangle$. Also, if $\varphi(m) = \varphi(n)$, then $c^m = c^n$, so $m = n$ by Proposition 5.2.3. Therefore, φ is injective. Putting this together, we conclude that φ is a bijection. For any $k, \ell \in \mathbb{Z}$, we have
$$\begin{aligned}\varphi(k + \ell) &= c^{k+\ell} \\ &= c^k \cdot c^\ell \\ &= \varphi(k) \cdot \varphi(\ell).\end{aligned}$$
Therefore, φ is an isomorphism. It follows that $\mathbb{Z} \cong G$ and hence $G \cong \mathbb{Z}$.

2. Suppose that $|G| = n$. Since G is cyclic, we may fix $c \in G$ with $G = \langle c \rangle$. Since $|G| = n$, it follows from Proposition 5.2.3 that $|c| = n$. Define $\varphi \colon \mathbb{Z}/n\mathbb{Z} \to G$ by letting $\varphi(\overline{k}) = c^k$. Since we are defining a function on equivalence classes, we first need to check that φ is well-defined.

   Suppose that $k, \ell \in \mathbb{Z}$ with $\overline{k} = \overline{\ell}$. We then have that $k \equiv \ell \pmod{n}$, so $n \mid (k - \ell)$. Fix $d \in \mathbb{Z}$ with $nd = k - \ell$. We then have $k = \ell + nd$, hence
$$\begin{aligned}\varphi(\overline{k}) &= c^k \\ &= c^{\ell+nd} \\ &= c^\ell (c^n)^d \\ &= c^\ell e^d \\ &= c^\ell \\ &= \varphi(\overline{\ell}).\end{aligned}$$

Thus, φ is well-defined.

We next check that φ is a bijection. Suppose that $k, \ell \in \mathbb{Z}$ with $\varphi(\overline{k}) = \varphi(\overline{\ell})$. We then have that $c^k = c^\ell$, hence $c^{k-\ell} = e$. Since $|c| = n$, we know from Proposition 4.6.5 that $n \mid (k - \ell)$. Therefore $k \equiv \ell \pmod{n}$, and hence $\overline{k} = \overline{\ell}$. It follows that φ is injective. To see this φ is surjective, if $a \in G$, then $a \in \langle c \rangle$, so we may fix $k \in \mathbb{Z}$ with $a = c^k$ and note that $\varphi(\overline{k}) = c^k = a$. Hence, φ is a bijection.

Finally notice that for any $k, \ell \in \mathbb{Z}$, we have

$$\begin{aligned} \varphi(\overline{k} + \overline{\ell}) &= \varphi(\overline{k + \ell}) \\ &= c^{k+\ell} \\ &= c^k \cdot c^\ell \\ &= \varphi(k) \cdot \varphi(\ell). \end{aligned}$$

Therefore, φ is an isomorphism. It follows that $\mathbb{Z}/n\mathbb{Z} \cong G$ and hence $G \cong \mathbb{Z}/n\mathbb{Z}$.

□

Now on Homework 3, we proved that $|\overline{11}| = 6$ in $U(\mathbb{Z}/18\mathbb{Z})$. Since $|U(\mathbb{Z}/18\mathbb{Z})| = 6$, it follows that $U(\mathbb{Z}/18\mathbb{Z})$ is a cyclic group of order 6, and hence $U(\mathbb{Z}/18\mathbb{Z}) \cong \mathbb{Z}/6\mathbb{Z}$.

Corollary 6.3.6. *Let $p \in \mathbb{N}^+$ be prime. Any two groups of order p are isomorphic.*

Proof. Suppose that G and H have order p. By Theorem 5.8.6, we know that each of G and H are cyclic, so we have both $G \cong \mathbb{Z}/p\mathbb{Z}$ and $H \cong \mathbb{Z}/p\mathbb{Z}$ by the previous theorem. Using symmetry and transitivity of $\cong$, it follows that $G \cong H$. □

Properties Preserved by Isomorphisms

We have spent a lot of time establishing the existence of isomorphisms between various groups. How do we show that two groups are *not* isomorphic? The first thing to note is that if $G \cong H$, the we must have $|G| = |H|$ simply because if there is a bijection between two sets, then they have the same size. But what can we do if $|G| = |H|$? Looking at all possible bijections and ruling them out is not particularly feasible. The fundamental idea is that isomorphic groups are really just "renamings" of each other, so they should have all of the same fundamental properties. The next proposition is an example of this idea.

Proposition 6.3.7. *Suppose that G and H are groups with $G \cong H$. If G is abelian, then H is abelian.*

Proof. Since $G \cong H$, we may fix an isomorphism $\varphi \colon G \to H$. Let $h_1, h_2 \in H$. Since φ is an isomorphism, it is in particular surjective, so we may fix $g_1, g_2 \in G$ with $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$. We then have

$$\begin{aligned} h_1 \cdot h_2 &= \varphi(g_1) \cdot \varphi(g_2) \\ &= \varphi(g_1 \cdot g_2) && \text{(since } \varphi \text{ is an isomorphism)} \\ &= \varphi(g_2 \cdot g_1) && \text{(since } G \text{ is abelian)} \\ &= \varphi(g_2) \cdot \varphi(g_1) && \text{(since } \varphi \text{ is an isomorphism)} \\ &= h_2 \cdot h_1. \end{aligned}$$

Since $h_1, h_2 \in H$ were arbitrary, it follows that H is abelian. □

As an example, even though $|S_3| = 6 = |\mathbb{Z}/6\mathbb{Z}|$ we have $S_3 \not\cong \mathbb{Z}/6\mathbb{Z}$ because S_3 is nonabelian while $\mathbb{Z}/6\mathbb{Z}$ is abelian.

Proposition 6.3.8. *Suppose that G and H are groups with $G \cong H$. If G is cyclic, then H is cyclic.*

Proof. Since $G \cong H$, we may fix an isomorphism $\varphi\colon G \to H$. Since G is cyclic, we may fix $c \in G$ with $G = \langle c \rangle$. We claim that $H = \langle \varphi(c) \rangle$. Let $h \in H$. Since φ is in particular a surjection, we may fix $g \in G$ with $\varphi(g) = h$. Since $g \in G = \langle c \rangle$, we may fix $n \in \mathbb{Z}$ with $g = c^n$. We then have

$$h = \varphi(g) = \varphi(c^n) = \varphi(c)^n,$$

so $h \in \langle \varphi(c) \rangle$. Since $h \in H$ was arbitrary, it follows that $H = \langle \varphi(c) \rangle$ and hence H is cyclic. □

As an example, consider the groups $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Each of these groups is abelian and has order 4. However, $\mathbb{Z}/4\mathbb{Z}$ is cyclic while $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not. It follows that $\mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proposition 6.3.9. *Suppose that $\varphi\colon G \to H$ is an isomorphism. For any $a \in G$, we have $|a| = |\varphi(a)|$ (in other words, the order of a in G equals the order of $\varphi(a)$ in H).*

Proof. Let $a \in G$. Suppose that $n \in \mathbb{N}^+$ and $a^n = e_G$. Using the fact that $\varphi(e_G) = e_H$ we have

$$\varphi(a)^n = \varphi(a^n) = \varphi(e_G) = e_H,$$

so $\varphi(a)^n = e_H$. Conversely suppose that $n \in \mathbb{N}^+$ and $\varphi(a)^n = e_H$. We then have that

$$\varphi(a^n) = \varphi(a^n) = e_H,$$

so $\varphi(a^n) = e_H = \varphi(e_G)$, and hence $a^n = e_G$ because φ is injective. Combining both of these, we have shown that

$$\{n \in \mathbb{N}^+ : a^n = e_G\} = \{n \in \mathbb{N}^+ : \varphi(a)^n = e_H\}.$$

It follows that both of these sets are either empty (and so $|a| = \infty = |\varphi(a)|$) or both have the same least element (equal to the common order of $|a|$ and $|\varphi(a)|$). □

Thus, for example, we have $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ because the latter group has an element of order 8 while $a^4 = e$ for all $a \in \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

6.4 Internal Direct Products

We know how to take two groups and "put them together" by taking the direct product. We now want to think about how to reverse this process. Given a group G which is not obviously a direct product, how can we recognize it as being naturally isomorphic to the direct product of two of its subgroups? Before jumping in, let's look at the direct product again.

Suppose then that H and K are groups and consider their direct product $H \times K$. Define

$$H' = \{(h, e_K) : h \in H\},$$

and

$$K' = \{(e_H, k) : k \in K\}.$$

We claim that H' is a normal subgroup of $H \times K$. To see that it is a subgroup, simply note that $(e_H, e_K) \in H'$, that

$$(h_1, e_K) \cdot (h_2, e_K) = (h_1 h_2, e_K e_K) = (h_1 h_2, e_K),$$

and that

$$(h, e_K)^{-1} = (h^{-1}, e_K^{-1}) = (h^{-1}, e_K).$$

To see that H' is a normal subgroup of $H \times K$, notice that if $(h, e_K) \in H'$ and $(a, b) \in H \times K$, then

$$\begin{aligned}(a,b) \cdot (h, e_K) \cdot (a,b)^{-1} &= (a,b) \cdot (h, e_K) \cdot (a^{-1}, b^{-1}) \\ &= (ah, be_K) \cdot (a^{-1}, b^{-1}) \\ &= (aha^{-1}, be_Kb^{-1}) \\ &= (aha^{-1}, e_K).\end{aligned}$$

which is an element of H'. Similarly, K' is a normal subgroup of $H \times K$. Notice further that $H \cong H'$ via the function $\varphi(h) = (h, e_K)$ and similarly $K \cong K'$ via the function $\psi(k) = (e_H, k)$.

We can say some more about the relationship between the subgroups H' and K' of $H \times K$. Notice that

$$H' \cap K' = \{(e_H, e_K)\} = \{e_{H\times K}\}.$$

In other words, the only thing that H' and K' have in common is the identity element of $H \times K$. Finally, note that any element of $H \times K$ can be written as a product of an element of H' and an element of K': If $(h, k) \in H \times K$, then $(h, k) = (h, e_K) \cdot (e_H, k)$.

It turns out that these few facts characterize when a given group G is naturally isomorphic to the direct product of two of its subgroups, as we will see in Theorem 6.4.4. Before proving this result, we first introduce a definition and a few lemmas.

Definition 6.4.1. *Let G be a group, and let H and K be subgroups of G. We define*

$$HK = \{hk : h \in H \text{ and } k \in K\}.$$

Notice that HK will be a *subset* of G, but in general it is *not* a subgroup of G. For an explicit example, consider $G = S_3$, $H = \langle(1\ 2)\rangle = \{id, (1\ 2)\}$ and $K = \langle(1\ 3)\rangle = \{id, (1\ 3)\}$. We have

$$\begin{aligned}HK &= \{id \circ id, id \circ (1\ 3), (1\ 2) \circ id, (1\ 2)(1\ 3)\} \\ &= \{id, (1\ 3), (1\ 2), (1\ 3\ 2)\}.\end{aligned}$$

Thus $(1\ 3) \in HK$ and $(1\ 2) \in HK$, but $(1\ 3)(1\ 2) = (1\ 2\ 3) \notin HK$. Therefore, HK is not a subgroup of G.

Lemma 6.4.2. *Suppose that H and K are both subgroups of a group G and $H \cap K = \{e\}$. Suppose that $h_1, h_2 \in H$ and $k_1, k_2 \in K$ are such that $h_1k_1 = h_2k_2$. We then have that $h_1 = h_2$ and $k_1 = k_2$.*

Proof. We have $h_1k_1 = h_2k_2$, so multiplying on the left by h_2^{-1} and on the right by k_1^{-1}, we see that $h_2^{-1}h_1 = k_2k_1^{-1}$. Now $h_2^{-1}h_1 \in H$ because H is a subgroup of G, and $k_2k_1^{-1} \in K$ because K is a subgroup of G. Therefore, this common value is an element of $H \cap K = \{e\}$. Thus, we have $h_2^{-1}h_1 = e$ and hence $h_1 = h_2$, and similarly we have $k_2k_1^{-1} = e$ and hence $k_1 = k_2$. □

Lemma 6.4.3. *Suppose that H and K are both normal subgroups of a group G and that $H \cap K = \{e\}$. We then have that $hk = kh$ for all $h \in H$ and $k \in K$.*

Proof. Let $h \in H$ and $k \in K$. Consider the element $hkh^{-1}k^{-1}$. Since K is normal in G, we have $hkh^{-1} \in K$ and since $k^{-1} \in K$ it follows that $hkh^{-1}k^{-1} \in K$. Similarly, since H is normal in G, we have $kh^{-1}k^{-1} \in H$ and since sine $h \in H$ it follows that $hkh^{-1}k^{-1} \in H$. Therefore, $hkh^{-1}k^{-1} \in H \cap K$ and hence $hkh^{-1}k^{-1} = e$. Multiplying on the right by kh, we conclude that $hk = kh$. □

Theorem 6.4.4. *Suppose that H and K are subgroups of G with the following properties:*

1. *H and K are both normal subgroups of G.*
2. *$H \cap K = \{e\}$.*

3. *$HK = G$, i.e. for all $g \in G$, there exists $h \in H$ and $k \in K$ with $g = hk$.*

We then have that the function $\varphi\colon H \times K \to G$ defined by $\varphi((h,k)) = h \cdot k$ is an isomorphism. Thus, we have $G \cong H \times K$.

Proof. Define $\varphi\colon H \times K \to G$ by letting $\varphi((h,k)) = h \cdot k$. We check the following:

- φ is injective: Suppose that $\varphi((h_1,k_1)) = \varphi((h_2,k_2))$. We then have $h_1k_1 = h_2k_2$, so since $H \cap K = \{e\}$, we can conclude that $h_1 = h_2$ and $k_1 = k_2$ using Lemma 6.4.2. Therefore, $(h_1,k_1) = (h_2,k_2)$.
- φ is surjective: This is immediate from the assumption that $G = HK$.
- φ preserves the group operation: Suppose that $(h_1,k_1) \in H \times K$ and $(h_2,k_2) \in H \times K$, we have

$$\begin{aligned}
\varphi((h_1,k_1)\cdot(h_2,k_2)) &= \varphi((h_1h_2,k_1k_2)) \\
&= h_1h_2k_1k_2 \\
&= h_1k_1h_2k_2 && \text{(by Lemma 6.4.3)} \\
&= \varphi((h_1,k_1)) \cdot \varphi((h_2,k_2)).
\end{aligned}$$

Therefore, φ is an isomorphism. □

Definition 6.4.5. *Let G a group. Let H and K be subgroups of G such that:*

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

We then say that G is the internal direct product *of H and K. In this situation, we have that $H \times K \cong G$ via the function $\varphi((h,k)) = hk$, as shown in Theorem 6.4.4.*

As an example, consider the group $G = U(\mathbb{Z}/8\mathbb{Z})$. Let $H = \langle \overline{3} \rangle = \{\overline{1}, \overline{3}\}$ and let $K = \langle \overline{5} \rangle = \{\overline{1}, \overline{5}\}$. We then have that H and K are both normal subgroups of G (because G is abelian), that $H \cap K = \{\overline{1}\}$, and that

$$HK = \{\overline{1}\cdot\overline{1}, \overline{3}\cdot\overline{1}, \overline{1}\cdot\overline{5}, \overline{3}\cdot\overline{5}\} = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} = G.$$

Therefore, $U(\mathbb{Z}/8\mathbb{Z})$ is the internal direct product of H and K. I want to emphasize that $U(\mathbb{Z}/8\mathbb{Z})$ does not *equal* $H \times K$. After all, as sets we have

$$U(\mathbb{Z}/8\mathbb{Z}) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\},$$

while

$$H \times K = \{(\overline{1},\overline{1}), (\overline{3},\overline{1}), (\overline{1},\overline{5}), (\overline{3},\overline{5})\}.$$

However, the above result shows that these two groups are isomorphic via the function $\varphi\colon H \times K \to U(\mathbb{Z}/8\mathbb{Z})$ given by $\varphi((h,k)) = h \cdot k$. Since H and K are each cyclic of order 2, it follows that each of H and K are isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Using the following result, we conclude that $U(\mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proposition 6.4.6. *If $G_1 \cong H_1$ and $G_2 \cong H_2$, then $G_1 \times G_2 \cong H_1 \times H_2$.*

Proof. Since $G_1 \cong H_1$, we may fix an isomorphism $\varphi_1\colon G_1 \to H_1$. Since $G_2 \cong H_2$, we may fix an isomorphism $\varphi_2\colon G_2 \to H_2$. Define $\psi\colon G_1 \times G_2 \to H_1 \times H_2$ by letting

$$\psi((a_1,a_2)) = (\varphi_1(a_1), \varphi_2(a_2)).$$

We check the following:

- ψ is injective: Suppose that $a_1, b_1 \in G_1$ and $a_2, b_2 \in G_2$ satisfy $\psi((a_1, a_2)) = \psi((b_1, b_2))$. We then have $(\varphi_1(a_1), \varphi_2(a_2)) = (\varphi_1(b_1), \varphi_2(b_2))$, so
$$\varphi_1(a_1) = \varphi_1(b_1) \qquad \text{and} \qquad \varphi_2(a_2) = \varphi_2(b_2)$$
Now φ_1 is an isomorphism, so φ_1 is injective, and hence the first equality implies that $a_1 = b_1$. Similarly, φ_2 is an isomorphism, so φ_2 is injective, and hence the second equality implies that $a_2 = b_2$. Therefore, $(a_1, a_2) = (b_1, b_2)$.

- ψ is surjective: Let $(c_1, c_2) \in H_1 \times H_2$. We then have that $c_1 \in H_1$ and $c_2 \in H_2$. Now φ_1 is an isomorphism, so φ_1 is surjective, so we may fix $a_1 \in G_1$ with $\varphi_1(a_1) = c_1$. Similarly, φ_2 is an isomorphism, so φ_2 is surjective, so we may fix $a_2 \in G_1$ with $\varphi_1(a_2) = c_2$. We then have
$$\psi((a_1, a_2)) = (\varphi_1(a_1), \varphi_2(a_2)) = (c_1, c_2),$$
so $(c_1, c_2) \in \text{range}(\psi)$.

- ψ preserves the group operation: Let $a_1, b_1 \in G_1$ and $a_2, b_2 \in G_2$. We have
$$\begin{aligned}
\psi((a_1, a_2) \cdot (b_1, b_2)) &= \psi((a_1b_1, a_2b_2)) \\
&= (\varphi_1(a_1b_1), \varphi_2(a_2b_2)) \\
&= (\varphi_1(a_1) \cdot \varphi_1(b_1), \varphi_2(a_2) \cdot \varphi_2(b_2)) \qquad \text{(since } \varphi_1 \text{ and } \varphi_2 \text{ preserve the operations)} \\
&= (\varphi_1(a_1), \varphi_2(a_2)) \cdot (\varphi_1(b_1), \varphi_2(b_2)) \\
&= \psi((a_1, a_2)) \cdot \psi((b_1, b_2)).
\end{aligned}$$

Putting it all together, we conclude that $\psi \colon G_1 \times G_2 \to H_1 \times H_2$ is an isomorphism, so $G_1 \times G_2 \cong H_1 \times H_2$. $\square$

Corollary 6.4.7. *Let G a finite group. Let H and K be subgroups of G such that:*

1. *H and K are both normal subgroups of G.*
2. *$H \cap K = \{e\}$.*
3. *$|H| \cdot |K| = |G|$.*

We then have that G is the internal direct product of H and K.

Proof. We need only prove that $HK = G$. In the above proof where we showed that $h_1k_1 = h_2k_2$ implies $h_1 = h_2$ and $k_1 = k_2$, we only used the fact that $H \cap K = \{e\}$. Therefore, since we are assuming that $H \cap K = \{e\}$, it follows that $|HK| = |H| \cdot |K|$. Since we are assuming that $|H| \cdot |K| = |G|$, it follows that $|HK| = |G|$, and since G is finite we conclude that $HK = G$. $\square$

Suppose that $G = D_6$. Let
$$H = \{e, r^2, r^4, s, r^2s, r^4s\}$$
and let
$$K = \{e, r^3\}.$$
We have that $K = Z(G)$ from the homework, so K is a normal subgroup of G. It is straightforward to check that H is a subgroup of G and
$$[G : H] = \frac{|G|}{|H|} = \frac{12}{6} = 2.$$
Using Proposition 6.2.6, we conclude that H is a normal subgroup of G. Now $H \cap K = \{e\}$ and $|H| \cdot |K| = 6 \cdot 2 = 12 = |G|$ (you can also check directly that $HK = G$). It follows that G is the internal direct product

of H and K, so in particular we have $G \cong H \times K$. Notice that K is cyclic of order 2, so $K \cong \mathbb{Z}/2\mathbb{Z}$. Furthermore, H is a group of order 6, and it is not hard to convince yourself that $H \cong D_3$ by sending r^2 (where r is rotation in D_6) to r (where r is rotation in D_3). Geometrically, when working with H, we are essentially looking at the regular hexagon and focusing only on the rotations by 120^o (corresponding to r^2), 240^o (corresponding to r^4) and the identity, along with the standard flip. This really just corresponds exactly to the rigid motions of the triangle. I hope that convinces you that $H \cong D_3$, but you can check formally by looking at the corresponding Cayley tables. Now $D_3 = S_3$, so it follows that $H \cong S_3$ and hence

$$D_6 \cong H \times K \cong S_3 \times \mathbb{Z}/2\mathbb{Z},$$

where the last line uses Proposition 6.4.6.

6.5 Classifying Groups up to Isomorphism

A natural and interesting question is to count how many groups there are of various orders up to isomorphism. It's easy to see that any two groups of order 1 are isomorphic, so there is only one group of order 1 up to isomorphism. The next case that we can quickly dispose of are groups of prime order.

Proposition 6.5.1. *For each prime $p \in \mathbb{Z}$, every group G of order p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Thus, there is exactly one group of order p up to isomorphism.*

Proof. Let $p \in \mathbb{Z}$ be prime. If G is a group of order p, then G is cyclic by Theorem 5.8.6, and hence isomorphic to $\mathbb{Z}/p\mathbb{Z}$ by Theorem 6.3.5. $\square$

The first nonprime case is 4. Before jumping in to that, we prove a useful little proposition.

Proposition 6.5.2. *If G is a group with the property that $a^2 = e$ for all $a \in G$, then G is abelian.*

Proof. Let $a, b \in G$. Since $ba \in G$, we have $(ba)^2 = e$, so $baba = e$. Multiplying on the left by b and using the fact that $b^2 = e$, we conclude that $aba = b$. Multiplying this on the right be a and using the fact that $a^2 = e$, we deduce that $ab = ba$. Since $a, b \in G$ were arbitrary, it follows that G is abelian. $\square$

Proposition 6.5.3. *Every group of order 4 is isomorphic to exactly one of $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Thus, there are exactly two groups of order 4 up to isomorphism.*

Proof. First, notice that $\mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ by Proposition 6.3.8 because the former is cyclic but the latter is not. Thus, there are at least two groups of order 4 up to isomorphism.

Let G be a group of order 4. By Lagrange's Theorem, we know that every nonidentity element of G has order either 2 or 4. We have two cases.

- *Case 1:* Suppose that G has an element of order 4. By Proposition 5.2.6, we then have that G is cyclic, so $G \cong \mathbb{Z}/4\mathbb{Z}$ by Theorem 6.3.5.
- *Case 2:* Suppose that G has no element of order 4. Thus, every nonidentity element of G has order 2. We then have that $a^2 = e$ for all $a \in G$, so G is abelian by Proposition 6.5.2. Fix distinct nonidentity elements $a, b \in G$. We then have that $|a| = 2 = |b|$. Let $H = \langle a \rangle = \{e, a\}$ and $K = \langle b \rangle = \{e, b\}$. Since G is abelian, we know that H and K are normal subgroups of G. We also have $H \cap K = \{e\}$ and $|H| \cdot |K| = 2 \cdot 2 = 4 = |G|$. Using Corollary 6.4.7, we conclude that G is the internal direct product of H and K. Now H and K are both cyclic of order 2, so they are both isomorphic to $\mathbb{Z}/2\mathbb{Z}$ by Theorem 6.3.5. It follows that

  $$G \cong H \times K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

  where the latter isomorphism follows from Proposition 6.4.6.

Thus, every group of order 4 is isomorphic to one of groups $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Furthermore, no group can be isomorphic to both because $\mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as mentioned above. $\square$

We've now shown that every group of order strictly less than 6 is abelian. We know that $S_3 = D_3$ is a nonabelian group of order 6, so this is the smallest possible size of a nonabelian group. In fact, up to isomorphism, it is the only nonabelian group of order 6.

Proposition 6.5.4. *Every group of order 6 is isomorphic to exactly one of $\mathbb{Z}/6\mathbb{Z}$ or S_3. Thus, there are exactly two groups of order 6 up to isomorphism.*

Proof. First, notice that $\mathbb{Z}/6\mathbb{Z} \not\cong S_3$ by Proposition 6.3.7 because the former is abelian but the latter is not. Thus, there are at least two groups of order 6 up to isomorphism.

Let G be a group of order 6. By Lagrange's Theorem, we know that every nonidentity element of G has order either 2, 3 or 6. We have two cases.

- *Case 1:* Suppose that G is abelian. By Theorem 6.2.12, we know that G has an element a of order 3 and an element b of order 2. Let $H = \langle a \rangle = \{e, a, a^2\}$ and $K = \langle b \rangle = \{e, b\}$. Since G is abelian, we know that H and K are normal subgroups of G. We also have $H \cap K = \{e\}$ (notice that $b \neq a^2$ because $|a^2| = 3$ also) and $|H| \cdot |K| = 3 \cdot 2 = 6 = |G|$. Using Corollary 6.4.7, we conclude that G is the internal direct product of H and K. Now H and K are both cyclic, so $H \cong \mathbb{Z}/3\mathbb{Z}$ and $K \cong \mathbb{Z}/2\mathbb{Z}$ by Theorem 6.3.5. It follows that
$$G \cong H \times K \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$
where the latter isomorphism follows from Proposition 6.4.6. Finally, notice that $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is cyclic by Problem 6c on Homework 4 (or by directly checking that $|(\overline{1}, \overline{1})| = 6$), so $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$ by Theorem 6.3.5. Thus, $G \cong \mathbb{Z}/6\mathbb{Z}$.

- *Case 2:* Suppose that G is not abelian. We then have that G is not cyclic by Proposition 5.2.7, so G has no element of order 6 by Proposition 5.2.6. Also, it is not possible for every element of G to have order 2 by Proposition 6.5.2. Thus, G must have an element of order 3. Fix $a \in G$ with $|a| = 3$. Notice that $a^2 \notin \{e, a\}$, that $a^2 = a^{-1}$, and that $|a^2| = 3$ (because $(a^2)^2 = a^4 = a$, and $(a^2)^3 = a^6 = e$). Now take an arbitrary $b \in G \backslash \{e, a, a^2\}$. We then have $ab \notin \{e, a, a^2, b\}$ (for example, if $ab = e$, then $b = a^{-1} = a^2$, while if $ab = a^2$ then $b = a$ by cancellation) and also $a^2 b \notin \{e, a, a^2, b, ab\}$. Therefore, the 6 element of G are e, a, a^2, b, ab, and $a^2 b$, i.e. $G = \{e, a, a^2, b, ab, a^2 b\}$.

  We next determine $|b|$. Now we know that $b \neq e$, so since G is not cyclic we know that either $|b| = 2$ or $|b| = 3$. Suppose then that $|b| = 3$. We know that b^2 must be one of the six elements of G. We do not have $b^2 = e$ because $|b| = 3$, and arguments similar to those above show that $b^2 \notin \{b, ab, a^2 b\}$ (for example, if $b^2 = ab$, then $a = b$ by cancellation). Now if $b^2 = a$, then multiplying both sides by b on the right, we could conclude that $b^3 = ab$, so $e = ab$, and hence $b = a^{-1} = a^2$, a contradiction. Similarly, if $b^2 = a^2$, then multiplying by b on the right gives $e = a^2 b$, so multiplying on the left by a allows us to conclude that $a = b$, a contradiction. Since all cases end in a contradiction, we conclude that $|b| \neq 3$, and hence we must have $|b| = 2$.

  Since $ba \in G$ and $G = \{e, a, a^2, b, ab, a^2 b\}$, we now determine which of the six elements equals ba. Notice that $ba \notin \{e, a, a^2, b\}$ for similar reasons as above. If $ba = ab$, then a and b commute, and from here it is straightforward to check that all element of G commute, contradicting the fact that G is nonabelian. It follows that we have $ba = a^2 b = a^{-1} b$.

  To recap, we have $|a| = 3$, $|b| = 2$, and $ba = a^{-1} b$. Now in D_3 we also have $|r| = 3$, $|s| = 2$, and $sr = r^{-1} s$. Define a bijection $\varphi \colon G \to D_3$ as follows:

  - $\varphi(e) = e$.
  - $\varphi(a) = r$.

- $\varphi(a^2) = r^2$.
- $\varphi(b) = s$.
- $\varphi(ab) = rs$.
- $\varphi(a^2b) = r^2s$.

Using the properties of $a, b \in G$ along with those for $r, s \in D_3$, it is straightforward to check that φ preserves the group operation. Therefore, $G \cong D_3$, and since $D_3 = S_3$, we conclude that $G \cong S_3$.

Thus, every group of order 6 is isomorphic to one of groups $\mathbb{Z}/6\mathbb{Z}$ or S_3. Furthermore, no group can be isomorphic to both because $\mathbb{Z}/6\mathbb{Z} \not\cong S_3$ as mentioned above. $\square$

We know that there are at least 5 groups of order 8 up to isomorphism:

$$\mathbb{Z}/8\mathbb{Z} \qquad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \qquad D_4 \qquad Q_8$$

The first three of these are abelian, while the latter two are not. Notice that $\mathbb{Z}/8\mathbb{Z}$ is not isomorphic to the other two abelian groups because they are not cyclic. Also, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ because the former has an element of order 4 while the latter does not. Finally, $D_4 \not\cong Q_8$ because D_4 has five elements of order 2 and two of order 4, while Q_8 has one element of order 2 and six of order 4. Now it is possible to show that every group of order 8 is isomorphic to one of these five, but this is difficult to do with our elementary methods. We need to build more tools, not only to tackle this problem, but also to think about groups of larger order. Although many of these methods will arise in later chapters, the following result is within our grasp now.

Theorem 6.5.5. *Let G be a group. If $G/Z(G)$ is cyclic, then G is abelian.*

Proof. Recall that $Z(G)$ is a normal subgroup of G by Proposition 5.6.2 and Proposition 6.2.5. Suppose that $G/Z(G)$ is cyclic. We may then fix $c \in G$ such that $G/Z(G) = \langle cZ(G) \rangle$. Now we have $(cZ(G))^n = c^nZ(G)$ for all $n \in \mathbb{Z}$, so

$$G/Z(G) = \{c^nZ(G) : n \in \mathbb{Z}\}.$$

We first claim that every $a \in G$ can be written in the form $a = c^nz$ for some $n \in \mathbb{Z}$ and $z \in Z(G)$. To see this, let $a \in G$. Now $aZ(G) \in G/Z(G)$, so we may fix $n \in \mathbb{Z}$ with $aZ(G) = c^nZ(G)$. Since $a \in Z(G)$, we have $a \in c^nZ(G)$, so there exists $z \in Z(G)$ with $a = c^nz$.

Suppose now that $a, b \in G$. From above, we may write $a = c^nz$ and $b = c^mw$ where $n, m \in \mathbb{Z}$ and $z, w \in Z(G)$. We have

$$\begin{aligned}
ab &= c^nzc^mw \\
&= c^nc^mzw && (\text{since } z \in Z(G)) \\
&= c^{n+m}zw \\
&= c^{m+n}wz && (\text{since } z \in Z(G)) \\
&= c^mc^nwz \\
&= c^mwc^nz && (\text{since } w \in Z(G)) \\
&= ba.
\end{aligned}$$

Since $a, b \in G$ were arbitrary, it follows that G is abelian. $\square$

Corollary 6.5.6. *Let G be a group with $|G| = pq$ for (not necessarily distinct) primes $p, q \in \mathbb{Z}$. We then have that either $Z(G) = G$ or $Z(G) = \{e\}$.*

Proof. We know that $Z(G)$ is a normal subgroup of G. Thus, $|Z(G)|$ divides $|G|$ by Lagrange's Theorem, so $|Z(G)|$ must be one of 1, p, q, or pq. Suppose that $|Z(G)| = p$. We then have that

$$|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{pq}{p} = q,$$

so $G/Z(G)$ is cyclic by Theorem 5.8.6. Using Theorem 6.5.5, it follows that G is abelian, and hence $Z(G) = G$, contradicting the fact that $|Z(G)| = p$. Similarly, we can not have $|Z(G)| = q$. Therefore, either $|Z(G)| = 1$, in which case $Z(G) = \{e\}$, or $|Z(G)| = pq$, in which case $Z(G) = G$. $\square$

For example, since S_3 is nonabelian and $|S_3| = 6 = 2{\cdot}3$, this result immediately implies that $Z(S_3) = \{id\}$. Similarly, since D_5 is nonabelian and $|D_5| = 10 = 2 \cdot 5$, we conclude that $Z(D_5) = \{id\}$. We will come back and use this result in more interesting contexts later.

6.6 Homomorphisms

Our definition of isomorphism had two requirements: that the function was a bijection and that it preserves the operation. We next investigate what happens if we drop the former and just require that the function preserves the operation.

Definition 6.6.1. *Let G and H be groups. A* homomorphism *from G to H is a function $\varphi \colon G \to H$ such that $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ for all $a, b \in G$.*

Consider the following examples:

- The determinant function $\det \colon GL_n(\mathbb{R}) \to \mathbb{R}\backslash\{0\}$ is a homomorphism (where the operation on $\mathbb{R}\backslash\{0\}$ is multiplication). This is because $\det(AB) = \det(A) \cdot \det(B)$ for any matrices A and B. Notice that det is certainly not an injective function.

- Consider the sign function $\varepsilon \colon S_n \to \{1, -1\}$ where the operation on $\{\pm 1\}$ is multiplication. Notice that ε is homomorphism by Proposition 5.3.8. Again, for $n \geq 3$, the function ε is very far from being injective.

- For any groups G and H, the function $\pi_1 \colon G \times H \to G$ given by $\pi_1((g, h)) = g$ and the function $\pi_2 \colon G \times H \to H$ given by $\pi_2((g, h)) = h$ are both homomorphisms. For examples, given any $g_1, g_2 \in G$ and $h_1, h_2 \in H$ we have

$$\begin{aligned} \pi_1((g_1, h_1) \cdot (g_2, h_2)) &= \pi_1((g_1 g_2, h_1 h_2)) \\ &= g_1 g_2 \\ &= \pi_1((g_1, h_1)) \cdot \pi_1((g_2, h_2)), \end{aligned}$$

  and similarly for π_2.

- For a given group G with normal subgroup N, the function $\pi \colon G \to G/N$ defined by letting $\pi(a) = aN$ for all $a \in G$ is a homomorphism, because for any $a, b \in G$, we have

$$\begin{aligned} \pi(ab) &= abN \\ &= aN \cdot bN \\ &= \pi(a) \cdot \pi(b). \end{aligned}$$

Proposition 6.6.2. *Let $\varphi \colon G \to H$ be an homomorphism. We have the following.*

1. $\varphi(e_G) = e_H$.
2. $\varphi(a^{-1}) = \varphi(a)^{-1}$ *for all* $a \in G$.
3. $\varphi(a^n) = \varphi(a)^n$ *for all* $a \in G$ *and all* $n \in \mathbb{Z}$.

Proof. In Proposition 6.3.4, the corresponding proof for isomorphisms, we only used the fact that φ preserves the group operation, not that it is a bijection. $\square$

Definition 6.6.3. *Let* $\varphi \colon G \to H$ *be a homomorphism. We define* $\ker(\varphi) = \{g \in G : \varphi(g) = e_H\}$*. The set* $\ker(\varphi)$ *is called the* kernel *of* φ.

For example, for $\det \colon GL_n(\mathbb{R}) \to \mathbb{R}\backslash\{0\}$, we have

$$\ker(\det) = \{A \in GL_n(\mathbb{R}) : det(A) = 1\} = SL_n(\mathbb{R}).$$

For the homomorphism $\varepsilon \colon S_n \to \{\pm 1\}$, we have

$$\ker(\varepsilon) = \{\sigma \in S_n : \varepsilon(\sigma) = 1\} = A_n.$$

Proposition 6.6.4. *If* $\varphi \colon G \to H$ *is a homomorphism, then* $\ker(\varphi)$ *is a normal subgroup of* G.

Proof. Let $K = \ker(\varphi)$. We first check that K is indeed a subgroup of G. Since $\varphi(e_G) = e_H$ by Proposition 6.6.2, we see that $e_G \in K$. Given $a, b \in K$, we have $\varphi(a) = e_H = \varphi(b)$, so

$$\varphi(ab) = \varphi(a) \cdot \varphi(b) = e_H \cdot e_H = e_H,$$

and hence $ab \in K$. Given $a \in K$, we have $\varphi(a) = e_H$, so

$$\varphi(a^{-1}) = \varphi(a)^{-1} = e_H^{-1} = e_H,$$

so $a^{-1} \in K$. Putting this all together, we see that K is a subgroup of G. Suppose now that $a \in K$ and $g \in G$. Since $a \in K$ we have $\varphi(a) = e_H$, so

$$\begin{aligned}
\varphi(gag^{-1}) &= \varphi(g) \cdot \varphi(a) \cdot \varphi(g^{-1}) \\
&= \varphi(g) \cdot e_H \cdot \varphi(g)^{-1} \\
&= \varphi(g) \cdot \varphi(g)^{-1} \\
&= e_H.
\end{aligned}$$

and hence $gag^{-1} \in K$. Therefore, K is a normal subgroup of G. $\square$

We've just seen that the kernel of a homomorphism is always a normal subgroup of G. It's a nice fact that every normal subgroup of a group arises in this way, so we get another equivalent characterization of a normal subgroup.

Theorem 6.6.5. *Let* G *be a group and let* K *be a normal subgroup of* G*. There exists a group* H *and a homomorphism* $\varphi \colon G \to H$ *with* $K = \ker(\varphi)$.

Proof. Suppose that K is a normal subgroup of G. We can then form the quotient group $H = G/K$. Define $\varphi \colon G \to H$ by letting $\varphi(a) = aK$ for all $a \in G$. As discussed above, φ is a homomorphism. Notice that for any $a \in G$, we have

$$\begin{aligned}
a \in \ker(\varphi) &\iff \varphi(a) = eK \\
&\iff aK = eK \\
&\iff eK = aK \\
&\iff e^{-1}a \in K \\
&\iff a \in K.
\end{aligned}$$

Therefore φ is a homomorphism with $\ker(\varphi) = K$. $\square$

Proposition 6.6.6. *Let $\varphi\colon G \to H$ be a homomorphism. φ is injective if and only if* $\ker(\varphi) = \{e_G\}$.

Proof. Suppose first that φ is injective. We know that $\varphi(e_G) = e_H$, so $e_G \in \ker(\varphi)$. Let $a \in \ker(\varphi)$ be arbitrary. We then have $\varphi(a) = e_H = \varphi(e_G)$, so since φ is injective we conclude that $a = e_G$. Therefore, $\ker(\varphi) = \{e_G\}$.

Suppose conversely that $\ker(\varphi) = \{e_G\}$. Let $a, b \in G$ be arbitrary with $\varphi(a) = \varphi(b)$. We then have

$$\begin{aligned}\varphi(a^{-1}b) &= \varphi(a^{-1}) \cdot \varphi(b) \\ &= \varphi(a)^{-1} \cdot \varphi(b) \\ &= \varphi(a)^{-1} \cdot \varphi(a) \\ &= e_H,\end{aligned}$$

so $a^{-1}b \in \ker(\varphi)$. Now we are assuming that $\ker(\varphi) = \{e_G\}$, so we conclude that $a^{-1}b = e_G$. Multiplying on the left by a, we see that $a = b$. Therefore, φ is injective. □

In contrast to Proposition 6.3.9, we only obtain the following for homomorphisms.

Proposition 6.6.7. *Suppose that $\varphi\colon G \to H$ is a homomorphism. If $a \in G$ has finite order, then $|\varphi(a)|$ divides $|a|$.*

Proof. Suppose that $a \in G$ has finite order and let $n = |a|$. We have $a^n = e_G$, so

$$\varphi(a)^n = \varphi(a^n) = \varphi(e_G) = e_H,$$

Thus, $\varphi(a)$ has finite order, and furthermore, if we let $m = |\varphi(a)|$, then $m \mid n$ by Proposition 4.6.5. □

Given a homomorphism $\varphi\colon G \to H$, it is possible that $|\varphi(a)| < |a|$ for an element $a \in G$. For example, if $\varepsilon\colon S_4 \to \{1, -1\}$ is the sign homomorphism, then $|(1\ 2\ 3\ 4)| = 4$ but $|\varepsilon((1\ 2\ 3\ 4))| = |-1| = 2$. For a more extreme example, given any group G, the function $\varphi\colon G \to \{e\}$ from G to the trivial group given by $\varphi(a) = e$ for all a is a homomorphism with the property that $|\varphi(a)| = 1$ for all $a \in G$. In particular, an element of infinite order can be sent by a homomorphism to an element of finite order.

For another example, suppose that N is a normal subgroup of G, and consider the homomorphism $\varphi\colon G \to G/N$ given by $\pi(a) = aN$. For any $a \in G$, we know by Proposition 6.6.7 that $|\pi(a)|$ must divide $|a|$, which is to say that $|aN|$ (the order of the *element* aN) must divide $|a|$. Thus, we have generalized Proposition 6.2.11.

Definition 6.6.8. *Suppose A and B are sets and that $f\colon A \to B$ is a function.*

- *Given a subset $S \subseteq A$, we let $f^{\to}[S] = \{f(a) : a \in S\} = \{b \in B : \text{There exists } a \in S \text{ with } f(a) = b\}$.*
- *Given a subset $T \subseteq B$, we let $f^{\leftarrow}[T] = \{a \in A : f(a) \in T\}$.*

In other words, $f^{\to}[S]$ is the set of outputs that arise when restricting inputs to S, an $f^{\leftarrow}[T]$ is the set of inputs that are sent to an output in T.

Given a function $f\colon A \to B$, some sources use the notation $f(S)$ for our $f^{\to}[S]$, and use $f^{-1}(T)$ for our $f^{\leftarrow}[T]$. This notation is quite standard, but also extraordinarily confusing. On the one hand, the notation $f(S)$ suggests that S is a valid input to f rather than a *set* of valid inputs. To avoid confusion here, we choose to use square brackets. In addition, the notation $f^{-1}(T)$, or even $f^{-1}[T]$, is additionally confusing because f may fail to have an inverse (after all, it need not be bijective). Thus, we will use our (somewhat unorthodox) notation.

Theorem 6.6.9. *Let G_1 and G_2 be groups, and let $\varphi\colon G_1 \to G_2$ be a homomorphism. We have the following:*

1. *If H_1 is a subgroup of G_1, then $\varphi^{\rightarrow}[H_1]$ is a subgroup of G_2.*
2. *If N_1 is a normal subgroup of G_1 and φ is surjective, then $\varphi^{\rightarrow}[N_1]$ is a normal subgroup of G_2.*
3. *If H_2 is a subgroup of G_2, then $\varphi^{\leftarrow}[H_2]$ is a subgroup of G_1.*
4. *If N_2 is a normal subgroup of G_2, then $\varphi^{\leftarrow}[N_2]$ is a normal subgroup of G_1.*

Proof. Throughout, let e_1 be the identity of G_1 and let e_2 be the identity of G_2.

1. Suppose that H_1 is a subgroup of G_1.
   - Notice that we have $e_1 \in H_1$ because H_1 is a subgroup of G_2, so $e_2 = \varphi(e_1) \in \varphi^{\rightarrow}[H_1]$.
   - Let $c, d \in \varphi^{\rightarrow}[H_1]$ be arbitrary. Fix $a, b \in H_1$ with $\varphi(a) = c$ and $\varphi(b) = d$. Since $a, b \in H_1$ and H_1 is a subgroup of G_1, it follows that $ab \in H_1$. Now
   $$\varphi(ab) = \varphi(a) \cdot \varphi(b) = cd,$$
   so $cd \in \varphi^{\rightarrow}[H_1]$.
   - Let $c \in \varphi^{\rightarrow}[H_1]$ be arbitrary. Fix $a \in H_1$ with $\varphi(a) = c$. Since $a \in H_1$ and H_1 is a subgroup of G_1, it follows that $a^{-1} \in H_1$. Now
   $$\varphi(a^{-1}) = \varphi(a)^{-1} = c^{-1},$$
   so $c^{-1} \in \varphi^{\rightarrow}[H_1]$.

   Putting it all together, we conclude that $\varphi^{\rightarrow}[H_1]$ is a subgroup of G_2.
2. Suppose that N_1 is a normal subgroup of G_1 and that φ is surjective. We know from part 1 that $\varphi^{\rightarrow}[N_1]$ is a subgroup of G_2. Suppose that $d \in G_2$ and $c \in \varphi^{\rightarrow}[N_1]$ are arbitrary. Since φ is surjective, we may fix $b \in G_1$ with $\varphi(b) = d$. Since $c \in \varphi^{\rightarrow}[N_1]$, we can fix $a \in G_1$ with $\varphi(a) = c$. We then have
   $$\begin{aligned} dcd^{-1} &= \varphi(b) \cdot \varphi(a) \cdot \varphi(b)^{-1} \\ &= \varphi(b) \cdot \varphi(a) \cdot \varphi(b^{-1}) \\ &= \varphi(bab^{-1}), \end{aligned}$$
   so $dcd^{-1} \in \varphi^{\rightarrow}[N_1]$. Since $d \in G_2$ and $c \in \varphi^{\rightarrow}[N_1]$ were arbitrary, we conclude that $\varphi^{\rightarrow}[N_1]$ is a normal subgroup of G_2.
3. Suppose that H_2 is a subgroup of G_2.
   - Notice that we have $e_2 \in H_2$ because H_2 is a subgroup of H_1. Since $\varphi(e_1) = e_2 \in H_2$, it follows that $e_1 \in \varphi^{\leftarrow}[H_2]$.
   - Let $a, b \in \varphi^{\leftarrow}[H_2]$ be arbitrary, so $\varphi(a) \in H_2$ and $\varphi(b) \in H_2$. We then have
   $$\varphi(ab) = \varphi(a) \cdot \varphi(b) \in H_2$$
   because H_2 is a subgroup of G_2, so $ab \in \varphi^{\leftarrow}[H_2]$.
   - Let $a \in \varphi^{\leftarrow}[H_2]$ be arbitrary, so $\varphi(a) \in H_2$. We then have
   $$\varphi(a^{-1}) = \varphi(a)^{-1} \in H_2$$
   because H_2 is a subgroup of G_2, so $a^{-1} \in \varphi^{\leftarrow}[H_2]$.

Putting it all together, we conclude that $\varphi^{\leftarrow}[H_2]$ is a subgroup of G_1.

4. Suppose that N_2 be a subgroup of G_2. We know from part 1 that $\varphi^{\leftarrow}[N_2]$ is a subgroup of G_1. Suppose that $b \in G_1$ and $a \in \varphi^{\leftarrow}[N_2]$ are arbitrary, so $\varphi(a) \in N_2$. We then have

$$\begin{aligned}\varphi(bab^{-1}) &= \varphi(b) \cdot \varphi(a) \cdot \varphi(b^{-1}) \\ &= \varphi(b) \cdot \varphi(a) \cdot \varphi(b)^{-1}.\end{aligned}$$

Now $\varphi(b) \in G_2$ and $\varphi(a) \in N_2$, so $\varphi(b) \cdot \varphi(a) \cdot \varphi(b)^{-1} \in N_2$ because N_2 is a normal subgroup of G_2. Therefore, $\varphi(bab^{-1}) \in N_2$, and hence $bab^{-1} \in \varphi^{\leftarrow}[N_2]$. Since $b \in G_1$ and $a \in \varphi^{\leftarrow}[N_2]$ were arbitrary, we conclude that $\varphi^{\leftarrow}[N_2]$ is a normal subgroup of G_1.

□

Corollary 6.6.10. *If $\varphi\colon G_1 \to G_2$ is a homomorphism, then range(φ) is a subgroup of G_2.*

Proof. This follows immediately from the previous theorem because G_1 is trivially a subgroup of G_1 and range$(\varphi) = \varphi^{\rightarrow}[G_1]$. □

6.7 The Isomorphism and Correspondence Theorems

Suppose that $\varphi\colon G \to H$ is a homomorphism. There are two ways in which φ can fail to be an isomorphism: φ can fail to be injective and φ can fail to be surjective. The latter is not really a problem at all, because range$(\varphi) = \varphi^{\rightarrow}[G]$ is a subgroup of H, and if we restrict the codomain down to this subgroup, then φ becomes surjective. The real issue is how to deal with a lack of injectivity. Let $K = \ker(\varphi)$. As we've seen in Proposition 6.6.6, if $K = \{e_G\}$, then φ is injective. But what if K is a nontrivial subgroup?

The general idea is as follows. All elements of K get sent to the same element of H via φ, namely to e_H. Now viewing K as a subgroup of G, the cosets of K break up G into pieces. The key insight is that two elements which belong to the same coset of K must get sent via φ to the same element of H, and conversely if two elements belong to different cosets of K then they must be sent via φ to distinct values of H. This is the content of the following lemma.

Lemma 6.7.1. *Suppose that $\varphi\colon G \to H$ is a homomorphism and let $K = \ker(\varphi)$. For any $a, b \in G$, we have that $a \sim_K b$ if and only if $\varphi(a) = \varphi(b)$.*

Proof. Suppose first that $a, b \in G$ satisfy $a \sim_K b$. Fix $k \in K$ with $ak = b$ and notice that

$$\begin{aligned}\varphi(b) &= \varphi(ak) \\ &= \varphi(a) \cdot \varphi(k) \\ &= \varphi(a) \cdot e_H \\ &= \varphi(a).\end{aligned}$$

Suppose conversely that $a, b \in G$ satisfy $\varphi(a) = \varphi(b)$. We then have

$$\begin{aligned}\varphi(a^{-1}b) &= \varphi(a^{-1}) \cdot \varphi(b) \\ &= \varphi(a)^{-1} \cdot \varphi(b) \\ &= \varphi(a)^{-1} \cdot \varphi(a) \\ &= e_H,\end{aligned}$$

so $a^{-1}b \in K$. It follows that $a \sim_K b$. □

In less formal terms, the lemma says that φ is constant on each coset of K, and assigns distinct values to distinct cosets. This sets up a well-defined injective function from the quotient group G/K to the group H. Restricting down to range(φ) on the right, this function is a bijection. Furthermore, this function is an isomorphism as we now prove in the following fundamental theorem.

Theorem 6.7.2 (First Isomorphism Theorem)**.** *Let $\varphi\colon G \to H$ be a homomorphism and let $K = \ker(\varphi)$. Define a function $\psi\colon G/K \to H$ by letting $\psi(aK) = \varphi(a)$. We then have that ψ is a well-defined function which is an isomorphism onto the subgroup range(φ) of H. Therefore*

$$G/\ker(\varphi) \cong \mathit{range}(\varphi).$$

Proof. We check the following.

- ψ is well-defined: Suppose that $a, b \in G$ with $aK = bK$. We then have $a \sim_K b$, so by Lemma 6.7.1, we have that $\varphi(a) = \varphi(b)$ and hence $\psi(aK) = \psi(bK)$.
- ψ is injective: Suppose that $a, b \in G$ with $\psi(aK) = \psi(bK)$. We then have that $\varphi(a) = \varphi(b)$, so $a \sim_K b$ by Lemma 6.7.1 (in the other direction), and hence $aK = bK$.
- ψ is surjective onto range(φ): First notice that since $\varphi\colon G \to H$ is a homomorphism, we know from Corollary 6.6.10 that range(φ) is a subgroup of H. Now for any $a \in G$, we have $\psi(aK) = \varphi(a) \in$ range(φ), so range$(\psi) \subseteq$ range(φ). Moreover, given an arbitrary $c \in$ range(φ), we can fix $a \in G$ with $\varphi(a) = c$, and then we have $\psi(aK) = \varphi(a) = c$. Thus, range$(\varphi) \subseteq$ range(ψ). Combining both of these, we conclude that range$(\psi) =$ range(φ).
- ψ preserves the group operation: For any $a, b \in G$, we have

$$\begin{aligned} \psi(aK \cdot bK) &= \psi(abK) \\ &= \varphi(ab) \\ &= \varphi(a) \cdot \varphi(b) \\ &= \psi(aK) \cdot \psi(bK). \end{aligned}$$

Putting it all together, the function $\psi\colon G/K \to H$ defined by $\psi(aK) = \varphi(a)$ is a well-defined injective homomorphism that maps G surjectively onto range(ϕ). This proves the result. ☐

For example, consider the homomorphism $\det\colon GL_n(\mathbb{R}) \to \mathbb{R}\backslash\{0\}$, where we view $\mathbb{R}\backslash\{0\}$ as a group under multiplication. As discussed in the previous section, we have $\ker(\det) = SL_n(\mathbb{R})$. Notice that det is a surjective function because every nonzero real number arises as the determinant of some invertible matrix (for example, the identity matrix with the $(1,1)$ entry replaced by r has determinant r). The First Isomorphism Theorem tells us that

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}\backslash\{0\}.$$

Here is what is happening intuitively. The subgroup $SL_n(\mathbb{R})$, which is the kernel of the determinant homomorphism, is the set of $n \times n$ matrices with determinant 1. This break up the $n \times n$ matrices into cosets which correspond exactly to the nonzero real numbers in the sense that all matrices of a given determinant form a coset. The First Isomorphism Theorem says that multiplication in the quotient (where you take representatives matrices from the corresponding cosets, multiply the matrices, and then expand to the resulting coset) corresponds exactly to just multiplying the real numbers which "label" the cosets.

For another example, consider the sign homomorphism $\varepsilon\colon S_n \to \{\pm 1\}$ where $n \geq 2$. We know that ε is a homomorphism by Proposition 5.3.8, and we have $\ker(\varepsilon) = A_n$ by definition of A_n. Notice that ε is surjective because $n \geq 2$ (so $\varepsilon(id) = 1$ and $\varepsilon((1\ 2)) = -1$). By the First Isomorphism Theorem we have

$$S_n/A_n \cong \{\pm 1\}.$$

Now the quotient group S_n/A_n consists of two cosets: the even permutations form one coset (namely A_n) and the odd permutations form the other coset. The isomorphism above is simply saying that we can label all of the even permutations with 1 and all of the odd permutations with -1, and in this way multiplication in the quotient corresponds exactly to multiplication of the labels.

Recall that if G is a group and H and K are subgroups of G, then we defined

$$HK = \{hk : h \in H \text{ and } k \in K\}.$$

(see Definition 6.4.1). Immediately after that definition we showed that HK is not in general a subgroup of G by considering the case where $G = S_3$, $H = H = \langle(1\ 2)\rangle = \{id, (1\ 2)\}$, and $K = \langle(1\ 3)\rangle = \{id, (1\ 3)\}$. In this case, we had

$$\begin{aligned} HK &= \{id \circ id, id \circ (1\ 3), (1\ 2) \circ id, (1\ 2)(1\ 3)\} \\ &= \{id, (1\ 3), (1\ 2), (1\ 3\ 2)\}, \end{aligned}$$

which is not a subgroup of G. Moreover, notice that

$$\begin{aligned} KH &= \{id \circ id, id \circ (1\ 2), (1\ 3) \circ id, (1\ 3)(1\ 2)\} \\ &= \{id, (1\ 2), (1\ 3), (1\ 2\ 3)\}, \end{aligned}$$

so we also have that $HK \neq KH$. Fortunately, if at least one of H or K is normal in G, then neither of these problems arise.

Proposition 6.7.3. *Let H and N be subgroups of a group G, and suppose that N is a normal subgroup of G. We have the following:*

1. *$HN = NH$.*
2. *HN is a subgroup of G (and hence NH is a subgroup of G).*

Proof. We first show that $HN = NH$.

- We show that $HN \subseteq NH$. Let $a \in HN$ be arbitrary, and fix $h \in H$ and $n \in N$ with $a = hn$. One can show that $a \in NH$ directly from Condition 2 of Proposition 6.2.2, but we work with the conjugate instead. Notice that
$$a = hn = (hnh^{-1})h,$$
where $hnh^{-1} \in N$ (because N is a normal subgroup of G) and $h \in H$. Thus, $a \in NH$.
- We show that $NH \subseteq HN$. Let $a \in NH$ be arbitrary, and fix $n \in N$ and $h \in H$ with $a = nh$. Again, one can use Condition 1 of Proposition 6.2.2 directly, or notice that
$$a = nh = h(h^{-1}nh),$$
where $h \in H$ and $h^{-1}nh = h^{-1}n(h^{-1})^{-1} \in N$ because N is a normal subgroup of G. Thus, $a \in HN$.

We now check that HN is a subgroup of G.

- Since H and N are subgroups of G, we have $e \in H$ and $e \in N$. Since $e = ee$, it follows that $e \in HN$.
- Let $a, b \in HN$ be arbitrary. Fix $h_1, h_2 \in H$ and $n_1, n_2 \in N$ with $a = h_1n_1$ and $b = h_2n_2$. Since N is a normal subgroup of G, $n_1 \in N$, and $h_2 \in G$, we may use Property 1 from Proposition 6.2.2 to fix $n_3 \in N$ with $n_1h_2 = h_2n_3$. We then have
$$ab = h_1n_1h_2n_2 = h_1h_2n_3n_2.$$
Now $h_1, h_2 \in H$ and H is a subgroup of G, so $h_1h_2 \in H$. Also, $n_3, n_2 \in N$ and N is a subgroup of G, so $n_3n_2 \in N$. Therefore
$$ab = (h_1h_2)(n_3n_2) \in HN.$$

- Let $a \in HN$. Fix $h \in H$ and $n \in N$ with $a = hn$. Notice that $n^{-1} \in N$ because N is a normal subgroup of G. Since N is a normal subgroup of G, $n^{-1} \in N$, and $h^{-1} \in G$, we may use Property 1 from Proposition 6.2.2 to fix $k \in N$ with $n^{-1}h^{-1} = h^{-1}k$. We then have

$$a^{-1} = (hn)^{-1} = n^{-1}h^{-1} = h^{-1}k.$$

  Now $h^{-1} \in H$ because H is a subgroup of G, so $a^{-1} = h^{-1}k \in HN$.

Therefore, HN is a subgroup of G. Since $NH = HN$ from above, it follows that NH is also a subgroup of G. □

Theorem 6.7.4 (Second Isomorphism Theorem). *Let G be a group, let H be a subgroup of G, and let N be a normal subgroup of G. We then have that HN is a subgroup of G, that N is a normal subgroup of HN, that $H \cap N$ is a normal subgroup of H, and that*

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

Proof. First notice that since N is a normal subgroup of G, we know from Proposition 6.7.3 that HN is a subgroup of G. Notice that for since $e \in H$, we have that that $n = en \in HN$ for all $n \in N$, so $N \subseteq HN$. Since N is a normal subgroup of G, it follows that N is a normal subgroup of HN because conjugation by elements of HN is just a special case of conjugation by elements of G. Therefore, we may form the quotient group HN/N. Notice that we also have $H \subseteq HN$ (because $e \in N$), so we may define $\varphi \colon H \to HN/N$ by letting $\varphi(h) = hN$. We check the following:

- φ is a homomorphism: For any $h_1, h_2 \in H$, we have

$$\begin{aligned}
\varphi(h_1h_2) &= h_1h_2N \\
&= h_1N \cdot h_2N \\
&= \varphi(h_1) \cdot \varphi(h_2).
\end{aligned}$$

- φ is surjective: Let $a \in HN$ be arbitrary. We need to show that $aN \in \text{range}(\varphi)$. Fix $h \in H$ and $n \in N$ with $a = hn$. Notice that we then have $h \sim_N a$ by definition of $\sim_N$, so $hN = aN$. It follows that $\varphi(h) = hN = aN$, so $aN \in \text{range}(\varphi)$.

- $\ker(\varphi) = H \cap N$: Suppose first that $a \in H \cap N$. We then have that $a \in N$, so $aN \cap eN \neq \emptyset$ and hence $aN = eN$. It follows that $\varphi(a) = aN = eN$, so $a \in \ker(\varphi)$. Since $a \in H \cap N$ was arbitrary, we conclude that $H \cap N \subseteq \ker(\varphi)$.

  Suppose conversely that $a \in \ker(\varphi)$ is arbitrary. Notice that the domain of φ is H, so $a \in H$. Since $a \in \ker(\varphi)$, we have $\varphi(a) = eN$, so $aN = eN$. It follows that $e^{-1}a \in N$, so $a \in N$. Therefore, $a \in H$ and $a \in N$, so $a \in H \cap N$. Since $a \in \ker(\varphi)$ was arbitrary, we conclude that $\ker(\varphi) \subseteq H \cap N$.

Therefore, $\varphi \colon H \to HN/N$ is a surjective homomorphism with kernel equal to $H \cap N$. Since $H \cap N$ is the kernel of a homomorphism with domain H, we know that $H \cap N$ is a normal subgroup of H. By the First Isomorphism Theorem, we conclude that

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

This completes the proof. □

Suppose that we have a normal subgroup N of a group G. We can then form the quotient group G/N and consider the projection homomorphism $\pi \colon G \to G/N$ given by $\pi(a) = aN$. Now if we have a subgroup of the quotient G/N, then Theorem 6.6.9 tells us that we can pull this subgroup back via π to obtain a subgroup of G. Call this resulting subgroup H. Now the elements of G/N are cosets, so when we pull back we see that H will be a union of cosets of N. In particular, since eN will be an element of G/N, we will have that $N \subseteq H$.

Conversely, suppose that H is a subgroup of G with the property that $N \subseteq H$. Suppose that $a \in H$ and $b \in G$ with $a \sim_N b$. We may then fix $n \in N$ with $an = b$. Since $N \subseteq H$, we have that $n \in H$, so $b = an \in H$. Thus, if H contains an element of a given coset of N, then H must contain every element of that coset. In other words, H is a union of cosets of N. Using Theorem 6.6.9 again, we can go across π and notice that the cosets which are subsets of H form a subgroup of the quotient. Furthermore, we have

$$\begin{aligned} \pi^{\rightarrow}[H] &= \{\pi(a) : a \in H\} \\ &= \{aN : a \in H\}, \end{aligned}$$

so we can view $\pi^{\rightarrow}[H]$ as simply the quotient group H/N.

Taken together, this is summarized in the following two important results. Most of the key ideas are discussed above and/or are included in Theorem 6.6.9, but I will omit a careful proof of the second.

Theorem 6.7.5 (Third Isomorphism Theorem)**.** *Let G be a group. Let N and H be normal subgroups of G with $N \subseteq H$. We then have that H/N is a normal subgroup of G/N and that*

$$\frac{G/N}{H/N} \cong \frac{G}{H}.$$

Proof. Define $\varphi\colon G/N \to G/H$ by letting $\varphi(aN) = aH$.

- φ is well-defined: If $a, b \in G$ with $aN = bN$, then $a \sim_N b$, so $a \sim_H b$ because $N \subseteq H$, and hence $aH = bH$.
- φ is a homomorphism: For any $a, b \in G$, we have

$$\begin{aligned} \varphi(aN \cdot bN) &= \varphi(abN) \\ &= abH \\ &= aH \cdot bH \\ &= \varphi(aN) \cdot \varphi(bN). \end{aligned}$$

- φ is surjective: For any $a \in G$, we have $\varphi(aN) = aH$, so $aH \in \text{range}(\varphi)$.
- $\ker(\varphi) = H/N$: For any $a \in G$, we have

$$\begin{aligned} aN \in \ker(\varphi) &\iff \varphi(aN) = eH \\ &\iff aH = eH \\ &\iff e^{-1}a \in H \\ &\iff a \in H. \end{aligned}$$

  Therefore, $\ker(\varphi) = \{aN : a \in H\} = H/N$.

Notice in particular that since H/N is the kernel of the homomorphism $\varphi\colon G/N \to G/H$, we know that H/N is a normal subgroup of G/N by Proposition 6.6.4. Now using the First Isomorphism Theorem, we conclude that

$$\frac{G/N}{H/N} \cong \frac{G}{H}.$$

This completes the proof. $\square$

Theorem 6.7.6 (Correspondence Theorem)**.** *Let G be a group and let N be a normal subgroup of G. For every subgroup H of G with $N \subseteq H$, we have that H/N is a subgroup of G/N and the function*

$$H \mapsto H/N$$

is a bijection from subgroups of G containing N to subgroups of G/N. Furthermore, we have the following properties for any subgroups H_1 and H_2 of G that both contain N:

1. *H_1 is a subgroup of H_2 if and only if H_1/N is a subgroup of H_2/N.*
2. *H_1 is a normal subgroup of H_2 if and only if H_1/N is a normal subgroup of H_2/N.*
3. *If H_1 is a subgroup of H_2, then $[H_2 : H_1] = [H_2/N : H_1/N]$.*

Chapter 7

Cyclic, Abelian, and Solvable Groups

7.1 Structure of Cyclic Groups

We know that every cyclic group of order $n \in \mathbb{N}^+$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, and that every infinite cyclic group is isomorphic to $\mathbb{Z}$. However, there is still more to say. In this section, we completely determine the subgroup structure of cyclic groups, as well as count the number of elements of each order. We begin with the following important fact.

Proposition 7.1.1. *Every subgroup of a cyclic group is cyclic.*

Proof. Suppose that G is a cyclic group and that H is a subgroup of G. Fix a generator c of G so that $G = \langle c \rangle$. If $H = \{e\}$ then $H = \langle e \rangle$, so H is cyclic. Suppose then that $H \neq \{e\}$. Since $H \neq \{e\}$ we can fix $b \in H$ with $b \neq e$. Since $G = \langle c \rangle$, we can fix $n \in \mathbb{Z}$ such that $c^n = b$. Notice that $c^n \in H$ and that $n \neq 0$ because $b \neq e$. Furthermore, we also have $c^{-n} = (c^n)^{-1} \in H$ because H is a subgroup of G, so

$$\{n \in \mathbb{N}^+ : c^n \in H\} \neq \emptyset.$$

Let m be the least element of this set (which exists by well-ordering). We show that $H = \langle c^m \rangle$. Since $c^m \in H$ and H is a subgroup of G, we know that $\langle c^m \rangle \subseteq H$ by Proposition 5.2.2. Let $a \in H$ be arbitrary. Since $H \subseteq G$, we also have $a \in G$, so we may fix $k \in \mathbb{Z}$ with $a = c^k$. Write $k = qm + r$ where $0 \leq r < m$. We then have

$$\begin{aligned} a &= c^k \\ &= c^{qm+r} \\ &= c^{mq}c^r, \end{aligned}$$

hence

$$\begin{aligned} c^r &= (c^{mq})^{-1} \cdot a \\ &= c^{-mq} \cdot a \\ &= (c^m)^{-q} \cdot a. \end{aligned}$$

Now $c^m \in H$ and $a \in H$. Since H is a subgroup of G, we know that it is closed under inverses and the group operation, hence $(c^m)^{-q} \cdot a \in H$ and so $c^r \in H$. By choice of m as the smallest positive power of c which lies in H, we conclude that we must have $r = 0$. Therefore,

$$a = c^k = c^{qm} = (c^m)^q \in \langle c^m \rangle.$$

Since $a \in H$ was arbitrary, it follows that $H \subseteq \langle c^m \rangle$. Combining this with the reverse containment above, we conclude that $H = \langle c^m \rangle$, so H is cyclic. □

Therefore, if G is a cyclic group and c is a generator for G, then every subgroup of G can be written in the form $\langle c^k \rangle$ for some $k \in \mathbb{Z}$ (since every element of G equals c^k for some $k \in \mathbb{Z}$). It is possible that the same subgroup can be written in two different such ways. For example, in $\mathbb{Z}/6\mathbb{Z}$ with generator $\overline{1}$, we have $\langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}\} = \langle \overline{4} \rangle$. We next determine when we have such equalities. We begin with the following lemma, which holds in any group.

Lemma 7.1.2. *Let G be a group, and let $a \in G$ have finite order $n \in \mathbb{N}^+$. Let $m \in \mathbb{Z}$ and let $d = \gcd(m, n)$. We then have that $\langle a^m \rangle = \langle a^d \rangle$.*

Proof. Since $d \mid m$, we may fix $k \in \mathbb{Z}$ with $m = dk$. We then have

$$a^m = a^{dt} = (a^d)^k.$$

Therefore, $a^m \in \langle a^d \rangle$ and hence $\langle a^m \rangle \subseteq \langle a^d \rangle$. We now prove the reverse containment. Since $d = \gcd(m, n)$, we may fix $k, \ell \in \mathbb{Z}$ with $d = mk + n\ell$. Now

$$\begin{aligned} a^d &= a^{mk+n\ell} \\ &= a^{mk} a^{n\ell} \\ &= (a^m)^k (a^n)^\ell \\ &= (a^m)^k e^\ell \\ &= (a^m)^k, \end{aligned}$$

so $a^d \in \langle a^m \rangle$, and hence $\langle a^d \rangle \subseteq \langle a^m \rangle$. Combing the two containments, we conclude that $\langle a^m \rangle = \langle a^d \rangle$. □

For example, in our above case where $G = \mathbb{Z}/6\mathbb{Z}$ and $a = \overline{1}$, we have $|a| = 6$ and $\overline{4} = a^4$. Since $\gcd(4, 6) = 2$, the lemma immediately implies that $\langle a^4 \rangle = \langle a^2 \rangle$, and hence $\langle \overline{4} \rangle = \langle \overline{2} \rangle$.

Proposition 7.1.3. *Let G be a finite cyclic group of order $n \in \mathbb{N}^+$, and let c be an arbitrary generator of G. If H is a subgroup of G, then $H = \langle c^d \rangle$ for some $d \in \mathbb{N}^+$ with $d \mid n$. Furthermore, if $H = \langle c^d \rangle$, then $|H| = \frac{n}{d}$.*

Proof. Let H be a subgroup of G. We know that H is cyclic by Proposition 7.1.1, so we may fix $a \in G$ with $H = \langle a \rangle$. Since $G = \langle c \rangle$, we can fix $m \in \mathbb{Z}$ with $a = c^m$. Let $d = \gcd(m, n)$ and notice that $d \in \mathbb{N}^+$ and $d \mid n$. We then have

$$H = \langle a \rangle = \langle c^m \rangle = \langle c^d \rangle$$

by Lemma 7.1.2. For the last claim, notice that if $H = \langle c^d \rangle$, then

$$\begin{aligned} |H| &= |\langle c^d \rangle| \\ &= |c^d| \\ &= \frac{n}{\gcd(d, n)} && \text{(by Proposition 4.6.8)} \\ &= \frac{n}{d}. \end{aligned}$$

This completes the proof. □

We can improve on the lemma to determine precisely when two powers of the same element generate the same subgroup.

Proposition 7.1.4. *Let G be a group and let $a \in G$.*

1. *Suppose that $|a| = n \in \mathbb{N}^+$. For any $\ell, m \in \mathbb{Z}$, we have that $\langle a^\ell \rangle = \langle a^m \rangle$ if and only if $\gcd(\ell, n) = \gcd(m, n)$.*
2. *Suppose that $|a| = \infty$. For any $\ell, m \in \mathbb{Z}$, we have $\langle a^\ell \rangle = \langle a^m \rangle$ if and only if either $\ell = m$ or $\ell = -m$.*

Proof. 1. Let $\ell, m \in \mathbb{Z}$ be arbitrary.

- Suppose first that $\langle a^\ell \rangle = \langle a^m \rangle$. By Proposition 4.6.8, we have
$$|\langle a^\ell \rangle| = |a^\ell| = \frac{n}{\gcd(\ell, n)},$$
and
$$|\langle a^m \rangle| = |a^m| = \frac{n}{\gcd(m, n)}.$$
Since $\langle a^\ell \rangle = \langle a^m \rangle$, it follows that $|\langle a^\ell \rangle| = |\langle a^m \rangle|$, and hence
$$\frac{n}{\gcd(\ell, n)} = \frac{n}{\gcd(m, n)}.$$
Thus, we have $n \cdot \gcd(\ell, n) = n \cdot \gcd(m, n)$. Since $n \neq 0$, we can divide by it to conclude that $\gcd(\ell, n) = \gcd(m, n)$.
- Suppose now that $\gcd(\ell, n) = \gcd(m, n)$, and let d be this common value. By Lemma 7.1.2, we have both $\langle a^\ell \rangle = \langle a^d \rangle$ and $\langle a^m \rangle = \langle a^d \rangle$. Therefore, $\langle a^\ell \rangle = \langle a^m \rangle$.

2. Let $\ell, m \in \mathbb{Z}$ be arbitrary.

- Suppose first that $\langle a^\ell \rangle = \langle a^m \rangle$. We then have $a^m \in \langle a^\ell \rangle$, so we may fix $k \in \mathbb{Z}$ with $a^m = (a^\ell)^k$. It follows that $a^m = a^{\ell k}$, hence $m = \ell k$ by Proposition 5.2.3, and so $\ell \mid m$. Similarly, using the fact that $a^\ell \in \langle a^m \rangle$, it follows that $m \mid \ell$. Since both $\ell \mid m$ and $m \mid \ell$, we can use Corollary 2.2.5 to conclude that either $\ell = m$ or $\ell = -m$.
- If $\ell = m$, then we trivially have $\langle a^\ell \rangle = \langle a^m \rangle$. Suppose then that $\ell = -m$. We then have $a^\ell = a^{-m} = (a^m)^{-1}$, so $a^\ell \in \langle a^m \rangle$ and hence $\langle a^\ell \rangle \subseteq \langle a^m \rangle$. We also have $a^m = a^{-\ell} = (a^\ell)^{-1}$, so $a^m \in \langle a^\ell \rangle$ and hence $\langle a^m \rangle \subseteq \langle a^\ell \rangle$. Combining both of these, we conclude that $\langle a^\ell \rangle = \langle a^m \rangle$.

□

We know by Lagrange's Theorem that if H is a subgroup of a finite group G, then $|H|$ is a divisor of $|G|$. In general, the converse to Lagrange's Theorem is false (although $|A_4| = 12$, it turns out that the group A_4 has no subgroup of order 6, as we will prove Chapter 8). However, for cyclic groups, we have the very strong converse that there is a unique subgroup order equal to each divisor of $|G|$.

Theorem 7.1.5. *Let G be a cyclic group, and let c be an arbitrary generator of G.*

1. *Suppose that $|G| = n \in \mathbb{N}^+$. For each $d \in \mathbb{N}^+$ with $d \mid n$, there is a unique subgroup of G of order d, namely $\langle c^{n/d} \rangle = \{a \in G : a^d = e\}$.*
2. *Suppose that $|G| = \infty$. Every subgroup of G equals $\langle c^m \rangle$ for some $m \in \mathbb{N}$, and each of these subgroups are distinct.*

Proof. 1. Let $d \in \mathbb{N}^+$ with $d \mid n$. We then have that $\frac{n}{d} \in \mathbb{Z}$ and $d \cdot \frac{n}{d} = n$. Thus, $\frac{n}{d} \mid n$, and we have $|\langle c^{n/d} \rangle| = \frac{n}{n/d} = d$ by Proposition 7.1.3. Therefore, $\langle c^{n/d} \rangle$ is a subgroup of G of order d.

We next show that $\langle c^{n/d} \rangle = \{a \in G : a^d = e\}$.

- $\langle c^{n/d}\rangle \subseteq \{a \in G : a^d = e\}$: Let $a \in \langle c^{n/d}\rangle$ be arbitrary. Fix $k \in \mathbb{Z}$ with $a = (c^{n/d})^k$. We then have $a = c^{nk/d}$, so
$$\begin{aligned} a^d &= c^{nk} \\ &= (c^n)^k \\ &= e^k \\ &= e. \end{aligned}$$
- $\{a \in G : a^d = e\} \subseteq \langle c^{n/d}\rangle$: Let $a \in G$ with $a^d = e$. Since c is a generator for G, we can fix $k \in \mathbb{Z}$ with $a = c^k$. We then have that
$$c^{kd} = (c^k)^d = a^d = e.$$
Since $|c| = n$, we may use Proposition 4.6.5 to conclude that $n \mid kd$. Fix $m \in \mathbb{Z}$ with $nm = kd$. We then have that $\frac{n}{d} \cdot m = k$, so
$$(c^{n/d})^m = c^{(n/d)\cdot m} = c^k = a,$$
and hence $a \in \langle c^{n/d}\rangle$.

Putting these containments together, we conclude that $\langle c^{n/d}\rangle = \{a \in G : a^d = e\}$.

Suppose now that H is an arbitrary subgroup of G with order d. By Lagrange's Theorem, every element of H has order dividing d, so $h^d = e$ for all $h \in H$. It follows that $H \subseteq \{a \in G : a^d = e\}$, and since each of these sets have cardinality d, we conclude that $H = \{a \in G : a^d = e\}$.

2. Let H be an arbitrary subgroup of G. We know that H is cyclic by Proposition 7.1.1, so we may fix $a \in G$ with $H = \langle a\rangle$. Since $G = \langle c\rangle$, we can fix $m \in \mathbb{Z}$ with $a = c^m$. If $m < 0$, then $-m > 0$, and $H = \langle c^m\rangle = \langle c^{-m}\rangle$ by Proposition 7.1.4.

   Finally, notice that if $m, n \in \mathbb{N}$ with $m \neq n$, then we also have $m \neq -n$ (because both m and n are nonnegative), so $\langle c^m\rangle \neq \langle c^n\rangle$ by Proposition 7.1.4 again.

□

Corollary 7.1.6. *The subgroups of $\mathbb{Z}$ are precisely $\langle n\rangle = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ for each $n \in \mathbb{N}$, and each of these are distinct.*

Proof. This is immediate from the fact that $\mathbb{Z}$ is a cyclic group generated by 1, and $1^n = n$ for all $n \in \mathbb{N}$. □

We now determine the number of *elements* of each order in a cyclic group. We start by determining the number of generators.

Proposition 7.1.7. *Let G be a cyclic group.*

1. *If $|G| = n \in \mathbb{N}^+$, then G has exactly $\varphi(n)$ distinct generators.*
2. *If $|G| = \infty$, then G has exactly 2 generators.*

Proof. Since G is cyclic, we may fix $c \in G$ with $G = \langle c\rangle$.

1. Suppose that $|G| = n \in \mathbb{N}^+$. We then have
$$G = \{c^0, c^1, c^2, \dots, c^{n-1}\},$$
and we know that $c^k \neq c^\ell$ whenever $0 \leq k < \ell < n$. Thus, we need only determine how many of these elements are generators. By Proposition 7.1.4, we have $\langle c^k\rangle = \langle c^1\rangle$ if and only if $\gcd(k, n) = \gcd(1, n)$. Since $\langle c\rangle = G$ and $\gcd(1, n) = 1$, we conclude that $\langle c^k\rangle = G$ if and only if $\gcd(k, n) = 1$. Therefore, the number of generators of G equals the number of $k \in \{0, 1, 2, \dots, n-1\}$ such that $\gcd(k, n) = 1$, which is $\varphi(n)$.

2. Suppose that $|G| = \infty$. We then have that $G = \{c^k : k \in \mathbb{Z}\}$ and that each of these elements are distinct by Proposition 5.2.3. Thus, we need only determine the number of $k \in \mathbb{Z}$ such that $\langle c^k \rangle = G$, which is the number of k in $\mathbb{Z}$ such that $\langle c^k \rangle = \langle c^1 \rangle$. Using Proposition 7.1.4, we have $\langle c^k \rangle = \langle c^1 \rangle$ if and only if either $k = 1$ or $k = -1$. Thus, G has exactly 2 generators.

□

Proposition 7.1.8. *Let G be a cyclic group of order n and let $d \mid n$. We then have that G has exactly $\varphi(d)$ many elements of order d.*

Proof. Let $H = \langle c^{n/d} \rangle = \{a \in G : a^d = e\}$. We know from Theorem 7.1.5 that H is the unique subgroup of G having order d. Since $H = \langle c^{n/d} \rangle$, we know that H is cyclic, and hence Proposition 7.1.7 tells us that H has exactly $\varphi(d)$ many element of order d. Now if $a \in G$ is any element with $|a| = d$, then $a^d = e$, and hence $a \in H$. Therefore, every element of G with order d lies in H, and hence G has exactly $\varphi(d)$ many elements of order d. □

Corollary 7.1.9. *For any $n \in \mathbb{N}^+$, we have*

$$n = \sum_{d \mid n} \varphi(d)$$

where the summation is over all positive divisors d of n.

Proof. Let $n \in \mathbb{N}^+$. Fix any cyclic group G of order n, such as $G = \mathbb{Z}/n\mathbb{Z}$. We know that every element of G has order some divisor of n, and furthermore we know that if $d \mid n$, then G has exactly $\varphi(d)$ many elements of order d. Therefore, the sum on the right-hand side simply counts the number of elements of G by breaking them up into the various possible orders. Since $|G| = n$, the result follows. □

Notice that the above proposition gives a recursive way to calculate $\varphi(n)$ because

$$\varphi(n) = n - \sum_{\substack{d \mid n \\ d < n}} \varphi(d)$$

for all $n \in \mathbb{N}^+$. Finally, we end this section by determining when two subgroups of a cyclic group are subgroups of each other.

Proposition 7.1.10. *Let G be a cyclic group.*

1. *Suppose that $|G| = n \in \mathbb{N}^+$. For each $d \in \mathbb{N}^+$ with $d \mid n$, let H_d be the unique subgroup of G of order d. We then have that $H_k \subseteq H_\ell$ if and only if $k \mid \ell$.*

2. *Suppose that $|G| = \infty$. Fix $c \in G$ with $G = \langle c \rangle$. For each $k \in \mathbb{N}$, let $H_k = \langle c^k \rangle$. For any $k, \ell \in \mathbb{N}$, we have $H_k \subseteq H_\ell$ if and only if $\ell \mid k$.*

Proof.

1. Let $k, \ell \in \mathbb{N}^+$ be arbitrary with $k \mid n$ and $\ell \mid n$. Notice that if $H_k \subseteq H_\ell$, then H_k is a subgroup of H_ℓ, so $k \mid \ell$ by Lagrange's Theorem. Conversely, suppose that $k \mid \ell$. Let $a \in H_k$ be arbitrary. By Theorem 7.1.5, we have $a^k = e$. Since $k \mid \ell$, we can fix $m \in \mathbb{Z}$ with $\ell = mk$, and notice that

$$a^\ell = a^{mk} = (a^k)^m = e^m = e$$

so $a \in H_\ell$ by Theorem 7.1.5. Therefore, $H_k \subseteq H_\ell$.

2. Let $k, \ell \in \mathbb{N}$ be arbitrary. If $\ell \mid k$, then we can fix $m \in \mathbb{Z}$ with $k = m\ell$, in which case we have $c^k = (c^\ell)^m \in \langle c^\ell \rangle$, so $\langle c^k \rangle \subseteq \langle c^\ell \rangle$ and hence $H_k \subseteq H_\ell$. Conversely, suppose that $H_k \subseteq H_\ell$. Since $c^k \in H_k$, we then have $c^k \in \langle c^\ell \rangle$, so we can fix $m \in \mathbb{Z}$ with $c^k = (c^\ell)^m$. We then have $c^k = c^{\ell m}$, so $k = \ell m$ by Proposition 5.2.3, and hence $\ell \mid k$.

□

Chapter 8

Group Actions

Our definition of a group involved axioms for an abstract algebraic object. However, many groups arise in a setting where the elements of the group naturally "move around" the elements of some set. For example, the elements of $GL_n(\mathbb{R})$ represent linear transformations on $\mathbb{R}^n$ and so "move around" points in n-dimensional space. When we discussed D_n, we thought of the elements of D_n as moving the vertices of a regular n-gon. The general notion of a group working on a set in this way is called a *group action*. Typically these sets are very geometric or combinatorial in nature, and we can understand the sets themselves by understanding how groups act on them. Perhaps more surprising, we can turn this idea around to obtain a great deal of information about groups by understanding the sets on which they act.

The concept of understanding an algebraic object by seeing it "act" on other objects, often from different areas of mathematics (geometry, topology, analysis, combinatorics, etc.), is a tremendously important part of modern mathematics. In practice, groups typically arise as symmetries of some object just like our introduction of D_n as the "symmetries" of the regular n-gon. Instead of n-gons, the objects can be graphs, manifolds, topological spaces, vector spaces, etc.

8.1 Actions, Orbits, and Stabilizers

We begin with a definition of a group action. Suppose that G is a group and X is a set. For G to act on X, we need to have a rule that takes a group element $g \in G$ and a set element $x \in X$, and tells us where g "sends" this element x. We codify this using a function $f\colon G \times X \to X$. But since we have a group G, we want this function to "play nice" with the group operation.

Definition 8.1.1. *Let G be a group and let X be a (nonempty) set. A* group action *of G on X is a function $f\colon G \times X \to X$, where we write $f(g, x)$ as $g * x$, such that*

- *$e * x = x$ for all $x \in X$.*
- *$a * (b * x) = (a \cdot b) * x$ for all $a, b \in G$ and $x \in X$.*

We describe this situation by saying that "G acts on X".

Here are several examples of group actions:

- $GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$ via the action $A * \vec{v} = A\vec{v}$. Notice that $I_n\vec{v} = \vec{v}$ for all $\vec{v} \in \mathbb{R}^n$ and $A(B\vec{v}) = (AB)\vec{v}$ for all $A, B \in GL_n(\mathbb{R})$ and all $\vec{v} \in \mathbb{R}^n$ from Linear Algebra.

- S_n acts on $\{1, 2, \ldots, n\}$ via the action $\sigma * i = \sigma(i)$. Notice that $id * i = i$ for all $i \in \{1, 2, \ldots, n\}$ and for any $\sigma, \tau \in S_n$ and $i \in \{1, 2, \ldots, n\}$, we have

$$\begin{aligned}\sigma * (\tau * i) &= \sigma * \tau(i) \\ &= \sigma(\tau(i)) \\ &= (\sigma \circ \tau)(i) \\ &= (\sigma \circ \tau) * i.\end{aligned}$$

- Let G be a group. G acts on G by left multiplication, i.e. $g * a = g \cdot a$. Notice that $e * a = e \cdot a = a$ for all $a \in G$. The second axiom of a group action follows from associativity of the group operation because for all $g, h, a \in G$ we have

$$\begin{aligned}g * (h * a) &= g * (h \cdot a) \\ &= g \cdot (h \cdot a) \\ &= (g \cdot h) \cdot a \\ &= (g \cdot h) * a.\end{aligned}$$

- Let G be a group. G acts on G by conjugation, i.e. $g * a = gag^{-1}$. Notice that $e * a = eae^{-1} = a$ for all $a \in G$. Also, for all $g, h, a \in G$ we have

$$\begin{aligned}g * (h * a) &= g * (hah^{-1}) \\ &= ghah^{-1}g^{-1} \\ &= gha(gh)^{-1} \\ &= (g \cdot h) * a.\end{aligned}$$

- If G acts on X, and H is a subgroup of G, then H acts on X by simply restricting the function. For example, since D_n is a subgroup of S_n, we see that D_n acts on $\{1, 2, \ldots, n\}$ via $\sigma * i = \sigma(i)$. Also, since $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$, it acts on $\mathbb{R}^n$ via matrix-vector products as well.

Proposition 8.1.2. *Suppose that G acts on X. Define a relation $\sim$ on X by letting $x \sim y$ if there exists $a \in G$ with $a * x = y$. The relation $\sim$ is an equivalence relation on X.*

Proof. We check the three properties:

- Reflexive: For any $x \in X$, we have $e * x = x$, so $x \sim x$.
- Symmetric: Suppose that $x, y \in X$ with $x \sim y$. Fix $a \in G$ with $a * x = y$. We then have

$$\begin{aligned}a^{-1} * y &= a^{-1} * (a * x) \\ &= (a^{-1} \cdot a) * x \\ &= e * x \\ &= x,\end{aligned}$$

  so $y \sim x$.
- Transitive: Suppose that $x, y, z \in X$ with $x \sim y$ and $y \sim z$. Fix $a, b \in G$ with $a * x = y$ and $b * y = z$. We then have

$$\begin{aligned}(b \cdot a) * x &= b * (a * x) \\ &= b * y \\ &= z,\end{aligned}$$

  so $x \sim z$.

$\square$

Definition 8.1.3. *Suppose that G acts on X. The equivalence class of x under the above relation $\sim$ is called the* orbit *of x. We denote this equivalence class by $\mathcal{O}_x$. Notice that $\mathcal{O}_x = \{a * x : a \in G\}$.*

If G acts on X, we know from our general theory of equivalence relations that the orbits partition X. For example, consider the case where $G = GL_2(\mathbb{R})$ and $X = \mathbb{R}^2$ with action $A * \vec{v} = A\vec{v}$. Notice that $\mathcal{O}_{(0,0)} = \{(0,0)\}$ because $A \cdot (0,0) = (0,0)$ for all $A \in GL_2(\mathbb{R})$. Let's next consider $\mathcal{O}_{(1,0)}$. That is, if we hit $(1,0)$ with every invertible 2×2 matrix, what is the resulting subset of $\mathbb{R}^2$? We claim that $\mathcal{O}_{(1,0)} = \mathbb{R}^2 \backslash \{(0,0)\}$. Since the orbits partition $\mathbb{R}^2$, we know that $(0,0) \notin \mathcal{O}_{(1,0)}$, so $\mathcal{O}_{(1,0)} \subseteq \mathbb{R}^2 \backslash \{(0,0)\}$. Now if $a, b \in \mathbb{R}$ with $a \neq 0$, then

$$\begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix}$$

is in $GL_2(\mathbb{R})$ since it has determinant $a \neq 0$, and

$$\begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix},$$

so $(a,b) \in \mathcal{O}_{(1,0)}$. If $b \in \mathbb{R}$ with $b \neq 0$, then

$$\begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}$$

is in $GL_2(\mathbb{R})$ since it has determinant $-b \neq 0$, and

$$\begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ b \end{pmatrix},$$

so $(0,b) \in \mathcal{O}_{(1,0)}$. Putting everything together, it follows that $\mathcal{O}_{(1,0)} = \mathbb{R}^2 \backslash \{(0,0)\}$. Since the orbits are equivalence classes, we conclude that $\mathcal{O}_{(x,y)} = \mathbb{R}^2 \backslash \{(0,0\}$ whenever $(x,y) \neq (0,0)$. Thus, the orbits partition $\mathbb{R}^2$ into the two pieces: the origin and the rest.

In contrast, consider what happens if we instead work with the following subgroup H of $GL_2(\mathbb{R})$. Let

$$H = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbb{R} \right\} \cup \left\{ \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} : \theta \in \mathbb{R} \right\}.$$

If you've seen the terminology, then H is the set of all *orthogonal* 2×2 matrices, i.e. matrices A such that $A^T = A^{-1}$ (where A^T is the transpose of A). Intuitively, the elements of the set on the left are rotations by angle θ and the elements of the set on the right are flips followed by rotations. One can show that elements of H preserve distance. That is, if $A \in H$ and $\vec{v} \in \mathbb{R}^2$, then $||A\vec{v}|| = ||\vec{v}||$ (this can be checked using general theory, or by checking directly using the above the matrices: Suppose that $(x,y) \in \mathbb{R}^2$ with $x^2 + y^2 = r^2$ and show that the same is true after hitting (x,y) with any of the above matrices). Thus, if we let H act on $\mathbb{R}^2$, it follows that every element of $\mathcal{O}_{(1,0)}$ is on the circle of radius 1 centered at the origin. Furthermore, $\mathcal{O}_{(1,0)}$ contains all of these points because

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$$

which gives all points on the unit circle as we vary θ. In general, by working through the details one can show that the orbits of this action are the circles centered at the origin.

Definition 8.1.4. *Suppose that G acts on X. For each $x \in X$, define $G_x = \{a \in G : a * x = x\}$. The set G_x is called the* stabilizer *of x.*

Proposition 8.1.5. *Suppose that G acts on X. For each $x \in X$, the set G_x is a subgroup of G.*

Proof. Let $x \in X$. Since $e * x = x$, we have $e \in G_x$. Suppose that $a, b \in G_x$. We then have that $a * x = x$ and $b * x = x$, so

$$\begin{aligned}(a \cdot b) * x &= a * (b * x) \\ &= a * x \\ &= x,\end{aligned}$$

and hence $a \cdot b \in G_x$. Suppose that $a \in G_x$. We then have $a * x = x$, so

$$\begin{aligned}a^{-1} * x &= a^{-1} * (a * x) \\ &= (a^{-1} * a) * x \\ &= e * x \\ &= x,\end{aligned}$$

hence $a^{-1} \in G_x$. Therefore, G_x is a subgroup of G. $\square$

Since D_4 is a subgroup of S_4, and S_4 acts on $\{1, 2, 3, 4\}$ via $\sigma * i = \sigma(i)$, it follows that D_4 acts on $\{1, 2, 3, 4\}$ as well. To see how this works, we should remember our formal definitions of r and s as elements of S_n. In D_4, we have $r = (1\ 2\ 3\ 4)$ and $s = (2\ 4)$. Working out all of the elements as permutations, we see that

$$\begin{array}{cccc} id & r = (1\ 2\ 3\ 4) & r^2 = (1\ 3)(2\ 4) & r^3 = (1\ 4\ 3\ 2) \\ s = (2\ 4) & rs = (1\ 2)(3\ 4) & r^2 s = (1\ 3) & r^3 s = (1\ 4)(2\ 3) \end{array}$$

For stabilizers, notice that

$$G_1 = G_3 = \{id, s\} \qquad \text{and} \qquad G_2 = G_4 = \{id, r^2 s\}.$$

On the orbit side, we have

$$\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_3 = \mathcal{O}_4 = \{1, 2, 3, 4\}.$$

Lemma 8.1.6. *Suppose that G acts on X, and let $x \in X$. For any $a, b \in G$, we have*

$$a * x = b * x \Longleftrightarrow a \sim_{G_x} b.$$

Proof. Suppose first that $a, b \in G$ with $a * x = b * x$. We then have that

$$\begin{aligned}(a^{-1} \cdot b) * x &= a^{-1} * (b * x) \\ &= a^{-1} * (a * x) \\ &= (a^{-1} \cdot a) * x \\ &= e * x \\ &= x.\end{aligned}$$

Therefore, $a^{-1} b \in G_x$ and hence $a \sim_{G_x} b$.

Suppose conversely that $a, b \in G$ with $a \sim_{G_x} b$. Fix $h \in G_x$ with $ah = b$. We then have that

$$\begin{aligned}b * x &= (a \cdot h) * x \\ &= a * (h * x) \\ &= a * x,\end{aligned}$$

so $a * x = b * x$. $\square$

Theorem 8.1.7 (Orbit-Stabilizer Theorem). *Suppose that G acts on X, and let $x \in X$. There is a bijection between $\mathcal{O}_x$ and the set of (left) cosets of G_x in G, so $|\mathcal{O}_x| = [G : G_x]$. In particular, if G is finite, then*

$$|G| = |\mathcal{O}_x| \cdot |G_x|$$

so $|\mathcal{O}_x|$ divides $|G|$.

Proof. Let $\mathcal{L}_{G_x}$ be the set of left cosets of G_x in G. Define $f \colon \mathcal{L}_{G_x} \to \mathcal{O}_x$ by letting $f(aG_x) = a * x$. Now we are defining a function on cosets, but the right-to-left direction of Lemma 8.1.6 tells us that f is well-defined. Also, the left-to-right direction of Lemma 8.1.6 tells us that f is injective. Now if $y \in \mathcal{O}_x$, then we may fix $a \in G$ with $y = a * x$, and notice that $f(aG_x) = a * x = y$, so f is surjective. Therefore, $f \colon \mathcal{L}_{G_x} \to \mathcal{O}_x$ is a bijection and hence $|\mathcal{O}_x| = [G : G_x]$.

Suppose now that G is finite. By Lagrange's Theorem, we know that

$$[G : G_x] = \frac{|G|}{|G_x|},$$

so

$$|\mathcal{O}_x| = \frac{|G|}{|G_x|},$$

and hence

$$|G| = |\mathcal{O}_x| \cdot |G_x|.$$

This completes the proof. □

For example, consider the standard action of S_n on $\{1, 2, \ldots, n\}$. For every $i \in \{1, 2, \ldots, n\}$, we have $\mathcal{O}_i = \{1, 2, \ldots, n\}$ (because for each j, there is a permutation sending i to j), so as $|S_n| = n!$, it follows that $|G_i| = \frac{n!}{n} = (n-1)!$. In other words, there are $(n-1)!$ permutations of $\{1, 2, \ldots, n\}$ which fix a given element of $\{1, 2, \ldots, n\}$. Of course, this could have been proven directly, but it is an immediate consequence of the Orbit-Stabilizer Theorem.

In the case of D_4 acting on $\{1, 2, 3, 4\}$ discussed above, we saw that $\mathcal{O}_i = \{1, 2, 3, 4\}$ for all i. Thus, each stabilizer G_i satisfies $|G_i| = \frac{|D_4|}{4} = \frac{8}{4} = 2$, as was verified above.

8.2 Permutations and Cayley's Theorem

With several examples in hand, we start with the following proposition, which says that given a group action, each fixed element of G actually permutes the elements of X.

Definition 8.2.1. *Suppose that G acts on X. Given $a \in G$, define a function $\pi_a \colon X \to X$ by letting $\pi_a(x) = a * x$.*

Proposition 8.2.2. *Suppose that G acts on X. For each fixed $a \in G$, the function π_a is a permutation of X, i.e. is a bijection from X to X.*

Proof. Let $a \in G$ be arbitrary. We first check that π_a is injective. Let $x, y \in X$ and assume that $\pi_a(x) = \pi_a(y)$. We then have $a * x = a * y$, so

$$\begin{aligned} x &= e * x \\ &= (a^{-1} \cdot a) * x \\ &= a^{-1} * (a * x) \\ &= a^{-1} * (a * y) \\ &= (a^{-1} \cdot a) * y \\ &= e * y \\ &= y. \end{aligned}$$

Thus, the function π_a is injective.

We now check that π_a is surjection. Let $x \in X$ be arbitrary. Notice that

$$\begin{aligned}\pi_a(a^{-1} * x) &= a * (a^{-1} * x) \\ &= (a \cdot a^{-1}) * x \\ &= e * x \\ &= x,\end{aligned}$$

hence $x \in \text{range}(\pi_a)$. It follows that π_a is surjective.

Therefore, $\pi_a \colon X \to X$ is a bijection, so π_a is a permutation of X. □

Thus, given a group action of G on X, we can associate to each $a \in G$ a bijection π_a. Since each π_a is a bijection from X to X, we can view it as an element of S_X. The function that takes a and produces the function π_a is in fact a homomorphism.

Proposition 8.2.3. *Suppose that G acts on X. The function $\varphi \colon G \to S_X$ defined by letting $\varphi(a) = \pi_a$ is a homomorphism.*

Proof. We know from Proposition 8.2.2 that $\pi_a \in S_X$ for all $a \in G$. Let $a, b \in G$ be arbitrary. For any $x \in X$, we have

$$\begin{aligned}\pi_{a\cdot b}(x) &= (a \cdot b) * x \\ &= a * (b * x) && \text{(by the axioms of a group action)} \\ &= a * \pi_b(x) \\ &= \pi_a(\pi_b(x)) \\ &= (\pi_a \circ \pi_b)(x).\end{aligned}$$

Since $x \in X$ was arbitrary, it follows that $\pi_{a\cdot b} = \pi_a \circ \pi_b$. Thus, we have

$$\begin{aligned}\varphi(a \cdot b) &= \pi_{a\cdot b} \\ &= \pi_a \circ \pi_b \\ &= \varphi(a) \circ \varphi(b).\end{aligned}$$

Since $a, b \in G$ were arbitrary, it follows that $\varphi \colon G \to S_X$ is a homomorphism. □

We have shown that given an action of G on X, we obtain a homomorphism from G to S_X. We now show that we can reverse this process. That is, if we start with a homomorphism from G to S_X, we obtain a group action. Thus, we can view group actions from either perspective.

Proposition 8.2.4. *Let G be a group and let X be a set. If $\varphi \colon G \to S_X$ is a homomorphism, then the function from $G \times X$ to X defined by letting $a * x = \varphi(a)(x)$ is a group action of G on X.*

Proof. Since φ is a homomorphism, we know that $\varphi(e) = id_X$, hence for any $x \in X$ we have

$$\begin{aligned}e * x &= \varphi(e)(x) \\ &= id_X(x) \\ &= x.\end{aligned}$$

Suppose now that $a, b \in G$ and $x \in X$ are arbitrary. We then have

$$\begin{aligned} a * (b * x) &= \varphi(a)(b * x) \\ &= \varphi(a)(\varphi(b)(x)) \\ &= (\varphi(a) \circ \varphi(b))(x) \\ &= \varphi(a \cdot b)(x) \\ &= (a \cdot b) * x. \end{aligned}$$

Therefore, the function $a * x = \varphi(a)(x)$ is a group action. $\square$

Historically, the concept of a group was originally studied in the context of permuting the roots of a given polynomial (which leads to Galois Theory). In particular, group theory in the 18th and early 19th centuries really consisted of the study of subgroups of S_n and thus had a much more "concrete" feel to it. The more general abstract definition of a group (as *any* set with *any* operation satisfying the axioms) didn't arise until later. In particular, Lagrange's Theorem was originally proved only for certain special subgroups of symmetric groups related to roots of polynomials. However, once the abstract definition of a group as we now know it came about, it was quickly proved that *every* finite group was isomorphic to a subgroup of a symmetric group. Thus, up to isomorphism, the older, more "concrete", study of groups is equivalent to the more abstract study we are conducting. This result is known as Cayley's Theorem, and we now go about proving it. Before jumping into the proof, we first handle some preliminaries about the symmetric groups.

Proposition 8.2.5. *Suppose that X and Y are sets and that $f\colon X \to Y$ is a bijection. For each $\sigma \in S_X$, the function $f \circ \sigma \circ f^{-1}$ is a permutation of Y. Furthermore, the function $\varphi\colon S_X \to S_Y$ given by $\varphi(\sigma) = f \circ \sigma \circ f^{-1}$ is an isomorphism. In particular, if $|X| = |Y|$, then $S_X \cong S_Y$.*

Proof. Notice that $f \circ \sigma \circ f^{-1}$ is a function from Y to Y, and is a composition of bijections, so is itself a bijection. Thus, $f \circ \sigma \circ f^{-1}$ is a permutation of Y. Define $\varphi\colon S_X \to S_Y$ by letting $\varphi(\sigma) = f \circ \sigma \circ f^{-1}$. We check the following.

- φ is bijective. To see this, we show that φ has an inverse. Define $\psi\colon S_Y \to S_X$ by letting $\psi(\tau) = f^{-1} \circ \tau \circ f$ (notice that $f^{-1} \circ \tau \circ f$ is indeed a permutation of X by a similar argument as above). For any $\sigma \in S_X$, we have

$$\begin{aligned} (\psi \circ \varphi)(\sigma) &= \psi(\varphi(\sigma)) \\ &= \psi(f \circ \sigma \circ f^{-1}) \\ &= f^{-1} \circ (f \circ \sigma \circ f^{-1}) \circ f \\ &= (f^{-1} \circ f) \circ \sigma \circ (f^{-1} \circ f) \\ &= id_X \circ \sigma \circ id_X \\ &= \sigma. \end{aligned}$$

- φ preserves the group operation. Let $\sigma_1, \sigma_2 \in S_X$. We then have

$$\begin{aligned} \varphi(\sigma_1 \circ \sigma_2) &= f \circ (\sigma_1 \circ \sigma_2) \circ f^{-1} \\ &= f \circ \sigma_1 \circ (f^{-1} \circ f) \circ \sigma_2 \circ f^{-1} \\ &= (f \circ \sigma_1 \circ f^{-1}) \circ (f \circ \sigma_2 \circ f^{-1}) \\ &= \varphi(\sigma_1) \circ \varphi(\sigma_2). \end{aligned}$$

Therefore, $\varphi\colon S_X \to S_Y$ is an isomorphism. $\square$

Corollary 8.2.6. *If X is a finite set with $|X| = n$, then $S_X \cong S_n$.*

Proof. If X is finite with $|X| = n$, we may fix a bijection $f \colon X \to \{1, 2, 3, \ldots, n\}$ and apply the previous proposition. $\square$

Theorem 8.2.7 (Cayley's Theorem)**.** *Let G be a group. There exists a subgroup H of S_G such that $G \cong H$. Therefore, if $|G| = n \in \mathbb{N}^+$, then G is isomorphic to a subgroup of S_n.*

Proof. Consider the action of G on G given by $a * b = a \cdot b$. We know by Proposition 8.2.3 that the function $\varphi \colon G \to S_G$ given by $\varphi(a) = \pi_a$ is a homomorphism. We now check that φ is injective. Suppose that $a, b \in G$ with $\varphi(a) = \varphi(b)$. We then have that $\pi_a = \pi_b$, so in particular we have $\pi_a(e) = \pi_b(e)$, hence $a \cdot e = b \cdot e$, and so $a = b$. It follows that φ is injective. Since range(φ) is a subgroup of S_G by Corollary 6.6.10, we can view φ as a isomorphism from G to range(φ). Therefore, G is isomorphic to a subgroup of S_G.

Suppose finally that $|G| = n \in \mathbb{N}^+$. We know from above that $S_G \cong S_n$, we we may fix an isomorphism $\psi \colon S_G \to S_n$. We then have that $\psi \circ \varphi \colon G \to S_n$ is injective (because the composition of injective functions is injective) and that $\psi \circ \varphi$ preserves the group operation (as in the proof that the composition of isomorphisms is an isomorphism), so G is isomorphic to the subgroup range($\psi \circ \varphi$) of S_n. $\square$

8.3 The Conjugation Action and the Class Equation

Conjugacy Classes and Centralizers

Let G be a group. Throughout this section, we will consider the special case of the action of G on G given by conjugation. That is, we are considering the action $g * a = gag^{-1}$. In this case, the orbits and the stabilizers of the action are given special names.

Definition 8.3.1. *Let G be a group and consider the action of G on G given by conjugation.*

- *The orbits of this action are called* conjugacy classes*. The conjugacy class of a is the set*
$$\mathcal{O}_a = \{g * a : g \in G\} = \{gag^{-1} : g \in G\}.$$
- *For $a \in G$, the stabilizer G_a is called the* centralizer *of a in G and is denoted $C_G(a)$. Notice that*
$$g \in C_G(a) \iff g * a = a \iff gag^{-1} = a \iff ga = ag.$$
Thus,
$$C_G(a) = \{g \in G : ga = ag\}$$
is the set of elements of G which commute with a.

By our general theory of group actions, we know that $C_G(a)$ is a subgroup of G for every $a \in G$. Now the conjugacy classes are orbits, so they are subsets of G which partition G, but in general they are certainly *not* subgroups of G. However, we do know that if G is finite, then the size of every conjugacy class divides $|G|$ by the Orbit-Stabilizer Theorem because the size of a conjugacy class is the index of the corresponding centralizer subgroup. In fact, in this case, the Orbit-Stabilizer Theorem says that if G is finite, then

$$|\mathcal{O}_a| \cdot |C_G(a)| = |G|$$

for all $a \in G$. Notice that if $a \in G$, then we have $a \in C_G(a)$ (because a trivially commutes with a), so since $C_G(a)$ is a subgroup of G containing a, it follows that $\langle a \rangle \subseteq C_G(a)$. It is often possible to use this simple fact together with the above equality to help calculate conjugacy classes

As an example, consider the group $G = S_3$. We work out the conjugacy class and centralizer of the various elements. Notice first that $C_G(id) = G$ because every elements commutes with the identity, and the conjugacy class of id is $\{id\}$ because $\sigma \circ id \circ \sigma^{-1} = id$ for all $\sigma \in G$. Now consider the element $(1\ 2)$. On the one hand, we know that $\langle (1\ 2) \rangle = \{id, (1\ 2)\}$ is a subset of $C_G((1\ 2))$, so $|C_G((1\ 2))| \geq 2$. Since $|G| = 6$, we conclude that $|\mathcal{O}_{(1\ 2)}| \leq 3$. Now we know that $(1\ 2) \in \mathcal{O}_{(1\ 2)}$ because $\mathcal{O}_{(1\ 2)}$ is the equivalence class of $(1\ 2)$. Since

- $(2\ 3)(1\ 2)(2\ 3)^{-1} = (2\ 3)(1\ 2)(2\ 3) = (1\ 3)$
- $(1\ 3)(1\ 2)(1\ 3)^{-1} = (1\ 3)(1\ 2)(1\ 3) = (2\ 3)$

it follows that $(1\ 3)$ and $(2\ 3)$ are also in $\mathcal{O}_{(1\ 2)}$. We now have three elements of $\mathcal{O}_{(1\ 2)}$, and since $|\mathcal{O}_{(1\ 2)}| \leq 3$, we conclude that

$$\mathcal{O}_{(1\ 2)} = \{(1\ 2), (1\ 3), (2\ 3)\}.$$

Notice that we can now conclude that $|C_G((1\ 2))| = 2$, so in fact we must have $C_G((1\ 2)) = \{id, (1\ 2)\}$ without doing any other calculations.

We have now found two conjugacy classes which take up 4 of the elements of $G = S_3$. Let's look at the conjugacy class of $(1\ 2\ 3)$. We know it contains $(1\ 2\ 3)$, and since

$$(2\ 3)(1\ 2\ 3)(2\ 3)^{-1} = (2\ 3)(1\ 2\ 3)(2\ 3) = (1\ 3\ 2),$$

it follows that $(1\ 3\ 2)$ is there as well. Since the conjugacy classes partition G, these are the only possible elements so we conclude that

$$\mathcal{O}_{(1\ 2\ 3)} = \{(1\ 2\ 3), (1\ 3\ 2)\}.$$

Using the Orbit-Stabilizer Theorem it follows that $|C_G((1\ 2\ 3))| = 3$, so since $\langle (1\ 2\ 3) \rangle \subseteq C_G((1\ 2\ 3))$ and $|\langle (1\ 2\ 3) \rangle| = 3$, we conclude that $C_G((1\ 2\ 3)) = \langle (1\ 2\ 3) \rangle$. Putting it all together, we see that S_3 breaks up into three conjugacy classes:

$$\{id\} \qquad \{(1\ 2), (1\ 3), (2\ 3)\} \qquad \{(1\ 2\ 3), (1\ 3\ 2)\}$$

The fact that the 2-cycles form one conjugacy class and the 3-cycles form another is a specific case of a general fact which we now prove.

Lemma 8.3.2. *Let $\sigma \in S_n$ be a k-cycle, say $\sigma = (a_1\ a_2\ \dots\ a_k)$. For any $\tau \in S_n$, the permutation $\tau\sigma\tau^{-1}$ is a k-cycle and in fact*

$$\tau\sigma\tau^{-1} = (\tau(a_1)\ \tau(a_2)\ \dots\ \tau(a_k)).$$

(Note: this k-cycle may not have the smallest element first, so we may have to "rotate" it to have it in standard cycle notation).

Proof. For any i with $1 \leq i \leq k-1$, we have $\sigma(a_i) = a_{i+1}$, hence

$$(\tau\sigma\tau^{-1})(\tau(a_i)) = \tau(\sigma(\tau^{-1}(\tau(a_i)))) = \tau(\sigma(a_i)) = \tau(a_{i+1}).$$

Furthermore, since $\sigma(a_k) = a_1$, we have

$$(\tau\sigma\tau^{-1})(\tau(a_k)) = \tau(\sigma(\tau^{-1}(\tau(a_k)))) = \tau(\sigma(a_k)) = \tau(a_1).$$

To finish the proof, we need to show that $\tau\sigma\tau^{-1}$ fixes all elements distinct from the $\tau(a_i)$. Suppose then that $b \neq \tau(a_i)$ for each i. We then have that $\tau^{-1}(b) \neq a_i$ for all i. Since σ fixes all elements other the a_i, it follows that σ fixes $\tau^{-1}(b)$. Therefore

$$(\tau\sigma\tau^{-1})(b) = \tau(\sigma(\tau^{-1}(b))) = \tau(\tau^{-1}(b)) = b.$$

Putting it all together, we conclude that $\tau\sigma\tau^{-1} = (\tau(a_1)\ \tau(a_2)\ \dots\ \tau(a_k))$. $\square$

For example, suppose that $\sigma = (1\ 6\ 3\ 4)$ and $\tau = (1\ 7)(2\ 4\ 9\ 6)(5\ 8)$. To determine $\tau\sigma\tau^{-1}$, we need only apply τ to each of the elements in the cycle σ. Thus,

$$\tau\sigma\tau^{-1} = (7\ 2\ 3\ 9) = (2\ 3\ 9\ 7)$$

This result extends beyond k-cycles, and in fact we get the reverse direction as well.

Theorem 8.3.3. *Two elements of S_n are conjugate in S_n if and only if they have the same cycle structure, i.e. if and only if their cycle notations have the same number of k-cycles for each $k \in \mathbb{N}^+$.*

Proof. Let $\sigma \in S_n$ and suppose that we write σ in cycle notation as $\sigma = \pi_1\pi_2 \cdots \pi_n$ with the π_i disjoint cycles. For any $\tau \in S_n$, we have

$$\tau\sigma\tau^{-1} = \tau\pi_1\pi_2 \cdots \pi_n\tau^{-1} = (\tau\pi_1\tau^{-1})(\tau\pi_2\tau^{-1}) \cdots (\tau\pi_n\tau^{-1}).$$

By the lemma, each $\tau\pi_i\tau^{-1}$ is a cycle of the same length as π_i. Furthermore, the various cycles $\tau\pi_i\tau^{-1}$ are disjoint from each other because they are obtained by applying τ to the elements of the cycles, and τ is a bijection. Therefore, $\tau\sigma\tau^{-1}$ has the same cycle structure as σ.

Suppose conversely that σ and ρ have the same cycle structure. Match up the cycles of σ with the cycles of ρ in a manner which preserves cycle length (including 1-cycles). Define $\tau \colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ as follows. Given $i \in \{1, 2, \ldots, n\}$, let $\tau(i)$ be the element of the corresponding cycle in the corresponding position. Notice that τ is a bijection because the cycles in a given cycle notation are disjoint. By inserting $\tau\tau^{-1}$ between the various cycles of σ, we can use the lemma to conclude that $\tau\sigma\tau^{-1} = \rho$. $\square$

As an illustration of the latter part of the theorem, suppose that we are working in S_8 and we have

$$\sigma = (1\ 8)(2\ 5)(4\ 7\ 6) \qquad \text{and} \qquad \rho = (2\ 7\ 3)(4\ 5)(6\ 8).$$

Notice that σ and ρ have the same cycle structure, so they are conjugate in S_8. Let's write σ and ρ above each other to align the cycle structures:

$$\begin{aligned} \sigma &= (3)(1\ 8)(2\ 5)(4\ 7\ 6) \\ \rho &= (1)(4\ 5)(6\ 8)(2\ 7\ 3). \end{aligned}$$

The proof then defines τ by matching up the corresponding numbers, i.e. $\tau(3) = 1$, $\tau(1) = 4$, $\tau(8) = 5$, etc. Working it out, we see that we can take

$$\tau = (1\ 4\ 2\ 6\ 3)(5\ 8)(7),$$

and then we will have $\tau\sigma\tau^{-1} = \rho$.

The Class Equation

Given an action of G on X, we know that the orbits partition X. In particular, the conjugacy classes of a group G partition the set G. Thus, if we pick a unique element b_i from each of the m conjugacy classes of G, then we have

$$|G| = |\mathcal{O}_{b_1}| + |\mathcal{O}_{b_2}| + \cdots + |\mathcal{O}_{b_m}|.$$

Furthermore, since we know by the Orbit-Stabilizer Theorem that the size of an orbit divides the order of G, it follows that every summand on the right is a divisor of G.

We can get a more useful version of the above equation if we bring together the orbits of size 1. Let's begin by examining which elements of G form a conjugacy class by themselves. We have

$$\begin{aligned} \mathcal{O}_a = \{a\} &\Longleftrightarrow gag^{-1} = a \text{ for all } g \in G \\ &\Longleftrightarrow ga = ag \text{ for all } g \in G \\ &\Longleftrightarrow a \in Z(G). \end{aligned}$$

Thus, the elements which form a conjugacy class by themselves are exactly the elements of $Z(G)$. Now if we bring together these elements, and pick a unique element a_i from each of the k conjugacy classes of size at least 2, we get the equation:

$$|G| = |Z(G)| + |\mathcal{O}_{a_1}| + |\mathcal{O}_{a_2}| + \cdots + |\mathcal{O}_{a_k}|.$$

Since $Z(G)$ is a subgroup of G, we may use Lagrange's Theorem to conclude that each of the summands on the right is a divisor of G. Furthermore, we have $|\mathcal{O}_{a_i}| \geq 2$ for all i, although it might happen that $|Z(G)| = 1$. Finally, using the Orbit-Stabilizer Theorem, we can rewrite this latter equation as

$$|G| = |Z(G)| + [G : C_G(a_1)] + [G : C_G(a_2)] + \cdots + [G : C_G(a_k)],$$

where again each of the summands on the right is a divisor of G, and $[G : C_G(a_i)] \geq 2$ for all i. Each of these latter two equalities (either variation) is known as the *Class Equation* for G.

We saw above that the class equation for S_3 reads as

$$6 = 1 + 2 + 3.$$

In Problem 5c on Homework 4, we computed the number of elements of S_5 of each given cycle structure, so the class equation for S_5 reads as

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

Theorem 8.3.4. *Let $p \in \mathbb{N}^+$ be prime and let G be a group with $|G| = p^n$ for some $n \in \mathbb{N}^+$. We then have that $Z(G) \neq \{e\}$.*

Proof. Let $a_1, a_2, \dots, a_k$ be representatives from the conjugacy classes of size at least 2. By the Class Equation, we know that

$$|G| = |Z(G)| + |\mathcal{O}_{a_1}| + |\mathcal{O}_{a_2}| + \cdots + |\mathcal{O}_{a_k}|.$$

By the Orbit-Stabilizer Theorem, we know that $|\mathcal{O}_{a_i}|$ divides p^n for each i. By the Fundamental Theorem of Arithmetic, it follows that each $|\mathcal{O}_{a_i}|$ is one of $1, p, p^2, \dots, p^n$. Now we know that $|\mathcal{O}_{a_i}| > 1$ for each i, so p divides each $|\mathcal{O}_{a_i}|$. Since

$$|Z(G)| = |G| - |\mathcal{O}_{a_1}| - |\mathcal{O}_{a_2}| - \cdots - |\mathcal{O}_{a_k}|$$

and p divides every term on the right-hand side, we conclude that $p \mid |Z(G)|$. In particular, $Z(G) \neq \{e\}$. □

Corollary 8.3.5. *Let $p \in \mathbb{N}^+$ be prime. Every group of order p^2 is abelian.*

Proof. Let G be a group of order p^2. Using Corollary 6.5.6, we know that either $Z(G) = \{e\}$ or $Z(G) = G$. The former is impossible by the Theorem 8.3.4, so $Z(G) = G$ and hence G is abelian. □

Proposition 8.3.6. *Let $p \in \mathbb{N}^+$ be prime. If G is a group of order p^2, then either*

$$G \cong \mathbb{Z}/p^2\mathbb{Z} \qquad \text{or} \qquad G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Therefore, up to isomorphism, there are exactly two groups of order p^2.

Proof. Suppose that G is a group of order p^2. By Corollary 8.3.5, G is abelian. If there exists an element of G with order p^2, then G is cyclic and $G \cong \mathbb{Z}/p^2\mathbb{Z}$. Suppose then that G has no element of order p^2. By Lagrange's Theorem, the order of every element divides p^2, so the order of every nonidentity element of G must be p. Fix $a \in G$ with $a \neq e$, and let $H = \langle a \rangle$. Since $|H| = p < |G|$, we may fix $b \in G$ with $b \notin H$ and let $K = \langle b \rangle$. Notice that H and K are both normal subgroups of G because G is abelian. Now $H \cap K$ is a subgroup of K, so $|H \cap K|$ divides $|K| = p$. We can't have $|H \cap K| = p$, because this would imply that $H \cap K = K$, which would contradict the fact that $b \notin H$. Therefore, we must have $|H \cap K| = 1$, and hence

$H \cap K = \{e\}$. Since $|H| \cdot |K| = p^2 = |G|$, we may use Corollary 6.4.7 to conclude that G is the internal direct product of H and K. Since H and K are both cyclic of order p, they are both isomorphic to $\mathbb{Z}/p\mathbb{Z}$, so

$$G \cong H \times K \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Finally notice that $\mathbb{Z}/p^2\mathbb{Z} \not\cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ because the first group is cyclic while the second is not (by Problem 8 on Homework 5, for example). □

We are now in a position to extend Theorem 6.2.12 to arbitrary groups.

Theorem 8.3.7 (Cauchy's Theorem)**.** *Let $p \in \mathbb{N}^+$ be prime. If G is a group with $p \mid |G|$, then G has an element of order p.*

Proof. The proof is by induction on $|G|$. If $|G| = 1$, then the result is trivial because $p \nmid 1$ (again if you don't like this vacuous base case, simply note the if $|G| = p$, then every nonidentity element of G has order p by Lagrange's Theorem). Suppose then that G is a finite group with $p \mid |G|$, and suppose that the result is true for all groups K satisfying $p \mid |K|$ and $|K| < |G|$. Let $a_1, a_2, \dots, a_k$ be representatives from the conjugacy classes of size at least 2. By the Class Equation, we know that

$$|G| = |Z(G)| + [G : C_G(a_1)] + [G : C_G(a_2)] + \cdots + [G : C_G(a_k)].$$

We have two cases:

- *Case 1:* Suppose that $p \mid [G : C_G(a_i)]$ for all i. Since

  $$|Z(G)| = |G| - [G : C_G(a_1)] - [G : C_G(a_2)] - \cdots - [G : C_G(a_k)]$$

  and p divides every term on the right, it follows that $p \mid |Z(G)|$. Now $Z(G)$ is an abelian group, so Theorem 6.2.12 tells us that $Z(G)$ has an element of order p. Thus, G has an element of order p.

- *Case 2:* Suppose that $p \nmid [G : C_G(a_i)]$ for some i. Fix such an i. By Lagrange's Theorem we have

  $$|G| = [G : C_G(a_i)] \cdot |C_G(a_i)|$$

  Since p is a prime number with both $p \mid |G|$ and $p \nmid [G : C_G(a_i)]$, we must have that $p \mid |C_G(a_i)|$. Now $|C_G(a_i)| < |G|$ because $a_i \notin Z(G)$, and hence, by induction, $C_G(a_i)$ has an element of order p. Therefore, G has an element of order p.

The result follows by induction. □

8.4 Simplicity of A_5

Suppose that H is a subgroup of G. We know that one of the equivalent conditions for H to be a normal subgroup of G is that $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$. This leads to following simple result.

Proposition 8.4.1. *Let H be a subgroup of G. We then have that H is a normal subgroup of G if and only if H is a union of conjugacy classes of G.*

Proof. Suppose first that H is a normal subgroup of G. Suppose that H includes an element h from some conjugacy class of G. Now the conjugacy class of h in G equals $\{ghg^{-1} : g \in G\}$, and since $h \in H$ and H is normal in G, it follows that $\{ghg^{-1} : g \in G\} \subseteq H$. Thus, if H includes an element of some conjugacy class of G, then H must include that entire conjugacy class. It follows that H is a union of conjugacy class of G.

Suppose conversely that H is a subgroup of G that is a union of conjugacy classes of G. Given any $g \in G$ and $h \in H$, we have that ghg^{-1} is an element of the conjugacy class of h in G, so since $h \in H$, we must have $ghg^{-1} \in H$ as well. Therefore, H is a normal subgroup of G. □

If we understand the conjugacy classes of a group G, we can use this proposition to help us understand the normal subgroups of G. Let's begin such an analysis by looking at S_4. Recall that in Homework 4 we counted the number of elements of S_n of various cycle types. In particular, we showed that if $k \leq n$, then the number of k-cycles in S_n equals:

$$\frac{n(n-1)(n-2)\cdots(n-k+1)}{k}.$$

Also, if $n \geq 4$, we showed that the number of permutations in S_n which are the product of two disjoint 2-cycles equals

$$\frac{n(n-1)(n-2)(n-3)}{8}.$$

Using these results, we see that S_4 consists of the following numbers of elements of each cycle type.

- Identity: 1.
- 2-cycles: $\frac{4\cdot 3}{2} = 6$.
- 3-cycles: $\frac{4\cdot 3\cdot 2}{3} = 8$.
- 4-cycles: $\frac{4\cdot 3\cdot 2\cdot 1}{4} = 6$.
- Product of two disjoint 2-cycles: $\frac{4\cdot 3\cdot 2\cdot 1}{8} = 3$.

Since two elements of S_4 are conjugates in S_4 exactly when they have the same cycle type, this breakdown gives the conjugacy classes of S_4. In particular, the class equation of S_4 is:

$$24 = 1 + 3 + 6 + 6 + 8.$$

Using this class equation, let's examine the possible normal subgroups of S_4. We already know that A_4 is a normal subgroup of S_4 since it has index 2 in S_4 (see Proposition 6.2.6). However another way to see this is that A_4 contains the identity, the 3-cycles, and the products of two disjoint 2-cycles, so it is a union of conjugacy classes of S_4. In particular, it arises from taking the 1, the 3, and the 8 in the above class equation and putting them together to form a subgroup of size $1 + 3 + 8 = 12$.

Aside from the trivial examples of $\{id\}$ and S_4 itself, are there any other normal subgroups of S_4? Suppose that H is a normal subgroup of S_4 with $\{id\} \subsetneq H \subsetneq S_4$ and $H \neq A_4$. We certainly know that $id \in H$. By Lagrange's Theorem, we know we must have that $|H| \mid 24$. We also know that H must be a union of conjugacy classes of S_4. Thus, we would need to find a way to add some collection of the various numbers in the above class equation, necessarily including the number 1, such that their sum is a divisor of 24. One way is $1 + 3 + 8 = 12$ which gave A_4. Working through the various possibilities, we see that the only other nontrivial way to make it work is $1 + 3 = 4$. This corresponds to the subset

$$\{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Now this subset is certainly closed under conjugation, but it is not immediately obvious that it is a subgroup. Each nonidentity element here has order 2, so it is closed under inverses. Performing the simple check, it turns out that it is also closed under composition, so indeed this is another normal subgroup of S_4. Thus, the normal subgroups of S_4 are $\{id\}$, S_4, A_4, and this subgroup of order 4.

Now let's examine the possible normal subgroups of A_4. We already know three examples: $\{id\}$, A_4, and the just discovered subgroup of S_4 of size 4 (it is contained in A_4, and it must be normal in A_4 because it is normal in S_4). Now the elements of A_4 are the identity, the 3-cycles, and the products of two disjoint 2-cycles. Although the set of 3-cycles forms one conjugacy class in S_4, the set of eight 3-cycles does not form one conjugacy class in A_4. We can see this immediately because $|A_4| = 12$ and $8 \nmid 12$. The problem is that the elements of S_4 which happen to conjugate one 3-cycle to another might all be odd permutations, and hence do not exist in A_4. How can we determine the conjugacy classes in A_4 without simply plowing through all of the calculations from scratch?

Let's try to work out the conjugacy class of $(1\ 2\ 3)$ in A_4. First notice that we know that the conjugacy class of $(1\ 2\ 3)$ in S_4 has size 8, so by the Orbit-Stabilizer Theorem we conclude that $|C_{S_4}((1\ 2\ 3))| = \frac{24}{8} = 3$. Since $\langle(1\ 2\ 3)\rangle \subseteq C_{S_4}((1\ 2\ 3))$ and $|\langle(1\ 2\ 3)\rangle| = 3$, it follows that $C_{S_4}((1\ 2\ 3)) = \langle(1\ 2\ 3)\rangle$. Now $\langle(1\ 2\ 3)\rangle \subseteq A_4$, so we conclude that $C_{A_4}((1\ 2\ 3)) = \langle(1\ 2\ 3)\rangle$ as well. Therefore, by the Orbit-Stabilizer Theorem, the conjugacy class of $(1\ 2\ 3)$ in A_4 has size $\frac{12}{3} = 4$. If we want to work out what exactly it is, it suffices to find 4 conjugates of $(1\ 2\ 3)$ in A_4. Fortunately, we know how to compute conjugates quickly in S_n using Lemma 8.3.2 and the discussion afterwards:

- $id(1\ 2\ 3)id^{-1} = (1\ 2\ 3)$.
- $(1\ 2\ 4)(1\ 2\ 3)(1\ 2\ 4)^{-1} = (2\ 4\ 3)$.
- $(2\ 3\ 4)(1\ 2\ 3)(2\ 3\ 4)^{-1} = (1\ 3\ 4)$.
- $(1\ 2)(3\ 4)(1\ 2\ 3)[(1\ 2)(3\ 4)]^{-1} = (2\ 1\ 4) = (1\ 4\ 2)$.

Thus, the conjugacy class of $(1\ 2\ 3)$ in A_4 is:

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

If we work with a 3-cycle not in this set (for example, $(1\ 2\ 4)$), the above argument works through to show that its conjugacy class also has size 4, so its conjugacy class must be the other four 3-cycles in A_4. Thus, we get the conjugacy class

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

Finally, let's look at the conjugacy class of $(1\ 2)(3\ 4)$ in A_4. We have:

- $id(1\ 2)(3\ 4)id^{-1} = (1\ 2)(3\ 4)$.
- $(2\ 3\ 4)(1\ 2)(3\ 4)(2\ 3\ 4)^{-1} = (1\ 3)(4\ 2) = (1\ 3)(2\ 4)$.
- $(2\ 4\ 3)(1\ 2)(3\ 4)(2\ 4\ 3)^{-1} = (1\ 4)(2\ 3)$.

Thus, the products of two disjoint 2-cycles still form one conjugacy class in A_4. Why did this conjugacy class not break up? By the Orbit-Stabilizer Theorem, we know that $|C_{S_4}((1\ 2)(3\ 4))| = \frac{24}{3} = 8$. If we actually compute this centralizer, we see that four of its elements are even permutations and four of its elements are odd permutations. Therefore, $|C_{A_4}((1\ 2)(3\ 4))| = 4$ (the four even permutations in $C_{S_4}((1\ 2)(3\ 4))$), hence using the Orbit-Stabilizer Theorem again we conclude that the conjugacy class of $(1\ 2)(3\ 4)$ in A_4 has size $\frac{12}{4} = 3$.

Putting everything together, we see that the class equation of A_4 is:

$$12 = 1 + 3 + 4 + 4.$$

Working through the possibilities as in S_4, we conclude that the three normal subgroups of A_4 that we found above are indeed all of the normal subgroups of A_4 (there is no other way to add some subcollection of these numbers which includes 1 to obtain a divisor of 12). Notice that we can also conclude that following.

Proposition 8.4.2. *A_4 has no subgroup of order 6, so the converse of Lagrange's Theorem is false.*

Proof. If H was a subgroup of A_4 with $|H| = 6$, then H would have index 2 in A_4, so would be normal in A_4. However, we just saw that A_4 has no normal subgroup of order 6. $\square$

In the case of S_4 that we just worked through, we saw that when we restrict down to A_4, some conjugacy classes split into two and others stay intact. This is a general phenomenon in S_n, as we now show. We first need the following fact.

Lemma 8.4.3. *Let H be a subgroup of S_n. If H contains an odd permutation, then $|H \cap A_n| = \frac{|H|}{2}$.*

Proof. Suppose that H contains an odd permutation, and fix such an element $\tau \in H$. Let $X = H \cap A_n$ be the set of even permutations in H and let $Y = H \backslash A_n$ be the set of odd permutations in H. Define $f \colon X \to S_n$ by letting $f(\sigma) = \sigma\tau$. We claim that f maps X bijectively onto Y. We check the following:

- f is injective: Suppose that $\sigma_1, \sigma_2 \in X$ with $f(\sigma_1) = f(\sigma_2)$. We then have $\sigma_1\tau = \sigma_2\tau$, so $\sigma_1 = \sigma_2$ by cancellation.
- range$(f) \subseteq Y$. Let $\sigma \in X$. We have $\sigma \in H$, so $\sigma\tau \in H$ because H is a subgroup of S_n. Also, σ is a even permutation and τ is an odd permutation, so $\sigma\tau$ is an odd permutation. It follows that $f(\sigma) = \sigma\tau \in Y$.
- $Y \subseteq$ range(f): Let $\rho \in Y$. We then have $\rho \in H$ and $\tau \in H$, so $\rho\tau^{-1} \in H$ because H is a subgroup of S_n. Also, we have that both ρ and τ^{-1} are odd permutations, so $\rho\tau^{-1}$ is an even permutation. It follows that $\rho\tau^{-1} \in X$ and since $f(\rho\tau^{-1}) = \rho\tau^{-1}\tau = \rho$, we conclude that $\rho \in$ range(f).

Therefore, f maps X bijectively onto Y, and hence $|X| = |Y|$. Since $H = X \cup Y$ and $X \cap Y = \emptyset$, we conclude that $|H| = |X| + |Y|$. It follows that $|H| = 2 \cdot |X|$, so $|X| = \frac{|H|}{2}$. □

Proposition 8.4.4. *Let $\sigma \in A_n$. Let X be the conjugacy class of σ in S_n, and let Y be the conjugacy class of σ in A_n.*

- *If σ commutes with some odd permutation in S_n, then $Y = X$.*
- *If σ does not commute with any odd permutation in S_n, then $Y \subseteq X$ with $|Y| = \frac{|X|}{2}$.*

Proof. First notice that $X \subseteq A_n$ because $\sigma \in A_n$ and all elements of X have the same cycle type as σ. Let $H = C_{S_n}(\sigma)$ and let $K = C_{A_n}(\sigma)$. Notice that $Y \subseteq X$ and $K = H \cap A_n$. By the Orbit-Stabilizer Theorem applied in each of S_n and A_n, we know that

$$|H| \cdot |X| = n! \qquad \text{and} \qquad |K| \cdot |Y| = \frac{n!}{2},$$

and therefore

$$2 \cdot |K| \cdot |Y| = |H| \cdot |X|.$$

Suppose first that σ commutes with some odd permutation in S_n. We then have H contains an odd permutation, so by the lemma we know that $|K| = |H \cap A_n| = \frac{|H|}{2}$. Plugging this into the above equation, we see that $|H| \cdot |Y| = |H| \cdot |X|$, so $|Y| = |X|$. Since $Y \subseteq X$, it follows that $Y = X$.

Suppose now that σ does not commute with any odd permutation in S_n. We then have that $H \subseteq A_n$, so $K = H \cap A_n = H$ and hence $|K| = |H|$. Plugging this into the above equation, we see that $2 \cdot |H| \cdot |Y| = |H| \cdot |X|$, so $|Y| = \frac{|X|}{2}$. □

Let's put all of the knowledge to work in order to study A_5. We begin by recalling Exercise 3 on Homework 4, where we computed the number of elements of S_5 of each given cycle type:

- Identity: 1.
- 2-cycles: $\frac{5 \cdot 4}{2} = 10$.
- 3-cycles: $\frac{5 \cdot 4 \cdot 3}{3} = 20$.

- 4-cycles: $\frac{5\cdot4\cdot3\cdot2}{4} = 30$.
- 5-cycles: $\frac{5\cdot4\cdot3\cdot2\cdot1}{5} = 24$.
- Product of two disjoint 2-cycles: $\frac{5\cdot4\cdot3\cdot2}{8} = 15$.
- Product of a 3-cycle and a 2-cycle which are disjoint: This equals the number of 3-cycles as discussed above, which is 20 from above.

This gives the following class equation for S_5:

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

Now in A_5 we only have the identity, the 3-cycles, the 5-cycles, and the product of two disjoint 2-cycles. Let's examine what happens to these conjugacy classes in A_5. By Proposition 8.4.4, we know that each of these conjugacy classes either stays intact or breaks in half.

- The set of 3-cycles has size 20, and since $(1\ 2\ 3)$ commutes with the odd permutation $(4\ 5)$, this conjugacy class stays intact in A_5.
- The set of 5-cycles has size 24, and since $24 \nmid 60$, it is not possible that this conjugacy class stays intact in A_5. Therefore, the set of 5-cycles breaks up into two conjugacy classes of size 12.
- The set of products of two disjoint 2-cycles has size 15. Since this is an odd number, it is not possible that it breaks into two pieces of size $\frac{15}{2}$, so it must remain a conjugacy class in A_5.

Therefore, the class equation for A_5 is:

$$60 = 1 + 12 + 12 + 15 + 20.$$

With this in hand, we can examine the normal subgroups of A_5. Of course we know that $\{id\}$ and A_5 are normal subgroups of S_5. Suppose that H is a normal subgroup of A_5 with $\{id\} \subsetneq H \subsetneq A_5$. We then have that $id \in H$, that $|H| \mid 60$, and that H is a union of conjugacy classes of A_5. Thus, we would need to find a way to add some collection of the various numbers in the above class equation, necessarily including the number 1, such that their sum is a divisor of 60. Working through the possibilities, we see that this is not possible except in the cases when we take all the numbers (corresponding to A_5) and we only take 1 (corresponding to $\{id\}$). We have proved the following important theorem.

Theorem 8.4.5. *A_5 is a simple group.*

In fact, A_n is a simple group for all $n \geq 5$, but the above method of proof falls apart for $n > 5$ (the class equations get too long and there occasionally are ways to add certain numbers to get divisors of $|A_n|$). Thus, we need some new techniques. One approach is to use induction on $n \geq 5$ starting with the base case that we just proved, but we will not go through all the details here.

8.5 Counting Orbits

Suppose that we color each vertex of a square with one of n colors. In total, there are n^4 many ways to do this because we have n choices for each of the 4 vertices. However, some of these colorings are the "same" up to symmetry. For example, if we color the upper left vertex red and the other 3 green, then we can get this by starting with the coloring the upper right vertex red, the others green, and rotating. How many possible colorings are there up to symmetry?

We can turn this question into a question about counting orbits of a given group action. We begin by letting

$$X = \{(a_1, a_2, a_3, a_4) : 1 \leq a_i \leq n \text{ for all } i\}.$$

Intuitively, we are labeling the four vertices of the square with the numbers $1, 2, 3, 4$, and we are letting a_i denote the color of vertex i. If we use the labeling where the upper left corner is 1, the upper right is 2, the lower right is 3, and the lower left is 4, then the above above colorings are

$$(R, G, G, G) \qquad \text{and} \qquad (G, R, G, G),$$

where R is number we associated to color red and G the number for color green. Of course, these are distinct elements of X, but we want to make them the "same". Notice that S_4 acts on X via the action:

$$\sigma * (a_1, a_2, a_3, a_4) = (a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}, a_{\sigma(4)}).$$

For example, we have

$$(1\ 2\ 3) * (a_1, a_2, a_3, a_4) = (a_2, a_3, a_1, a_4),$$

so

$$(1\ 2\ 3) * (R, B, Y, G) = (B, Y, R, G).$$

Now we really don't want to consider these two colorings to be the same, because although we can get from one to the other via an element of S_4, we can't do it from a rigid motion of the square. However, since D_4 is a subgroup of S_4, we can restrict the above to an action of D_4 on X. Recall that when viewed as a subgroup of S_4 we can list the elements of D_4 as:

$$\begin{array}{cccc} e & r = (1\ 2\ 3\ 4) & r^2 = (1\ 3)(2\ 4) & r^3 = (1\ 4\ 3\ 2) \\ s = (2\ 4) & rs = (1\ 2)(3\ 4) & r^2s = (1\ 3) & r^3s = (1\ 4)(2\ 3) \end{array}$$

The key insight is that two colorings are the same exactly when they are in the same orbit of this action by D_4. For example, we have the following orbits:

- $\mathcal{O}_{(R,R,R,R)} = \{(R, R, R, R)\}$.
- $\mathcal{O}_{(R,G,G,G)} = \{(R, G, G, G), (G, R, G, G), (G, G, R, G), (G, G, G, R)\}$.
- $\mathcal{O}_{(R,G,R,G)} = \{(R, G, R, G), (G, R, G, R)\}$.

Thus, to count the number of colorings up to symmetry, we want to count the number of orbits of this action. The problem in attacking this problem directly is that the orbits have different sizes, so we can not simply divide n^4 by the common size of the orbits. We need a better way to count the number of orbits of an action.

Definition 8.5.1. *Suppose that G acts on X. For each $g \in G$, let $X_g = \{x \in X : g * x = x\}$. The set X_g is called the* fixed-point set *of g.*

Theorem 8.5.2 (Burnside's Lemma - due originally to Cauchy - sometimes also attributed to Frobenius)**.** *Suppose that G acts on X and that both G and X are finite. If k is the number of orbits of the action, then*

$$k = \frac{1}{|G|} \sum_{g \in G} |X_g|.$$

Thus, the number of orbits is the average number of elements fixed by each $g \in G$.

Proof. We the count the set $A = \{(g,x) \in G \times X : g * x = x\}$ in two different ways. On the one hand, for each $g \in G$, there are $|X_g|$ many elements of A in the "row" corresponding to g, so $|A| = \sum_{g \in G} |X_g|$. On the other hand, for each $x \in X$, there are $|G_x|$ many elements of A in the "column" corresponding to x, so $|A| = \sum_{x \in X} |G_x|$. Using the Orbit-Stabilizer Theorem, we know that

$$\sum_{g \in G} |X_g| = |A| = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|\mathcal{O}_x|} = |G| \cdot \sum_{x \in X} \frac{1}{|\mathcal{O}_x|},$$

and therefore

$$\frac{1}{|G|} \sum_{g \in G} |X_g| = \sum_{x \in X} \frac{1}{|\mathcal{O}_x|}.$$

Let's examine this latter sum. Let $P_1, P_2, \dots, P_k$ be the distinct orbits of X. We then have that

$$\sum_{x \in X} \frac{1}{|\mathcal{O}_x|} = \sum_{i=1}^{k} \sum_{x \in P_i} \frac{1}{|P_i|} = \sum_{i=1}^{k} |P_i| \cdot \frac{1}{|P_i|} = \sum_{i=1}^{k} 1 = k.$$

Therefore,

$$\frac{1}{|G|} \sum_{g \in G} |X_g| = \sum_{x \in X} \frac{1}{|\mathcal{O}_x|} = k.$$

□

Of course, Burnside's Lemma will only be useful if it is not hard to compute the various values $|X_g|$. Let's return to our example of D_4 acting on the set X above. First notice that $X_e = X$, so $|X_e| = n^4$. Let move on to $|X_r|$ where $r = (1\ 2\ 3\ 4)$. Which elements (a_1, a_2, a_3, a_4) are fixed by r? We have $r * (a_1, a_2, a_3, a_4) = (a_2, a_3, a_4, a_1)$, so $r * (a_1, a_2, a_3, a_4) = (a_1, a_2, a_3, a_4)$ if and only if $a_1 = a_2$, $a_2 = a_3$, $a_3 = a_4$, and $a_4 = a_1$. Thus, an element (a_1, a_2, a_3, a_4) is fixed by r exactly when all the a_i are equal. There are n such choices (because we can pick a_1 arbitrarily, and then all the others are determined), so $|X_r| = n$. In general, given any $\sigma \in D_4$, an element of X is in X_σ exactly when all of the entries in each cycle of σ get the same color. Therefore, we have $|X_\sigma| = n^d$ where d is the number of cycles in the cycle notation of σ, assuming that we include the 1-cycles. For example, we have $|X_{r^2}| = n^2$ and $|X_s| = n^3$. Working this out in the above cases and using the fact that $|D_4| = 8$, we conclude from Burnside's Lemma that the number of ways to color the vertices of the square with n colors up to symmetry is:

$$\frac{1}{8}(n^4 + n + n^2 + n + n^3 + n^2 + n^3 + n^2) = \frac{1}{8}(n^4 + 2n^3 + 3n^2 + 2n).$$

Let's examine the problem of coloring the faces of a cube. We will label the faces of a cube as a 6-sided die is labeled so that opposing faces sum to 7. For example, we could take the top face to be 1, the bottom 6, the front 2, the back 5, the right 3, and the left 4. With this labeling, the symmetries of the cube form a subgroup of S_6. Letting G be this subgroup, notice that $|G| = 24$ because we can put any of the 6 faces on top, and then rotate around the top in 4 distinct ways. Working through the actual elements, one sees that G equals the following subset of S_6:

id	$(2\ 3\ 5\ 4)$	$(2\ 5)(3\ 4)$	$(2\ 4\ 5\ 3)$
$(1\ 2)(3\ 4)(5\ 6)$	$(1\ 3\ 2)(4\ 5\ 6)$	$(1\ 5\ 6\ 2)$	$(1\ 4\ 2)(3\ 5\ 6)$
$(1\ 2\ 3)(4\ 6\ 5)$	$(1\ 3)(2\ 5)(4\ 6)$	$(1\ 5\ 3)(2\ 4\ 6)$	$(1\ 4\ 6\ 3)$
$(1\ 2\ 4)(3\ 6\ 5)$	$(1\ 3\ 6\ 4)$	$(1\ 5\ 4)(2\ 3\ 6)$	$(1\ 4)(2\ 5)(3\ 6)$
$(1\ 2\ 6\ 5)$	$(1\ 3\ 5)(2\ 6\ 4)$	$(1\ 5)(2\ 6)(3\ 4)$	$(1\ 4\ 5)(2\ 6\ 3)$
$(1\ 6)(3\ 4)$	$(1\ 6)(2\ 3)(4\ 5)$	$(1\ 6)(2\ 5)$	$(1\ 6)(2\ 4)(3\ 5)$

Let's examine how these elements arise.

- Identity: 1 of these, and it fixes all n^6 many colorings.
- 4-cycles: These are 90^o rotations around the line through the center of two opposing faces. There are 6 of these (3 such lines, and we can rotate in either direction), and each fixes n^3 many colorings.
- Product of two 2-cycles: These are 180^o rotations around the line through the center of two opposing faces. There are 3 of these, and each fixes n^4 many colorings.
- Product of two 3-cycles: These are rotations around the line through opposite corners of the cube. There are 8 of these (there are four pairs of opposing corners, and then we can rotate either 120^o or 240^o for each), and each fixes n^2 many colorings .
- Product of three 2-cycles: These are 180^o rotations around a line through the middle of opposing edges of the cube. There are 6 of these (there are 6 such pairs of opposing edges), and each fixes n^3 many colorings.

Using Burnside's Lemma, we conclude that the total number of colorings of the faces of a cube using n colors up to symmetry is:

$$\frac{1}{24}(n^6 + 3n^4 + 12n^3 + 8n^2).$$

Chapter 9

Introduction to Rings

9.1 Definitions and Examples

We now define another fundamental algebraic structure. Whereas groups have one binary operation, rings come equipped with two. We tend to think of them as "addition" and "multiplication", although just like for groups all that matters is the properties that they satisfy.

Definition 9.1.1. *A* ring *is a set R equipped with two binary operations $+$ and $\cdot$ and two elements $0, 1 \in R$ satisfying the following properties:*

1. $a + (b + c) = (a + b) + c$ *for all* $a, b, c \in R$.
2. $a + b = b + a$ *for all* $a, b \in R$.
3. $a + 0 = a = 0 + a$ *for all* $a \in R$.
4. *For all $a \in R$, there exists $b \in R$ with $a + b = 0 = b + a$.*
5. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *for all* $a, b, c \in R$.
6. $a \cdot 1 = a$ *and* $1 \cdot a = a$ *for all* $a \in R$.
7. $a \cdot (b + c) = a \cdot b + a \cdot c$ *for all* $a, b, c \in R$.
8. $(a + b) \cdot c = a \cdot c + b \cdot c$ *for all* $a, b, c \in R$.

Notice that the first four axioms simply say that $(R, +, 0)$ is an abelian group.

Some sources omit property 6 and so do not require that their rings have a multiplicative identity. They call our rings either "rings with identity" or "rings with 1". We will not discuss such objects here, and for us "ring" implies that there is a multiplicative identity. Notice that we are requiring that $+$ is commutative but we do *not* require that $\cdot$ is commutative. Also, we are *not* requiring that elements have multiplicative inverses.

For example, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all rings with the standard notions of addition and multiplication along with the usual 0 and 1. For each $n \in \mathbb{N}^+$, the set $M_n(\mathbb{R})$ of *all* $n \times n$ matrices with entries from $\mathbb{R}$ is a ring, where $+$ and $\cdot$ are the usual matrix addition and multiplication, 0 is the zero matrix, and $1 = I_n$ is the $n \times n$ identity matrix. Certainly some matrices in $M_n(\mathbb{R})$ fail to be invertible, but that is not a problem because the ring axioms say nothing about the existence of multiplicative inverses. Notice that the multiplicative *group* $GL_n(\mathbb{R})$ is not a ring because it is not closed under addition. For example

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

but this latter matrix is not an element of $GL_2(\mathbb{R})$. The next proposition gives some examples of finite rings.

Proposition 9.1.2. *Let $n \in \mathbb{N}^+$. The set $\mathbb{Z}/n\mathbb{Z}$ of equivalence classes of the relation $\equiv_n$ with operations*

$$\overline{a} + \overline{b} = \overline{a+b} \qquad \textit{and} \qquad \overline{a} \cdot \overline{b} = \overline{ab},$$

is a ring with additive identity $\overline{0}$ and multiplicative identity $\overline{1}$.

Proof. We already know that $(\mathbb{Z}/n\mathbb{Z}, +, \overline{0})$ is an abelian group. We proved that multiplication of equivalence classes given by $\overline{a} \cdot \overline{b} = \overline{ab}$ is well-defined in Proposition 3.6.4, so it gives a binary operation on $\mathbb{Z}/n\mathbb{Z}$. It is now straightforward to check that $\overline{1}$ is a multiplicative identity, that $\cdot$ is associative, and that $\cdot$ distributes over addition by appealing to these facts in $\mathbb{Z}$. □

Initially, it may seem surprising that we require that $+$ is commutative in rings. In fact, this axiom follows from the others (so logically we could omit it). To see this, suppose that R satisfies all of the above axioms except possibly axiom 2. Let $a, b \in R$ be arbitrary. We then have

$$\begin{aligned}(1+1) \cdot (a+b) &= (1+1) \cdot a + (1+1) \cdot b \\ &= 1 \cdot a + 1 \cdot a + 1 \cdot b + 1 \cdot b \\ &= a + a + b + b,\end{aligned}$$

and also

$$\begin{aligned}(1+1) \cdot (a+b) &= 1 \cdot (a+b) + 1 \cdot (a+b) \\ &= a + b + a + b,\end{aligned}$$

hence

$$a + a + b + b = a + b + a + b.$$

Now we are assuming that $(R, +, 0)$ is a group because we have axioms 1, 3, and 4, so by left and right cancellation we conclude that $a + b = b + a$.

If R is a ring, then we know that $(R, +, 0)$ is a group. In particular, every $a \in R$ has a unique additive inverse. Since we have another binary operation in multiplication, we choose different notation new notation for the additive inverse of a (rather than use the old a^{-1} which looks multiplicative).

Definition 9.1.3. *Let R be a ring. Given $a \in R$, we let $-a$ be the unique additive inverse of a, so $a + (-a) = 0$ and $(-a) + a = 0$.*

Proposition 9.1.4. *Let R be a ring.*

1. *For all $a \in R$, we have $a \cdot 0 = 0 = 0 \cdot a$.*
2. *For all $a, b \in R$, we have $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$.*
3. *For all $a, b \in R$, we have $(-a) \cdot (-b) = a \cdot b$.*
4. *For all $a \in R$, we have $-a = (-1) \cdot a$.*

Proof.

1. Let $a \in R$ be arbitrary. We have

$$\begin{aligned} a \cdot 0 &= a \cdot (0+0) \\ &= (a \cdot 0) + (a \cdot 0). \end{aligned}$$

   Therefore

$$0 + (a \cdot 0) = (a \cdot 0) + (a \cdot 0)$$

   By cancellation in the group $(R, +, 0)$, it follows that $a \cdot 0 = 0$. Similarly we have

$$\begin{aligned} 0 \cdot a &= (0+0) \cdot a \\ &= (0 \cdot a) + (0 \cdot a). \end{aligned}$$

   Therefore

$$0 + (0 \cdot a) = (0 \cdot a) + (0 \cdot a).$$

   By cancellation in the group $(R, +, 0)$, it follows that $0 \cdot a = 0$.

2. Let $a, b \in R$ be arbitrary. We have

$$\begin{aligned} 0 &= a \cdot 0 && \text{(by 1)} \\ &= a \cdot (b + (-b)) \\ &= (a \cdot b) + (a \cdot (-b)). \end{aligned}$$

   Therefore, $a \cdot (-b)$ is the additive inverse of $a \cdot b$ (since $+$ is commutative), which is to say that $a \cdot (-b) = -(a \cdot b)$. Similarly

$$\begin{aligned} 0 &= 0 \cdot b && \text{(by 1)} \\ &= (a + (-a)) \cdot b \\ &= (a \cdot b) + ((-a) \cdot b), \end{aligned}$$

   so $(-a) \cdot b$ is the additive inverse of $a \cdot b$, which is to say that $(-a) \cdot b = -(a \cdot b)$.

3. Let $a, b \in R$ be arbitrary. Using 2, we have

$$\begin{aligned} (-a) \cdot (-b) &= -(a \cdot (-b)) \\ &= -(-(a \cdot b)) \\ &= a \cdot b, \end{aligned}$$

   where we have used the group theoretic fact that the inverse of the inverse is the original element (i.e. Proposition 4.2.6).

4. Let $a \in R$ be arbitrary. We have

$$\begin{aligned} (-1) \cdot a &= -(1 \cdot a) && \text{(by 2)} \\ &= -a. \end{aligned}$$

□

Definition 9.1.5. *Let R be a ring. Given $a, b \in R$, we define $a - b = a + (-b)$.*

Proposition 9.1.6. *If R is a ring with $1 = 0$, then $R = \{0\}$.*

Proof. Suppose that $1 = 0$. For every $a \in R$, we have

$$a = a \cdot 1 = a \cdot 0 = 0.$$

Thus, $a = 0$ for all $a \in R$. It follows that $R = \{0\}$. $\square$

Definition 9.1.7. *A* commutative ring *is a ring R such that $\cdot$ is commutative, i.e. such that $a \cdot b = b \cdot a$ for all $a, b \in R$.*

Definition 9.1.8. *Let R be a ring. A* subring *of R is a subset $S \subseteq R$ with the following properties:*

- *S is an additive subgroup of R (so S contains 0, is closed under $+$, and closed under additive inverses).*
- *$1 \in S$.*
- *$ab \in S$ whenever $a \in S$ and $b \in S$.*

Here are two important examples of subrings:

1. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a subring of $\mathbb{R}$. To see this, first notice that $0 = 0 + 0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ and $1 = 1 + 0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Suppose that $x, y \in \mathbb{Q}[\sqrt{2}]$ and fix $a, b, c, d \in \mathbb{Q}$ with $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$. We then have that

$$\begin{aligned} x + y &= (a + b\sqrt{2}) + (c + d\sqrt{2}) \\ &= (a + c) + (b + d)\sqrt{2}, \end{aligned}$$

so $x + y \in \mathbb{Q}[\sqrt{2}]$. We also have

$$-x = -(a + b\sqrt{2}) = (-a) + (-b)\sqrt{2} \in \mathbb{Q},$$

so $-x \in \mathbb{Q}[\sqrt{2}]$, and

$$\begin{aligned} xy &= (a + b\sqrt{2})(c + d\sqrt{2}) \\ &= ac + ad\sqrt{2} + bc\sqrt{2} + 2bd \\ &= (ac + 2bd) + (ad + bc)\sqrt{2}, \end{aligned}$$

so $xy \in \mathbb{Q}[\sqrt{2}]$. Therefore, $\mathbb{Q}[\sqrt{2}]$ is a subring of $\mathbb{R}$.

2. $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$. To see this, first notice that $0 = 0 + 0i \in \mathbb{Z}[i]$ and $1 = 1 + 0i \in \mathbb{Z}[i]$. Suppose that $x, y \in \mathbb{Z}[i]$ and fix $a, b, c, d \in \mathbb{Z}$ with $x = a + bi$ and $y = c + di$. We then have that

$$\begin{aligned} x + y &= (a + bi) + (c + di) \\ &= (a + c) + (b + d)i, \end{aligned}$$

so $x + y \in \mathbb{Z}[i]$. We also have

$$-x = -(a + bi) = (-a) + (-b)i \in \mathbb{Z}[i],$$

so $-x \in \mathbb{Z}[i]$, and also

$$\begin{aligned} xy &= (a + bi)(c + di) \\ &= ac + adi + bci + bdi^2 \\ &= (ac - bd) + (ad + bc)i, \end{aligned}$$

so $xy \in \mathbb{Z}[i]$. Therefore, $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$. The ring $\mathbb{Z}[i]$ is called the ring of *Gaussian Integers*

In our work on group theory, we made extensive use of subgroups of a given group G to understand G. In our discussion of rings, the concept of subrings will play a much smaller role. Some rings of independent interest can be seen as subrings of larger rings, such as $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Z}[i]$ above. However, we will not typically try to understand R by looking at its subrings. Partly, this is due to the fact that we will spend a large amount of time working with infinite rings (as opposed to the significant amount of time we spent on finite groups, where Lagrange's Theorem played a key role). As we will see, our attention will turn toward certain subsets of a ring called *ideals* which play a role similar to normal subgroups of a group.

Finally, one small note. Some authors use a slightly different definition of a subring in that they do not require that $1 \in S$. They use the idea that a subring of R should be a subset $S \subseteq R$ which forms a ring with the inherited operations, but the multiplicative identity of S could be different from the multiplicative identity of R. Again, since subrings will not play a particularly important role for us, we will not dwell on this distinction.

9.2 Units and Zero Divisors

As we mentioned, our ring axioms do not require that elements have multiplicative inverses. Those elements which do have multiplicative inverses are given special names.

Definition 9.2.1. *Let R be a ring. An element $u \in R$ is a* unit *if it has a multiplicative inverse, i.e. there exists $v \in R$ with $uv = 1 = vu$. We denote the set of units of R by $U(R)$.*

In other words, that units of R are the invertible elements of R under the associative operation $\cdot$ with identity 1 as in Section 4.3. For example, the units in $\mathbb{Z}$ are $\{\pm 1\}$ and the units in $\mathbb{Q}$ are $\mathbb{Q}\backslash\{0\}$ (and similarly for $\mathbb{R}$ and $\mathbb{C}$). The units in $M_n(\mathbb{R})$ are the invertible $n \times n$ matrices.

Proposition 9.2.2. *Let R be a ring and let $u \in U(R)$. There is a unique $v \in R$ with $uv = 1$ and $vu = 1$.*

Proof. Existence follows from the assumption that u is a unit, and uniqueness is immediate from Proposition 4.3.2. □

Definition 9.2.3. *Let R be a ring and let $u \in U(R)$. We let u^{-1} be the unique multiplicative inverse of u, so $uu^{-1} = 1$ and $u^{-1}u = 1$.*

Proposition 9.2.4. *Let R be a ring. The set $U(R)$ forms an group under multiplication with identity* 1.

Proof. Immediate from Corollary 4.3.5. □

This finally explains our notation for the group $U(\mathbb{Z}/n\mathbb{Z})$; namely, we are considering $\mathbb{Z}/n\mathbb{Z}$ as a ring and forming the corresponding unit group of that ring. Notice that for any $n \in \mathbb{N}^+$, we have $GL_n(\mathbb{R}) = U(M_n(\mathbb{R}))$.

Let's recall the multiplication table of $\mathbb{Z}/6\mathbb{Z}$:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Looking at the table, we see that $U(\mathbb{Z}/6\mathbb{Z}) = \{\overline{1}, \overline{5}\}$ as we already know. As remarked when we first saw this table in Section 4.4, there are some other interesting things. For example, we have $\overline{2} \cdot \overline{3} = \overline{0}$, so it is possible to have the product of two nonzero elements result in 0. Elements which are part of such a pair are given a name.

Definition 9.2.5. *Let R be ring. A* zero divisor *is a nonzero element $a \in R$ such that there exists a nonzero $b \in R$ such that* either *$ab = 0$ or $ba = 0$ (or both).*

In the above case of $\mathbb{Z}/6\mathbb{Z}$, we see that the zero divisors are $\{\overline{2}, \overline{3}, \overline{4}\}$. The concept of unit and zero divisor are antithetical as we now see.

Proposition 9.2.6. *Let R be a ring. No element is both a unit and zero divisor.*

Proof. Suppose that R is a ring and that $a \in R$ is a unit. If $b \in R$ satisfies $ab = 0$, then

$$\begin{aligned} b &= 1 \cdot b \\ &= (a^{-1}a) \cdot b \\ &= a^{-1} \cdot (ab) \\ &= a^{-1} \cdot 0 \\ &= 0. \end{aligned}$$

Thus, there is no nonzero $b \in R$ with $ab = 0$. Similarly, if $b \in R$ satisfies $ba = 0$, then

$$\begin{aligned} b &= b \cdot 1 \\ &= b \cdot (aa^{-1}) \\ &= (ba) \cdot a^{-1} \\ &= 0 \cdot a^{-1} \\ &= 0. \end{aligned}$$

Thus, there is no nonzero $b \in R$ with $ba = 0$. It follows that a is not a zero divisor. □

Proposition 9.2.7. *Let $n \in \mathbb{N}^+$ and let $a \in \mathbb{Z}$.*

- *If $\gcd(a, n) = 1$, then $\overline{a}$ is a unit in $\mathbb{Z}/n\mathbb{Z}$.*
- *If $\gcd(a, n) > 1$ and $\overline{a} \neq \overline{0}$, then $\overline{a}$ is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$.*

Proof. The first part is given by Proposition 4.4.4. Suppose that $\gcd(a, n) > 1$ and $\overline{a} \neq \overline{0}$. Let $d = \gcd(a, n)$ and notice that $0 < d < n$ because $n \nmid a$ (since we are assuming $\overline{a} \neq \overline{0}$). We have $d \mid n$ and $d \mid a$, so we may fix $b, c \in \mathbb{Z}$ with $db = n$ and $dc = a$. Notice that $0 < b < n$ because $d, n \in \mathbb{N}$ and $d > 1$, hence $\overline{b} \neq 0$. Now

$$ab = (dc)b = (db)c = nc,$$

so $n \mid ab$. It follows that $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{0}$. Since $\overline{b} \neq 0$, we conclude that $\overline{a}$ is a zero divisor. □

Therefore, every nonzero element of $\mathbb{Z}/n\mathbb{Z}$ is either a unit or a zero divisor. However, this is not true in every ring. The units in $\mathbb{Z}$ are $\{\pm 1\}$ but there are no zero divisors in $\mathbb{Z}$. We now define three important classes of rings.

Definition 9.2.8. *Let R be a ring.*

- *R is a* division ring *if $1 \neq 0$ and every nonzero element of R is a unit.*
- *R is a* field *if R is a commutative division ring. Thus, a field is a commutative ring with $1 \neq 0$ for which every nonzero element is a unit.*
- *R is an* integral domain *if R is a commutative ring with $1 \neq 0$ which has no zero divisors. Equivalently, an integral domain is a commutative ring R with $1 \neq 0$ such that whenever $ab = 0$, either $a = 0$ or $b = 0$.*

Clearly every field is a division ring. We also have the following.

Proposition 9.2.9. *Every field is an integral domain.*

Proof. Suppose that R is a field. If $a \in R$ is nonzero, then it is a unit, so it is not a zero divisor by Proposition 9.2.6. $\square$

For example, each of $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields. The ring $\mathbb{Z}$ is an example of an integral domain which is not a field, so the concept of integral domain is strictly weaker. There also exist division rings which are not fields, such as the Hamiltonian Quaternions as discussed in Section 1.2:

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

with

$$\begin{array}{ccc} i^2 = -1 & j^2 = -1 & k^2 = -1 \\ ij = k & jk = i & ki = j \\ ji = -k & kj = -i & ik = -j \end{array}$$

We will return to such objects (and will actually prove that $\mathbb{H}$ really is a division ring) later.

Corollary 9.2.10. *We have the following:*

- *For each prime $p \in \mathbb{N}^+$, the ring $\mathbb{Z}/p\mathbb{Z}$ is a field (and hence also an integral domain).*
- *For each composite $n \in \mathbb{N}^+$ with $n \geq 2$, the ring $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain.*

Proof. If $p \in \mathbb{N}^+$ is prime, then every nonzero element of $\mathbb{Z}/p\mathbb{Z}$ is a unit by Proposition 9.2.7 (because if $a \in \{1, 2, \dots, p-1\}$, then $\gcd(a, p) = 1$ because p is prime). Suppose that $n \in \mathbb{N}^+$ with $n \geq 2$ is composite. Fix $d \in \mathbb{N}^+$ with $1 < d < n$ such that $d \mid n$. We then have that $\gcd(d, n) = d \neq 1$ and $\overline{d} \neq \overline{0}$, so $\overline{d}$ is a zero divisor by Proposition 9.2.7. Therefore, $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain. $\square$

Since there are infinitely many primes, this corollary provides us with an infinite supply of finite fields. Here are the addition and multiplication tables of $\mathbb{Z}/5\mathbb{Z}$ to get a picture of one of one of these objects.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Another example of a field is the ring $\mathbb{Q}[\sqrt{2}]$ discussed in the last section. Since $\mathbb{Q}[\sqrt{2}]$ is a subring of $\mathbb{R}$, it is a commutative ring with $1 \neq 0$. To see that it is a field, we need only check that every nonzero element has an inverse. Suppose that $a, b \in \mathbb{Q}$ are arbitrary with $a + b\sqrt{2} \neq 0$.

- We first claim that $a - b\sqrt{2} \neq 0$. Suppose instead that $a - b\sqrt{2} = 0$. We then have $a = b\sqrt{2}$. Now if $b = 0$, then we would have $a = 0$, so $a + b\sqrt{2} = 0$, which is a contradiction. Thus, $b \neq 0$. Dividing both sides of $a = b\sqrt{2}$ by b gives $\sqrt{2} = \frac{a}{b}$, contradicting the fact that $\sqrt{2}$ is irrational. Thus, we must have $a - b\sqrt{2} \neq 0$.

Since $a - b\sqrt{2} \neq 0$, we have $a^2 - 2b^2 = (a + b\sqrt{2})(a - b\sqrt{2}) \neq 0$, and

$$\begin{aligned}\frac{1}{a + b\sqrt{2}} &= \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} \\ &= \frac{a - b\sqrt{2}}{a^2 - 2b^2} \\ &= \frac{1}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}.\end{aligned}$$

Since $a, b \in \mathbb{Q}$, we have both $\frac{1}{a^2-2b^2} \in \mathbb{Q}$ and $\frac{-b}{a^2-2b^2} \in \mathbb{Q}$, so $\frac{1}{a+b\sqrt{2}} \in \mathbb{Q}[\sqrt{2}]$.

Although we will spend a bit of time discussing noncommutative rings, the focus of our study will be commutative rings and often we will be working with integral domains (and sometimes more specifically with fields). The next proposition is a fundamental tool when working in integral domains. Notice that it can fail in arbitrary commutative rings. For example, in $\mathbb{Z}/6\mathbb{Z}$ we have $\overline{3} \cdot \overline{2} = \overline{3} \cdot \overline{4}$, but $\overline{2} \neq \overline{4}$

Proposition 9.2.11. *Suppose that R is an integral domain and that $ab = ac$ with $a \neq 0$. We then have that $b = c$.*

Proof. Since $ab = ac$, we have $ab - ac = 0$. Using the distributive law, we see that $a(b - c) = 0$ (more formally, we have $ab + (-ac) = 0$, so $ab + a(-c) = 0$, hence $a(b + (-c)) = 0$, and thus $a(b - c) = 0$). Since R is an integral domain, either $a = 0$ or $b - c = 0$. Now the former is impossible by assumption, so we conclude that $b - c = 0$. Adding c to both sides, we conclude that $b = c$. □

Although $\mathbb{Z}$ is an example of integral domain which is not a field, it turns out that all such examples are infinite.

Proposition 9.2.12. *Every finite integral domain is a field.*

Proof. Suppose that R is a finite integral domain. Let $a \in R$ with $a \neq 0$. Define $\lambda_a \colon R \to R$ by letting $\lambda_a(b) = ab$. Now if $b, c \in R$ with $\lambda_a(b) = \lambda_a(c)$, then $ab = ac$, so $b = c$ by Proposition 9.2.11. Therefore, $\lambda_a \colon R \to R$ is injective. Since R is finite, it must be the case that λ_a is surjective. Thus, there exists $b \in R$ with $\lambda_a(b) = 1$, which is to say that $ab = 1$. Since R is commutative, we also have $ba = 1$. Therefore, a is a unit in R. Since $a \in R$ with $a \neq 0$ was arbitrary, it follows that R is a field. □

We can define direct products of rings just we did for direct products of groups. The proof that the componentwise operations give rise to a ring are straightforward.

Definition 9.2.13. *Suppose that $R_1, R_2, \ldots, R_n$ are all rings. Consider the Cartesian product*

$$R_1 \times R_2 \times \cdots \times R_n = \{(a_1, a_2, \ldots, a_n) : a_i \in R_i \text{ for } 1 \leq i \leq n\}.$$

Define operations $+$ and $\cdot$ on $R_1 \times R_2 \times \cdots \times R_n$ by letting

$$\begin{aligned}(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) &= (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \\ (a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) &= (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_n \cdot b_n),\end{aligned}$$

where we are using the operations from R_i in the i^{th} components. We then have that $R_1 \times R_2 \times \cdots \times R_n$ with these operations is a ring which is called the (external) direct product *of $R_1, R_2, \ldots, R_n$.*

Notice that if R and S are nonzero rings, then $R \times S$ is *never* an integral domain (even if R and S are both integral domains, or even fields) because $(1, 0) \cdot (0, 1) = (0, 0)$.

9.3 Polynomial Rings

Given a ring R, we show in this section how to build a new and important ring from R. The idea is to form the set of all "polynomials with coefficients in R". For example, we are used to working with polynomials over the real number $\mathbb{R}$, and example of which is

$$3x^7 + \sqrt{5}x^4 - 2x^2 + 142x - \pi.$$

Intuitively, we add and multiply polynomials in the obvious way:

- $(4x^2 + 3x - 2) + (8x^3 - 2x^2 - 81x + 14) = 8x^3 + 2x^2 - 78x + 12.$
- $(2x^2 + 5x - 3) \cdot (-7x^2 + 2x + 1) = -14x^4 - 31x^3 + 33x^2 - x - 3.$

In more detail, we multiplied by collecting like powers of x as follows:

$$(2 \cdot (-7))x^4 + (2 \cdot 2 + 5 \cdot (-7))x^3 + (2 \cdot 1 + 5 \cdot 2 + (-3) \cdot (-7))x^2 + (5 \cdot 1 + (-3) \cdot 2)x + (-3) \cdot 1$$

In general, we aim to carry over the above idea except we will allow our coefficients to come from a general ring R. Thus, a typical element should look like:

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where each $a_i \in R$. Before we dive into giving a formal definition, we first discuss polynomials a little more deeply.

In previous math courses, we typically thought of a polynomial with real coefficients as describing a certain function from $\mathbb{R}$ to $\mathbb{R}$ resulting from "plugging in for x". Thus, when we wrote the polynomial $4x^2 + 3x - 2$, we were probably thinking of it as the function which sends 1 to $4 + 3 - 2 = 5$, sends 2 to $16 + 6 - 2 = 20$, etc. In contrast, we will consciously avoid defining a polynomial as the resulting function obtained by "plugging in for x". To see why this distinction matters, consider the case where we are we working with the ring $R = \mathbb{Z}/2\mathbb{Z}$ and we have the two polynomials $\overline{1}x^2 + \overline{1}x + \overline{1}$ and $\overline{1}$. These look like different polynomials on the face of it. However, notice that

$$\overline{1} \cdot \overline{0}^2 + \overline{1} \cdot \overline{0} + \overline{1} = \overline{1}$$

and also

$$\overline{1} \cdot \overline{1}^2 + \overline{1} \cdot \overline{1} + \overline{1} = \overline{1},$$

so these two distinct polynomials "evaluate" to same thing whenever we plug in elements of R (namely they both produce the same function, i.e. the function that outputs $\overline{1}$ for each input). Therefore, the resulting functions are indeed equal as functions despite the fact the polynomials have distinct forms.

We will enforce this distinction between polynomials and the resulting functions, so we will simply define our ring in a manner that two different looking polynomials are really distinct elements of our ring. In order to do this carefully, let's go back and look at our polynomials. For example, consider the polynomial with real coefficients given by $5x^3 + 9x - 2$. Since we are not "plugging in" for x, this polynomial is determined by its sequence of coefficients. In other words, if we order the sequence from coefficients of smaller powers to coefficients of larger powers, we can represent this polynomial as the sequence $(-2, 9, 0, 5)$. Performing this step gets rid of the superfluous x which was really just serving as a placeholder, and honestly did not have any real meaning. We will adopt this perspective and simply *define* a polynomial to be such a sequence. However, since polynomials can have arbitrarily large degree, these finite sequences would all of different lengths. We get around this problem by defining polynomials as *infinite* sequences of elements of R in which only finitely many of the terms are nonzero.

Definition 9.3.1. *Let A be a set. An* infinite sequence *of elements of A is an infinite list $(a_0, a_1, a_2, \dots)$ where $a_n \in A$ for all $n \in \mathbb{N}$. We use the notation $(a_n)_{n\in\mathbb{N}}$ for an infinite sequence. More formally, an infinite sequence is a function $f : \mathbb{N} \to A$ which we can view as the sequence of values $f(0), f(1), f(2), \dots$.*

Definition 9.3.2. *Let R be a ring. We define a new ring denoted $R[x]$ whose elements are the set of all infinite sequences $(a_n)_{n\in\mathbb{N}}$ of elements of R such that $\{n \in \mathbb{N} : a_n \neq 0\}$ is finite. We define two binary operations on $R[x]$ as follows:*

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}}$$

and

$$\begin{aligned}(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} &= (a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0)_{n\in\mathbb{N}} \\ &= (\sum_{k=0}^{n} a_k b_{n-k})_{n\in\mathbb{N}} \\ &= (\sum_{i+j=n} a_i b_j)_{n\in\mathbb{N}}.\end{aligned}$$

We will see below that this makes $R[x]$ into a ring called the polynomial ring *over R.*

Let's pause for a moment to ensure that the above definition makes sense. Suppose that $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ are both infinite sequences of elements of R for which only finitely many nonzero terms. Fix $M, N \in \mathbb{N}$ such that $a_n = 0$ for all $n > M$ and $b_n = 0$ for all $n > N$. We then have that $a_n + b_n = 0$ for all $n > \max\{M, N\}$, so the infinite sequence $(a_n + b_n)_{n\in\mathbb{N}}$ only has finitely many nonzero terms. Also, we have

$$\sum_{i+j=n} a_i b_j = 0$$

for all $n > M + N$ (because if $n > M + N$ and $i + j = n$, then either $i > M$ or $j > N$, so either $a_i = 0$ or $b_j = 0$), hence the infinite sequence $(\sum_{i+j=n} a_i b_j)_{n\in\mathbb{N}}$ only has finitely many nonzero terms. We now check that these operations turn $R[x]$ into a ring.

Theorem 9.3.3. *Let R be a ring. The set $R[x]$ with the above operations is a ring with additive identity the infinite sequence $(0, 0, 0, 0, \dots)$ and multiplicative identity the infinite sequence $(1, 0, 0, 0, \dots)$. Furthermore, if R is commutative, then $R[x]$ is commutative.*

Proof. Many of these checks are routine. For example, $+$ is associative on $R[x]$ because for any infinite sequences $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$, and $(c_n)_{n\in\mathbb{N}}$, we have

$$\begin{aligned}(a_n)_{n\in\mathbb{N}} + [(b_n)_{n\in\mathbb{N}} + (c_n)_{n\in\mathbb{N}}] &= (a_n)_{n\in\mathbb{N}} + (b_n + c_n)_{n\in\mathbb{N}} \\ &= (a_n + (b_n + c_n))_{n\in\mathbb{N}} \\ &= ((a_n + b_n) + c_n)_{n\in\mathbb{N}} && \text{(since } + \text{ is associative on } R) \\ &= (a_n + b_n)_{n\in\mathbb{N}} + (c_n)_{n\in\mathbb{N}} \\ &= [(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}}] + (c_n)_{n\in\mathbb{N}}.\end{aligned}$$

The other ring axioms involving addition are completely analogous. However, checking the axioms involving multiplication is more interesting because our multiplication operation is much more complicated than componentwise multiplication. For example, let $(e_n)_{n\in\mathbb{N}}$ be the infinite sequence $1, 0, 0, 0, \dots$, i.e.

$$e_n = \begin{cases} 1 & \text{if } n = 0 \\ 0 & \text{if } n > 0 \end{cases}$$

Now for any infinite sequence $(a_n)_{n\in\mathbb{N}}$, we have

$$\begin{aligned}(e_n)_{n\in\mathbb{N}} \cdot (a_n)_{n\in\mathbb{N}} &= (\sum_{k=0}^{n} e_k a_{n-k})_{n\in\mathbb{N}} \\ &= (e_0 a_{n-0})_{n\in\mathbb{N}} \\ &= (1 \cdot a_{n-0})_{n\in\mathbb{N}} \\ &= (a_n)_{n\in\mathbb{N}},\end{aligned}$$

where we have used the fact that $e_k = 0$ whenever $k > 0$. We also have

$$\begin{aligned}(a_n)_{n\in\mathbb{N}} \cdot (e_n)_{n\in\mathbb{N}} &= (\sum_{k=0}^{n} a_k e_{n-k})_{n\in\mathbb{N}} \\ &= (a_n e_0)_{n\in\mathbb{N}} \\ &= (a_n \cdot 1)_{n\in\mathbb{N}} \\ &= (a_n)_{n\in\mathbb{N}},\end{aligned}$$

where we have used the fact that if $0 \le k < n$, then $n - k > 1$, so $e_{n-k} = 0$. Therefore, the infinite sequence $(1, 0, 0, 0, \dots)$ is indeed a multiplicative identity of $R[x]$.

The most interesting (i.e. difficult) check is that $\cdot$ is associative on $R[x]$. For any $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}}, (c_n)_{n\in\mathbb{N}}$, we have

$$\begin{aligned}(a_n)_{n\in\mathbb{N}} \cdot [(b_n)_{n\in\mathbb{N}} \cdot (c_n)_{n\in\mathbb{N}}] &= (a_n)_{n\in\mathbb{N}} \cdot (\sum_{\ell=0}^{n} b_\ell c_{n-\ell})_{n\in\mathbb{N}} \\ &= (\sum_{k=0}^{n} a_k \cdot (\sum_{\ell=0}^{n-k} b_\ell c_{n-k-\ell}))_{n\in\mathbb{N}} \\ &= (\sum_{k=0}^{n} \sum_{\ell=0}^{n-k} a_k (b_\ell c_{n-k-\ell}))_{n\in\mathbb{N}} \\ &= (\sum_{k+\ell+m=n} a_k (b_\ell c_m))_{n\in\mathbb{N}}\end{aligned}$$

and also

$$\begin{aligned}[(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}}] \cdot (c_n)_{n\in\mathbb{N}} &= (\sum_{k=0}^{n} a_k b_{n-k})_{n\in\mathbb{N}} \cdot (c_n)_{n\in\mathbb{N}} \\ &= (\sum_{\ell=0}^{n} (\sum_{k=0}^{\ell} a_k b_{\ell-k}) \cdot c_{n-\ell})_{n\in\mathbb{N}} \\ &= (\sum_{\ell=0}^{n} \sum_{k=0}^{\ell} (a_k b_{\ell-k}) c_{n-\ell})_{n\in\mathbb{N}} \\ &= (\sum_{k+\ell+m=n} (a_k b_\ell) c_m)_{n\in\mathbb{N}}.\end{aligned}$$

Since multiplication in R is associative, we know that $a_k(b_\ell c_m) = (a_k b_\ell)c_m$ for all $k, \ell, m \in \mathbb{N}$, so

$$(\sum_{k+\ell+m=n} a_k (b_\ell c_m))_{n\in\mathbb{N}} = (\sum_{k+\ell+m=n} (a_k b_\ell) c_m)_{n\in\mathbb{N}}$$

and hence
$$(a_n)_{n\in\mathbb{N}} \cdot [(b_n)_{n\in\mathbb{N}} \cdot (c_n)_{n\in\mathbb{N}}] = [(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}}] \cdot (c_n)_{n\in\mathbb{N}}.$$
One also needs to check the two distributive laws, and also that $R[x]$ is commutative when R is commutative, but these are notably easier than associativity of multiplication, and are left as an exercise. □

The above formal definition of $R[x]$ is precise and useful when trying to prove theorems about polynomials, but it is terrible to work with intuitively. Thus, when discussing elements of $R[x]$, we will typically use standard polynomial notation. For example, if we are dealing with $\mathbb{Q}[x]$, we will simply write the formal element
$$\left(5, 0, 0, -\frac{1}{3}, 7, 0, \frac{22}{7}, 0, 0, 0, \dots\right)$$
as
$$5 - \frac{1}{3}x^3 + 7x^4 + \frac{22}{7}x^6$$
or
$$\frac{22}{7}x^6 + 7x^4 - \frac{1}{3}x^3 + 5,$$
and we will treat the x as a meaningless placeholder symbol called an *indeterminate*. This is where the x comes from in the notation $R[x]$ (if for some reason we want to use a different indeterminate, say t, we instead use the notation $R[t]$). Formally, $R[x]$ will be the set of infinite sequences, but we often use this more straightforward notation in the future when working with polynomials. When working in $R[x]$ with this notation, we will typically call elements of $R[x]$ by names like $p(x)$ and $q(x)$ and write something like "Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be an element of $R[x]$". Since I can't say this enough, do *not* simply view this as saying that $p(x)$ is the resulting function. Keep a clear distinction in your mind between an element of $R[x]$ and the function it represents via "evaluation" that we discuss in Definition 10.1.9 below!

It is also possible to connect up the formal definition of $R[x]$ (as infinite sequences of elements of R with finitely many nonzero terms) and the more gentle standard notation of polynomials as follows. Every element $a \in R$ can be naturally associated with the sequence $(a, 0, 0, 0, \dots)$ in $R[x]$. If we simply *define* x to be the sequence $(0, 1, 0, 0, 0, \dots)$, then working in the ring R it is not difficult to check that $x^2 = (0, 0, 1, 0, 0, \dots)$, that $x^3 = (0, 0, 0, 1, 0, \dots)$, etc. With these identifications, if we interpret the additions and multiplications implicit in the polynomial
$$\frac{22}{7}x^6 + 7x^4 - \frac{1}{3}x^3 + 5$$
as their formal counterparts defined above, then everything matches up as we would expect.

Definition 9.3.4. *Let R be a ring. Given a* nonzero *element $(a_n)_{n\in\mathbb{N}} \in R[x]$, we define the* degree *of $(a_n)_{n\in\mathbb{N}}$ to be $\max\{n \in \mathbb{N} : a_n \neq 0\}$. In the more relaxed notation, given a* nonzero *polynomial $p(x) \in R[x]$, say*
$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
with $a_n \neq 0$, we define the degree *of $p(x)$ to be n. We write $\deg(p(x))$ for the degree of $p(x)$. Notice that we do not define the degree of the zero polynomial.*

The next proposition gives some relationship between the degrees of polynomials and the degrees of their sum/product.

Proposition 9.3.5. *Let R be a ring and let $p(x), q(x) \in R[x]$ be nonzero.*

1. *Either $p(x) + q(x) = 0$ or $\deg(p(x) + q(x)) \leq \max\{\deg(p(x)), \deg(q(x))\}$.*
2. *If $\deg(p(x)) \neq \deg(q(x))$, then $p(x) + q(x) \neq 0$ and $\deg(p(x) + q(x)) = \max\{\deg(p(x)), \deg(q(x))\}$.*
3. *Either $p(x) \cdot q(x) = 0$ or $\deg(p(x)q(x)) \leq \deg(p(x)) + \deg(q(x))$.*

Proof. We give an argument using our formal definitions. Let $p(x)$ be the sequence $(a_n)_{n\in\mathbb{N}}$ and let $q(x)$ be the sequence $(b_n)_{n\in\mathbb{N}}$. Let $M = \deg(p(x))$ so that $a_M \neq 0$ and $a_n = 0$ for all $n > M$. Let $N = \deg(q(x))$ so that $a_N \geq 0$ and $a_N = 0$ for all $n > N$.

1. Suppose that $p(x) + q(x) \neq 0$. For any $n > \max\{M, N\}$, we have $a_n + b_n = 0 + 0 = 0$, so $\deg(p(x) + q(x)) \leq \max\{M, N\}$.

2. Suppose that $M \neq N$. Suppose first that $M > N$. We then have $a_M + b_M = a_M + 0 = a_M \neq 0$, so $p(x)+q(x) \neq 0$ and $\deg(p(x)+q(x)) \geq \max\{\deg(p(x)), \deg(q(x))\}$. Combining this with the inequality in part 1, it follows that $\deg(p(x) + q(x)) = \max\{\deg(p(x)), \deg(q(x))\}$. A similar argument works if $N > M$.

3. Suppose that $p(x)q(x) \neq 0$. Let $n > M + N$ and consider the sum
$$\sum_{k=0}^{n} a_k b_{n-k} = 0.$$
Notice that if $k > M$, then $a_k = 0$ so $a_k b_{n-k} = 0$. Also, if $k < M$, then $n - k > M + N - k = N + (M - k) > N$, hence $b_{n-k} = 0$ and so $a_k b_{n-k} = 0$. Thus, $a_k b_{n-k} = 0$ for all k with $0 \leq k \leq n$, so it follows that
$$\sum_{k=0}^{n} a_k b_{n-k} = 0.$$
Therefore, $\deg(p(x)q(x)) \leq M + N$.

□

Notice that in the ring $\mathbb{Z}/6\mathbb{Z}[x]$, we have
$$(\overline{2}x^2 + \overline{5}x + \overline{4})(\overline{3}x + \overline{1}) = \overline{5}x^2 + \overline{5}x + \overline{4}$$
so the product of a degree 2 polynomial and a degree 1 polynomial results in a degree 2 polynomial. It follows that we can indeed have a strict inequality in the latter case. In fact, we can have the product of two nonzero polynomials result in the zero polynomial, i.e. there may exist zero divisors in $R[x]$. For example, working in $\mathbb{Z}/6\mathbb{Z}[x]$ again we have
$$(\overline{4}x + \overline{2}) \cdot \overline{3}x^2 = \overline{0}$$
Fortunately, for well-behaved rings, the degree of the product always equals the sum of the degrees.

Proposition 9.3.6. *Let R be an integral domain. If $p(x), q(x) \in R[x]$ are both nonzero, then $p(x)q(x) \neq 0$ and $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$.*

Proof. Let $p(x)$ be the sequence $(a_n)_{n\in\mathbb{N}}$ and let $q(x)$ be the sequence $(b_n)_{n\in\mathbb{N}}$. Let $M = \deg(p(x))$ so that $a_M \neq 0$ and $a_n = 0$ for all $n > M$. Let $N = \deg(q(x))$ so that $a_N \geq 0$ and $a_N = 0$ for all $n > N$. Now consider
$$\sum_{k=0}^{M+N} a_k b_{M+N-k}$$
Notice that if $k > M$, then $a_k = 0$ so $a_k b_{M+N-k} = 0$. Also, if $k < M$, then $M + N - k = N + (M - k) > N$, hence $b_{M+N-k} = 0$ and so $a_k b_{M+N-k} = 0$. Therefore, we have
$$\sum_{k=0}^{M+N} a_k b_{M+N-k} = a_M b_{M+N-M} = a_M b_N$$

Now we have $a_M \neq 0$ and $b_N \neq 0$, so since R is an integral domain we know that $a_M b_N \neq 0$. Therefore,

$$\sum_{k=0}^{M+N} a_k b_{M+N-k} = a_M b_N \neq 0$$

It follows that $p(x)q(x) \neq 0$, and furthermore that $\deg(p(x)q(x)) \geq M + N$. Since we already know that $\deg(p(x)q(x)) \leq M + N$ from Proposition 9.3.5, we conclude that $\deg(p(x)q(x)) = M + N$. $\square$

Corollary 9.3.7. *If R is an integral domain, then $R[x]$ is an integral domain. Hence, if F is a field, then $F[x]$ is an integral domain.*

Proof. Immediate form Proposition 9.3.6 and Proposition 9.2.9. $\square$

Proposition 9.3.8. *Let R be an integral domain. The units in $R[x]$ are precisely the units in R. In other words, if we identify an element of R with the corresponding constant polynomial, then $U(R[x]) = U(R)$.*

Proof. Recall that the identity of $R[x]$ is the constant polynomial 1. If $a \in U(R)$, then considering a and a^{-1} and 1 all as constant polynomials in $R[x]$, we have $aa^{-1} = 1$ and $a^{-1}a = 1$, so $a \in U(R[x])$. Suppose conversely that $p(x) \in R[x]$ is a unit. Fix $q(x) \in F[x]$ with $p(x) \cdot q(x) = 1 = q(x) \cdot p(x)$. Notice that we must have both $p(x)$ and $q(x)$ be nonzero because $1 \neq 0$. Using Proposition 9.3.6, we then have

$$0 = \deg(1) = \deg(p(x) \cdot q(x)) = \deg(p(x)) + \deg(q(x))$$

Since $\deg(p(x)), \deg(q(x)) \in \mathbb{N}$, it follows that $\deg(p(x)) = 0 = \deg(q(x))$. Therefore, $p(x)$ and $q(x)$ are both nonzero constant polynomials, say $p(x) = a$ and $q(x) = b$. We then have $ab = 1$ and $ba = 1$ in $R[x]$, so these equations are true in R as well. It follows that $a \in U(R)$. $\square$

This proposition can be false when R is only a commutative ring (see the homework).

Corollary 9.3.9. *Let F be a field. The units in $F[x]$ are precisely the nonzero constant polynomials. In other words, if we identify an element of F with the corresponding constant polynomial, then $U(F[x]) = F\backslash\{0\}$.*

Proof. Immediate from Proposition 9.3.8 and the fact that $U(F) = F\backslash\{0\}$. $\square$

Recall Theorem 2.3.1, which said that if $a, b \in \mathbb{Z}$ and $b \neq 0$, then there exists $q, r \in \mathbb{Z}$ with

$$a = qb + r$$

and $0 \leq r < |b|$. Furthermore, the q and r and unique. Intuitively, if $b \neq 0$, then we can always divide by b and obtain a "smaller" remainder. This simple result was fundamental in proving results about greatest common divisors (such as the fact that they exist!). If we hope to generalize this to other rings, we need a way to interpret "smaller" in new ways. Fortunately, for polynomial rings, we can use the notion of degrees. We're already used to this in $\mathbb{R}[x]$ from polynomial long division. However, in $R[x]$ for a general ring R, things may not work out so nicely. The process of polynomial long division involves dividing by the leading coefficient of the divisor, so we need to assume that it is a unit.

Theorem 9.3.10. *Let R be a ring, and let $f(x), g(x) \in R[x]$ with $g(x) \neq 0$. Write*

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

where $b_m \neq 0$.

1. *If $b_m \in U(R)$, then there exist $q(x), r(x) \in R[x]$ with $f(x) = q(x) \cdot g(x) + r(x)$ and either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$.*

2. *If R is an integral domain, then there exist at most one pair $q(x), r(x) \in R[x]$ with $f(x) = q(x) \cdot g(x) + r(x)$ and either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$.*

Proof. 1. Suppose that $b_m \in U(R)$. We prove the existence of $q(x)$ and $r(x)$ for all $f(x) \in R[x]$ by induction on $\deg(f(x))$. We begin by handling some simple cases that will serve as base cases for our induction. Notice first that if $f(x) = 0$, then we may take $q(x) = 0$ and $r(x) = 0$ because

$$f(x) = 0 \cdot g(x) + 0.$$

Also, if $f(x) \neq 0$ but $\deg(f(x)) < \deg(g(x))$, then we may take $q(x) = 0$ and $r(x) = f(x)$ because

$$f(x) = 0 \cdot g(x) + f(x).$$

We handle all other polynomials $f(x)$ using induction on $\deg(f(x))$. Suppose then that $\deg(f(x)) \geq \deg(g(x))$ and that we know the existence result is true for all $p(x) \in R[x]$ with either $p(x) = 0$ or $\deg(p(x)) < \deg(f(x))$. Write

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where $a_n \neq 0$. Since we are assuming that $\deg(f(x)) \geq \deg(g(x))$, we have $n \geq m$. Consider the polynomial

$$p(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x).$$

We have

$$\begin{aligned}
p(x) &= f(x) - a_n b_m^{-1} x^{n-m} g(x) \\
&= (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) - a_n b_m^{-1} x^{n-m} \cdot (b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0) \\
&= (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) - (a_n b_m^{-1} b_m x^n + a_n b_m^{-1} b_{m-1} x^{n-1} + \cdots + a_n b_m^{-1} b_0 x^{n-m}) \\
&= (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) - (a_n x^n + a_n b_m^{-1} b_{m-1} x^{n-1} + \cdots + a_n b_m^{-1} b_0 x^{n-m}) \\
&= (a_{n-1} - a_n b_m^{-1} b_{m-1}) x^{n-1} + \cdots + (a_{n-m} - a_n b_m^{-1} b_0) x^{n-m} + a_{n-m-1} x^{n-m-1} + \cdots + a_0.
\end{aligned}$$

Therefore, either $p(x) = 0$ or $\deg(p(x)) < n = \deg(f(x))$. By induction, we may fix $q^*(x), r^*(x) \in R[x]$ with

$$p(x) = q^*(x) \cdot g(x) + r^*(x)$$

where either $r^*(x) = 0$ or $\deg(r^*(x)) < \deg(g(x))$. We then have

$$f(x) - a_n b_m^{-1} x^{n-m} \cdot g(x) = q^*(x) \cdot g(x) + r^*(x),$$

hence

$$\begin{aligned}
f(x) &= a_n b_m^{-1} x^{n-m} \cdot g(x) + q^*(x) \cdot g(x) + r^*(x) \\
&= (a_n b_m^{-1} x^{n-m} + q^*(x)) \cdot g(x) + r^*(x).
\end{aligned}$$

Thus, if we let $q(x) = (a_n b_m^{-1} x^{n-m} + q^*(x))$ and $r(x) = r^*(x)$, we have either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$, so we have proven existence for $f(x)$.

2. Suppose that R is an integral domain. Suppose that

$$q_1(x) \cdot g(x) + r_1(x) = f(x) = q_2(x) \cdot g(x) + r_2(x)$$

where $q_i(x), r_i(x) \in R[x]$ and either $r_i(x) = 0$ or $\deg(r_i(x)) < \deg(g(x))$ for each i. We then have

$$q_1(x) \cdot g(x) - q_2(x) \cdot g(x) = r_2(x) - r_1(x)$$

hence

$$(q_1(x) - q_2(x)) \cdot g(x) = r_2(x) - r_1(x)$$

Suppose that $r_2(x) - r_1(x) \neq 0$. Since R is an integral domain, we know that $R[x]$ is an integral domain by Corollary 9.3.7. Thus, we must have $q_1(x) - q_2(x) \neq 0$ and $g(x) \neq 0$, and also

$$\deg(r_2(x) - r_1(x)) = \deg(q_1(x) - q_2(x)) + \deg(g(x)) \geq \deg(g(x))$$

by Proposition 9.3.6. However, this is a contradiction because $\deg(r_2(x) - r_1(x)) < \deg(g(x))$ since for each i, we have either $r_i(x) = 0$ or $\deg(r_i(x)) < \deg(g(x))$. We conclude that we must have $r_2(x) - r_1(x) = 0$ and thus $r_1(x) = r_2(x)$. Canceling this common term from

$$q_1(x) \cdot g(x) - q_2(x) \cdot g(x) = r_2(x) - r_1(x),$$

we conclude that

$$q_1(x) \cdot g(x) = q_2(x) \cdot g(x)$$

Since $g(x) \neq 0$ and $R[x]$ is an integral domain, it follows that $q_1(x) = q_2(x)$ as well. □

Corollary 9.3.11. *Let F be a field, and let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. There exist unique $q(x), r(x) \in F[x]$ with $f(x) = q(x) \cdot g(x) + r(x)$ and either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$.*

Proof. Immediate from the previous theorem together with the fact that fields are integral domains, and $U(F) = F\backslash\{0\}$. □

Let's compute an example when $F = \mathbb{Z}/7\mathbb{Z}$. Working in $\mathbb{Z}/7\mathbb{Z}[x]$, let

$$f(x) = \overline{3}x^4 + \overline{6}x^3 + \overline{1}x^2 + \overline{2}x + \overline{2},$$

and let

$$g(x) = \overline{2}x^2 + \overline{5}x + \overline{1}.$$

We perform long division, i.e. follow the proof, to find $q(x)$ and $r(x)$. Notice that the leading coefficient of $g(x)$ is $\overline{2}$ and that in $\mathbb{Z}/7\mathbb{Z}$ we have $\overline{2}^{-1} = \overline{4}$. We begin by computing

$$\overline{3} \cdot \overline{4} \cdot x^{4-2} = \overline{5}x^2$$

This will be the first term in our resulting quotient. We then multiply this by $g(x)$ and subtract from $f(x)$ to obtain

$$\begin{aligned}
f(x) - \overline{5}x^2 \cdot g(x) &= (\overline{3}x^4 + \overline{6}x^3 + \overline{1}x^2 + \overline{2}x + \overline{2}) - \overline{5}x^2 \cdot (\overline{2}x^2 + \overline{5}x + \overline{1}) \\
&= (\overline{3}x^4 + \overline{6}x^3 + \overline{1}x^2 + \overline{2}x + \overline{2}) - (\overline{3}x^4 + \overline{4}x^3 + \overline{5}x^2) \\
&= \overline{2}x^3 + \overline{3}x^2 + \overline{2}x + \overline{2}
\end{aligned}$$

We now continue on with this new polynomial (this is where we appealed to induction in the proof) as our "new" $f(x)$. We follow the proof recursively and compute

$$\overline{2} \cdot \overline{4} \cdot x = \overline{1}x$$

This will be our next term in the quotient. We now subtract $\overline{1}x \cdot g(x)$ from our current polynomial to obtain

$$\begin{aligned}
(\overline{2}x^3 + \overline{3}x^2 + \overline{2}x + \overline{2}) - \overline{x} \cdot g(x) &= (\overline{2}x^3 + \overline{3}x^2 + \overline{2}x + \overline{2}) - \overline{x} \cdot (\overline{2}x^2 + \overline{5}x + \overline{1}) \\
&= (\overline{2}x^3 + \overline{3}x^2 + \overline{2}x + \overline{2}) - (\overline{2}x^3 + \overline{5}x^2 + \overline{1}x) \\
&= \overline{5}x^2 + \overline{1}x + \overline{2}.
\end{aligned}$$

Continuing on, we compute

$$\overline{5} \cdot \overline{4} = \overline{6}$$

and add this to our quotient. We now subtract $\overline{6} \cdot g(x)$ from our current polynomial to obtain

$$\begin{aligned}(\overline{5}x^2 + \overline{1}x + \overline{2}) - \overline{6} \cdot g(x) &= (\overline{5}x^2 + \overline{1}x + \overline{2}) - \overline{6} \cdot (\overline{2}x^2 + \overline{5}x + \overline{1}) \\ &= (\overline{5}x^2 + \overline{1}x + \overline{2}) - (\overline{5}x^2 + \overline{2}x + \overline{6}) \\ &= \overline{6}x + \overline{3}.\end{aligned}$$

We have arrived at a point with our polynomial has degree less than that of $g(x)$, so we have bottomed out in the above proof at a base case. Adding up our contributions to the quotient gives

$$q(x) = \overline{5}x^2 + \overline{1}x + \overline{6},$$

and we are left with the remainder

$$r(x) = \overline{6}x + \overline{3}.$$

Therefore, we have written

$$\overline{3}x^4 + \overline{6}x^3 + \overline{1}x^2 + \overline{2}x + \overline{2} = (\overline{5}x^2 + \overline{1}x + \overline{6}) \cdot (\overline{2}x^2 + \overline{5}x + \overline{1}) + (\overline{6}x + \overline{3}).$$

Notice that if R is not a field, then such $q(x)$ and $r(x)$ may not exist, even if R is a nice ring like $\mathbb{Z}$. For example, there are no $q(x), r(x) \in \mathbb{Z}[x]$ with

$$x^2 = q(x) \cdot 2x + r(x)$$

and either $r(x) = 0$ or $\deg(r(x)) < \deg(2x) = 1$. To see this, first notice that $r(x)$ would have to be a constant polynomial, say $r(x) = c$. If

$$q(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with $a_n \neq 0$, then we would have

$$x^2 = 2a_n x^{n+1} + 2a_{n-1}x^n + \cdots + 2a_1 x^2 + 2a_0 x + c.$$

Since $2a_n \neq 0$ (because $\mathbb{Z}$ is an integral domain), we must have $n = 1$ and hence

$$x^2 = 2a_1 x^2 + 2a_0 x + c$$

It follows that $2a_1 = 1$, which is a contradiction because $2 \nmid 1$ in $\mathbb{Z}$. Thus, no such $q(x)$ and $r(x)$ exist in this case.

Furthermore, if R is not an integral domain, we may not have uniqueness. For example, in $\mathbb{Z}/6\mathbb{Z}$ with $f(x) = \overline{4}x^2 + \overline{1}$ and $g(x) = \overline{2}x$, we have each of the following:

$$\begin{aligned}\overline{4}x^2 + \overline{1} &= \overline{2}x \cdot \overline{2}x + \overline{1}. \\ \overline{4}x^2 + \overline{1} &= \overline{5}x \cdot \overline{2}x + \overline{1}. \\ \overline{4}x^2 + \overline{1} &= (\overline{5}x + \overline{3}) \cdot \overline{2}x + \overline{1}.\end{aligned}$$

Thus, it's possible to have obtain several different quotients. We can even have different quotients and remainders. If we stay in $\mathbb{Z}/6\mathbb{Z}[x]$ but use $f(x) = \overline{4}x^2 + \overline{2}x$ and $g(x) = \overline{2}x + \overline{1}$, then we have:

$$\begin{aligned}\overline{4}x^2 + \overline{2}x &= \overline{2}x \cdot (\overline{2}x + \overline{1}) + \overline{0}. \\ \overline{4}x^2 + \overline{2}x &= (\overline{2}x + \overline{3}) \cdot (\overline{2}x + \overline{1}) + \overline{3}.\end{aligned}$$

9.4 Further Examples of Rings

Power Series Rings

When we defined $R[x]$, the ring of polynomials with coefficients in R, we restricted our infinite sequences to have only a finite number of nonzero terms so that they "correspond" to polynomials. However, the entire apparatus we constructed goes through without a hitch if we take the set of all infinite sequences with no restriction. Intuitively, an infinite sequence $(a_n)_{n\in\mathbb{N}}$ corresponds to the "power series"

$$a_0 + a_1x + a_2x^2 + a_3x^3 + \dots$$

The nice thing about defining our objects as infinite sequences is that there is no confusion at all about "plugging in for x", because there is no x. Thus, there are no issues about convergence or whether this is a well-defined function at all. We define our $+$ and $\cdot$ on these infinite sequences exactly as in the polynomial ring case, and the proofs of the ring axioms follows word for word (actually, the proof is a bit easier because we don't have to worry about the resulting sequences having only a finite number of nonzero terms).

Definition 9.4.1. *Let R be a ring. Let $R[[x]]$ be the set of all infinite sequences $(a_n)_{n\in\mathbb{N}}$ where each $a_n \in R$. We define two binary operations on $R[[x]]$ as follows.*

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}}$$

and

$$\begin{aligned}(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} &= (a_0b_n + a_1b_{n-1} + \dots + a_{n-1}b_1 + a_nb_0)_{n\in\mathbb{N}} \\ &= (\sum_{k=0}^{n} a_kb_{n-k})_{n\in\mathbb{N}} \\ &= (\sum_{i+j=n} a_ib_j)_{n\in\mathbb{N}}.\end{aligned}$$

Theorem 9.4.2. *Let R be a ring. The above operation make $R[[x]]$ into a ring with additive identity the infinite sequence $(0, 0, 0, 0, \dots)$ and multiplicative identity the infinite sequence $(1, 0, 0, 0, \dots)$. Furthermore, if R is commutative, then $R[[x]]$ is commutative. We call $R[[x]]$ the* ring of formal power series *over R, or simply the* power series ring *over R.*

If you have worked with generating functions in combinatorics as strictly combinatorial objects (i.e. you did not worry about values of x where convergence made sense, or work with resulting function on the restricted domain), then you were in fact working in the ring $\mathbb{R}[[x]]$ (or perhaps the larger $\mathbb{C}[[x]]$). From another perspective, if you have worked with infinite series, then you know that

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \dots$$

for all real numbers x with $|x| < 1$. You have probably used this fact when you worked with generating functions as well, even if you weren't thinking about these as functions. If you are not thinking about the above equality in terms of functions, and thus ignored issues about convergence on the right, then what you are doing is that you are working in the ring $\mathbb{R}[[x]]$ and saying that $1 - x$ is a unit with inverse $1 + x + x^2 + x^3 + \dots$. We now verify this fact. In fact, for *any* ring R, we have

$$(1-x)(1 + x + x^2 + x^3 + \dots) = 1 \qquad \text{and} \qquad (1 + x + x^2 + x^3 + \dots)(1-x) = 1$$

in $R[[x]]$. To see this, one can simply multiply out the left hand sides naively and notice the coefficient of x^k equals 0 for all $k \geq 2$. For example, we have

$$\begin{aligned}(1-x)(1+x+x^2+x^3+\dots) &= 1\cdot 1 + (1\cdot 1 + (-1)\cdot 1)\cdot x + (1\cdot 1 + (-1)\cdot 1)\cdot x^2 + \dots \\ &= 1 + 0\cdot x + 0\cdot x^2 + \dots \\ &= 1,\end{aligned}$$

and similarly for the other order. More formally, we can argue this as follows. Let R be a ring. Let $(a_n)_{n\in\mathbb{N}}$ be the infinite sequence defined by

$$a_n = \begin{cases} 1 & \text{if } n = 0 \\ -1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

and notice that $(a_n)_{n\in\mathbb{N}}$ is the formal version of $1-x$. Let $(b_n)_{n\in\mathbb{N}}$ be the infinite sequence defined by $b_n = 1$ for all $n \in \mathbb{N}$, and notice that $(b_n)_{n\in\mathbb{N}}$ is the formal version of $1 + x + x^2 + \dots$. Finally, let $(e_n)_{n\in\mathbb{N}}$ be the finite sequence defined by

$$e_n = \begin{cases} 1 & \text{if } n = 0 \\ 0 & \text{otherwise} \end{cases}$$

and notice that $(e_n)_{n\in\mathbb{N}}$ is the formal version of 1. Now $a_0 \cdot b_0 = 1 \cdot 1 = 1 = e_0$, and for any $n \in \mathbb{N}^+$, we have

$$\begin{aligned}\sum_{k=0}^{n} a_k b_{n-k} &= a_0 b_n + a_1 b_{n-1} && \text{(since } a_k = 0 \text{ if } k \geq 2) \\ &= 1\cdot 1 + (-1)\cdot 1 \\ &= 1 - 1 \\ &= 0 \\ &= e_n.\end{aligned}$$

Therefore $(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} = (e_n)_{n\in\mathbb{N}}$. The proof that $(b_n)_{n\in\mathbb{N}} \cdot (a_n)_{n\in\mathbb{N}} = (e_n)_{n\in\mathbb{N}}$ is similar.

Matrix Rings

One of our fundamental examples of a ring is the ring $M_n(\mathbb{R})$ of all $n \times n$ matrices with entries in $\mathbb{R}$. In turns out that we can generalize this construction to $M_n(R)$ for any ring R.

Definition 9.4.3. *Let R be a ring and let $n \in \mathbb{N}^+$. We let $M_n(R)$ be the ring of all $n \times n$ matrices with entries in R with the following operations. Writing an element of R as $[a_{i,j}]$, we define*

$$[a_{i,j}] + [b_{i,j}] = [a_{i,j} + b_{i,j}] \qquad \text{and} \qquad [a_{i,j}] \cdot [b_{i,j}] = [\sum_{k=1}^{n} a_{i,k} b_{k,j}]$$

With these operations, $M_n(R)$ is a ring with additive identity the matrix of all zeros and multiplicative identity the matrix with all zeros except for ones on the diagonal, i.e.

$$e_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

The verification of the ring axioms on $M_n(R)$ are mostly straightforward (we know the necessary results in the case $R = \mathbb{R}$ from linear algebra). The hardest check once again is that $\cdot$ is associative. We formally carry that out now. Given matrices $[a_{i,j}]$, $[b_{i,j}]$, and $[c_{i,j}]$ in $M_n(R)$, we have

$$\begin{aligned}
[a_{i,j}] \cdot ([b_{i,j}] \cdot [c_{i,j}]) &= [a_{i,j}] \cdot [\sum_{\ell=1}^{n} b_{i,\ell} c_{\ell,j}] \\
&= [\sum_{k=1}^{n} a_{i,k} \cdot (\sum_{\ell=1}^{n} b_{k,\ell} c_{\ell,j})] \\
&= [\sum_{k=1}^{n} \sum_{\ell=1}^{n} a_{i,k}(b_{k,\ell} c_{\ell,j})] \\
&= [\sum_{k=1}^{n} \sum_{\ell=1}^{n} (a_{i,k} b_{k,\ell}) c_{\ell,j}] \\
&= [\sum_{\ell=1}^{n} \sum_{k=1}^{n} (a_{i,k} b_{k,\ell}) c_{\ell,j}] \\
&= [\sum_{\ell=1}^{n} (\sum_{k=1}^{n} a_{i,k} b_{k,\ell}) \cdot c_{\ell,j}] \\
&= [\sum_{k=1}^{n} a_{i,k} b_{k,j}] \cdot [c_{i,j}] \\
&= ([a_{i,j}] \cdot [b_{i,j}]) \cdot [c_{i,j}].
\end{aligned}$$

One nice thing about this more general construction of matrix rings is that it provides us with a decent supply of noncommutative rings.

Proposition 9.4.4. *Let R be a ring with $1 \neq 0$. For each $n \geq 2$, the ring $M_n(R)$ is noncommutative.*

Proof. We claim that the matrix of all zeros except for a 1 in the $(1, 2)$ position does not commute with the matrix of all zeroes except for a 1 in the $(2, 1)$ position. To see this, let $A = [a_{i,j}]$ be the matrix where

$$a_{i,j} = \begin{cases} 1 & \text{if } i = 1 \text{ and } j = 2 \\ 0 & \text{otherwise,} \end{cases}$$

and let $B = [b_{i,j}]$ be the matrix where

$$b_{i,j} = \begin{cases} 1 & \text{if } i = 2 \text{ and } j = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Now the $(1, 1)$ entry of AB equals

$$\begin{aligned}
\sum_{k=1}^{n} a_{1,i} b_{i,1} &= a_{1,1} b_{1,1} + a_{1,2} b_{2,1} + a_{1,3} b_{3,1} + \cdots + a_{1,n} b_{n,1} \\
&= 0 + 1 + 0 + \cdots + 0 \\
&= 1,
\end{aligned}$$

while the $(1,1)$ entry of BA equals

$$\begin{aligned}\sum_{k=1}^{n} b_{1,i}a_{i,1} &= b_{1,1}a_{1,1} + b_{1,2}a_{2,1} + b_{1,3}a_{3,1} + \cdots + b_{1,n}a_{n,1} \\ &= 0 + 0 + 0 + \cdots + 0 \\ &= 0.\end{aligned}$$

Therefore, $AB \neq BA$, and hence $M_n(R)$ is noncommutative. □

In particular, this construction gives us examples of finite noncommutative rings. For example, the ring $M_2(\mathbb{Z}/2\mathbb{Z})$ is a noncommutative ring with $2^4 = 16$ elements.

Rings of Functions Under Pointwise Operations

Consider the set $\mathcal{F}$ of all functions $f \colon \mathbb{R} \to \mathbb{R}$. For example, the function $f(x) = x^2 + 1$ is an element of $\mathcal{F}$, as is $g(x) = \sin x$ and $h(x) = e^x$. We add and multiply functions pointwise as usual, so $f \cdot g$ is the function $(f \cdot g)(x) = (x^2 + 1)\sin x$. Since $\mathbb{R}$ is a ring and everything happens pointwise, it's not difficult to see that $\mathcal{F}$ is a ring under these pointwise operations, with 0 equal to the constant function $f(x) = 0$, and 1 equal to the constant function $f(x) = 1$. In fact, we can vastly generalize this construction.

Definition 9.4.5. *Let X be a set and let R be a ring. Consider the set $\mathcal{F}$ of all functions $f \colon X \to R$. We define $+$ and $\cdot$ on $\mathcal{F}$ to be pointwise addition and multiplication, i.e. given $f, g \in \mathcal{F}$, we define $f + g \colon X \to R$ to be the function such that*

$$(f + g)(x) = f(x) + g(x)$$

for all $x \in X$, and we define $f \cdot g \colon X \to R$ to be the function such that

$$(f \cdot g)(x) = f(x) \cdot g(x)$$

for all $x \in X$. With these operations, $\mathcal{F}$ is a ring with additive identity equal to the constant function $f(x) = 0$ and multiplicative identity equal to the constant function $f(x) = 1$. Furthermore, if R is commutative, then $\mathcal{F}$ is commutative.

Notice that if R is a ring and $n \in \mathbb{N}$, then the direct product $R^n = R \times R \times \cdots \times R$ can be viewed as a special case of this construction where $X = \{1, 2, \ldots, n\}$. To see this, notice that function $f \colon \{1, 2, \ldots, n\} \to R$ naturally corresponding to an n-tuple $(a_1, a_2, \ldots, a_n)$ where each $a_i \in R$ by letting $a_i = f(i)$. Since the operations in both $\mathcal{F}$ and R^n are pointwise, the operations of $+$ and $\cdot$ correspond as well. Although these two descriptions really are just different ways of defining the same object, we can formally verify that these rings are indeed isomorphic once we define ring isomorphisms in the next section.

Now if R is a ring and we let $X = \mathbb{N}$, then elements of $\mathcal{F}$ correspond to infinite sequences $(a_n)_{n \in \mathbb{N}}$ of elements of R. Although this is same underlying set as $R[[x]]$, and both $\mathcal{F}$ and $R[[x]]$ have the same addition operation (namely $(a_n)_{n \in \mathbb{N}} + (b_n)_{n \in \mathbb{N}} = (a_n + b_n)_{n \in \mathbb{N}}$), the multiplication operations are different. In $\mathcal{F}$, we have pointwise multiplication, so $(a_n)_{n \in \mathbb{N}} \cdot (b_n)_{n \in \mathbb{N}} = (a_n \cdot b_n)_{n \in \mathbb{N}}$, while the operation in $R[[x]]$ is more complicated (and more interesting!).

We obtain other fundamental and fascinating rings by taking subrings of these examples. For instance, let $\mathcal{F}$ be our original example of the set of all functions $f \colon \mathbb{R} \to \mathbb{R}$ (so we are taking $R = \mathbb{R}$ and $X = \mathbb{R}$). Let $\mathcal{C} \subseteq \mathcal{F}$ be the subset of all *continuous* functions from $\mathbb{R}$ to $\mathbb{R}$ (i.e. continuous at every point). By results from calculus and/or analysis, the sum and product of continuous functions is continuous, as are the constant functions 0 and 1, along with $-f$ for every continuous function f. It follows that $\mathcal{C}$ is a subring of $\mathcal{F}$.

Polynomial Rings in Several Variables

Let R be a ring. In Section 9.3, we defined the polynomial ring $R[x]$. In this setting, elements of $\mathbb{Z}[x]$ look like $12x+7$, $x^3+2x^2-5x+13$, etc. In other words, elements of $R[x]$ correspond to polynomials in *one* variable. What about polynomials in many variables? For example, suppose to want to consider polynomials like the following:

$$7x^5y^2 - 4x^3y^2 + 11xy^2 - 16xy + 5x^2 - 3y + 42$$

There are two ways to go about making the ring of such "polynomials" precise. One way is to start from scratch like we did for polynomials of one variable. Thinking about infinite sequences $(a_n)_{n\in\mathbb{N}}$ of elements of R as functions $f\colon \mathbb{N} \to R$, we had that the underlying set of $R[x]$ consisted of those functions $f\colon \mathbb{N} \to R$ such that $\{n \in \mathbb{N} : f(n) \neq 0\}$ is finite. For polynomials of two variables, we can instead consider the set of all functions $f\colon \mathbb{N}^2 \to R$ such that $\{(k,\ell) \in \mathbb{N}^2 : f((k,\ell)) \neq 0\}$ is finite. For example, the above polynomial would be given by the function $f((5,2)) = 7$, $f((3,2)) = -4$, $f((2,0)) = 5$, etc. We then add by simply adding the functions pointwise as we've just seen, but multiplication is more interesting. Given two such functions $f, g\colon \mathbb{N}^2 \to \mathbb{R}$, to find out what $(f\cdot g)(k,\ell)$ is, we need to find all pairs of pairs that sum pointwise to (k,ℓ), and add up all of their contributions. For example, we would have

$$\begin{aligned}(f\cdot g)((2,1)) = f((0,0))\cdot g((2,1)) + f((0,1))\cdot g((2,0)) + f((1,0))\cdot g((1,1))\\ + f((1,1))\cdot g((1,0)) + f((2,0))\cdot g((0,1)) + f((2,1))\cdot g((0,0))\end{aligned}$$

With such a definition, it is possible (but tedious) to check that we obtain a ring.

An alternate approach is to define $R[x,y]$ to simply be the ring $(R[x])[y]$ obtained by first taking $R[x]$, and then forming a new polynomial ring from it. From this perspective, one can view the above polynomial as

$$(7x^5 - 4x^3 + 11x)\cdot y^2 + (-16x - 3)\cdot y + (5x^2 + 42).$$

We could also define it as $(R[y])[x]$, in which case we view the above polynomial as

$$(y^2)\cdot x^5 + (-4y^2)\cdot x^3 + (5)\cdot x^2 + (11y^2 - 16y)\cdot x + (-3y + 42).$$

This approach is particularly nice because we do not need to recheck the ring axioms, as they follow from our results on polynomial rings (of one variable). The downside is that working with polynomials in this way, rather than as summands like the original polynomial above, is slightly less natural. Nonetheless, it is possible to prove that all three definitions result in naturally isomorphic rings. We will return to these ideas later, along with working in polynomial rings of more than two variables.

Chapter 10

Ideals and Ring Homomorphisms

10.1 Ideals, Quotients, and Homomorphisms

Ideals

Suppose that R is a ring and that I is a subset of R which is an additive subgroup. Since $(R, +, 0)$ is an group, we know that I breaks up R into (additive) cosets of the form

$$r + I = \{r + a : a \in I\}.$$

These cosets are the equivalence classes of the equivalence relation $\sim_I$ on R defined by $r \sim_I s$ if there exists $a \in I$ with $r + a = s$. Since $(R, +, 0)$ is abelian, we know that the additive subgroup I of R is normal in R, so we can take the quotient R/I as additive groups. In this quotient, we know from our general theory of quotient groups that addition is well-defined by:

$$(r + I) + (s + I) = (r + s) + I.$$

Now if we want to turn the resulting quotient into a ring (rather than just an abelian group), we would certainly require that multiplication of cosets is well-defined as well. In other words, we would need to know that if $r, s, t, u \in R$ with $r \sim_I t$ and $s \sim_I u$, then $rs \sim_I tu$. A first guess might be that we should require that I is closed under multiplication as well. Before jumping to conclusions, let's work out whether this happens for free, or if it looks grim, then what additional conditions on I we might want to require.

Suppose then that $r, s, t, u \in R$ with $r \sim_I t$ and $s \sim_I u$. Fix $a, b \in I$ with $r + a = t$ and $s + b = u$. We then have

$$\begin{aligned} tu &= (r + a)(s + b) \\ &= r(s + b) + a(s + b) \\ &= rs + rb + as + ab. \end{aligned}$$

Now in order for $rs \sim_I tu$, we would want $rb + as + ab \in I$. To ensure this, it would suffice to know that $rb \in I$, $as \in I$, and $ab \in I$ because we are assuming that I is an additive subgroup. The last of these, that $ab \in I$, would follow if we include the additional assumption that I is closed under multiplication as we guessed above. However, a glance at the other two suggests that we might need to require more. These other summands suggest that we want I to be closed under "super multiplication", i.e. that if we take an element of I and multiply it by any element of R on either side, then we stay in I. If we have these conditions on I (which at this point looks like an awful lot to ask), then everything should work out fine. We give a special name to subsets of R that have this property.

Definition 10.1.1. *Let R be a ring. An ideal of R is a subset $I \subseteq R$ with the following properties:*

- $0 \in I$.
- $a + b \in I$ *whenever* $a \in I$ *and* $b \in I$.
- $-a \in I$ *whenever* $a \in I$.
- $ra \in I$ *whenever* $r \in R$ *and* $a \in I$.
- $ar \in I$ *whenever* $r \in R$ *and* $a \in I$.

Notice that the first three properties simply say that I is an additive subgroup of R.

For example, consider the ring $R = \mathbb{Z}$. Suppose $n \in \mathbb{N}$ and let $I = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. We then have that I is an ideal of R. To see this, first notice that we already know that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. Now for any $m \in \mathbb{Z}$ and $k \in \mathbb{Z}$, we have

$$m \cdot (nk) = n \cdot (mk) \in n\mathbb{Z} \qquad \text{and} \qquad (nk) \cdot m = n \cdot (km) \in n\mathbb{Z}$$

Therefore, $I = n\mathbb{Z}$ does satisfy the additional conditions necessary, so $I = n\mathbb{Z}$ is an ideal of R. Before going further, let's note one small simplification in the definition of an ideal.

Proposition 10.1.2. *Let R be a ring. Suppose that $I \subseteq R$ satisfies the following:*

- $0 \in I$.
- $a + b \in I$ *whenever* $a \in I$ *and* $b \in I$.
- $ra \in I$ *whenever* $r \in R$ *and* $a \in I$.
- $ar \in I$ *whenever* $r \in R$ *and* $a \in I$.

We then have that I is an ideal of R.

Proof. Notice that the only condition that is missing is that I is closed under additive inverses. For any $a \in R$, we have $-a = (-1) \cdot a$, so $-a \in R$ by the third condition (notice here that we are using the fact that all our rings have a multiplicative identity). $\square$

When R is commutative, we can even pare this to three conditions.

Corollary 10.1.3. *Let R be a commutative ring. Suppose that $I \subseteq R$ satisfies the following:*

- $0 \in I$.
- $a + b \in I$ *whenever* $a \in I$ *and* $b \in I$.
- $ra \in I$ *whenever* $r \in R$ *and* $a \in I$.

We then have that I is an ideal of R.

Proof. Use the previous proposition together with the fact that if $r \in R$ and $a \in I$, then $ar = ra \in I$ because R is commutative. $\square$

For another example of an ideal, consider the ring $R = \mathbb{Z}[x]$. Let I be set of all polynomials with 0 constant term. Formally, we are letting I be the set of infinite sequences $(a_n)_{n\in\mathbb{N}}$ with $a_0 = 0$. Let's prove that I is an ideal using a more informal approach to the polynomial ring (make sure you know how to translate everything we are saying into formal terms). Notice that the zero polynomial is trivially in I and that I is closed under addition because the constant term of the sum of two polynomials is the sum of their constant terms. Finally, if $f(x) \in R$ and $p(x) \in I$, then we can write

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

and

$$p(x) = b_m x^n + b_{n-1}x^{n-1} + \cdots + b_1 x.$$

Multiplying out the polynomials, we see that the constant term of $f(x)p(x)$ is $a_0 \cdot 0 = 0$ and similarly the constant term of $p(x)f(x)$ is $0 \cdot a_0 = 0$. Therefore, we have both $f(x)p(x) \in I$ and $p(x)f(x) \in I$. It follows that I is an ideal of R.

From the above discussion, it appears that if I is an ideal of R, then it makes sense to take the quotient of R by I and have both addition and multiplication of cosets be well-defined. However, our definition was motivated by what conditions would ensure that checking that multiplication is well-defined easy. As in our definition of a normal subgroup, it is a pleasant surprise that the implication can be reversed so our conditions are precisely what is needed for the quotient to make sense.

Proposition 10.1.4. *Let R be a ring and let $I \subseteq R$ be an additive subgroup of $(R, +, 0)$. The following are equivalent:*

1. *I is an ideal of R.*

2. *Whenever $r, s, t, u \in R$ with $r \sim_I t$ and $s \sim_I u$, we have $rs \sim_I tu$.*

Proof. We first prove (1) ⇒ (2). Let $r, s, t, u \in R$ be arbitrary with $r \sim_I t$ and $s \sim_I u$. Fix $a, b \in I$ with $r + a = t$ and $s + b = u$. We then have

$$\begin{aligned} tu &= (r + a)(s + b) \\ &= r(s + b) + a(s + b) \\ &= rs + rb + as + ab. \end{aligned}$$

Since I is an ideal of R and $b \in I$, we know that both $rb \in I$ and $ab \in I$. Similarly, since I is an ideal of R and $a \in I$, we know that $as \in I$. Now I is an ideal of R, so it is an additive subgroup of R, and hence $rb + as + ab \in I$. Since

$$tu = rs + (rb + as + ab)$$

we conclude that $rs \sim_I tu$.

We now prove (2) ⇒ (1). We are assuming that I is an additive subgroup of R and condition (2). Let $r \in R$ and let $a \in I$ be arbitrary. Now $r \sim_I r$ because $r + 0 = r$ and $0 \in I$. Also, we have $a \sim_I 0$ because $a + (-a) = 0$ and $-a \in I$ (as $a \in I$ and I is an additive subgroup).

- Since $r \sim_I r$ and $a \sim_I 0$, we may use condition (2) to conclude that $ra \sim_I r0$, which is to say that $ra \sim_I 0$. Thus, we may fix $b \in I$ with $ra + b = 0$. Since $b \in I$ and I is an additive subgroup, it follows that $ra = -b \in I$.

- Since $a \sim_I 0$ and $r \sim_I r$, we may use condition (2) to conclude that $ar \sim_I 0r$, which is to say that $ar \sim_I 0$. Thus, we may fix $b \in I$ with $ar + b = 0$. Since $b \in I$ and I is an additive subgroup, it follows that $ar = -b \in I$.

Therefore, we have both $ra \in I$ and $ar \in I$. Since $r \in R$ and $a \in I$ were arbitrary, we conclude that I is an ideal of R. $\square$

We are now ready to formally define quotient rings.

Definition 10.1.5. *Let R be a ring and let I be an ideal of R. Let R/I be the set of additive cosets of I in R, i.e. the set of equivalence classes of R under $\sim_I$. Define operation on R/I by letting*

$$(r + I) + (s + I) = (r + s) + I \qquad \textit{and} \qquad (r + I) \cdot (s + I) = rs + I.$$

With these operations, the set R/I becomes a ring with additive identity $0 + I$ and multiplicative identity $1 + I$ (we did the hard part of checking that the operations are well-defined, and from here the ring axioms follow because the ring axioms hold in R). Furthermore, if R is commutative, then R/I is also commutative.

Let $n \in \mathbb{N}^+$. As discussed above, the set $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$. Our familiar ring $\mathbb{Z}/n\mathbb{Z}$ defined in the first section is precisely the quotient of $\mathbb{Z}$ by this ideal $n\mathbb{Z}$, hence the notation again.

As we have seen, ideals of a ring correspond to normal subgroups of a group in that they are the “special” subsets for which it makes sense to take a quotient. There is one small but important note to be made here. Of course, every normal subgroup of a group G is a subgroup of G. However, it is *not* true that every ideal of a ring R is a subring of R. The reason is that for I to be an ideal of R, it is *not* required that $1 \in I$. In fact, if I is an ideal of R and $1 \in R$, then $r = r \cdot 1 \in I$ for all $r \in R$, so $I = R$. Since every subring S of R must satisfy $1 \in S$, it follows that the only ideal of R which is a subring of R is the whole ring itself. This might seem to be quite a nuisance, but as mentioned above, we will pay very little attention to subrings of a given ring, and the vast majority of our focus will be on ideals.

We end with our discussion of ideals in general rings with a simple characterization for when two elements of a ring R represent the same coset.

Proposition 10.1.6. *Let R be a ring and let I be an ideal of R. Let $r, s \in R$. The following are equivalent:*

1. $r + I = s + I$.
2. $r \sim_I s$.
3. $r - s \in I$.
4. $s - r \in I$.

Proof.
- Notice that (1) $\Leftrightarrow$ (2) from our general theory of equivalence relations because $r + I$ is simply the equivalence class of r under the relation $\sim_I$.
- (2) $\Rightarrow$ (3): Suppose that $r \sim_I s$, and fix $a \in I$ with $r + a = s$. Subtracting s and a from both sides, it follows that $r - s = -a$ (you should work through the details of this if you are nervous). Now $a \in I$ and I is an additive subgroup of R, so $-a \in I$. It follows that $r - s \in I$.
- (3) $\Rightarrow$ (4): Suppose that $r - s \in I$. Since I is an additive subgroup of R, we know that $-(r - s) \in I$. Since $-(r - s) = s - r$, it follows that $s - r \in I$.
- (4) $\Rightarrow$ (2): Suppose that $s - r \in I$. Since $r + (s - r) = s$, it follows that $r \sim_I s$.

$\square$

We now work through an example of a quotient ring other than $\mathbb{Z}/n\mathbb{Z}$. Let $R = \mathbb{Z}[x]$ and notice that R is commutative. We consider two different quotients of R.

- First, let
$$I = (x^2 - 2) \cdot \mathbb{Z}[x] = \{(x^2 - 2) \cdot p(x) : p(x) \in \mathbb{Z}[x]\}.$$
For example, $3x^3 + 5x^2 - 6x - 10 \in I$ because
$$3x^3 + 5x^2 - 6x - 10 = (x^2 - 2) \cdot (3x + 5)$$
and $3x + 5 \in \mathbb{Z}[x]$. We claim that I is an ideal of $\mathbb{Z}[x]$:
  - Notice that $0 \in I$ because $0 = (x^2 - 2) \cdot 0$.
  - Let $f(x), g(x) \in I$ be arbitrary. By definition of I, we can fix $p(x), q(x) \in \mathbb{Z}[x]$ with $f(x) = (x^2 - 2) \cdot p(x)$ and $g(x) = (x^2 - 2) \cdot q(x)$. We then have
$$\begin{aligned} f(x) + g(x) &= (x^2 - 2) \cdot p(x) + (x^2 - 2) \cdot q(x) \\ &= (x^2 - 2) \cdot (p(x) + q(x)). \end{aligned}$$
Since $p(x) + q(x) \in \mathbb{Z}[x]$, it follows that $f(x) + g(x) \in I$.
  - Let $h(x) \in \mathbb{Z}[x]$ and $f(x) \in I$ be arbitrary. By definition of I, we can fix $p(x) \in \mathbb{Z}[x]$ with $f(x) = (x^2 - 2) \cdot p(x)$. We then have
$$\begin{aligned} h(x) \cdot f(x) &= h(x) \cdot (x^2 - 2) \cdot p(x) \\ &= (h(x) \cdot p(x)) \cdot (x^2 - 2). \end{aligned}$$
Since $h(x) \cdot p(x) \in \mathbb{Z}[x]$, it follows that $h(x) \cdot f(x) \in I$.

Since $\mathbb{Z}[x]$ is commutative, it follows that I is an ideal of $\mathbb{Z}[x]$. Consider the quotient ring $\mathbb{Z}[x]/I$. Notice that we have
$$(7x^3 + 3x^2 - 13x - 2) + I = (x + 4) + I$$
because
$$\begin{aligned} (7x^3 + 3x^2 - 13x - 2) - (x + 4) &= 7x^3 + 3x^2 - 14x - 6 \\ &= (x^2 - 2) \cdot (7x + 3) \\ &\in I. \end{aligned}$$
In fact, for every polynomial $f(x) \in \mathbb{Z}(x)$, there exists $r(x) \in \mathbb{Z}[x]$ with either $r(x) = 0$ or $\deg(r(x)) < 2$ such that $f(x) + I = r(x) + I$. To see this, notice that the leading coefficient of $x^2 - 2$ is 1, which is a unit in $\mathbb{Z}$. Now given any $f(x) \in \mathbb{Z}[x]$, Theorem 9.3.10 tells us that there exists $q(x), r(x) \in \mathbb{Z}[x]$ with
$$f(x) = q(x) \cdot (x^2 - 2) + r(x)$$
and either $r(x) = 0$ or $\deg(r(x)) < 2$. We then have that
$$f(x) - r(x) = (x^2 - 2) \cdot q(x),$$
so $f(x) - r(x) \in I$, and hence $f(x) + I = r(x) + I$. Furthermore, if $r_1(x), r_2(x)$ are such that either $r_i(x) = 0$ or $\deg(r_i(x)) < 2$, and $r_1(x) + I = r_2(x) + I$, then one can show show that $r_1(x) = r_2(x)$. This is a good exercise now, but we will prove more general facts later. In other words, elements of $R[x]/I$, which are additive cosets, can be uniquely represented by the zero polynomial together with polynomials of degree less than 2.

- Let
$$J = 2x \cdot \mathbb{Z}[x] = \{2x \cdot f(x) : f(x) \in \mathbb{Z}[x]\}.$$
As in the previous example, it's straightforward to check that J is an ideal of R. Consider the quotient ring $\mathbb{Z}[x]/J$. Notice that we have
$$(2x^2 + x - 7) + J = (3x - 7) + J$$
because
$$\begin{aligned}(2x^2 + x - 7) - (3x - 7) &= 2x^2 - 2x \\ &= 2x \cdot (x - 1) \\ &\in J.\end{aligned}$$
However, notice that the leading coefficient of $2x$ is 2, which is not a unit in $\mathbb{Z}$. Thus, we can't make an argument like the one above work, and it is indeed harder to find unique representatives of the cosets in $\mathbb{Z}[x]/J$. For example, one can show that $x^3 + I \neq r(x) + I$ for any $r(x) \in \mathbb{Z}[x]$ of degree at most 2.

Ring Homomorphisms

Definition 10.1.7. *Let R and S be rings. A (ring) homomorphism from R to S is a function $\varphi\colon R \to S$ such that*

- *$\varphi(r + s) = \varphi(r) + \varphi(s)$ for all $r, s \in R$.*
- *$\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$ for all $r, s \in R$.*
- *$\varphi(1_R) = 1_S$.*

A (ring) isomorphism from R to S is a homomorphism $\varphi\colon R \to S$ which is a bijection.

Definition 10.1.8. *Given two rings R and S, we say that R and S are* isomorphic*, and write $R \cong S$, if there exists an isomorphism $\varphi\colon R \to S$.*

Notice that we have the additional requirement that $\varphi(1_R) = 1_S$. When we discussed group homomorphisms, we derived $\varphi(e_G) = e_H$ rather than explicitly require it (see Proposition 6.6.2 and Proposition 6.3.4). Unfortunately, it does not follow for free from the other two conditions in the ring case. If you go back and look at the proof that $\varphi(e_G) = e_H$ in the group case, you will see that we used the fact that $\varphi(e_G)$ has an inverse but it is not true in rings that every element must have a multiplicative inverse. To see an example where the condition can fail consider the ring $\mathbb{Z} \times \mathbb{Z}$ (we have not formally defined the direct product of rings, but it works in the same way). Define $\varphi\colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ by $\varphi(n) = (n, 0)$. It is not hard to check that φ satisfies the first two conditions for a ring homomorphism, but $\varphi(1) = (1, 0)$ while the identity of $\mathbb{Z} \times \mathbb{Z}$ is $(1, 1)$.

Definition 10.1.9. *Let R be a ring and let $c \in R$. Define $Ev_c\colon R[x] \to R$ by letting*
$$Ev_c((a_n)_{n\in\mathbb{N}}) = \sum_n a_n c^n.$$
Notice that the above sum makes sense because elements $(a_n)_{n\in\mathbb{N}} \in R[x]$ have only finitely many nonzero terms (if $(a_n)_{n\in\mathbb{N}}$ is nonzero, we can stop the sum at $M = \deg((a_n)_{n\in\mathbb{N}})$). Intuitively, we are defining
$$Ev_c(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) = a_n c^n + a_{n-1}c^{n-1} + \cdots + a_1 c + a_0$$
Thus, Ev_c is the function which says “evaluate the polynomial at c”.

The next proposition is really fundamental. Intuitively, it says the following. Suppose that we are given a *commutative* ring R, and we take two polynomials in R. Given any $c \in R$, we obtain the same result if we first add/multiply the polynomials and then plug c into the result, or if we first plug c into each polynomial and then add/multiply the results.

Proposition 10.1.10. *Let R be a commutative ring and let $c \in R$. The function Ev_c is a ring homomorphism.*

Proof. We clearly have $Ev_c(1) = 1$ (where the 1 in parenthesis is the constant polynomial 1). For any $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in R[x]$, we have

$$\begin{aligned}
Ev_c((a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}}) &= Ev_c((a_n + b_n)_{n\in\mathbb{N}}) \\
&= \sum_n (a_n + b_n)c^n \\
&= \sum_n (a_n c^n + b_n c^n) \\
&= \sum_n a_n c^n + \sum_n b_n c^n \\
&= Ev_c((a_n)_{n\in\mathbb{N}}) + Ev_c((b_n)_{n\in\mathbb{N}})
\end{aligned}$$

Thus, Ev_c preserves addition. We now check that Ev_c preserves multiplication. Suppose that $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in R[x]$. Let $M_1 = \deg((a_n)_{n\in\mathbb{N}})$ and $M_2 = \deg((b_n)_{n\in\mathbb{N}})$ (for this argument, let $M_i = 0$ if the corresponding polynomial is the zero polynomial). We know that $M_1 + M_2 \geq \deg((a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}})$, so

$$\begin{aligned}
Ev_c((a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}}) &= Ev_c((\sum_{i+j=n} a_ib_j)_{n\in\mathbb{N}}) \\
&= \sum_{n=0}^{M_1+M_2} (\sum_{i+j=n} a_ib_j)c^n \\
&= \sum_{n=0}^{M_1+M_2} \sum_{i+j=n} a_ib_jc^n \\
&= \sum_{n=0}^{M_1+M_2} \sum_{i+j=n} a_ib_jc^{i+j} \\
&= \sum_{n=0}^{M_1+M_2} \sum_{i+j=n} a_ib_jc^ic^j \\
&= \sum_{n=0}^{M_1+M_2} \sum_{i+j=n} a_ic^ib_jc^j && \text{(since } R \text{ is commutative)} \\
&= \sum_{i=0}^{M_1} \sum_{j=0}^{M_2} a_ic^ib_jc^j && \text{(since } a_i = 0 \text{ if } i > M_1 \text{ and } b_j = 0 \text{ if } j > M_2\text{)} \\
&= \sum_{i=0}^{M_1} (a_ic^i \cdot (\sum_{j=0}^{M_2} b_jc^j)) \\
&= (\sum_{i=0}^{M_1} a_ic^i) \cdot (\sum_{j=0}^{M_2} b_jc^j) \\
&= Ev_c((a_n)_{n\in\mathbb{N}}) \cdot Ev_c((b_n)_{n\in\mathbb{N}})
\end{aligned}$$

Thus, Ev_c preserves multiplication. It follows that Ev_c is a ring homomorphism. □

Let's take a look at what can fail when R is noncommutative. Consider the polynomials $p(x) = ax$ and $q(x) = bx$. We then have that $p(x)q(x) = abx^2$. Now if $c \in R$, then

$$Ev_c(p(x)q(x)) = Ev_c(abx^2) = abc^2$$

and

$$Ev_c(p(x)) \cdot Ev_c(q(x)) = acbc$$

It seems impossible to argue that these are equal in general if you can not commute b with c. To find a specific counterexample, it suffices to find a noncommutative ring with two elements b and c such that $bc^2 \neq cbc$ (because then we can take $a = 1$). It's not hard to find two matrices which satisfy this, so the corresponding Ev_c will not be a ring homomorphism.

In the future, given $p(x) \in R[x]$ and $c \in R$, we will tend to write the informal $p(c)$ for the formal notion $Ev_c(p(x))$. In this informal notation, the proposition says that if R is commutative, $c \in R$, and $p(x), q(x) \in R[x]$, then

$$(p + q)(c) = p(c) + q(c) \qquad \text{and} \qquad (p \cdot q)(c) = p(c) \cdot q(c).$$

Definition 10.1.11. *Let $\varphi \colon R \to S$ be a ring homomorphism. We define* $\ker(\varphi)$ *to be the kernel of φ when viewed as a homomorphism of the additive groups, i.e.* $\ker(\varphi) = \{a \in R : \varphi(a) = 0_S\}$.

Recall that the normal subgroups of a group G are precisely the kernels of group homomorphisms with domain G. Continuing on the analogy between normal subgroups of a group and ideal of a ring, we might hope that the ideals of a ring R are precisely the kernels of ring homomorphisms with domain R. The next two propositions confirm this.

Proposition 10.1.12. *If $\varphi\colon R \to S$ is a ring homomorphism, then $\ker(\varphi)$ is an ideal of R.*

Proof. Let $K = \ker(\varphi)$. Since we know in particular in that φ is a additive group homomorphism, we know from our work on groups that K is an additive subgroup of R (see Proposition 6.6.4). Let $a \in K$ and $r \in R$ be arbitrary. Since $a \in K$, we have $\varphi(a) = 0$. Therefore

$$\begin{aligned} \varphi(ra) &= \varphi(r) \cdot \varphi(a) \\ &= \varphi(r) \cdot 0_S \\ &= 0_S, \end{aligned}$$

so $ra \in K$, and

$$\begin{aligned} \varphi(ar) &= \varphi(a) \cdot \varphi(r) \\ &= 0_S \cdot \varphi(r) \\ &= 0_S, \end{aligned}$$

so $ar \in K$. Therefore, K is an ideal of R. □

Proposition 10.1.13. *Let R be a ring and let I be an ideal of R. There exists a ring S and a ring homomorphism $\varphi\colon R \to S$ such that $I = \ker(\varphi)$.*

Proof. Consider the ring $S = R/I$ and the projection $\pi\colon R \to R/I$ defined by $\pi(a) = a + I$. As in the group case, it follows that π is a ring homomorphism and that $\ker(\pi) = I$. □

Now many of the results about group homomorphisms carry over to ring homomorphisms. For example, we have the following.

Proposition 10.1.14. *Let $\varphi\colon R \to S$ be a ring homomorphism. φ is injective if and only if $\ker(\varphi) = \{0_R\}$.*

Proof. Notice that φ is in particular a homomorphism of additive groups. Thus, the result follows from the corresponding result about groups. However, let's prove it again because it is an important result.

Suppose first that φ is injective. We know that $\varphi(0_R) = 0_S$, so $0_R \in \ker(\varphi)$. If $a \in \ker(\varphi)$, then $\varphi(a) = 0_S = \varphi(0_R)$, so $a = 0_R$ because φ is injective. Therefore, $\ker(\varphi) = \{0_R\}$.

Suppose conversely that $\ker(\varphi) = \{0_R\}$. Let $r, s \in R$ with $\varphi(r) = \varphi(s)$. We then have

$$\begin{aligned} \varphi(r - s) &= \varphi(r + (-s)) \\ &= \varphi(r) + \varphi(-s) \\ &= \varphi(r) - \varphi(s) \\ &= 0_S \end{aligned}$$

so $r - s \in \ker(\varphi)$. We are assuming that $\ker(\varphi) = \{0_R\}$, so $r - s = 0_R$ and hence $r = s$. □

Next we discuss the ring theoretic analogues of Theorem 6.6.9.

Theorem 10.1.15. *Let R_1 and R_2 be rings, and let $\varphi\colon R_1 \to R_2$ be a homomorphism. We have the following:*

1. *If S_1 is a subring of R_1, then $\varphi^{\to}[S_1]$ is a subring of R_2.*

2. *If I_1 is an ideal of R_1 and φ is surjective, then $\varphi^{\to}[I_1]$ is an ideal of R_2.*

3. *If S_2 is a subring of R_2, then $\varphi^{\leftarrow}[S_2]$ is a subring of R_1.*

4. *If I_2 is an ideal of R_2, then $\varphi^{\leftarrow}[I_2]$ is an ideal of R_1.*

Proof. 1. Suppose that S_1 is a subring of R_1. We then have that S_1 is an additive subgroup of R_1, so $\varphi^{\to}[S_1]$ is an additive subgroup of R_2 by Theorem 6.6.9. Since $1 \in S_1$ and $\varphi(1) = 1$ by definition of subrings and ring homomorphisms, we have that $1 \in \varphi^{\to}[S_1]$ as well. Now let $c, d \in \varphi^{\to}[S_1]$ be arbitrary. Fix $a, b \in S_1$ with $\varphi(a) = c$ and $\varphi(b) = d$. Since $a, b \in S_1$ and S_1 is a subring of R_1, it follows that $ab \in S_1$. Now

$$\varphi(ab) = \varphi(a) \cdot \varphi(b) = cd$$

so $cd \in \varphi^{\to}[S_1]$. Thus, $\varphi^{\to}[S_1]$ is a subring of R_1.

2. Suppose that I_1 is an ideal of R_1 and that φ is surjective. Since I_1 is an additive subgroup of R_1, we know from Theorem 6.6.9 that $\varphi^{\to}[I_1]$ is an additive subgroup of R_2. Suppose that $d \in R_2$ and $c \in \varphi^{\to}[I_1]$ are arbitrary. Since φ is surjective, we may fix $b \in R_1$ with $\varphi(b) = d$. Since $c \in \varphi^{\to}[I_1]$, we can fix $a \in I_1$ with $\varphi(a) = c$. We then have

$$\begin{aligned} dc &= \varphi(b) \cdot \varphi(a) \\ &= \varphi(ba) \end{aligned}$$

so $dc \in \varphi^{\to}[I_1]$. Also, we have

$$\begin{aligned} cd &= \varphi(a) \cdot \varphi(b) \\ &= \varphi(ab) \end{aligned}$$

so $cd \in \varphi^{\to}[I_1]$. It follows that $\varphi^{\to}[I_1]$ is an ideal of R_2.

3. Suppose that S_2 is a subring of R_2. We then have that S_2 is an additive subgroup of R_2, so $\varphi^{\leftarrow}[S_2]$ is an additive subgroup of R_1 by Theorem 6.6.9. Since $1 \in S_2$ and $\varphi(1) = 1$ by definition of subrings and ring homomorphisms, we have that $1 \in \varphi^{\leftarrow}[S_2]$ as well. Now let $a, b \in \varphi^{\leftarrow}[S_2]$ be arbitrary, so $\varphi(a) \in S_2$ and $\varphi(b) \in S_2$. We then have

$$\varphi(ab) = \varphi(a) \cdot \varphi(b) \in S_2$$

because S_2 is a subring of R_2, so $ab \in \varphi^{\leftarrow}[S_2]$. Thus, $\varphi^{\leftarrow}[S_2]$ is a subring of R_1.

4. Suppose that I_2 be an ideal of R_2. Since I_2 is an additive subgroup of R_2, we know from Theorem 6.6.9 that $\varphi^{\leftarrow}[I_2]$ is an additive subgroup of R_1. Let $b \in R_1$ and $a \in \varphi^{\leftarrow}[I_2]$ be arbitrary, so $\varphi(a) \in I_2$. We then have that $\varphi(ba) = \varphi(b) \cdot \varphi(a) \in I_2$ because I_2 is an ideal of R_2, so $ba \in \varphi^{\leftarrow}[I_2]$. Similarly, we have $\varphi(ab) = \varphi(a) \cdot \varphi(b) \in I_2$ because I_2 is an ideal of R_2, so $ab \in \varphi^{\leftarrow}[I_2]$. Since $b \in R_1$ and $a \in \varphi^{\leftarrow}[I_2]$ were arbitrary, we conclude that $\varphi^{\leftarrow}[I_2]$ is an ideal of R_1.

□

Corollary 10.1.16. *If $\varphi \colon R_1 \to R_2$ is a (ring) homomorphism, then range(φ) is a subring of R_2.*

Proof. This follows immediately from the previous theorem because R_1 is trivially a subgroup of R_1 and $\text{range}(\varphi) = \varphi^{\to}[R_1]$. □

We end with brief statements of the Isomorphism and Correspondence Theorems. As one might expect, the corresponding results from group theory do a lot of the heavy lifting in the following proofs, but we still need to check a few extra things in each case (like the corresponding functions preserve multiplication).

Theorem 10.1.17 (First Isomorphism Theorem)**.** *Let $\varphi\colon R \to S$ be a ring homomorphism and let $K = \ker(\varphi)$. Define a function $\psi\colon R/K \to S$ by letting $\psi(a+K) = \varphi(a)$. We then have that ψ is a well-defined function which is a ring isomorphism onto the subring range(φ) of S. Therefore*

$$R/\ker(\varphi) \cong \mathit{range}(\varphi).$$

Let's see the First Isomorphism Theorem in action. Let $R = \mathbb{Z}[x]$ and let I be the ideal of all polynomials with 0 constant term, i.e.

$$\begin{aligned} I &= \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] : a_0 = 0\} \\ &= \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x : a_i \in \mathbb{Z} \text{ for } 1 \leq i \leq n\}. \end{aligned}$$

It is straightforward to check that I is an ideal. Consider the ring R/I. Intuitively, taking the quotient by I we "trivialize" all polynomials without a constant term. Thus, it seems reasonable to suspect that two polynomials will be in the same coset in the quotient exactly when they have the same constant term (because then the difference of the two polynomials will be in I). As a result, we might expect that $R/I \cong \mathbb{Z}$. Although it is possible to formalize and prove all of these statements directly, we can also deduce them all from the First Isomorphism Theorem, as we now show.

Since $\mathbb{Z}$ is commutative, the function $Ev_0\colon \mathbb{Z}[x] \to \mathbb{Z}$ is a ring homomorphism by Proposition 10.1.10. Notice that Ev_0 is surjective because $Ev_0(a) = a$ for all $a \in \mathbb{Z}$ (where we interpret the a in parentheses as the constant polynomial a). Now $\ker(Ev_0) = I$ because for any $p(x) \in \mathbb{Z}[x]$, we have that $p(0) = Ev_0(p(x))$ is the constant term of $p(x)$. Since $I = \ker(Ev_0)$, we know that I is an ideal of $\mathbb{Z}[x]$ by Proposition 10.1.12. Finally, using the First Isomorphism Theorem together with the fact that φ is surjective, we conclude that $\mathbb{Z}[x]/I \cong \mathbb{Z}$.

We end by stating the remaining theorems. Again, most of the work can be outsourced to the corresponding theorems about groups, and all that remains is to check that multiplication behaves appropriately in each theorem.

Theorem 10.1.18 (Second Isomorphism Theorem)**.** *Let R be a ring, let S be a subring of R, and let I be an ideal of R. We then have that $S + I = \{r + a : r \in S, a \in I\}$ is a subring of R, that I is an ideal of $S + I$, that $S \cap I$ is an ideal of S, and that*

$$\frac{S+I}{I} \cong \frac{S}{S \cap I}$$

Theorem 10.1.19 (Correspondence Theorem)**.** *Let R be a ring and let I be an ideal of R. For every subring S of R with $I \subseteq S$, we have that S/I is a subring of R/I and the function*

$$S \mapsto S/I$$

is a bijection from subrings of R containing I to subrings of R/I. Also, for every ideal J of R with $I \subseteq J$, we have that J/I is an ideal of R/I and the function

$$J \mapsto J/I$$

is a bijection from ideals of R containing J to ideals of R/J. Furthermore, we have the following properties for any subgroups S_1 and S_2 of R that both contain I, and ideal J_1 and J_2 of R that both contain I:

1. *S_1 is a subring of S_2 if and only if S_1/I is a subring of S_2/I.*
2. *J_1 is an ideal of J_2 if and only if J_1/I is an ideal of J_2/I.*

Theorem 10.1.20 (Third Isomorphism Theorem)**.** *Let R be a ring. Let I and J be ideals of R with $I \subseteq J$. We then have that J/I is an ideal of R/I and that*

$$\frac{R/I}{J/I} \cong \frac{R}{J}$$

10.2 The Characteristic of a Ring

Let R be a ring (not necessarily commutative). We know that R has an element 1, so it makes sense to consider $1+1$, $1+1+1$, etc. It is natural to call these resulting ring elements 2, 3, etc. However, we need to be careful when we interpret these. For example, in the ring $\mathbb{Z}/2\mathbb{Z}$, the multiplicative identity is $\overline{1}$, and we have $\overline{1}+\overline{1}=\overline{0}$. Thus, in the above notation, we would have $2=0$ in the ring $\mathbb{Z}/2\mathbb{Z}$. To avoid such confusion, we introduce new notation by putting an underline beneath a number n to denote the corresponding result of adding $1 \in R$ to itself n times. Here is the formal definition.

Definition 10.2.1. *Let R be a ring. For each $n \in \mathbb{Z}$, we define an element $\underline{n}$ recursively as follows. Let*

- $\underline{0} = 0$
- $\underline{n+1} = \underline{n} + 1$ *for all* $n \in \mathbb{N}$
- $\underline{n} = -(\underline{-n})$ *if* $n \in \mathbb{Z}$ *with* $n < 0$

For example, if we unravel the above definition, we have

$$\underline{4} = 1+1+1+1 \qquad \text{and} \qquad \underline{-3} = -\underline{3} = -(1+1+1) = (-1)+(-1)+(-1).$$

As these example illustrate, if n is negative, the element $\underline{n}$ is just the result of adding $-1 \in R$ to itself $|n|$ many times. Let's analyze how to add and multiply elements of the form $\underline{m}$ and $\underline{n}$. Notice that we have

$$\begin{aligned} \underline{3}+\underline{4} &= (1+1+1)+(1+1+1+1) \\ &= 1+1+1+1+1+1+1 \\ &= \underline{7}, \end{aligned}$$

and using the distributive law we have

$$\begin{aligned} \underline{3}\cdot\underline{4} &= (1+1+1)(1+1+1+1) \\ &= (1+1+1)\cdot 1 + (1+1+1)\cdot 1 + (1+1+1)\cdot 1 + (1+1+1)\cdot 1 \\ &= (1+1+1)+(1+1+1)+(1+1+1)+(1+1+1) \\ &= 1+1+1+1+1+1+1+1+1+1+1+1 \\ &= \underline{12}. \end{aligned}$$

At least for positive m and n, these computations illustrate the following result.

Proposition 10.2.2. *Let R be a ring. For any $m, n \in \mathbb{Z}$, we have*

- $\underline{m}+\underline{n} = \underline{m+n}$
- $\underline{m\cdot n} = \underline{m}\cdot\underline{n}$

Therefore the function $\varphi\colon \mathbb{Z} \to R$ defined by $\varphi(n) = \underline{n}$ is a ring homomorphism.

Proof. The first of these follows from the exponent rules for groups in Proposition 4.6.2 by viewing 1 as an element of the additive group $(R, +, 0)$ (in this additive setting, the group theory notation 1^n and our new notation $\underline{n}$ denote the same elements). The second can be proven using the distribute law and induction on n (for positive n), but we omit the details. □

Proposition 10.2.3. *Let R be a ring. For all $a \in R$ and $n \in \mathbb{Z}$, we have $\underline{n}\cdot a = a \cdot \underline{n}$. Thus, elements of the set $\{\underline{n} : n \in \mathbb{Z}\}$ commute with all elements of R.*

Proof. Let $a \in R$. Notice that

$$\begin{aligned}\underline{0} \cdot a &= 0 \cdot a \\ &= 0 \\ &= a \cdot 0 \\ &= a \cdot \underline{0}.\end{aligned}$$

If $n \in \mathbb{N}^+$, we have

$$\begin{aligned}\underline{n} \cdot a &= (1 + 1 + \cdots + 1) \cdot a \\ &= 1 \cdot a + 1 \cdot a + \cdots + 1 \cdot a \\ &= a + a + \cdots + a \\ &= a \cdot 1 + a \cdot 1 + \cdots + a \cdot 1 \\ &= a \cdot (1 + 1 + \cdots + 1) \\ &= a \cdot \underline{n},\end{aligned}$$

where each of the above sums have n terms (if you find the $\dots$ not sufficiently formal, you can again give a formal inductive argument). Suppose now that $n \in \mathbb{Z}$ with $n < 0$. We then have $-n > 0$, hence

$$\begin{aligned}\underline{n} \cdot a &= (-(\underline{-n})) \cdot a \\ &= -((\underline{-n}) \cdot a) \\ &= -(a \cdot (\underline{-n})) && \text{(from above)} \\ &= a \cdot (-(\underline{-n})) \\ &= a \cdot \underline{n}.\end{aligned}$$

□

Definition 10.2.4. *Let R be a ring. We define the* characteristic *of R, denoted $char(R)$, as follows. If there exists $n \in \mathbb{N}^+$ with $\underline{n} = 0$, we define $char(R)$ to be the least such n. If no such n exists, we define $char(R) = 0$. In other words, $char(R)$ is the order of 1 when viewed as an element of the additive group $(R, +, 0)$ if this order is finite, but equals 0 if this order is infinite.*

Notice that $char(R)$ is the order of 1 when viewed as an element of the abelian group $(R, +, 0)$, unless that order is infinite (in which case we defined $char(R) = 0$). For example, $char(\mathbb{Z}/n\mathbb{Z}) = n$ for all $n \in \mathbb{N}^+$ and $char(\mathbb{Z}) = 0$. Also, we have $char(\mathbb{Q}) = 0$ and $char(\mathbb{R}) = 0$. For an example of an infinite ring with nonzero characteristic, notice that $char(\mathbb{Z}/n\mathbb{Z}[x]) = n$ for all $n \in \mathbb{N}^+$.

Proposition 10.2.5. *Let R be a ring with $char(R) = n$ and let $\varphi\colon \mathbb{Z} \to R$ be the ring homomorphism $\varphi(m) = \underline{m}$. Let S be the subgroup of $(R, +, 0)$ generated by 1, so $S = \{\underline{m} : m \in \mathbb{Z}\}$. We then have that $S = range(\varphi)$, so S is a subring of R. Furthermore:*

- *If $n \neq 0$, then $\ker(\varphi) = n\mathbb{Z}$ and so by the First Isomorphism Theorem it follows that $\mathbb{Z}/n\mathbb{Z} \cong S$.*
- *If $n = 0$, then $\ker(\varphi) = \{0\}$, so φ is injective and hence $\mathbb{Z} \cong S$.*

In particular, if $char(R) = n \neq 0$, then R has a subring isomorphic to $\mathbb{Z}/n\mathbb{Z}$, while if $char(R) = 0$, then R has a subring isomorphic to $\mathbb{Z}$.

Proof. The additive subgroup of $(R, +, 0)$ generated by 1 is

$$S = \{\underline{m} : m \in \mathbb{Z}\} = \{\varphi(m) : m \in \mathbb{Z}\} = \text{range}(\varphi).$$

Since S is the range of ring homomorphism, we have that S is a subring of R by Corollary 10.1.16. Now if $n = 0$, then $\underline{m} \neq 0$ for all nonzero $m \in \mathbb{Z}$, so $\ker(\varphi) = \{0\}$. Suppose that $n \neq 0$. To see that $\ker(\varphi) = n\mathbb{Z}$, note that the order of 1 when viewed as an element of the abelian group $(R, +, 0)$ equals n, so $\underline{m} = 0$ if and only if $n \mid m$ by Proposition 4.6.5. $\square$

Definition 10.2.6. *Let R be a ring. The subring $S = \{\underline{m} : m \in \mathbb{Z}\}$ of R defined in the previous proposition is called the* prime subring *of R.*

Proposition 10.2.7. *If R is an integral domain, then either $char(R) = 0$ or $char(R)$ is prime.*

Proof. Let R be an integral domain and let $n = char(R)$. Notice that $n \neq 1$ because $1 \neq 0$ as R is an integral domain. Suppose that $n \geq 2$ and that n is composite. Fix $k, \ell \in \mathbb{N}$ with $2 \leq k, \ell < n$ and $n = k\ell$. We then have

$$0 = \underline{n} = \underline{k \cdot \ell} = \underline{k} \cdot \underline{\ell}$$

Since R is an integral domain, either $\underline{k} = 0$ or $\underline{\ell} = 0$. However, this is a contradiction because $k, \ell < n$ and $n = char(R)$ is the least positive value of m with $\underline{m} = 0$. Therefore, either $n = 0$ or n is prime. $\square$

10.3 Polynomial Evaluation and Roots

In this section, we will investigate the idea of roots of polynomials (i.e. those values that give 0 when plugged in) along with the question of when two different polynomials determine the same function. All of these results will rely heavily on the fact that evaluation at a point is a ring homomorphism, which holds in any commutative ring (Proposition 10.1.10). In other words, if R is commutative, $a \in R$, and $p(x), q(x) \in R[x]$, then

$$(p + q)(a) = p(a) + q(a) \qquad \text{and} \qquad (p \cdot q)(a) = p(a) \cdot q(a).$$

Therefore, all of our results will assume that R is commutative, and occasionally we will need to assume more.

Definition 10.3.1. *Let R be a commutative ring. A* root *of a polynomial $f(x) \in R[x]$ is an element $a \in R$ such that $f(a) = 0$ (or more formally $Ev_a(f(x)) = 0$).*

Proposition 10.3.2. *Let R be a commutative ring, let $a \in R$, and let $f(x) \in R[x]$. The following are equivalent:*

1. *a is a root of $f(x)$.*
2. *There exists $g(x) \in R[x]$ with $f(x) = (x - a) \cdot g(x)$.*

Proof. Suppose first that there exists $g(x) \in R[x]$ with $f(x) = (x - a) \cdot g(x)$. We then have

$$\begin{aligned} f(a) &= (a - a) \cdot g(a) \\ &= 0 \cdot g(a) \\ &= 0. \end{aligned}$$

Written more formally, we have

$$\begin{aligned} Ev_a(f(x)) &= Ev_a((x - a) \cdot g(x)) \\ &= Ev_a(x - a) \cdot Ev_a(g(x)) && \text{(since } Ev_a \text{ is a ring homomorphism)} \\ &= 0 \cdot Ev_a(g(x)) \\ &= 0. \end{aligned}$$

Therefore, a is a root of $f(x)$.

Suppose conversely that a is a root of $f(x)$. Since the leading coefficient of $x - a$ is 1, which is a unit in R, we can apply Theorem 9.3.10 to fix $q(x), r(x) \in R[x]$ with

$$f(x) = q(x) \cdot (x - a) + r(x),$$

and either $r(x) = 0$ or $\deg(r(x)) < \deg(x - a)$. Since $\deg(x - a) = 1$, we have that $r(x)$ is a constant polynomial, so we can fix $c \in R$ with $r(x) = c$. We then have

$$f(x) = q(x) \cdot (x - a) + c.$$

Now plugging in a (or applying Ev_a) we see that

$$\begin{aligned} f(a) &= q(a) \cdot (a - a) + c \\ &= q(a) \cdot 0 + c \\ &= c. \end{aligned}$$

Since we are assuming that $f(a) = 0$, it follows that $c = 0$, and thus

$$f(x) = q(x) \cdot (x - a).$$

Thus, we can take $g(x) = q(x)$. □

Proposition 10.3.3. *If R is an integral domain and $f(x) \in R[x]$ is a nonzero polynomial, then $f(x)$ has at most $\deg(f(x))$ many roots in R. In particular, every nonzero polynomial in $R[x]$ has finitely many roots.*

Proof. We prove the result by induction on $\deg(f(x))$. If $\deg(f(x)) = 0$, then $f(x)$ is a nonzero constant polynomial, so has 0 roots in R. Suppose that the statement is true for all polynomials of degree n, and let $f(x) \in R[x]$ with $\deg(f(x)) = n+1$. If $f(x)$ has no roots in R, then we are done because $0 \leq n+1$. Suppose then that $f(x)$ has at least one root in R, and fix such a root $a \in R$. Using Proposition 10.3.2, we can fix $g(x) \in F[x]$ with

$$f(x) = (x - a) \cdot g(x).$$

We now have

$$\begin{aligned} n + 1 &= \deg(f(x)) \\ &= \deg((x - a) \cdot g(x)) \\ &= \deg(x - a) + \deg(g(x)) && \text{(by Proposition 9.3.6)} \\ &= 1 + \deg(g(x)), \end{aligned}$$

so $\deg(g(x)) = n$. By induction, we know that $g(x)$ has at most n roots in R. Notice that if b is a root of $f(x)$, then

$$0 = f(b) = (b - a) \cdot g(b)$$

so either $b - a = 0$ or $g(b) = 0$ (because R is an integral domain), and hence either $b = a$ or b is a root of $g(x)$. Therefore, $f(x)$ has at most $n + 1$ roots in R, namely the roots of $g(x)$ together with a. The result follows by induction. □

Corollary 10.3.4. *Let R be an integral domain and let $n \in \mathbb{N}$. Let $f(x), g(x) \in R[x]$ be polynomials of degree at most n (including possibly the zero polynomial). If there exists at least $n + 1$ many $a \in R$ such that $f(a) = g(a)$, then $f(x) = g(x)$.*

Proof. Suppose that there are at least $n+1$ many points $a \in R$ with $f(a) = g(a)$. Consider the polynomial $h(x) = f(x) - g(x) \in R[x]$. Notice that either $h(x) = 0$ or $\deg(h(x)) \leq n$ by Proposition 9.3.5. Since $h(x)$ has at least $n+1$ many roots in R, we must have $h(x) = 0$ by Proposition 10.3.3. Thus, $f(x) - g(x) = 0$. Adding $g(x)$ to both sides, we conclude that $f(x) = g(x)$. $\square$

Back when we defined the polynomial ring $R[x]$, we were very careful to define an element as a sequence of coefficients rather than as the function defined from R to R given by evaluation. As we saw, if $R = \mathbb{Z}/2\mathbb{Z}$, then the two distinct polynomials

$$\overline{1}x^2 + \overline{1}x + \overline{1} \qquad \text{and} \qquad \overline{1}$$

give the same function on $\mathbb{Z}/2\mathbb{Z}$ because they evaluate to the same value for each element of $\mathbb{Z}/2\mathbb{Z}$. Notice that each of these polynomials has degree at most 2, but they only agree at the 2 points in $\mathbb{Z}/2\mathbb{Z}$, and hence we can not apply the previous corollary.

Corollary 10.3.5. *Let R be an infinite integral domain. If $f(x), g(x) \in R[x]$ are such that $f(a) = g(a)$ for all $a \in R$, then $f(x) = g(x)$. Thus, distinct polynomials give different functions from R to R.*

Proof. Suppose that $f(a) = g(a)$ for all $a \in R$. Consider the polynomial $h(x) = f(x) - g(x) \in R[x]$. For every $a \in R$, we have $h(a) = f(a) - g(a) = 0$. Since R is infinite, we conclude that $h(x)$ has infinitely many roots, so by the Proposition 10.3.3 we must have that $h(x) = 0$. Thus, $f(x) - g(x) = 0$. Adding $g(x)$ to both sides, we conclude that $f(x) = g(x)$. $\square$

Let R be an integral domain and let $n \in \mathbb{N}$. Suppose that we have $n+1$ many *distinct* points $a_1, a_2, \dots, a_{n+1} \in R$, along with $n+1$ many values $b_1, b_2, \dots, b_{n+1} \in R$ (which may not be distinct, and may equal some of the a_i). We know from Corollary 10.3.4 that there can be *at most* one polynomial $f(x) \in R[x]$ with either $f(x) = 0$ or $\deg(f(x)) \leq n$ such that $f(a_i) = b_i$ for all i. Must one always exist?

In $\mathbb{Z}$, the answer is no. Suppose, for example, that $n = 1$, and we want to find a polynomial of degree at most 1 such that $f(0) = 1$ and $f(2) = 2$. Writing $f(x) = ax + b$, we then need $1 = f(0) = a \cdot 0 + b$, so $b = 1$, and hence $f(x) = ax + 1$. We also need $2 = f(2) = a \cdot 2 + 1$, which would require $2 \cdot (1 - a) = 1$. Since $2 \nmid 1$, there is no $a \in \mathbb{Z}$ satisfying this. Notice, however, that if we go up to $\mathbb{Q}$, then $f(x) = \frac{1}{2} \cdot x + 1$ works as an example here. In general, such polynomials always exist when working over a *field* F.

Theorem 10.3.6 (Lagrange Interpolation)**.** *Let F be a field and let $n \in \mathbb{N}$. Suppose that we have $n+1$ many* distinct *points $a_1, a_2, \dots, a_{n+1} \in F$, along with $n+1$ many values $b_1, b_2, \dots, b_{n+1} \in F$ (which may not be distinct, and may equal some of the a_i). There exists a unique polynomial $f(x) \in F[x]$ with either $f(x) = 0$ or $\deg(f(x)) \leq n$ such that $f(a_i) = b_i$ for all i.*

Before jumping into the general proof of this result, we first consider the case when $b_k = 1$ and $b_i = 0$ for all $i \neq k$. In order to build a polynomial $f(x)$ of degree at most n such that $f(a_i) = b_i = 0$ for all $i \neq k$, we need to make the a_i with $i \neq k$ roots of our polynomial. The idea is to consider the polynomial

$$h_k(x) = (x - a_1) \cdots (x - a_{k-1})(x - a_{k+1}) \cdots (x - a_n).$$

Now for all $i \neq k$, we have $h_k(a_i) = 0 = b_i$, so we are good there. However, when we plug in a_k, we obtain

$$h_k(a_k) = (a_k - a_1) \cdots (a_k - a_{k-1})(a_k - a_{k+1}) \cdots (a_k - a_n),$$

which is most likely not equal to 1. However, since the a_i are distinct, we have that $a_k - a_i \neq 0$ for all $i \neq k$. Now F is integral domain (because it is a field), so the product above is nonzero. Since F is a field, we can divide by the resulting value. This suggests considering the polynomial

$$g_k(x) = \frac{(x - a_1) \cdots (x - a_{k-1})(x - a_{k+1}) \cdots (x - a_{n+1})}{(a_k - a_1) \cdots (a_k - a_{k-1})(a_k - a_{k+1}) \cdots (a_k - a_{n+1})}.$$

Notice now that $g_k(a_i) = 0 = b_i$ for all $i \neq k$, and $g_k(a_k) = 1 = b_k$. Thus, we are successful in the very special case where one of the b_i equals 1 and the rest are 0.

How do we generalize this? First, if $b_k \neq 0$ (but possibly not 1) while $b_i = 0$ for all $i \neq k$, then we just scale $g_k(x)$ accordingly and consider the polynomial $b_k \cdot g_k(x)$. Fortunately, to handle the general case, we need only add up the corresponding polynomials!

Proof of Theorem 10.3.6. For each k, let

$$g_k(x) = \frac{(x-a_1)\cdots(x-a_{k-1})(x-a_{k+1})\cdots(x-a_{n+1})}{(a_k-a_1)\cdots(a_k-a_{k-1})(a_k-a_{k+1})\cdots(a_k-a_{n+1})}.$$

Notice that $\deg(g_k(x)) = n$ for each k (since there are n terms in the product, each of which as degree 1), that $g_k(a_i) = 0$ whenever $i \neq k$, and that $g_k(a_k) = 1$. Now let

$$f(x) = b_1 \cdot g_1(x) + b_2 \cdot g_2(x) + \cdots + b_n \cdot g_n(x) + b_{n+1} \cdot g_{n+1}(x).$$

Since $\deg(b_k \cdot g_k(x)) = n$ for all k, it follows that either $f(x) = 0$ or $\deg(f(x)) \leq n$. Furthermore, for any i, we have

$$\begin{aligned} f(a_i) &= b_1 \cdot g_1(a_i) + \cdots + b_i \cdot g_i(a_i) + \cdots + b_{n+1} \cdot g_{n+1}(a_i) \\ &= 0 + \cdots + 0 + b_i \cdot g_i(a_i) + 0 + \cdots + 0 \\ &= b_i \cdot 1 \\ &= b_i. \end{aligned}$$

This proves existence. Uniqueness follow from Corollary 10.3.4. □

10.4 Generating Subrings and Ideals in Commutative Rings

In Section 5.2, we proved that if G is a group and $A \subseteq G$, then there is a "smallest" subgroup of G that contains A, i.e. there exists a subgroup H of G containing A with the property that H is a subset of any other subgroup of G containing A. We proved this result in Proposition 5.2.8, and called the resulting H the subgroup generated by A. We now prove the analogue for subrings.

Proposition 10.4.1. *Let R be a ring and let $A \subseteq R$. There exists a subring S of R with the following properties:*

- *$A \subseteq S$.*
- *Whenever T is a subring of R with the property that $A \subseteq T$, we have $S \subseteq T$.*

Furthermore, the subring S is unique (i.e. if both S_1 and S_2 have the above properties, then $S_1 = S_2$).

Proof. The idea is to intersect all of the subrings of R that contain A, and argue that the result is a subgroup. We first prove existence. Notice that there is at least one subring of R containing A, namely R itself. Define

$$S = \{a \in R : a \in T \text{ for all subrings } T \text{ of } R \text{ with } A \subseteq T\}.$$

Notice we certainly have $A \subseteq S$ by definition. Moreover, if T is a subring of R with the property that $A \subseteq T$, then we have $T \subseteq S$ by definition of S. We now show that S is indeed a subring of R.

- Since $0, 1 \in T$ for every subring T of R with $A \subseteq T$, we have $0, 1 \in S$.

- Let $a, b \in S$. For any subring T of R such that $A \subseteq T$, we must have both $a, b \in T$ by definition of S, hence $a + b \in T$ because T is a subring. Since this is true for all such T, we conclude that $a + b \in S$ by definition of S.

- Let $a \in S$. For any subring T of R such that $A \subseteq T$, we must have both $a \in T$ by definition of S, hence $-a \in T$ because T is a subring. Since this is true for all such K, we conclude that $a^{-1} \in H$ by definition of H.

- Let $a, b \in S$. For any subring T of R such that $A \subseteq T$, we must have both $a, b \in T$ by definition of S, hence $ab \in T$ because T is a subring. Since this is true for all such T, we conclude that $ab \in S$ by definition of S.

Combining these four properties, we conclude that S is a subring of R. This finishes the proof of existence.

Finally, suppose that S_1 and S_2 both have the above properties. Since S_2 is a subring of R with $A \subseteq S_2$, we know that $S_1 \subseteq S_2$. Similarly, since S_1 is a subring of R with $A \subseteq S_1$, we know that $S_2 \subseteq S_1$. Therefore, $S_1 = S_2$. □

In group theory, when G was a group and $A = \{a\}$ consisted of a single element, the corresponding subgroup was $\{a^n : a \in \mathbb{Z}\}$. We want to develop a similar explicit description in the commutative ring case (one can also look at noncommutative rings, but the description is significantly more complicated). However, instead of just looking at the smallest ring containing one element, we are going to generalize the construction as follows. Assume that we already have a subring S of R. With this base in hand, suppose that we now want to include one other element $a \in R$ in our subring. We then want to know what is the smallest subring containing $S \cup \{a\}$? Notice that if we really want just the smallest ring that contains one $a \in R$, we can simply take S to be the prime subring of R from Definition 10.2.6 (because every subring of R must contain 1, it follows that every subring of R must also contain the prime subring of R).

Proposition 10.4.2. *Suppose that R is a commutative ring, that S is a subring of R, and that $a \in R$. Let*

$$\begin{aligned} S[a] &= \{p(a) : p(x) \in S[x]\} \\ &= \{s_n a^n + s_{n-1} a^{n-1} + \cdots + s_1 a + s_0 : n \in \mathbb{N} \text{ and } s_1, s_2, \ldots, s_n \in S\}. \end{aligned}$$

We have the following:

1. *$S[a]$ is a subring of R with $S \cup \{a\} \subseteq S[a]$.*

2. *If T is a subring R with $S \cup \{a\} \subseteq T$, then $S[a] \subseteq T$.*

Therefore, $S[a]$ is the smallest subring of R containing $S \cup \{a\}$.

Proof. We first check (1):

- Notice that $0, 1 \in \{p(a) : p(x) \in S[x]\}$ by considering the zero polynomial and one polynomial.

- Given two elements of $S[a]$, say $p(a)$ and $q(a)$ where $p(x), q(x) \in S[x]$, we have that $p(a) + q(a) = (p + q)(a)$ and $p(a) \cdot q(a) = (pq)(a)$. Since $p(x) + q(x) \in S[x]$ and $p(x), q(x) \in S[x]$, it follows that $S[a]$ is closed under addition and multiplication.

- Consider an arbitrary element $p(a) \in S[a]$, where $p(x) \in S[x]$. Since evaluation is a ring homomorphism, we then have that $-p(a) = (-p)(a)$, where $-p$ is the additive inverse of p in $S[x]$. Thus, $S[a]$ is closed under additive inverses.

Therefore, $S[a]$ is subring of R. Finally, notice that $S \cup \{a\} \subseteq S[a]\}$ by considering the constant polynomials and $x \in S[x]$.

Suppose now that T is an arbitrary subring of R with $S \cup \{a\} \subseteq T$. Let $n \in \mathbb{N}^+$ and let $s_1, s_2, \dots, s_n \in S$ be arbitrary. Notice that $a^0 = 1 \in T$ because T is a subring of R, and $a^k \in T$ for all $k \in \mathbb{N}^+$ because $a \in T$ and T is closed under multiplication. Since $s_k \in T$ for all k (because $S \subseteq T$), we can use the fact that T is closed under multiplication to conclude that $s_k a^k \in T$ for all k. Finally, since T is closed under addition, we conclude that $s_n a^n + s_{n-1}a^{n-1} + \dots + s_1 a + s_0 \in T$. Therefore, $S[a] \subseteq T$. $\square$

In group theory, we know that if $|a| = n$, then we can write $\langle a \rangle = \{a^k : 0 \leq k \leq n-1\}$ in place of $\{a^k : k \in \mathbb{Z}\}$. In other words, sometimes we have redundancy in the set $\{a^k : k \in \mathbb{Z}\}$ and can express $\langle a \rangle$ with less. The same holds true now, and sometimes we can obtain all elements of $S[a]$ using fewer than all polynomials in $S[x]$. For example, consider $\mathbb{Q}$ as a subring of $\mathbb{R}$. Suppose that we now want to include $\sqrt{2}$. From above, we then have that

$$\begin{aligned}\mathbb{Q}[\sqrt{2}] &= \{p(\sqrt{2}) : p(x) \in \mathbb{Q}\} \\ &= \{b_n(\sqrt{2})^n + b_{n-1}(\sqrt{2})^{n-1} + \dots + b_1(\sqrt{2}) + b_0 : n \in \mathbb{N} \text{ and } b_1, b_2, \dots, b_n \in \mathbb{Q}\}.\end{aligned}$$

Although this certainly works, there is a lot of redundancy in the set on the right. For example when we plug $\sqrt{2}$ into $x^3 + x^2 - 7$, we obtain

$$\begin{aligned}(\sqrt{2})^3 + (\sqrt{2})^2 - 7 &= \sqrt{8} + 2 - 7 \\ &= 2\sqrt{2} - 5\end{aligned}$$

which is the same thing as plugging $\sqrt[3]{2}$ into $2x - 5$. In fact, since $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is subring of $\mathbb{R}$, as we checked in Section 9.1, it suffices to plug $\sqrt{2}$ into only the polynomials of the form $a + bx$ where $a, b \in \mathbb{Q}$. A similar thing happened with $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, where if we want to find the smallest subring of $\mathbb{C}$ containing $\mathbb{Z} \cup \{i\}$, we just needed to plug i into linear polynomials with coefficients in $\mathbb{Z}$.

Suppose instead that we consider $\mathbb{Q}$ as a subring of $\mathbb{R}$, and we now want to include $\sqrt[3]{2}$. We know from above that

$$\begin{aligned}\mathbb{Q}[\sqrt[3]{2}] &= \{p(\sqrt[3]{2}) : p(x) \in \mathbb{Q}\} \\ &= \{b_n(\sqrt[3]{2})^n + b_{n-1}(\sqrt[3]{2})^{n-1} + \dots + b_1(\sqrt[3]{2}) + b_0 : n \in \mathbb{N} \text{ and } b_0, b_1, \dots, b_n \in \mathbb{Q}\}.\end{aligned}$$

Can we express $\mathbb{Q}[\sqrt[3]{2}]$ as $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\}$? Notice that $(\sqrt[3]{2})^2 = \sqrt[3]{4}$ must be an element of $\mathbb{Q}[\sqrt[3]{2}]$, but it is not clear whether it is possible to write $\sqrt[3]{4}$ in the form $a + b\sqrt[3]{2}$ where $a, b \in \mathbb{Q}$. In fact, it is impossible to find such a and b, although it is tedious to verify this fact now. However, it is true that

$$\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\},$$

so we need only plug $\sqrt[3]{2}$ into quadratic polynomials with coefficients in $\mathbb{Q}$. We will verify all of these facts, and investigate these kinds of questions in more detail later.

Suppose now that S is a subring of a commutative ring R and $a_1, a_2, \dots, a_n \in R$. How do we obtain an explicit description of $S[a_1, a_2, \dots, a_n]$? It is natural to guess that one obtains $S[a_1, a_2, \dots, a_n]$ by plugging the point $(a_1, a_2, \dots, a_n)$ into all polynomials in n variables over S. This is indeed the case, but we will wait until we develop the theory of such multivariable polynomials more deeply.

We now move on to generating ideals. Analogously to Proposition 5.2.8 and Proposition 10.4.1, we have the following result. Since the argument is completely analogous, we omit the proof.

Proposition 10.4.3. *Let R be a ring and let $A \subseteq R$. There exists an ideal I of R with the following properties:*

- *$A \subseteq I$.*
- *Whenever J is an ideal of R with the property that $A \subseteq J$, we have $I \subseteq J$.*

Furthermore, the ideal is unique (i.e. if both I_1 and I_2 have the above properties, then $I_1 = I_2$).

Let R be a commutative ring. Suppose that $a \in R$, and we want an explicit description of the smallest ideal that contains the element a (so we are considering the case where $A = \{a\}$). Notice that ra must be an element of this ideal for all $r \in R$. Fortunately, the resulting set turns out to be an ideal

Proposition 10.4.4. *Let R be a commutative ring and let $a \in R$. Let $I = \{ra : r \in R\}$.*

1. *I is an ideal of R with $a \in I$.*
2. *If J is an ideal of R with $a \in J$, then $I \subseteq J$.*

Therefore, I is the smallest ideal of R containing a.

Proof. We first prove (1). We begin by noting that $a = 1 \cdot a \in I$ and that $0 = 0 \cdot a \in I$. For any $r, s \in R$, we have

$$ra + sa = (r + s)a \in I,$$

so I is closed under addition. For any $r, s \in R$, we have

$$r \cdot (sa) = (rs) \cdot a \in I.$$

Therefore I is an ideal of R with $a \in I$ by Corollary 10.1.3.

We now prove (2). Let J be an ideal of R with $a \in J$. For any $r \in R$, we have $ra \in J$ because J is a ideal of R and $a \in J$. It follows that $I \subseteq J$. □

Since we will be looking at these types of ideals often, and they are sometime analogous to cyclic subgroups, we steal the notation that we used in group theory.

Definition 10.4.5. *Let R be a commutative ring and let $a \in R$. We define $\langle a \rangle = \{ra : r \in R\}$. The ideal $\langle a \rangle$ is called the* ideal generated by *a.*

Be careful with this overloaded notation! If G is a group and $a \in G$, then $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$. However, if R is commutative ring and $a \in R$, then $\langle a \rangle = \{ra : r \in R\}$.

Definition 10.4.6. *Let R be a commutative ring and let I be an ideal of R. We say that I is a* principal ideal *if there exists $a \in R$ with $I = \langle a \rangle$.*

Proposition 10.4.7. *The ideals of $\mathbb{Z}$ are precisely the sets $n\mathbb{Z} = \langle n \rangle$ for every $n \in \mathbb{N}$. Thus, every ideal of $\mathbb{Z}$ is principal.*

Proof. For each $n \in \mathbb{N}$, we know that $\langle n \rangle = \{kn : k \in \mathbb{Z}\}$ is an ideal by Proposition 10.4.4. Suppose now that I is an arbitrary ideal of $\mathbb{Z}$. Since ideals of $\mathbb{Z}$ are in particular additive subgroups of $\mathbb{Z}$, one can use Corollary 7.1.6 to argue that every ideal of $\mathbb{Z}$ is of this form. However, we give a direct argument.

Let I be an arbitrary ideal of $\mathbb{Z}$. We know that $0 \in I$. If $I = \{0\}$, then $I = \langle 0 \rangle$, and we are done. Suppose then that $I \neq \{0\}$. Notice that if $k \in I$, then $-k \in I$ as well, hence $I \cap \mathbb{N}^+ \neq \emptyset$. By well-ordering, we may let $n = \min(I \cap \mathbb{N}^+)$. We claim that $I = \langle n \rangle$.

First notice that since $n \in I$ and I is an ideal of R, it follows from Proposition 10.4.4 that $\langle n \rangle \subseteq I$. Let $m \in I$ be arbitrary. Fix $q, r \in \mathbb{Z}$ with $m = qn + r$ and $0 \leq r < n$. We then have that $r = m - qn = m + (-q)n$. Since $m, n \in I$ and I is an ideal, we know that $(-q)n \in I$ and so $r = m + (-q)n \in I$. Now $0 \leq r < n$ and $n = \min(I \cap \mathbb{N}^+)$, so we must have $r = 0$. It follows that $m = qn$, so $k \in \langle n \rangle$. Now $m \in I$ was arbitrary, so $I \subseteq \langle n \rangle$. Putting this together with the above, we conclude that $I = \langle n \rangle$. □

Lemma 10.4.8. *Let R be a commutative ring and let I be an ideal of R. We have that $I = R$ if and only if I contains a unit of R.*

Proof. If $I = R$, then $1 \in I$, so I contains a unit. Suppose conversely that I contains a unit, and fix such a unit $u \in I$. Since u is a unit, we may fix $v \in R$ with $vu = 1$. Since $u \in I$ and I is an ideal, we conclude that $1 \in I$. Now for any $r \in R$, we have $r = r \cdot 1 \in I$ again because I is an ideal of R. Thus, $R \subseteq I$, and since $I \subseteq R$ trivially, it follows that $I = R$. □

Using principal ideals, we can prove the following simple but important result.

Proposition 10.4.9. *Let R be a commutative ring. The following are equivalent:*

1. *R is a field.*
2. *The only ideals of R are $\{0\}$ and R.*

Proof. We first prove that (1) implies (2). Suppose that R is field. Let I be an ideal of R with $I \neq \{0\}$. Fix $a \in I$ with $a \neq 0$. Since R is a field, every nonzero element of R is a unit, so a is a unit. Since $a \in I$, we may use the lemma to conclude that $I = R$.

We now prove that (2) implies (1) by proving the contrapositive. Suppose that R is not a field. Fix a nonzero element $a \in R$ such that a is not a unit. Let $I = \langle a \rangle = \{ra : r \in R\}$. We know from above that I is an ideal of R. If $1 \in I$, then we may fix $r \in R$ with $ra = 1$, which implies that a is a unit (remember that we are assuming that R is commutative). Therefore, $1 \notin I$, and hence $I \neq R$. Since $a \neq 0$ and $a \in I$, we have $I \neq \{0\}$. Therefore, I is an ideal of R distinct from $\{0\}$ and R. □

Given finitely many elements $a_1, a_2, \dots, a_n$ of a commutative ring R, we can also describe the smallest ideal of R containing $\{a_1, a_2, \dots, a_n\}$ in a simple manner. We leave the verification as an exercise.

Definition 10.4.10. *Let R be a commutative ring and let $a_1, a_2, \dots, a_n \in R$. We define*

$$\langle a_1, a_2, \dots, a_n \rangle = \{r_1a_1 + r_2a_2 + \dots + r_na_n : r_i \in R \textit{ for each } i\}.$$

This set is the smallest ideal of R containing $a_1, a_2, \dots, a_n$, and we call it the ideal generated by $a_1, a_2, \dots, a_n$.

For example, consider the ring $\mathbb{Z}$. We know that $\langle 15, 42 \rangle$ is an ideal of $\mathbb{Z}$. Now

$$\langle 15, 42 \rangle = \{15k + 42\ell : k, \ell \in \mathbb{Z}\}$$

is an ideal of $\mathbb{Z}$, so it must equal $\langle n \rangle$ for some $n \in \mathbb{Z}$ by Proposition 10.4.7. Since $\gcd(15, 42) = 3$, we know that 3 divides every element in $\langle 15, 42 \rangle$, and we also know that 3 is an actual element of $\langle 15, 42 \rangle$. Working out the details, one can show that $\langle 15, 42 \rangle = \langle 3 \rangle$. Generalizing this argument, one can show that if $a, b \in \mathbb{Z}$, then $\langle a, b \rangle = \langle \gcd(a, b) \rangle$.

10.5 Prime and Maximal Ideals in Commutative Rings

Throughout this section, we work in the special case when R is a commutative ring. In this context, we define two very special kinds of ideals.

Definition 10.5.1. *Let R be a commutative ring.*

- *A* prime ideal *of R is an ideal $P \subseteq R$ such that $P \neq R$ and whenever $ab \in P$, then either $a \in P$ or $b \in P$.*
- *A* maximal ideal *of R is an ideal $M \subseteq R$ such that $M \neq R$ and there exists no ideal I of R with $M \subsetneq I \subsetneq R$.*

For an example, consider the ideal $\langle x\rangle$ in the commutative ring $\mathbb{Z}[x]$. We have

$$\begin{aligned}\langle x\rangle &= \{x\cdot p(x) : p(x)\in\mathbb{Z}[x]\}\\ &= \{x\cdot(a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0) : n\in\mathbb{N}\text{ and }a_0,a_1,\dots,a_n\in\mathbb{Z}\}\\ &= \{a_nx^{n+1}+a_{n-1}x^n+\cdots+a_1x^2+a_0x : n\in\mathbb{N}\text{ and }a_0,a_1,\dots,a_n\in\mathbb{Z}\}\\ &= \{f(x)\in\mathbb{Z}[x] : \text{ The constant term of } f(x) \text{ is } 0\}\\ &= \{f(x)\in\mathbb{Z}[x] : f(0)=0\}.\end{aligned}$$

We claim that $\langle x\rangle$ is a prime ideal of $\mathbb{Z}[x]$. To see this, suppose that $f(x),g(x)\in\mathbb{Z}[x]$ and that $f(x)g(x)\in\langle x\rangle$. We then have that $f(0)g(0)=0$, so either $f(0)=0$ or $g(0)=0$ (because $\mathbb{Z}$ is an integral domain). It follows that either $f(x)\in\langle x\rangle$ or $g(x)\in\langle x\rangle$.

For an example of an ideal that is *not* a prime ideal, consider the ideal $\langle 6\rangle = 6\mathbb{Z}$ in $\mathbb{Z}$. We have that $2\cdot 3\in 6\mathbb{Z}$ but $2\notin 6\mathbb{Z}$ and $3\notin 3\mathbb{Z}$. Also, $\langle 6\rangle$ is not a maximal ideal because $\langle 6\rangle\subsetneq\langle 3\rangle$ (because every multiple of 6 is a multiple of 3, but $3\notin\langle 6\rangle$).

Proposition 10.5.2. *Let R be a commutative ring with $1\neq 0$. The ideal $\{0\}$ is a prime ideal of R if and only if R is an integral domain.*

Proof. Suppose first that $\{0\}$ is a prime ideal of R. Let $a,b\in R$ be arbitrary with $ab=0$. We then have that $ab\in\{0\}$, so either $a\in\{0\}$ or $b\in\{0\}$ because $\{0\}$ is a prime ideal of R. Thus, either $a=0$ or $b=0$. Since R has no zero divisors, we conclude that R is an integral domain.

Conversely, suppose that R is an integral domain. Notice that $\{0\}$ is an ideal of R with $\{0\}\neq R$ (since $1\neq 0$). Let $a,b\in R$ be arbitrary with $ab\in\{0\}$. We then have that $ab=0$, so as R is an integral domain we can conclude that either $a=0$ or $b=0$. Thus, either $a\in\{0\}$ or $b\in\{0\}$. It follows that $\{0\}$ is a prime ideal of R. ☐

We can now classify the prime and maximal ideals of $\mathbb{Z}$.

Proposition 10.5.3. *Let I be an ideal of $\mathbb{Z}$.*

1. *I is a prime ideal if and only if either $I=\{0\}$ or $I=\langle p\rangle$ for some prime $p\in\mathbb{N}^+$.*
2. *I is a maximal ideal if and only if $I=\langle p\rangle$ for some prime $p\in\mathbb{N}^+$.*

Proof.

1. First notice that $\{0\}$ is a prime ideal of $\mathbb{Z}$ by Proposition 10.5.2 because $\mathbb{Z}$ is an integral domain. Suppose now that $p\in\mathbb{N}^+$ is prime and let $I=\langle p\rangle=\{pk : k\in\mathbb{Z}\}$. We then have that $I=\langle p\rangle$, so I is indeed an ideal of $\mathbb{Z}$ by Proposition 10.4.4. Suppose that $a,b\in\mathbb{Z}$ are such that $ab\in p\mathbb{Z}$. Fix $k\in\mathbb{Z}$ with $ab=pk$. We then have that $p\mid ab$, so as p is prime, either $p\mid a$ or $p\mid b$ by Proposition 2.5.6. If $p\mid a$, then we can fix $\ell\in\mathbb{Z}$ with $a=p\ell$, from which we can conclude that $a\in p\mathbb{Z}$. Similarly, if $p\mid b$, then we can fix $\ell\in\mathbb{Z}$ with $b=p\ell$, from which we can conclude that $b\in p\mathbb{Z}$. Thus, either $a\in p\mathbb{Z}$ or $b\in p\mathbb{Z}$. Therefore, $p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.

   Suppose conversely that I is a prime ideal of $\mathbb{Z}$. By Proposition 10.4.7, we can fix $n\in\mathbb{N}$ with $I=\langle n\rangle$. We need to prove that either $n=0$ or n is prime. Notice that $n\neq 1$ because $\langle 1\rangle=\mathbb{Z}$ is not a prime ideal of $\mathbb{Z}$ by definition. Suppose that $n\geq 2$ is not prime. We can then fix $c,d\in\mathbb{N}$ with $n=cd$ and both $1<c<n$ and $1<d<n$. Notice that $cd=n\in\langle n\rangle$. However, if $c\in\langle n\rangle$, then fixing $k\in\mathbb{Z}$ with $c=nk$, we notice that $k>0$ (because $c,n>0$), so $c=nk\geq n$, a contradiction. Thus, $c\notin\langle n\rangle$. Similarly, $d\notin\langle n\rangle$. It follows that $\langle n\rangle$ is not prime ideal when $n\geq 2$ is composite. Therefore, if $I=\langle n\rangle$ is a prime ideal, then either $n=0$ or n is prime.

2. Suppose first that $I=\langle p\rangle$ for some prime $p\in\mathbb{N}^+$. Let J be an ideal of $\mathbb{Z}$ with $I\subseteq J$. We prove that either $I=J$ or $I=\mathbb{Z}$. By Proposition 10.4.7, we can fix $n\in\mathbb{N}$ with $J=\langle n\rangle$. Since $I\subseteq J$ and $p\in I$,

we have that $p \in J = \langle n \rangle$. Thus, we can fix $k \in \mathbb{Z}$ with $p = nk$. Notice that $k > 0$ because $p, n > 0$. Since p is prime, it follows that either $n = 1$ or $n = p$. If $n = 1$, then $J = \langle 1 \rangle = \mathbb{Z}$. If $n = p$, then $J = \langle p \rangle = I$. Therefore, $I = \langle p \rangle$ is a maximal ideal of $\mathbb{Z}$.

Suppose conversely that I is a maximal ideal of $\mathbb{Z}$. By Proposition 10.4.7, we can fix $n \in \mathbb{N}$ with $I = \langle n \rangle$. We need to prove that either n is prime. Notice that $n \neq 0$ because $\langle 0 \rangle$ is not a maximal ideal of $\mathbb{Z}$ (we have $\langle 0 \rangle \subsetneq \langle 2 \rangle \subsetneq \mathbb{Z}$). Also, $n \neq 1$ because $\langle 1 \rangle = \mathbb{Z}$ is not a maximal ideal of $\mathbb{Z}$ by definition. Suppose that $n \geq 2$ is not prime. We can then fix $c, d \in \mathbb{N}$ with $n = cd$ and both $1 < c < n$ and $1 < d < n$. Notice that $\langle n \rangle \subseteq \langle d \rangle$ because every multiple of n is a multiple of d. However, we have $d \notin \langle n \rangle$ because $n \nmid d$ (as $1 < d < n$). Furthermore, we have $\langle d \rangle \neq \mathbb{Z}$ because $1 \notin \langle d \rangle$. Since $\langle n \rangle \subsetneq \langle d \rangle \subsetneq \mathbb{Z}$, we conclude that $\langle n \rangle$ is not a maximal ideal of $\mathbb{Z}$. Therefore, if $I = \langle n \rangle$ is a maximal ideal, then n is prime.

□

We can classify the prime and maximal ideals of a commutative ring by the properties of the corresponding quotient ring.

Theorem 10.5.4. *Let R be a commutative ring and let P be an ideal of R. P is a prime ideal of R if and only if R/P is an integral domain.*

Proof. Suppose first that P is a prime ideal of R. Since R is commutative, we know that R/P is commutative. By definition, we have $P \neq R$, so $1 \notin P$, and hence $1 + P \neq 0 + P$. Finally, suppose that $a, b \in R$ with $(a + P) \cdot (b + P) = 0 + P$. We then have that $ab + P = 0 + P$, so $ab \in P$. Since P is a prime ideal, either $a \in P$ or $b \in P$. Therefore, either $a + P = 0 + P$ or $b + P = 0 + P$. It follows that R/P is an integral domain.

Suppose conversely that R/P is an integral domain. We then have that $1 + P \neq 0 + P$ by definition of an integral domain, hence $1 \notin P$ and so $P \neq R$. Suppose that $a, b \in R$ with $ab \in P$. We then have

$$(a + P) \cdot (b + P) = ab + P = 0 + P$$

Since R/P is an integral domain, we conclude that either $a + P = 0 + P$ or $b + P = 0 + P$. Therefore, either $a \in P$ or $b \in P$. It follows that P is a prime ideal of R. □

Theorem 10.5.5. *Let R be a commutative ring and let M be an ideal of R. M is a maximal ideal of R if and only if R/M is a field.*

Proof. We give two proofs. The first is the slick "highbrow" proof. Using the Correspondence Theorem and Proposition 10.4.9, we have

$$\begin{aligned} M \text{ is a maximal ideal of } R &\iff \text{There are no ideals } I \text{ of } R \text{ with } M \subsetneq I \subsetneq R \\ &\iff \text{There are no ideals of } R/M \text{ other than } \{0 + I\} \text{ and } R/M \\ &\iff R/M \text{ is a field} \end{aligned}$$

If you don't like appealing to the Correspondence Theorem (which is a shame, because it's awesome), we can prove it directly via a "lowbrow" proof.

Suppose first that M is a maximal ideal of R. Fix a nonzero element $a + M \in R/M$. Since $a + M \neq 0 + M$, we have that $a \notin M$. Let $I = \{ra + m : s \in R, m \in M\}$. We then have that I is an ideal of M (check it) with $M \subseteq I$ and $a \in I$. Since $a \notin M$, we have $M \subsetneq I$, so as M is maximal it follows that $I = R$. Thus, we may fix $r \in R$ and $m \in M$ with $ra + m = 1$. We then have $ra - 1 = -m \in M$, so $ra + M = 1 + M$. It follows that $(r + M)(a + M) = 1 + M$, so $a + M$ has an inverse in R/M (recall that R and hence R/M is commutative, so we only need an inverse on one side).

Suppose conversely that R/M is a field. Since R/M is a field, we have $1 + M \neq 0 + M$, so $1 \notin M$ and hence $M \subsetneq R$. Fix an ideal I of R with $M \subsetneq I$. Since $M \subsetneq I$, we may fix $a \in I \backslash M$. Since $a \notin M$, we have

$a+M \neq 0+M$, and using the fact that R/M is a field we may fix $b+M \in R/M$ with $(a+M)(b+M) = 1+M$. We then have $ab + M = 1 + M$, so $ab - 1 \in M$. Fixing $m \in M$ with $ab - 1 = m$, we then have $ab - m = 1$. Now $a \in I$, so $ab \in I$ as I is an ideal. Also, we have $m \in M \subseteq I$. It follows that $1 = ab - m \in I$, and thus $I = R$. Therefore, M is a maximal ideal of R. □

From the theorem, we see that $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$ for every prime $p \in \mathbb{N}^+$ because we know that $\mathbb{Z}/p\mathbb{Z}$ is a field, which gives a much faster proof of one part of Proposition 10.5.3. We also obtain the following nice corollary.

Corollary 10.5.6. *Let R be a commutative ring. Every maximal ideal of R is a prime ideal of R.*

Proof. Suppose that M is a maximal ideal of R. We then have that R/M is a field by Theorem 10.5.5, so R/M is an integral domain by Proposition 9.2.9. Therefore, M is a prime ideal of R by Theorem 10.5.4. □

The converse is not true. As we've seen, the ideal $\{0\}$ is a prime ideal of $\mathbb{Z}$, but it is certainly not a maximal ideal of $\mathbb{Z}$.

10.6 Field of Fractions

Let R be an integral domain. In this section, we show that R can be embedded in a field F. Furthermore, our construction gives a "smallest" such field F in a sense to be made precise below. We call this field the *field of fractions* of R and denote it $Frac(R)$. Our method for building $Frac(R)$ generalizes the construction of the rationals from the integers we outlined in Chapter 3, and in particular we will carry out all of the necessary details that we omitted there. Notice that the fact that every integral domain R can be embedded in a field "explains" why we have cancellation in integral domains (because when viewed in the larger field $Frac(R)$, we can multiply both sides by the multiplicative inverse).

Definition 10.6.1. *Let R be an integral domain. Define $P = R \times (R \backslash \{0\})$. We define a relation $\sim$ on P by letting $(a, b) \sim (c, d)$ if $ad = bc$.*

Proposition 10.6.2. *$\sim$ is an equivalence relation on P.*

Proof. We check the properties:

- Reflexive: For any $a, b \in R$ with $b \neq 0$, we have $(a, b) \sim (a, b)$ because $ab = ba$, so $\sim$ is reflexive.
- Symmetric: Suppose that $a, b, c, d \in R$ with $b, d \neq 0$ and $(a, b) \sim (c, d)$. We then have $ad = bc$, hence $cb = bc = ad = da$. It follows that $(c, d) \sim (a, b)$.
- Transitive: Suppose that $a, b, c, d, e, f \in \mathbb{Z}$ with $b, d, f \neq 0$, $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. We then have $ad = bc$ and $cf = de$. Hence,

$$\begin{aligned}
(af)d &= (ad)f \\
&= (bc)f && \text{(since } ad = bc\text{)} \\
&= b(cf) \\
&= b(de) && \text{(since } cf = de\text{)} \\
&= (be)d
\end{aligned}$$

  Therefore, $af = be$ because R is an integral domain and $d \neq 0$.

□

We now define $Frac(R)$ to be the set of equivalence classes, i.e. $Frac(R) = P/\sim$. We need to define addition and multiplication on F to make it into a field. Mimicking addition and multiplication of rationals, we want to define

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc,bd)} \qquad\qquad \overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac,bd)}$$

Notice first that since $b, d \neq 0$, we have $bd \neq 0$ because R is an integral domain, so we have no issues there. However, we need to check that the operations are well-defined.

Proposition 10.6.3. *Let $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in R$ with $b_1, b_2, d_1, d_2 \neq 0$. Suppose that $(a_1, b_1) \sim (a_2, b_2)$ and $(c_1, d_1) \sim (c_2, d_2)$. We then have*

- $(a_1d_1 + b_1c_1, b_1d_1) \sim (a_2d_2 + b_2c_2, b_2d_2)$
- $(a_1c_1, b_1d_1) \sim (a_2c_2, b_2d_2)$

Thus, the above operations of $+$ and $\cdot$ on $Frac(R)$ are well-defined.

Proof. Since $(a_1, b_1) \sim (a_2, b_2)$ and $(c_1, d_1) \sim (c_2, d_2)$, it follows that $a_1b_2 = b_1a_2$ and $c_1d_2 = d_1c_2$. We have

$$\begin{aligned}
(a_1d_1 + b_1c_1) \cdot b_2d_2 &= a_1b_2d_1d_2 + c_1d_2b_1b_2 \\
&= b_1a_2d_1d_2 + d_1c_2b_1b_2 \\
&= b_1d_1 \cdot (a_2d_2 + b_2c_2)
\end{aligned}$$

so $(a_1d_1 + b_1c_1, b_1d_1) \sim (a_2d_2 + b_2c_2, b_2d_2)$.

Multiplying $a_1b_2 = b_1a_2$ and $c_1d_2 = d_1c_2$, we conclude that

$$a_1b_2 \cdot c_1d_2 = b_1a_2 \cdot d_1c_2$$

and hence

$$a_1c_1 \cdot b_2d_2 = b_1d_1 \cdot a_2c_2$$

Therefore, $(a_1c_1, b_1d_1) \sim (a_2c_2, b_2d_2)$. ☐

Now that we have successfully defined addition and multiplication, we are ready to prove that the resulting object is a field.

Theorem 10.6.4. *If R is an integral domain, then $Frac(R)$ is a field with the following properties.*

- *The additive identity of $Frac(R)$ is $\overline{(0,1)}$.*
- *The multiplicative identity of $Frac(R)$ is $\overline{(1,1)}$.*
- *The additive inverse of $\overline{(a,b)} \in Frac(R)$ is $\overline{(-a,b)}$.*
- *If $\overline{(a,b)} \in Frac(R)$ with $\overline{(a,b)} \neq \overline{(0,1)}$, then $a \neq 0$ and the multiplicative inverse of $\overline{(a,b)}$ is $\overline{(b,a)}$.*

Proof. We check each of the field axioms.

1. Associativity of $+$: Let $q, r, s \in Frac(R)$. Fix $a, b, c, d, e, f \in R$ with $b, d, f \neq 0$ such that $q = \overline{(a, b)}$, $r = \overline{(c, d)}$, and $s = \overline{(e, f)}$. We then have

$$\begin{aligned} q + (r + s) &= \overline{(a, b)} + (\overline{(c, d)} + \overline{(e, f)}) \\ &= \overline{(a, b)} + \overline{(cf + de, df)} \\ &= \overline{(a(df) + b(cf + de), b(df))} \\ &= \overline{(adf + bcf + bde, bdf)} \\ &= \overline{((ad + bc)f + (bd)e, (bd)f)} \\ &= \overline{(ad + bc, bd)} + \overline{(e, f)} \\ &= [\overline{(a, b)} + \overline{(c, d)}] + \overline{(e, f)} \\ &= (q + r) + s \end{aligned}$$

2. Commutativity of $+$: Let $q, r \in Frac(R)$. Fix $a, b, c, d \in R$ with $b, d \neq 0$ such that $q = \overline{(a, b)}$, and $r = \overline{(c, d)}$. We then have

$$\begin{aligned} q + r &= \overline{(a, b)} + \overline{(c, d)} \\ &= \overline{(ad + bc, bd)} \\ &= \overline{(cb + da, db)} \\ &= \overline{(c, d)} + \overline{(a, b)} \\ &= r + q \end{aligned}$$

3. $\overline{(0, 1)}$ is an additive identity: Let $q \in Frac(R)$. Fix $a, b \in R$ with $b \neq 0$ such that $q = \overline{(a, b)}$. We then have

$$\begin{aligned} q + \overline{(0, 1)} &= \overline{(a, b)} + \overline{(0, 1)} \\ &= \overline{(a \cdot 1 + b \cdot 0, b \cdot 1)} \\ &= \overline{(a, b)} \\ &= q \end{aligned}$$

   Since we already proved commutativity of $+$, we conclude that $\overline{(0, 1)} + q = q$ also.

4. Additive inverses: Let $q \in Frac(R)$. Fix $a, b \in R$ with $b \neq 0$ such that $q = \overline{(a, b)}$. Let $r = \overline{(-a, b)}$. We then have

$$\begin{aligned} q + r &= \overline{(a, b)} + \overline{(-a, b)} \\ &= \overline{(ab + b(-a), bb)} \\ &= \overline{(ab - ab, bb)} \\ &= \overline{(0, bb)} \\ &= \overline{(0, 1)} \end{aligned}$$

   where the last line follows from the fact that $0 \cdot 1 = 0 = 0 \cdot bb$. Since we already proved commutativity of $+$, we conclude that $r + q = \overline{(0, 1)}$ also.

5. Associativity of $\cdot$: Let $q, r, s \in Frac(R)$. Fix $a, b, c, d, e, f \in R$ with $b, d, f \neq 0$ such that $q = \overline{(a, b)}$, $r = \overline{(c, d)}$, and $s = \overline{(e, f)}$. We then have

$$\begin{aligned} q \cdot (r \cdot s) &= \overline{(a, b)} \cdot (\overline{(c, d)} \cdot \overline{(e, f)}) \\ &= \overline{(a, b)} \cdot \overline{(ce, df)} \\ &= \overline{(a(ce), b(df))} \\ &= \overline{((ac)e, (bd)f)} \\ &= \overline{(ac, bd)} \cdot \overline{(e, f)} \\ &= (\overline{(a, b)} \cdot \overline{(c, d)}) \cdot \overline{(e, f)} \\ &= (q \cdot r) \cdot s \end{aligned}$$

6. Commutativity of $\cdot$: Let $q, r \in Frac(R)$. Fix $a, b, c, d \in R$ with $b, d \neq 0$ such that $q = \overline{(a, b)}$, and $r = \overline{(c, d)}$. We then have

$$\begin{aligned} q \cdot r &= \overline{(a, b)} \cdot \overline{(c, d)} \\ &= \overline{(ac, bd)} \\ &= \overline{(ca, db)} \\ &= \overline{(c, d)} \cdot \overline{(a, b)} \\ &= r \cdot q \end{aligned}$$

7. $\overline{(1, 1)}$ is a multiplicative identity: Let $q \in Frac(R)$. Fix $a, b \in R$ with $b \neq 0$ such that $q = \overline{(a, b)}$. We then have

$$\begin{aligned} q \cdot \overline{(1, 1)} &= \overline{(a, b)} \cdot \overline{(1, 1)} \\ &= \overline{(a \cdot 1, b \cdot 1)} \\ &= \overline{(a, b)} \\ &= q \end{aligned}$$

Since we already proved commutativity of $\cdot$, we conclude that $\overline{(1, 1)} \cdot q = q$ also.

8. Multiplicative inverses: Let $q \in Frac(R)$ with $q \neq \overline{(0, 1)}$. Fix $a, b \in R$ with $b \neq 0$ such that $q = \overline{(a, b)}$. Since $\overline{(a, b)} \neq \overline{(0, 1)}$, we know that $(a, b) \not\sim (0, 1)$, so $a \cdot 1 \neq b \cdot 0$ which means that $a \neq 0$. Let $r = \overline{(b, a)}$ which makes sense because $a \neq 0$. We then have

$$\begin{aligned} q \cdot r &= \overline{(a, b)} \cdot \overline{(b, a)} \\ &= \overline{(ab, ba)} \\ &= \overline{(ab, ab)} \\ &= \overline{(1, 1)} \end{aligned}$$

where the last line follows from the fact that $ab \cdot 1 = ab = ab \cdot 1$. Since we already proved commutativity of $+$, we conclude that $r \cdot q = \overline{(1, 1)}$ also.

9. Distributivity: Let $q, r, s \in Frac(R)$. Fix $a, b, c, d, e, f \in R$ with $b, d, f \neq 0$ such that $q = \overline{(a, b)}$,

$r = \overline{(c,d)}$, and $s = \overline{(e,f)}$. We then have

$$\begin{aligned}
q \cdot (r+s) &= \overline{(a,b)} \cdot (\overline{(c,d)} + \overline{(e,f)}) \\
&= \overline{(a,b)} \cdot \overline{(cf+de,df)} \\
&= \overline{(a(cf+de),b(df))} \\
&= \overline{(acf+ade,bdf)} \\
&= \overline{(b(acf+ade),b(bdf))} \\
&= \overline{(abcf+abde,bbdf)} \\
&= \overline{((ac)(bf)+(bd)(ae),(bd)(bf))} \\
&= \overline{(ac,bd)} + \overline{(ae,bf)} \\
&= \overline{(a,b)} \cdot \overline{(c,d)} + \overline{(a,b)} \cdot \overline{(e,f)} \\
&= q \cdot r + q \cdot s
\end{aligned}$$

□

Although R is certainly not a subring of $Frac(R)$ (it is not even a subset), our next proposition says that R can be embedded in $Frac(R)$.

Proposition 10.6.5. *Let R be an integral domain. Define $\theta\colon R \to Frac(R)$ by $\theta(a) = \overline{(a,1)}$. We then have that θ is an injective ring homomorphism.*

Proof. Notice first that $\theta(1) = \overline{(1,1)}$, which is the multiplicative identity of $Frac(R)$. Now for any $a, b \in R$, we have

$$\begin{aligned}
\theta(a+b) &= \overline{(a+b,1)} \\
&= \overline{(a\cdot 1 + 1\cdot b, 1\cdot 1)} \\
&= \overline{(a,1)} + \overline{(b,1)} \\
&= \theta(a) + \theta(b)
\end{aligned}$$

and

$$\begin{aligned}
\theta(ab) &= \overline{(ab,1)} \\
&= \overline{(a\cdot b, 1\cdot 1)} \\
&= \overline{(a,1)} \cdot \overline{(b,1)} \\
&= \theta(a)\cdot\theta(b)
\end{aligned}$$

Thus, $\theta\colon R \to Frac(R)$ is a homomorphism. Suppose now that $a, b \in R$ with $\theta(a) = \theta(b)$. We then have that $\overline{(a,1)} = \overline{(b,1)}$, so $(a,1) \sim (b,1)$. It follows that $a \cdot 1 = 1 \cdot b$, so $a = b$. Therefore, θ is injective. □

We have now completed our primary objective in showing that every integral domain can be embedded in a field. Our final result about $Frac(R)$ is that it is the "smallest" such field. We can't hope to prove that it is a subset of every field containing R because of course we can always rename elements. However, we can show that if R embeds in some field K, then you can also embed $Frac(R)$ in K. In fact, we show that there is a unique way to do it so that you "extend" the embedding of R.

Theorem 10.6.6. *Let R be an integral domain. Let $\theta\colon R \to Frac(R)$ be defined by $\theta(a) = \overline{(a,1)}$ as above. Suppose that K is a field and that $\psi\colon R \to K$ is an injective ring homomorphism. There exists a unique injective ring homomorphism $\varphi\colon Frac(R) \to K$ such that $\varphi \circ \theta = \psi$.*

Proof. First notice that if $b \in R$ with $b \neq 0$, then $\psi(b) \neq 0$ (because $\psi(0) = 0$ and ψ is assumed to be injective). Thus, if $b \in R$ with $b \neq 0$, then $\psi(b)$ has a multiplicative inverse in K. Define $\varphi \colon Frac(R) \to K$ by letting

$$\varphi(\overline{(a,b)}) = \psi(a) \cdot \psi(b)^{-1}$$

We check the following.

- φ is well-defined: Suppose that $\overline{(a,b)} = \overline{(c,d)}$. We then have $(a,b) \sim (c,d)$, so $ad = bc$. From this we conclude that $\psi(ad) = \psi(bc)$, and since ψ is a ring homomorphism it follows that $\psi(a) \cdot \psi(d) = \psi(c) \cdot \psi(b)$. We have $b, d \neq 0$, so $\psi(b) \neq 0$ and $\psi(d) \neq 0$ by our initial comment. Multiplying both sides by $\psi(b)^{-1} \cdot \psi(d)^{-1}$, we conclude that $\psi(a) \cdot \psi(b)^{-1} = \psi(a) \cdot \psi(d)^{-1}$. Therefore, $\varphi(\overline{(a,b)}) = \varphi(\overline{(c,d)})$.

- $\varphi(1_{Frac(R)}) = 1_K$: We have

$$\varphi(\overline{(1,1)}) = \psi(1) \cdot \psi(1)^{-1} = 1 \cdot 1^{-1} = 1$$

- φ preserves addition: Let $a, b, c, d \in R$ with $b, d \neq 0$. We have

$$\begin{aligned} \varphi(\overline{(a,b)} + \overline{(c,d)}) &= \varphi(\overline{(ad+bc, bd)}) \\ &= \psi(ad+bc) \cdot \psi(bd)^{-1} \\ &= (\psi(ad) + \psi(bc)) \cdot (\psi(b) \cdot \psi(d))^{-1} \\ &= (\psi(a) \cdot \psi(d) + \psi(b) \cdot \psi(c)) \cdot \psi(b)^{-1} \cdot \psi(d)^{-1} \\ &= \psi(a) \cdot \psi(b)^{-1} + \psi(c) \cdot \psi(d)^{-1} \\ &= \varphi(\overline{(a,b)}) + \varphi(\overline{(c,d)}) \end{aligned}$$

- φ preserves multiplication: Let $a, b, c, d \in R$ with $b, d \neq 0$. We have

$$\begin{aligned} \varphi(\overline{(a,b)} \cdot \overline{(c,d)}) &= \varphi(\overline{(ac, bd)}) \\ &= \psi(ac) \cdot \psi(bd)^{-1} \\ &= \psi(a) \cdot \psi(c) \cdot (\psi(b) \cdot \psi(d))^{-1} \\ &= \psi(a) \cdot \psi(c) \cdot \psi(b)^{-1} \cdot \psi(d)^{-1} \\ &= \psi(a) \cdot \psi(b)^{-1} \cdot \psi(c) \cdot \psi(d)^{-1} \\ &= \varphi(\overline{(a,b)}) \cdot \varphi(\overline{(c,d)}) \end{aligned}$$

- φ is injective: Let $a, b, c, d \in R$ with $b, d \neq 0$ and suppose that $\varphi(\overline{(a,b)}) = \varphi(\overline{(c,d)})$. We then have that $\psi(a) \cdot \psi(b)^{-1} = \psi(c) \cdot \psi(d)^{-1}$. Multiplying both sides by $\psi(b) \cdot \psi(d)$, we conclude that $\psi(a) \cdot \psi(d) = \psi(b) \cdot \psi(c)$. Since ψ is a ring homomorphism, it follows that $\psi(ad) = \psi(bc)$. Now ψ is injective, so we conclude that $ad = bc$. Thus, we have $(a,b) \sim (c,d)$ and so $\overline{(a,b)} = \overline{(c,d)}$.

- $\varphi \circ \theta = \psi$: For any $a \in R$, we have

$$\begin{aligned} (\varphi \circ \theta)(a) &= \varphi(\theta(a)) \\ &= \varphi(\overline{(a,1)}) \\ &= \psi(a) \cdot \psi(1)^{-1} \\ &= \psi(a) \cdot 1^{-1} \\ &= \psi(a) \end{aligned}$$

  It follows that $(\varphi \circ \theta)(a) = \psi(a)$ for all $a \in R$.

We finally prove uniqueness. Suppose that $\phi\colon Frac(R) \to K$ is a ring homomorphism with $\phi \circ \theta = \psi$. For any $a \in R$, we have

$$\phi(\overline{(a,1)}) = \phi(\theta(a)) = \psi(a)$$

Now for any $b \in R$ with $b \neq 0$, we have

$$\begin{aligned}
\psi(b) \cdot \phi(\overline{(1,b)}) &= \phi(\overline{(b,1)}) \cdot \phi(\overline{(1,b)}) \\
&= \phi(\overline{(b,1)} \cdot \overline{(1,b)}) \\
&= \phi(\overline{(b \cdot 1, 1 \cdot b})) \\
&= \phi(\overline{(b,b)}) \\
&= \phi(\overline{(1,1)}) \\
&= 1
\end{aligned}$$

where we used the fact that $(b,b) \sim (1,1)$ and that ϕ is a ring homomorphism so sends the multiplicative identity to $1 \in K$. Thus, for every $b \in R$ with $b \neq 0$, we have

$$\phi(\overline{(1,b)}) = \psi(b)^{-1}$$

Now for any $a, b \in R$ with $b \neq 0$, we have

$$\begin{aligned}
\phi(\overline{(a,b)}) &= \phi(\overline{(a,1)} \cdot \overline{(1,b)}) \\
&= \phi(\overline{(a,1)}) \cdot \phi(\overline{(1,b)}) \\
&= \psi(a) \cdot \psi(b)^{-1} && \text{(from above)} \\
&= \varphi(\overline{(a,b)})
\end{aligned}$$

Therefore, $\phi = \varphi$. □

Corollary 10.6.7. *Suppose that R is an integral domain which is a subring of a field K. If every element of K can be written as ab^{-1} for some $a, b \in R$ with $b \neq 0$, then $K \cong Frac(R)$.*

Proof. Let $\psi\colon R \to K$ be the trivial map $\psi(r) = r$ and notice that ψ is an injective ring homomorphism. By the proof of the previous result, the function $\varphi\colon Frac(R) \to K$ defined by

$$\varphi(\overline{(a,b)}) = \psi(a) \cdot \psi(b)^{-1} = ab^{-1}$$

is an injective ring homomorphism. By assumption, φ is surjective, so φ is an isomorphism. Therefore, $K \cong Frac(R)$. □

Chapter 11

Divisibility and Factorizations in Integral Domains

Our primary example of an integral domain that is not a field is $\mathbb{Z}$. We spent a lot of time developing the arithmetic of $\mathbb{Z}$ in Chapter 2, and there we worked through the notions of divisibility, greatest common divisors, and prime factorizations. In this chapter, we explore how much of this arithmetic of $\mathbb{Z}$ we can carry over to other types of integral domains.

11.1 Divisibility and Associates

We begin with the development of divisibility in integral domains. It is possible, but more involved, to discuss these concepts in more general rings. However, in a noncommutative ring, we would need to refer constantly to which side we are working on and this brings attention away from our primary concerns. Even in a commutative ring, divisibility can have some undesirable properties (see below). Although the general commutative case is worthy of investigation, the fundamental examples for us will be integral domains anyway, so we want to focus on the interesting questions in this setting.

Definition 11.1.1. *Let R be an integral domain and let $a, b \in R$. We say that a* divides *b, and write $a \mid b$, if there exists $d \in R$ with $b = ad$.*

Of course, this is just our definition of divisibility in $\mathbb{Z}$ generalized to an arbitrary integral domain R. For example, in the ring $\mathbb{Z}[x]$, we have

$$x^2 + 3x - 1 \mid x^4 - x^3 - 11x^2 + 10x - 2$$

because

$$(x^2 + 3x - 1)(x^2 - 4x + 2) = x^4 - x^3 - 11x^2 + 10x - 2.$$

If R is a field, then for any $a, b \in R$ with $a \neq 0$, we have $a \mid b$ because $b = a(a^{-1}b)$. Thus, the divisibility relation is trivial in fields. Also notice that we have that $a \in R$ is a unit if and only if $a \mid 1$.

Proposition 11.1.2. *Let R be an integral domain and let $a, b, c \in R$.*

1. *If $a \mid b$ and $b \mid c$, then $a \mid c$.*
2. *If $a \mid b$ and $a \mid c$, then $a \mid (rb + sc)$ for all $r, s \in R$.*

Proof.

1. Fix $k, m \in R$ with $b = ak$ and $c = bm$. We then have $c = bm = (ak)m = a(km)$, so $a \mid c$.

2. Fix $k, m \in R$ with $b = ak$ and $c = am$. Let $r, s \in R$. We then have

$$\begin{aligned} rb + sc &= r(ak) + s(am) \\ &= a(rk) + a(sm) && \text{(since } R \text{ is commutative)} \\ &= a(rk + sm), \end{aligned}$$

   so $a \mid (rb + sc)$.

$\square$

For an example of where working in an integral domain makes divisibility have more desirable properties, consider the following proposition, which would be false in general commutative rings. Working in $R = \mathbb{Z} \times \mathbb{Z}$ (which is not integral domain), notice that $(2,0) \mid (6,0)$ via both $(2,0) \cdot (3,0) = (6,0)$ and also $(2,0) \cdot (3,5) = (6,0)$.

Proposition 11.1.3. *Let R be an integral domain. Suppose that $a, b \in R$ with $a \neq 0$ and that $a \mid b$. There exists a unique $d \in R$ such that $ad = b$.*

Proof. The existence of a d follows immediately from the definition of divisibility. Suppose that $c, d \in R$ satisfy $ac = b$ and $ad = b$. We then have that $ac = ad$. Since $a \neq 0$ and R is an integral domain, we may use Proposition 9.2.11 to cancel the a's to conclude that $c = d$. $\square$

Recall that if R is a ring, then we denote the set of units of R by $U(R)$, and that $U(R)$ forms a multiplicative group by Proposition 9.2.4.

Definition 11.1.4. *Let R be an integral domain. Define a relation $\sim$ on R by letting $a \sim b$ if there exists a $u \in U(R)$ such that $b = au$.*

Proposition 11.1.5. *Let R be an integral domain. The relation $\sim$ is an equivalence relation.*

Proof. We check the properties.

- Reflexive: Given $a \in R$, we have $a = a \cdot 1$, so since $1 \in U(R)$ it follows that $a \sim a$.
- Symmetric: Suppose that $a, b \in R$ with $a \sim b$. Fix $u \in U(R)$ with $b = au$. Multiplying on the right by u^{-1}, we see that $a = bu^{-1}$. Since $u^{-1} \in U(R)$ (by Proposition 9.2.4), it follows that $b \sim a$.
- Transitive: Suppose that $a, b, c \in R$ with $a \sim b$ and $b \sim c$. Fix $u, v \in U(R)$ with $b = au$ and $c = bv$. We then have $c = bv = (au)v = a(uv)$. Since $uv \in U(R)$ by (Proposition 9.2.4), it follows that $a \sim c$.

Therefore, $\sim$ is an equivalence relation. $\square$

Definition 11.1.6. *Let R be an integral domain. Elements of the same equivalence class are called* associates*. In other words, given $a, b \in R$, then a and b are associates if there exists $u \in U(R)$ with $b = au$.*

For example, we have $U(\mathbb{Z}) = \{\pm 1\}$, so the associates of a given $n \in \mathbb{Z}$ are exactly $\pm n$. Thus, the equivalence classes partition $\mathbb{Z}$ into the sets $\{0\}$, $\{\pm 1\}$, $\{\pm 2\}$, $\dots$.

Proposition 11.1.7. *Let R be an integral domain and let $a, b \in R$. The following are equivalent.*

1. *a and b are associates in R.*
2. *Both $a \mid b$ and $b \mid a$.*

Proof. Suppose first that a and b are associates. Fix $u \in U(R)$ with $b = au$. We then clearly have $a \mid b$, and since $a = bu^{-1}$ we have $b \mid a$.

Suppose conversely that both $a \mid b$ and $b \mid a$. Fix $c, d \in R$ with $b = ac$ and $a = bd$. Notice that if $a = 0$, then $b = ac = 0c = 0$, so $a = b1$ and a and b are associates. Suppose instead that $a \neq 0$. We then have

$$a1 = a = bd = (ac)d = acd$$

Since R is an integral domain and $a \neq 0$, it follows that $cd = 1$ (using Proposition 9.2.11), so both $c, d \in U(R)$. Therefore, as $b = ac$, it follows that a and b are associates. □

It will be very useful for us to rephrase the definition of divisibility and associates in terms of principal ideals. Notice that the elements a and b switch sides in the next proposition.

Proposition 11.1.8. *Let R be an integral domain and let $a, b \in R$. We have $a \mid b$ if and only if $\langle b \rangle \subseteq \langle a \rangle$.*

Proof. Suppose first that $a \mid b$. Fix $d \in R$ with $b = ad$. We then have $b \in \langle a \rangle$, hence $\langle b \rangle \subseteq \langle a \rangle$ because $\langle b \rangle$ is the smallest ideal containing b.

Suppose conversely that $\langle b \rangle \subseteq \langle a \rangle$. Since $b \in \langle b \rangle$, we then have in particular that $b \in \langle a \rangle$. Thus, we may fix $d \in R$ with $b = ad$. It follows that $a \mid b$. □

Corollary 11.1.9. *Let R be an integral domain and let $a, b \in R$. We have $\langle a \rangle = \langle b \rangle$ if and only if a and b are associates.*

Proof. We have

$$\begin{aligned}
\langle a \rangle = \langle b \rangle &\iff \langle a \rangle \subseteq \langle b \rangle \text{ and } \langle b \rangle \subseteq \langle a \rangle \\
&\iff b \mid a \text{ and } a \mid b && \text{(by Proposition 11.1.8)} \\
&\iff a \text{ and } b \text{ are associates.} && \text{(by Proposition 11.1.7)}
\end{aligned}$$

□

Finally, we begin a discussion of greatest common divisors in integral domains. Recall that in our discussion about $\mathbb{Z}$, we avoided defining the greatest common divisor as the *largest* common divisor of a and b, and instead said that it had the property that every other common divisor of a and b was also a divisor of it. Taking this approach was useful in $\mathbb{Z}$ (after all, $\gcd(a, b)$ had this much stronger property anyway, and otherwise $\gcd(0, 0)$ would not make sense), but it is absolutely essential when we try to generalize it to other integral domains since a general integral domain has no notion of "order" or "largest".

Definition 11.1.10. *Let R be an integral domain and let $a, b \in R$.*

1. *A common divisor of a and b is an element $c \in R$ such that $c \mid a$ and $c \mid b$.*
2. *An element $d \in R$ is called a* greatest common divisor *of a and b if*
   - *d is a common divisor of a and b.*
   - *For every common divisor c of a and b, we have $c \mid d$.*

When we worked in $\mathbb{Z}$, we added the additional requirement that $\gcd(a, b)$ was nonnegative so that it would be unique. However, just like with "order", there is no notion of "positive" in a general integral domain. Thus, we will have to live with a lack of uniqueness in general. Fortunately, any two greatest common divisors are associates, as we now prove.

Proposition 11.1.11. *Suppose that R is an integral domain and $a, b \in R$.*

- *If d is a greatest common divisor of a and b, then every associate of d is also a greatest common divisor of a and b.*
- *If d and d' are both greatest common divisors of a and b, then d and d' are associates.*

Proof. Suppose that d is a greatest common divisor of a and b. Suppose that d' is an associate of d. We then have that $d' \mid d$, so since d is a common divisor of a and b and divisibility is transitive, it follows that d' is a common divisor of a and b. Let c be a common divisor of a and b. Since d is a greatest common divisor of a and b, we know that $c \mid d$. Now $d \mid d'$ because d and d' are associates, so by transitivity of divisibility, we conclude that $c \mid d'$. Therefore, every common divisor of a and b divides d', and hence d' is a greatest common divisor of a and b.

Suppose that d and d' are both greatest common divisors of a and b. We then have that d' is a common divisor of a and b, so $d' \mid d$ because d is a greatest common divisor of a and b. Similarly, we have that d is a common divisor of a and b, so $d \mid d'$ because d' is a greatest common divisor of a and b. Using Proposition Proposition 11.1.7, we conclude that either d and d' are associates. □

So far, we have danced around the fundamental question: Given an integral domain R and elements $a, b \in R$, must there exist a greatest common divisor of a and b? The answer is **no** in general, so proving existence in "nice" integral domains will be a top priority for us.

11.2 Irreducible Elements

Our next goal is to generalize the notion of a prime number in $\mathbb{Z}$ to an arbitrary integral domain. In our original definition of a prime, the idea was that we could not factor the element in any nontrivial way. Since units divide everything, we adopt the following definition.

Definition 11.2.1. *Let R be an integral domain and let $p \in R$ be nonzero and not a unit. We say that p is* irreducible *if whenever $p = ab$, then either a is a unit or b is a unit.*

Notice that we are using the more descriptive word *irreducible* instead of the word prime (we will define a different but related notion of *prime* elements in Section 11.4). By definition, an element is irreducible exactly when every possible factorization contains a "trivial" element. The next proposition says that an element is irreducible exactly when it has only "trivial" divisors.

Proposition 11.2.2. *Let R be an integral domain. A nonzero nonunit $p \in R$ is irreducible if and only if the only divisors of p are the units and the associates of p.*

Proof. Let $p \in R$ be nonzero and not a unit.

Suppose that p is irreducible. Let $a \in R$ with $a \mid p$. Fix $d \in R$ with $p = ad$. Since p is irreducible, we conclude that either a is a unit or d is a unit. If a is a unit, we are done. If d is a unit, then have that p and a are associates. Therefore, every divisor of p is either a unit or an associate of p.

Suppose conversely that the only divisors of p are the units and associates of p. Suppose that $p = ab$ and that a is not a unit. Notice that $a \neq 0$ because $p \neq 0$. We have that $a \mid p$, so since a is not a unit, we must have that a is an associate of p. Fix a unit u with $p = au$. We then have $ab = p = au$, so since R is in integral domain and $a \neq 0$, it follows that $b = u$. Therefore b is a unit. □

Let's examine this concept in the context of the integral domain $\mathbb{Z}$. In Chapter 2, we only worked with *positive* elements $p \in \mathbb{Z}$ when talking about primes and their divisors. However, it's straightforward to check that if $a, b \in \mathbb{Z}$, and $a \mid b$, then $(-a) \mid b$. Thus, our old definition of $p \in \mathbb{Z}$ being prime is the same as saying that $p \geq 2$ and the the only divisors of p are ± 1 and $\pm p$, i.e. the units and associates. If we no longer insist that $p \geq 2$, then this is precisely the same as saying that p is irreducible in $\mathbb{Z}$. Notice now that after dropping that requirement, we have that $-2, -3, -5, \dots$ are irreducibles in $\mathbb{Z}$. This is generalized in the following result.

Proposition 11.2.3. *Let R be an integral domain. If $p \in R$ is irreducible, then every associate of p is irreducible.*

Proof. Exercise (see homework). □

Let's examine some elements of the integral domain $\mathbb{Z}[x]$. We know that $U(\mathbb{Z}[x]) = U(\mathbb{Z}) = \{1, -1\}$ by Proposition 9.3.8. Notice that $2x^2 + 6$ is not irreducible in $\mathbb{Z}[x]$ because $2x^2 + 6 = 2 \cdot (x^2 + 3)$, and neither 2 nor $x^2 + 3$ is a unit. Also, $x^2 - 4x + 21 = (x + 3)(x - 7)$, and neither $x + 3$ nor $x - 7$ is a unit in $\mathbb{Z}[x]$, so $x^2 - 4x + 21$ is not irreducible in $\mathbb{Z}[x]$.

In contrast, we claim that $x + 3$ is irreducible in $\mathbb{Z}[x]$. To see this, suppose that $f(x), g(x) \in \mathbb{Z}[x]$ are such that $x + 3 = f(x)g(x)$. Notice that we must have that $f(x)$ and $g(x)$ are both nonzero. By Proposition 9.3.6, we know that

$$\deg(x + 3) = \deg(f(x)) + \deg(g(x)),$$

so

$$1 = \deg(f(x)) + \deg(g(x)).$$

It follows that one of $\deg(f(x))$ and $\deg(g(x))$ equals 0, while the other is 1. Suppose without loss of generality that $\deg(f(x)) = 0$, so $f(x)$ is a nonzero constant, say $f(x) = c$. Since $\deg(g(x)) = 1$, we can fix $a, b \in \mathbb{Z}$ with $g(x) = ax + b$. We then have

$$x + 3 = c \cdot (ax + b) = ac \cdot x + b$$

It follows that $ac = 1$ in $\mathbb{Z}$, so $c \in \{1, -1\}$, and hence $f(x) = c$ is a unit in $\mathbb{Z}[x]$. Therefore, $x+3$ is irreducible in $\mathbb{Z}[x]$.

Recall from Corollary 9.3.9 that if F is a field, then $U(F[x]) = U(F)$ is the set of nonzero constant polynomials. Using this classification of the units, we can give a simple characterization of the irreducible elements in $F[x]$ as those polynomials that can not be factored into two polynomials of smaller degree.

Proposition 11.2.4. *Let F be a field and let $f(x) \in F[x]$ be a nonconstant polynomial. The following are equivalent:*

1. *$f(x)$ is irreducible in $F[x]$.*
2. *There do not exist nonzero polynomials $g(x), h(x) \in F[x]$ with $f(x) = g(x) \cdot h(x)$ and both $\deg(g(x)) < \deg(f(x))$ and $\deg(h(x)) < \deg(f(x))$.*

Proof. We prove (1) $\Leftrightarrow$ (2) by instead proving $Not(1) \Leftrightarrow Not(2)$.

- $Not(1) \Rightarrow Not(2)$: Suppose that (1) is false, so $f(x)$ is not irreducible in $F[x]$. Since $f(x)$ is a nonconstant polynomial, we know that $f(x)$ is nonzero and not a unit in $F[x]$. Therefore, there exists $g(x), h(x) \in F[x]$ with $f(x) = g(x)h(x)$ and such that neither $g(x)$ nor $h(x)$ are units. Notice that $g(x)$ and $h(x)$ are both nonzero (because $f(x)$ is nonzero), so since $U(F[x]) = U(F) = F\backslash\{0\}$ by Corollary 9.3.9, it follows that $g(x)$ and $h(x)$ are both nonconstant polynomials. Now

$$\deg(f(x)) = \deg(g(x) \cdot h(x)) = \deg(g(x)) + \deg(h(x))$$

by Proposition 9.3.6. Since $h(x)$ is nonconstant, we have $\deg(h(x)) \geq 1$, and hence $\deg(g(x)) < \deg(f(x))$. Similarly, since $g(x)$ is nonconstant, we have $\deg(g(x)) \geq 1$, and hence $\deg(h(x)) < \deg(f(x))$. Thus, we've shown that (2) is false.

- $Not(2) \Rightarrow Not(1)$: Suppose that (2) is false, and fix nonzero polynomials $g(x), h(x) \in F[x]$ with $f(x) = g(x) \cdot h(x)$ and both $\deg(g(x)) < \deg(f(x))$ and $\deg(h(x)) < \deg(f(x))$. Since

$$\deg(f(x)) = \deg(g(x) \cdot h(x)) = \deg(g(x)) + \deg(h(x))$$

by Proposition 9.3.6, we must have $\deg(g(x)) \neq 0$ and $\deg(h(x)) \neq 0$. Since $U(F[x]) = U(F) = F \backslash \{0\}$ by Corollary 9.3.9, it follows that neither $g(x)$ nor $h(x)$ is a unit. Thus, $f(x)$ is not irreducible in $F[x]$, and so (1) is false.

□

Life is not as nice if we are working over an integral domain that is not a field. For example, we showed above that $2x^2+6$ is not irreducible in $\mathbb{Z}[x]$ because $2x^2+6 = 2\cdot(x^2+3)$, and neither 2 nor x^2+3 is a unit in $\mathbb{Z}[x]$. However, it is not possible to write $2x^2+6 = g(x)\cdot h(x)$ where $g(x), h(x) \in \mathbb{Z}[x]$ and both $\deg(g(x)) < 2$ and $\deg(h(x)) < 2$.

Proposition 11.2.5. *Let F be a field and let $f(x) \in F[x]$ be a nonzero polynomial with $\deg(f(x)) \geq 2$. If $f(x)$ has a root in F, then $f(x)$ is not irreducible in $F[x]$.*

Proof. Suppose that $f(x)$ has a root in F, and fix such a root $a \in F$. By Proposition 10.3.2, it follows that $(x-a) \mid f(x)$ in $F[x]$. Fixing $g(x) \in F[x]$ with $f(x) = (x-a)\cdot g(x)$, we then have that $g(x)$ is nonzero (since $f(x)$ is nonzero) and also

$$\deg(f(x)) = \deg(x-a) + \deg(g(x)) = 1 + \deg(g(x)).$$

Therefore, $\deg(g(x)) = \deg(f(x)) - 1 \geq 2 - 1 = 1$. Since $x-a$ and $g(x)$ both have degree at least 1, we conclude that neither is a unit in $F[x]$ by Corollary 9.3.9, and hence $f(x)$ is not irreducible in $F[x]$. □

Theorem 11.2.6. *Let F be a field and let $f(x) \in F[x]$ be a nonzero polynomial.*

1. *If $\deg(f(x)) = 1$, then $f(x)$ is irreducible in $F[x]$.*
2. *If $\deg(f(x)) = 2$ or $\deg(f(x)) = 3$, then $f(x)$ is irreducible in $F[x]$ if and only if $f(x)$ has no roots in F.*

Proof.

1. This follows immediately from Proposition 11.2.4 and Proposition 9.3.6.
2. Suppose that either $\deg(f(x)) = 2$ or $\deg(f(x)) = 3$. If $f(x)$ has a root in $F[x]$, then $f(x)$ is not irreducible immediately by Proposition 11.2.5. Suppose conversely that $f(x)$ is not irreducible if $F[x]$. Write $f(x) = g(x)h(x)$ where $g(x), h(x) \in F[x]$ are nonunits. We have

$$\deg(f(x)) = \deg(g(x)) + \deg(h(x))$$

Now $g(x)$ and $h(x)$ are not units, so they each have degree at least 1. Since $\deg(f(x)) \in \{2, 3\}$, it follows that at least one of $g(x)$ or $h(x)$ has degree equal to 1. Suppose without loss of generality that $\deg(g(x)) = 1$ and write $g(x) = ax+b$ where $a, b \in F$ with $a \neq 0$. We then have

$$\begin{aligned} f(-ba^{-1}) &= g(-ba^{-1}) \cdot h(-ba^{-1}) \\ &= (a\cdot(-ba^{-1}) + b)\cdot h(-ba^{-1}) \\ &= (-b+b)\cdot h(-ba^{-1}) \\ &= 0 \cdot h(-ba^{-1}) \\ &= 0 \end{aligned}$$

so $-ba^{-1} \in F$ is a root of $f(x)$.

□

Notice that this theorem can be false if we are working in $R[x]$ for an integral domain R. For example, in $\mathbb{Z}[x]$, we have that $\deg(3x+12) = 1$, but $3x+12$ is not irreducible in $\mathbb{Z}[x]$ because $3x+12 = 3 \cdot (x+4)$, and neither 3 nor $x+4$ is a unit in $\mathbb{Z}[x]$. Of course, the theorem implies that $3x+12$ is irreducible in $\mathbb{Q}[x]$ (the factorization $3x+12 = 3\cdot(x+4)$ does not work here because 3 is a unit in $\mathbb{Q}[x]$).

Also, note that even in the case of $F[x]$ for a field F, in order to use the nonexistence of roots to prove that a polynomial is irreducible, we require that the polynomial has degree 2 or 3. This restriction is essential. Consider the polynomial x^4+6x^2+5 in $\mathbb{Q}[x]$. Since $x^4+6x^2+5 = (x^2+1)(x^2+5)$, it follows that x^4+6x^2+5 is not irreducible in $\mathbb{Q}[x]$. However, notice that x^4+6x^2+5 has no roots in $\mathbb{Q}$ (or even in $\mathbb{R}$) because $a^4+6a^2+5 > 0$ for all $a \in \mathbb{Q}$.

For an example of how to use the theorem affirmatively, consider the polynomial $f(x) = x^3 - 2$ in the ring $\mathbb{Q}[x]$. We know that $f(x)$ has no roots in $\mathbb{Q}$ because $\pm\sqrt[3]{2}$ are not rational by Theorem 2.5.13. Thus, $f(x)$ is irreducible in $\mathbb{Q}[x]$. Notice that $f(x)$ is not irreducible when viewed as an element of $\mathbb{R}[x]$ because it does have a root in $\mathbb{R}$. In fact, no polynomial in $\mathbb{R}[x]$ of odd degree is irreducible because every such polynomial has a root (this uses the Intermediate Value Theorem because as $x \to \pm\infty$, on one side we must have $f(x) \to \infty$ and on the other we must have $f(x) \to -\infty$). Moreover, it turns out that every irreducible polynomial in $\mathbb{R}[x]$ has degree either 1 or 2, though this is far from obvious at this point, and relies on an important result called the Fundamental Theorem of Algebra.

11.3 Irreducible Polynomials in $\mathbb{Q}[x]$

We spend this section developing a basic understanding of the irreducible elements in $\mathbb{Q}[x]$. Notice that every element of $\mathbb{Q}[x]$ is an associate with a polynomial in $\mathbb{Z}[x]$ because we can simply multiply through by the product of all denominators (which is a unit because it is a constant polynomial). Thus, up to associates, it suffices to examine polynomials with integer coefficients. We begin with a simple but important result about potential rational roots of such a polynomial.

Theorem 11.3.1 (Rational Root Theorem)**.** *Suppose that $f(x) \in \mathbb{Z}[x]$ is a nonzero polynomial and write*

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0,$$

where each $a_i \in \mathbb{Z}$ and $a_n \neq 0$. Suppose that $q \in \mathbb{Q}$ is a root of $f(x)$. If $q = \frac{b}{c}$ where $b \in \mathbb{Z}$ and $c \in \mathbb{N}^+$ are relatively prime (so we write q in "lowest terms"), then $b \mid a_0$ and $c \mid a_n$.

Proof. We have

$$a_n \cdot (b/c)^n + a_{n-1}\cdot(b/c)^{n-1} + \cdots + a_1\cdot(b/c) + a_0 = 0$$

Multiplying through by c^n we get

$$a_nb^n + a_{n-1}b^{n-1}c + \cdots + a_1bc^{n-1} + a_0c^n = 0.$$

From this, we see that

$$a_nb^n = c\cdot[-(a_{n-1}b^{n-1} + \cdots + a_1bc^{n-2} + a_0c^{n-1})],$$

and hence $c \mid a_nb^n$ in $\mathbb{Z}$. Using the fact that $\gcd(b,c) = 1$, it follows that $c \mid a_n$ (either repeatedly apply Proposition 2.4.12, or use Exercise 1 on Homework 2 to conclude that $\gcd(b^n, c) = 1$ followed by one application of Proposition 2.4.12). On the other hand, we see that

$$a_0c^n = b\cdot[-(a_nb^{n-1} + a_{n-1}b^{n-2}c + \cdots + a_1c^{n-1})],$$

and hence $b \mid a_0c^n$. Using the fact that $\gcd(b,c) = 1$ as above, it follows as above that $b \mid a_0$. □

As an example, we show that the polynomial $f(x) = 2x^3 - x^2 + 7x - 9$ is irreducible in $\mathbb{Q}[x]$. By the Rational Root Theorem, the only possible roots of $f(x)$ in $\mathbb{Q}$ are ± 9, ± 3, ± 1, $\pm\frac{9}{2}$, $\pm\frac{3}{2}$, $\pm\frac{1}{2}$. We check the values:

- $f(9) = 1431$ and $f(-9) = -1611$.
- $f(3) = 57$ and $f(-3) = -93$.
- $f(1) = -1$ and $f(-1) = -19$.
- $f(\frac{9}{2}) = \frac{369}{2}$ and $f(-\frac{9}{2}) = -243$.
- $f(\frac{1}{2}) = -\frac{11}{2}$ and $f(-\frac{1}{2}) = -13$.
- $f(\frac{3}{2}) = 6$ and $f(-\frac{3}{2}) = -\frac{57}{2}$.

Thus, $f(x)$ has no roots in $\mathbb{Q}$. Since $\deg(f(x)) = 3$, we can use Theorem 11.2.6 to conclude that $f(x)$ is irreducible in $\mathbb{Q}[x]$. Notice that $f(x)$ is *not* irreducible in $\mathbb{R}[x]$ because it has a root between in the interval $(1, \frac{3}{2})$ by the Intermediate Value Theorem.

As we mentioned above, we are focusing on polynomials in $\mathbb{Q}[x]$ which have integer coefficients since every polynomial in $\mathbb{Q}[x]$ is an associate of such a polynomial. However, even if $f(x) \in \mathbb{Z}[x]$, when we check for irreducibility in $\mathbb{Q}[x]$, we have to consider the possibility that a potential factorization involves polynomials whose coefficients are fractions. For example, we have

$$x^2 = (2x) \cdot \left(\frac{1}{2}x\right).$$

Of course, in this case there also exists a factorization into smaller degree degree polynomials in $\mathbb{Z}[x]$ because we can write $x^2 = x \cdot x$. Our first task is to prove that this is always the case. We will need the following lemma.

Lemma 11.3.2. *Suppose that $g(x), h(x) \in \mathbb{Z}[x]$ and that $p \in \mathbb{Z}$ is a prime which divides all coefficients of $g(x)h(x)$. We then have that either p divides all coefficients of $g(x)$, or p divides all coefficients of $h(x)$.*

Proof. Let $g(x)$ be the polynomial $(b_n)_{n\in\mathbb{N}}$, let $h(x)$ be the polynomial $(c_n)_{n\in\mathbb{N}}$, and let $g(x)h(x)$ be the polynomial $(a_n)_{n\in\mathbb{N}}$. We are supposing that $p \mid a_n$ for all n. Suppose the $p \nmid b_n$ for some n and also that $p \nmid c_n$ for some n (possibly different). Let k be least such that $p \nmid b_k$, and let ℓ be least such that $p \nmid c_\ell$. Notice that

$$\begin{aligned} a_{k+\ell} &= \sum_{i=0}^{k+\ell} b_i c_{k+\ell-i} \\ &= b_k c_\ell + \left(\sum_{i=0}^{k-1} b_i c_{k+\ell-i}\right) + \left(\sum_{i=k+1}^{k+\ell} b_i c_{k+\ell-i}\right), \end{aligned}$$

hence

$$b_k c_\ell = a_{k+\ell} - \left(\sum_{i=0}^{k-1} b_i c_{k+\ell-i}\right) - \left(\sum_{i=k+1}^{k+\ell} b_i c_{k+\ell-i}\right).$$

Now if $0 \le i \le k-1$, then $p \mid b_i$ by choice of k, hence $p \mid b_i c_{k+\ell-i}$. Also, if $k+1 \le i \le k+\ell$, then $k+\ell-i < \ell$, so $p \mid c_{k+\ell-i}$ by choice of ℓ, hence $p \mid b_i c_{k+\ell-i}$. Since $p \mid a_{k+\ell}$ by assumption, it follows that p divides every summand on the right hand side. Therefore, p divides the right hand side, and thus $p \mid b_k c_\ell$. Since p is prime, it follows that either $p \mid b_k$ or $p \mid c_\ell$, but both of these are impossible by choice of k and ℓ. Therefore, it must be the case that either $p \mid b_n$ for all n, or $p \mid c_n$ for all n. ☐

Proposition 11.3.3 (Gauss' Lemma). *Suppose that $f(x) \in \mathbb{Z}[x]$ and that $g(x), h(x) \in \mathbb{Q}[x]$ with $f(x) = g(x)h(x)$. There exist polynomials $g^*(x), h^*(x) \in \mathbb{Z}[x]$ such that $f(x) = g^*(x)h^*(x)$ and both $\deg(g^*(x)) = \deg(g(x))$ and $\deg(h^*(x)) = \deg(h(x))$. In fact, there exist nonzero $s, t \in \mathbb{Q}$ with the following properties:*

- $f(x) = g^*(x)h^*(x)$.
- $g^*(x) = s \cdot g(x)$.
- $h^*(x) = t \cdot h(x)$.

Proof. If each of the coefficients of $g(x)$ and $h(x)$ happen to be integers, then we are happy. Suppose not. Let $a \in \mathbb{Z}$ be the least common multiple of the denominators of the coefficients of g, and let $b \in \mathbb{Z}$ be the least common multiple of the denominators of the coefficients of h. Let $d = ab$. Multiplying both sides of the equation $f(x) = g(x)h(x)$ through by d to "clear denominators", we see that

$$d \cdot f(x) = (a \cdot g(x)) \cdot (b \cdot h(x)),$$

where each of the three factors $d \cdot f(x)$, $a \cdot g(x)$, and $b \cdot h(x)$ is a polynomial in $\mathbb{Z}[x]$. We have at least one of $a > 1$ or $b > 1$, hence $d = ab > 1$.

Fix a prime divisor p of d. We then have that p divides all coefficients of $d \cdot f(x)$, so by the previous lemma either p divides all coefficients of $a \cdot g(x)$, or p divides all coefficients of $b \cdot h(x)$. In the former case, we have

$$\frac{d}{p} \cdot f(x) = \left(\frac{a}{p} \cdot g(x)\right) \cdot (b \cdot h(x)),$$

where each of the three factors is a polynomial in $\mathbb{Z}[x]$. In the latter case, we have

$$\frac{d}{p} \cdot f(x) = (a \cdot g(x)) \cdot \left(\frac{b}{p} \cdot h(x)\right),$$

where each of the three factors is a polynomial in $\mathbb{Z}[x]$. Now if $\frac{d}{p} = 1$, then we are done by letting $g^*(x)$ be the first factor and letting $h^*(x)$ be the second. Otherwise, we continue the argument by dividing out another prime factor of $\frac{d}{p}$ from all coefficients of one of the two polynomials. Continue until we have handled all primes which occur in a factorization of d. Formally, you can do induction on d. $\square$

An immediate consequence of Gauss' Lemma is the following, which greatly simplifies the check for whether a given polynomial with integer coefficients is irreducible in $\mathbb{Q}[x]$.

Corollary 11.3.4. *Let $f(x) \in \mathbb{Z}[x]$. If there do not exist nonconstant polynomials $g(x), h(x) \in \mathbb{Z}[x]$ with $f(x) = g(x) \cdot h(x)$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$. Furthermore, if $f(x)$ is monic, then it suffices to show that no such monic $g(x)$ and $h(x)$ exist.*

Proof. The first part is immediate from Proposition 11.2.4 and Gauss' Lemma. Now suppose that $f(x) \in \mathbb{Z}[x]$ is monic. Suppose that $g(x), h(x) \in \mathbb{Z}$ with $f(x) = g(x)h(x)$. Notice that the leading term of $f(x)$ is the product of the leading terms of $g(x)$ and $h(x)$, so as $f(x)$ is monic and all coefficients are in $\mathbb{Z}$, either both $g(x)$ and $h(x)$ are monic or both have leading terms -1. In the latter case, we can multiply both through by -1 to get a factorization into monic polynomials in $\mathbb{Z}[x]$ of the same degree. $\square$

As an example, consider the polynomial $f(x) = x^4 + 3x^3 + 7x^2 - 9x + 1 \in \mathbb{Q}[x]$. We claim that $f(x)$ is irreducible in $\mathbb{Q}[x]$. We first check for rational roots. By the Rational Root Theorem, we know that the only possibilities are ± 1 and we check these:

- $f(1) = 1 + 3 + 7 - 9 + 1 = 3$
- $f(-1) = 1 - 3 + 7 + 9 + 1 = 15$

Thus, $f(x)$ has no rational roots.

By the corollary, it suffices to show that $f(x)$ is not the product of two monic nonconstant polynomials in $\mathbb{Z}[x]$. Notice that $f(x)$ has no monic divisor of degree 1 because such a divisor would imply that $f(x)$ has a rational root, which we just ruled out. Thus, we need only consider the possibility that $f(x)$ is the product of two monic polynomials in $\mathbb{Z}[x]$ of degree 2. Consider a factorization:

$$f(x) = (x^2 + ax + b)(x^2 + cx + d)$$

where $a, b, c, d \in \mathbb{Z}$. We then have

$$x^4 + 3x^3 + 7x^2 - 9x + 1 = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd$$

We therefore have the following equations:

1. $a + c = 3$.
2. $b + ac + d = 7$.
3. $ad + bc = -9$.
4. $bd = 1$.

Since $bd = 1$ and $b, d \in \mathbb{Z}$, we have that $b \in \{1, -1\}$. We check the possibilities:

- Suppose that $b = 1$. By equation (4), we conclude that $d = 1$. Thus, by equation (3), we conclude that $a + c = -9$, but this contradicts equation (1).
- Suppose that $b = -1$. By equation (4), we conclude that $d = -1$. Thus, by equation (3), we conclude that $-a - c = -9$, so $a + c = 9$, but this contradicts equation (1).

In all cases, we have reached a contradiction. We conclude that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

The following theorem, when it applies, is a simple way to determine that certain polynomials in $\mathbb{Z}[x]$ are irreducible in $\mathbb{Q}[x]$. Although it has limited general use (a polynomial taken at random typically does not satisfy the hypotheses), it is surprising how often it applies to "natural" polynomials that we want to show to be irreducible.

Theorem 11.3.5 (Eisenstein's Criterion)**.** *Suppose that $f(x) \in \mathbb{Z}[x]$ and write*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where $a_n \in \mathbb{Z}$. Suppose that there exists a prime $p \in \mathbb{N}^+$ with the following properties:

- *$p \nmid a_n$.*
- *$p \mid a_i$ for $0 \leq i \leq n - 1$.*
- *$p^2 \nmid a_0$.*

Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof. Fix such a prime p. We use Corollary 11.3.4. Suppose that $g(x), h(x) \in \mathbb{Z}[x]$ are nonconstant polynomials with $f(x) = g(x)h(x)$. We then have

$$n = \deg(f(x)) = \deg(g(x)) + \deg(h(x)).$$

Since we are assuming that $g(x)$ and $h(x)$ are not constant, they each have degree at least 1, and so by the above equality they both have degree at most $n - 1$.

Let $g(x)$ be the polynomial $(b_n)_{n\in\mathbb{N}}$ and let $h(x)$ be the polynomial $(c_n)_{n\in\mathbb{N}}$. We have $a_0 = b_0c_0$, so since $p \mid a_0$ and p is prime, either $p \mid b_0$ or $p \mid c_0$. Furthermore, since $p^2 \nmid a_0$ by assumption, we can not have both $p \mid b_0$ and $p \mid c_0$. Without loss of generality (by switching the roles of $g(x)$ and $h(x)$ if necessary), suppose that $p \mid b_0$ and $p \nmid c_0$.

We now prove that $p \mid b_k$ for $0 \le k \le n-1$ by (strong) induction. Suppose that we have k with $0 \le k \le n-1$ and we know that $p \mid b_i$ for $0 \le i < k$. Now

$$a_k = b_kc_0 + b_{k-1}c_1 + \cdots + b_1c_{k-1} + b_0c_k,$$

and hence

$$b_kc_0 = a_k - b_{k-1}c_1 - \cdots - b_1c_{k-1} - b_0c_k.$$

By assumption, we have $p \mid a_k$, and by induction we have $p \mid b_i$ for $0 \le i < k$. It follows that p divides every term on the right-hand side, so $p \mid b_kc_0$. Since p is prime and $p \nmid c_0$, it follows that $p \mid b_k$.

Thus, we have shown that $p \mid b_k$ for $0 \le k \le n-1$. Now we have

$$\begin{aligned} a_n &= b_nc_0 + b_{n-1}c_1 + \cdots + b_1c_{n-1} + b_0c_n \\ &= b_{n-1}c_1 + \cdots + b_1c_{n-1} + b_0c_n, \end{aligned}$$

where the last line follows from the fact that $b_n = 0$ (since we are assuming $\deg(g(x)) < n$). Now we know $p \mid b_k$ for $0 \le k \le n-1$, so p divides every term on the right. It follows that $p \mid a_n$, contradicting our assumption. Therefore, by Corollary 11.3.4, $f(x)$ is irreducible in $\mathbb{Q}[x]$. □

For example, the polynomial $x^4 + 6x^3 + 27x^2 - 297x + 24$ is irreducible in $\mathbb{Q}[x]$ using Eisenstein's Criterion with $p = 3$. For each $n \in \mathbb{N}^+$ the polynomial $x^n - 2$ is irreducible in $\mathbb{Q}[x]$ using Eisenstein's Criterion with $p = 2$. In particular, we have shown that $\mathbb{Q}[x]$ has irreducible polynomials of every positive degree.

11.4 Prime Elements

When we were working with $\mathbb{Z}$, we noticed the fundamental fact about prime numbers that we used again and again was Proposition 2.5.6, which stated that if $p \in \mathbb{Z}$ is a prime and $p \mid ab$, then either $p \mid a$ or $p \mid b$. However, in a general integral domain, it is far from obvious that this property is equivalent to our concept of irreducibility. Thus, we introduce a new notion.

Definition 11.4.1. *Let R be an integral domain and let $p \in R$ be nonzero and not a unit. We say that p is* prime *if whenever $p \mid ab$, either $p \mid a$ or $p \mid b$.*

Proposition 11.4.2. *Let R be an integral domain. If $p \in R$ is prime, then every associate of p is prime.*

Proof. Exercise (see homework). □

In Section 11.2, we argued that $x+3$ is irreducible in $\mathbb{Q}[x]$. We now show that $x+3$ is also prime in $\mathbb{Q}[x]$. The key fact to use here is Proposition 10.3.2, from which we conclude that for any $h(x) \in \mathbb{Z}[x]$, we have that $x+3 \mid h(x)$ in $\mathbb{Z}[x]$ if and only if $h(-3) = 0$. Suppose then that $f(x), g(x) \in \mathbb{Z}[x]$ are such that $x+3 \mid f(x)g(x)$. We then have that $f(-3)g(-3) = 0$, so since $\mathbb{Z}$ is an integral domain, either $f(-3) = 0$ or $g(-3) = 0$. It follows that either $x+3 \mid f(x)$ in $\mathbb{Z}[x]$ or $x+3 \mid g(x)$ in $\mathbb{Z}[x]$.

As this example suggests, there certainly does appear to be some connection between the concepts of irreducible and prime, but they also have a slightly different flavor. In $\mathbb{Z}$, it is true that an element is prime exactly when it is irreducible. The hard direction here is essentially the content of Proposition 2.5.6 (although again we technically only dealt with positive elements there, but we can use Proposition 11.4.2). In general, one direction of this equivalence from $\mathbb{Z}$ holds in every integral domain, as we now show.

Proposition 11.4.3. *Let R be an integral domain. If p is prime, then p is irreducible.*

Proof. Suppose that p is prime. By definition of prime, p is nonzero and not a unit. Let $a, b \in R$ be arbitrary with $p = ab$. We then have $p1 = ab$, so $p \mid ab$. Since p is prime, we conclude that either $p \mid a$ or $p \mid b$. Suppose that $p \mid a$. Fix $c \in R$ with $a = pc$. We then have

$$p1 = p = ab = (pc)b = p(cb).$$

Since R is an integral domain and $p \neq 0$, we may cancel it to conclude that $1 = cb$, so b is a unit. Suppose instead that $p \mid b$. Fix $d \in R$ with $b = pd$. We then have

$$p1 = p = ab = a(pd) = p(ad).$$

Since R is an integral domain and $p \neq 0$, we may cancel it to conclude that $1 = ad$, so a is a unit. Therefore, either a or b is a unit. It follows that p is irreducible. $\square$

As in divisibility, it is helpful to rephrase our definition of prime elements in terms of principal ideals, and fortunately our common names here coincide.

Proposition 11.4.4. *Let R be an integral domain and let $p \in R$ be nonzero. The ideal $\langle p \rangle$ is a prime ideal of R if and only if p is a prime element of R.*

Proof. Suppose first that $\langle p \rangle$ is a prime ideal of R. Notice that $p \neq 0$ by assumption and that p is not a unit because $\langle p \rangle \neq R$. Suppose that $a, b \in R$ and $p \mid ab$. We then have that $ab \in \langle p \rangle$, so as $\langle p \rangle$ is a prime ideal we know that either $a \in \langle p \rangle$ or $b \in \langle p \rangle$. In the former case, we conclude that $p \mid a$, and in the latter case we conclude that $p \mid b$. Since $a, b \in R$ were arbitrary, it follows that p is a prime element of R.

Suppose conversely that p is a prime element of R. By definition, we know that p is not a unit, so $1 \notin \langle p \rangle$ and hence $\langle p \rangle \neq R$. Suppose that $a, b \in R$ and $ab \in \langle p \rangle$. We then have that $p \mid ab$, so as p is a prime element we know that either $p \mid a$ or $p \mid b$. In the former case, we conclude that $a \in \langle p \rangle$ and in the latter case we conclude that $b \in \langle p \rangle$. Since $a, b \in R$ were arbitrary, it follows that $\langle p \rangle$ is a prime ideal of R. $\square$

One word of caution here is that if R is an integral domain, then $\langle 0 \rangle = \{0\}$ is a prime ideal, but 0 is not a prime element.

By Proposition 11.4.3, we know that in an integral domain R, every prime element of R is irreducible in R. Although in the special case of $\mathbb{Z}$ we know that every irreducible is prime, this is certainly not obvious in general. For example, we showed that $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$ at the end of Section 11.4, but it's much less clear whether $x^3 - 2$ is prime in $\mathbb{Q}[x]$. In fact, for general integral domains R, there can be irreducible elements that are not prime. For a somewhat exotic but interesting example of this, let R be the subring of $\mathbb{Q}[x]$ consisting of those polynomials whose constant term and coefficient of x are both elements of $\mathbb{Z}$. In other words, let

$$R = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}[x] : a_0 \in \mathbb{Z} \text{ and } a_1 \in \mathbb{Z}\}.$$

It is straightforward to check that R is indeed a subring of $\mathbb{Q}[x]$. Furthermore, since $\mathbb{Q}[x]$ is an integral domain, it follows that R is an integral domain as well. We also still have that $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$ for all $f(x), g(x) \in R$ because this property holds in $\mathbb{Q}[x]$. From this, it follows that $U(R) = \{1, -1\}$ and that $3 \in R$ is irreducible in R. Notice that $3 \mid x^2$, i.e. $3 \mid x \cdot x$, because $\frac{1}{3}x^2 \in R$ and

$$3 \cdot \frac{1}{3}x^2 = x^2.$$

However, we also have that $3 \nmid x$ in R, essentially because $\frac{1}{3} \cdot x$ is not an element of R. To see this more formally, suppose that $h(x) \in R$ and $3 \cdot h(x) = x$. Since the degree of the product of two elements of R is the sum of the degrees, we have $\deg(h(x)) = 1$. Since $h(x) \in R$, we can write $h(x) = ax + b$ where $a, b \in \mathbb{Z}$.

We then have $3a \cdot x + 3b = x$, so $3a = 1$, contradicting the fact that $3 \nmid 1$ in $\mathbb{Z}$. Since $3 \mid x \cdot x$ in R, but $3 \nmid x$ in R, it follows that 3 is not prime in R.

Another example of an integral domain where some irreducibles are not prime is the integral domain

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}.$$

Although this also looks like a bizarre example, we will see that $\mathbb{Z}[\sqrt{-5}]$ and many other examples like it play a fundamental role in algebraic number theory. In $\mathbb{Z}[\sqrt{-5}]$, we have two different factorizations of 6:

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3.$$

It turns out that each of the four factors that appear are irreducible in $\mathbb{Z}[\sqrt{-5}]$, but none are prime. We will establish all of these facts later, but here we can at least argue that 2 is not prime. Notice that since $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, we have that $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$. Now if $2 \mid 1+\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$, then we can fix $a, b \in \mathbb{Z}$ with $2(a + b\sqrt{-5}) = 1 + \sqrt{-5}$, which gives $2a + 2b\sqrt{-5} = 1 + \sqrt{-5}$, so $2a = 1$, a contradiction. Thus, $2 \nmid 1 + \sqrt{-5}$. A similar argument shows that $2 \nmid 1 - \sqrt{-5}$.

11.5 Unique Factorization Domains

An element of an integral domain R is irreducible if we can not break it down nontrivially. In $\mathbb{Z}$, we proved the Fundamental Theorem of Arithmetic, which said that every element could be broken down into irreducibles in an essentially unique way. Of course, our uniqueness of irreducible factorizations was only up to order, but there was another issue that we were able to sweep under the rug in $\mathbb{Z}$ by working only with positive elements. For example, consider the following factorizations of 30 in $\mathbb{Z}$:

$$\begin{aligned} 30 &= 2 \cdot 3 \cdot 5 \\ &= (-2) \cdot (-3) \cdot 5 \\ &= (-2) \cdot 3 \cdot (-5) \end{aligned}$$

In $\mathbb{Z}$, the elements -2, -3, and -5 are also irreducible/prime in $\mathbb{Z}$ under our new definition of these concepts. Thus, if we move away from working only with positive primes, then we lose a bit more uniqueness. However, if we slightly loosen the requirements that any two factorizations are "the same up to order" to "the same up to order and associates", we might have a chance.

Definition 11.5.1. *A* Unique Factorization Domain*, or UFD, is an integral domain R such that:*

1. *Every nonzero nonunit is a product of irreducible elements.*
2. *If $q_1 q_2 \cdots q_n = r_1 r_2 \dots r_m$ where each q_i and r_i are irreducible, then $n = m$ and there exists a permutation $\sigma \in S_n$ such that q_i and $r_{\sigma(i)}$ are associates for all i.*

Thus, a UFD is an integral domain in which the analogue of the Fundamental Theorem of Arithmetic (Theorem 2.5.8) holds. We want to prove that several important integral domains that we have studied are indeed UFDs, and to set the stage for this, we first go back and think about the proofs in $\mathbb{Z}$.

In Proposition 2.5.2, we proved that every $n \geq 2$ was a product of irreducible elements of $\mathbb{Z}$ by induction. Intuitively, if n is not irreducible, then factor it, and if those factors are not irreducible, then factor them, etc. The key fact forcing this process to "bottom out", and hence making the induction work, is that the numbers are getting smaller upon factorization and we can not have an infinite descending sequence of natural numbers. In a general integral domain, however, there may not be something that is getting "smaller" and hence this argument could conceivably break down. In fact, there are exotic integral domains where it is possible factor an element forever without ever reaching an irreducible. For an example of this situation, consider the subring R of $\mathbb{Q}[x]$ consisting of those polynomials whose constant term is an integer. In other words, let

$$\begin{aligned} R &= \{p(x) \in \mathbb{Q}[x] : p(0) \in \mathbb{Z}\} \\ &= \{a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Q}[x] : a_0 \in \mathbb{Z}\}. \end{aligned}$$

It is straightforward to check that R is a subring of $\mathbb{Q}[x]$. Furthermore, since $\mathbb{Q}[x]$ is an integral domain, it follows that R is an integral domain as well. We still have that $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$ for all $f(x), g(x) \in R$ because this property holds in $\mathbb{Q}[x]$. From this, it follows that any element of $U(R)$ must be a constant polynomial. Since the constant terms of elements of R are integers, we conclude that $U(R) = \{1, -1\}$. Now consider the element $x \in R$, which is nonzero and not a unit. Notice that x is not irreducible in R because we can write $x = 2 \cdot (\frac{1}{2}x)$, and neither 2 nor $\frac{1}{2}x$ is a unit in R. In fact, we claim that x can not be written as a product of irreducibles in R. To see this, suppose that $p_1(x), p_2(x), \dots, p_n(x) \in R$ and that

$$x = p_1(x)p_2(x)\cdots p_n(x).$$

Since $\deg(x) = 1$, one of the $p_i(x)$ must have degree 1 and the rest must have degree 0 (notice that it is not possible that some $p_i(x)$ is the zero polynomial since x is a nonzero polynomial). Since R is commutative, we can assume that $\deg(p_1(x)) = 1$ and $\deg(p_i(x)) = 0$ for $2 \leq i \leq n$. Write $p_1(x) = ax + b$, and $p_i(x) = c_i$ for $2 \leq i \leq n$ where $b, c_2, c_3, \dots, c_n \in \mathbb{Z}$, each $c_i \neq 0$, and $a \in \mathbb{Q}$. We then have

$$x = (ac_2c_3 \dots c_k)x + bc_2c_3 \cdots c_k.$$

This implies that $bc_2c_3 \cdots c_k = 0$, and since each $c_i \neq 0$, it follows that $b = 0$. Thus, we have $p_1(x) = ax$. Now notice that

$$p_1(x) = ax = 2 \cdot \left(\frac{a}{2}x\right)$$

and neither 2 nor $\frac{a}{2}x$ are units in R. Therefore, $p_1(x)$ is not irreducible in R. We took an arbitrary way to write x as a product of elements of R, and showed that at least of the factors was not irreducible. It follows that x can not be written as a product of irreducible elements in R. From this example, we realize that it is hopeless to prove the existence part of factorizations in general integral domains, so we will need to isolate some special properties of integral domains that will rule out such "infinite descent". In general, relations that do not have such infinite descent are given a special name.

Definition 11.5.2. *A relation $\sim$ on a set A is* well-founded *if there does not exist a sequence of elements $a_1, a_2, a_3, \dots$ from A such that $a_{n+1} \sim a_n$ for all $n \in \mathbb{N}^+$.*

Notice that $<$ is well-founded on $\mathbb{N}$ but not on $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$. If we instead define $\sim$ by saying that $a \sim b$ if $|a| < |b|$, then $\sim$ is well-founded on $\mathbb{Z}$, but not on $\mathbb{Q}$ or $\mathbb{R}$. The fact that $<$ is well-founded on $\mathbb{N}$ is the foundation for well-ordering and induction proofs on $\mathbb{N}$.

We want to think about whether a certain divisibility relation is well-founded. However, the relation we want to think about is not ordinary divisibility, but a slightly different notion.

Definition 11.5.3. *Let R be an integral domain and let $a, b \in R$. We write $a \parallel b$ to mean that $a \mid b$ and that a is not an associate of b. We call $\parallel$ the* strict divisibility relation*.*

For example, in $\mathbb{Z}$ the strict divisibility relation is well-founded because if $a, b \in \mathbb{Z}\backslash\{0\}$ and $a \parallel b$, then $|a| < |b|$. However, if R is the subring of $\mathbb{Q}[x]$ consisting of those polynomials whose constant term is an integer, then the strict divisibility relation is not well-founded. To see this, let $a_n = \frac{1}{2^n}x$ for each $n \in \mathbb{N}^+$. Notice that $a_n \in R$ for all $n \in \mathbb{N}^+$. Also, we have $a_n = 2a_{n+1}$ for each $n \in \mathbb{N}^+$. Since 2 is not a unit in R, we also have that a_n and a_{n+1} are not associates for each $n \in \mathbb{N}^+$. Therefore, $a_{n+1} \parallel a_n$ for each $n \in \mathbb{N}^+$. The fact that the strict divisibility relation is not well-founded on R is the fundamental reason why elements of R may not factor into irreducibles.

Proposition 11.5.4. *Let R be an integral domain. If the strict divisibility relation on R is well-founded (i.e. there does not exist $d_1, d_2, d_3, \ldots$ in R such that $d_{n+1} \parallel d_n$ for all $n \in \mathbb{N}^+$), then every nonzero nonunit in R is a product of irreducibles.*

Proof. We prove the contrapositive. Suppose that there is a nonzero nonunit element of R that is not a product of irreducibles. Fix such an element a. We define a sequence of nonzero nonunit elements $d_1, d_2, \ldots$ in R with $d_{n+1} \parallel d_n$ recursively as follows. Start by letting $d_1 = a$. Assume inductively that d_n is a nonzero nonunit which is not a product of irreducibles. In particular, d_n is itself not irreducible, so we may write $d_n = bc$ for some choice of nonzero nonunits b and c. Now it is not possible that both b and c are products of irreducibles because otherwise d_n would be as well. Thus, we may let d_{n+1} be one of b and c, chosen so that d_{n+1} is also not a product of irreducibles. Notice that d_{n+1} is a nonzero nonunit, that $d_{n+1} \mid d_n$, and that d_{n+1} is not an associate of d_n because neither b nor c are units. Therefore, $d_{n+1} \parallel d_n$. Since we can continue this recursive construction for all $n \in \mathbb{N}^+$, it follows that the strict divisibility relation on R is not well-founded. □

We can also give another proof of Proposition 11.5.4 by using an important combinatorial result.

Definition 11.5.5. *Let $\{0,1\}^*$ be the set of all finite sequences of 0's and 1's (including the "empty string" λ). A* tree *is a subset $T \subseteq \{0,1\}^*$ which is closed under initial segments. In other words, if $\sigma \in T$ and τ is an initial segment of σ, then $\tau \in T$.*

For example, the set $\{\lambda, 0, 1, 00, 01, 011, 0110, 0111\}$ is a tree.

Lemma 11.5.6 (König's Lemma)**.** *Every infinite tree has an infinite branch. In other words, if T is a tree with infinitely many elements, then there is an infinite sequence of 0's and 1's such that every finite initial segment of this sequence is an element of T.*

Proof. Let T be a tree with infinitely many elements. We build the infinite sequences in stages. That is, we define finite sequences $\sigma_0 \prec \sigma_1 \prec \sigma_2 \prec \ldots$ recursively where each $|\sigma_n| = n$. In our construction, we maintain the invariant that there are infinitely many element of T extending σ_n.

We begin by defining $\sigma_0 = \lambda$ and notice that there are infinitely many element of T extending λ because λ is an initial segment of every element of T trivially. Suppose that we have defined σ_n in such a way that $|\sigma_n| = n$ and there are infinitely many elements of T extending σ_n. We then must have that either there are infinitely many elements of T extending $\sigma_n 0$ or there are infinitely many elements of T extending $\sigma_n 1$. Thus, we may fix an $i \in \{0,1\}$ such that there are infinitely many elements of T extending $\sigma_n i$, and define $\sigma_{n+1} = \sigma_n i$.

We now take the unique infinite sequence extending all of the σ_n and notice that it has the required properties. □

Proof 2 of Proposition 11.5.4. Suppose that $a \in R$ is a nonzero nonunit. Recursively factor a into two nonunits, and hence two nonassociate divisors, down a tree. If we ever reach an irreducible, stop that branch but continue down the others. This tree can not have an infinite path because this this would violate the fact that the strict divisibility relation is well-founded on R. Therefore, by König's Lemma, the tree is finite. It follows that a is the product of the leaves, and hence a product of irreducibles. □

Now that we have a decent handle on when an integral domain will have the property that every element is a product of irreducibles, we now move on to the uniqueness aspect. In the proof of the Fundamental Theorem of Arithmetic in $\mathbb{Z}$, we made essential use of Proposition 2.5.6 saying that irreducibles in $\mathbb{Z}$ are prime, and this will be crucial in our generalizations as well. Hence, we are again faced with the question of when irreducibles are guaranteed to be prime. As we saw in the Section 11.4, irreducibles need not be prime in general integral domains either. We now spend the rest of this section showing that if irreducibles are prime, then we do in fact obtain uniqueness.

Definition 11.5.7. *Let R be an integral domain and $c \in R$. Define a function $ord_c \colon R \to \mathbb{N} \cup \{\infty\}$ as follows. Given $a \in R$, let $ord_c(a)$ be the largest $k \in \mathbb{N}$ such that $c^k \mid a$ if one exists, and otherwise let $ord_c(a) = \infty$. Here, we interpret $c^0 = 1$, so we always have $0 \in \{k \in \mathbb{N} : c^k \mid a\}$.*

Notice that we have $ord_0(a) = 0$ whenever $a \neq 0$ and $ord_0(0) = \infty$. Also, for any $a \in R$ and $u \in U(R)$, we have $ord_u(a) = \infty$ because $u^k \in U(R)$ for all $k \in \mathbb{N}$, hence $u^k \mid a$ for all $k \in \mathbb{N}$.

Lemma 11.5.8. *Let R be an integral domain. Let $a, c \in R$ with $c \neq 0$, and let $k \in \mathbb{N}$. The following are equivalent:*

1. *$ord_c(a) = k$.*
2. *$c^k \mid a$ and $c^{k+1} \nmid a$.*
3. *There exists $m \in R$ with $a = c^k m$ and $c \nmid m$.*

Proof.

- (1) $\Rightarrow$ (2) is immediate.
- (2) $\Rightarrow$ (3): Suppose that $c^k \mid a$ and $c^{k+1} \nmid a$. Fix $m \in R$ with $a = c^k m$. If $c \mid m$, then we may fix $n \in R$ with $m = cn$, which would imply that $a = c^k cn = c^{k+1} n$ contradicting the fact that $c^{k+1} \nmid a$. Therefore, we must have $c \nmid m$.
- (3) $\Rightarrow$ (1): Suppose that (3) is true. Fix $m \in R$ with $a = c^k m$ and $c \nmid m$. Since $c^k \mid a$, we clearly have that $ord_c(a) \geq k$. Suppose instead that $ord_c(a) > k$. We can then fix $\ell > k$ with $c^\ell \mid a$, and then fix $n \in R$ with $a = c^\ell n$. We then have

$$\begin{aligned} c^k m &= a \\ &= c^\ell n \\ &= c^k c^{\ell - k} n. \end{aligned}$$

  Since R is an integral domain and $c \neq 0$, we know that $c^k \neq 0$. Using the fact that R is an integral domain again, we may cancel the nonzero c^k from both sides to conclude that $m = c^{\ell-k} n$. Since $\ell > k$, we have $\ell - k \geq 1$, which implies that $c \mid m$, a contradiction. Therefore, we can not have $ord_c(a) > k$, and hence $ord_c(a) = k$.

$\square$

A rough intuition is that $ord_c(a)$ intends to count the number of "occurrences" of c inside of a. A natural hope would be that $ord_c(ab) = ord_c(a) + ord_c(b)$ for all $a, b, c \in R$, but this fails in general. For example, consider $\mathbb{Z}$. We have $ord_{10}(70) = 1$ but $ord_{10}(14) = 0$ and $ord_{10}(5) = 0$, so $ord_{10}(70) \neq ord_{10}(14) + ord_{10}(5)$. Since $10 = 2 \cdot 5$, what is happening in this example is that the 2 was split off into the 14, while the 5 went into the other factor. One might hope that since irreducibles can not be factored nontrivially, this kind of behavior would not happen if we replace 10 by an irreducible element. Although this is true in $\mathbb{Z}$, it is not necessarily the case in general.

As introduced in Section 11.4, in the integral domain

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\},$$

we have

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3,$$

where all four factors are irreducible. Now $ord_2(6) = 1$ because $6 = 2 \cdot 3$ and $2 \nmid 3$ in $\mathbb{Z}[\sqrt{-5}]$. However, we have $ord_2(1 + \sqrt{-5}) = 0 = ord_2(1 - \sqrt{-5})$. Thus,

$$ord_2((1 + \sqrt{-5})(1 - \sqrt{-5})) \neq ord_2(1 + \sqrt{-5}) + ord_2(1 - \sqrt{-5}).$$

In other words, although 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$ and we can "find it" in the product $6 = (1+\sqrt{-5})(1-\sqrt{-5})$, we can not "find it" in either of the factors. This strange behavior takes some getting used to, and we will explore it much further in later chapters. The fundamental obstacle is that although 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$, it is not prime there. In fact, although $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$, we have both $2 \nmid 1+\sqrt{-5}$ and $2 \nmid 1-\sqrt{-5}$.

For an even worse example, consider the subring R of $\mathbb{Q}[x]$ consisting of those polynomials whose constant term and coefficient of x are both elements of $\mathbb{Z}$. In Section 11.4, we showed that 3 was not prime in R because $3 \mid x^2$ but $3 \nmid x$. However, we still have that $U(R) = \{1, -1\}$, so 3 is irreducible in R. However, notice that $ord_3(x^2) = \infty$ and $ord_3(x) = 0$. Thus, we certainly do not have $ord_3(x^2) = ord_3(x) + ord_3(x)$.

The takeaway fact from these examples is that although irreducibility was defined to mean that we could not further "split" the element nontrivially, this definition does not carry with it the nice properties that we might expect. The next theorem shows that everything works much better for the possibly smaller class of prime elements.

Theorem 11.5.9. *Let R be an integral domain and let $p \in R$ be prime. We have the following:*

1. *$ord_p(ab) = ord_p(a) + ord_p(b)$ for all $a, b \in R$.*
2. *$ord_p(a^n) = n \cdot ord_p(a)$ for all $a \in R$ and $n \in \mathbb{N}$.*

Proof. We prove 1, from which 2 follows by induction. Let $a, b \in R$. First notice that if $ord_p(a) = \infty$, then $p^k \mid a$ for all $k \in \mathbb{N}$, hence $p^k \mid ab$ for all $k \in \mathbb{N}$, and thus $ord_p(ab) = \infty$. Similarly, if $ord_p(b) = \infty$, then $ord_p(ab) = \infty$. Suppose then that both $ord_p(a)$ and $ord_p(b)$ are finite, and let $k = ord_p(a)$ and $\ell = ord_p(b)$. Using Lemma 11.5.8, we may then write $a = p^k m$ where $p \nmid m$ and $b = p^\ell n$ where $p \nmid n$. We then have

$$ab = p^k m p^\ell n = p^{k+\ell} \cdot mn$$

Now if $p \mid mn$, then since p is prime, we conclude that either $p \mid m$ or $p \mid n$, but both of these are contradictions. Therefore, $p \nmid mn$. Using Lemma 11.5.8 again, it follows that $ord_p(ab) = k + \ell$. □

Proposition 11.5.10. *Let R be an integral domain, and let $p \in R$ be irreducible.*

1. *For any irreducible q that is an associate of p, we have $ord_p(q) = 1$.*
2. *For any irreducible q that is not an associate of p, we have $ord_p(q) = 0$.*
3. *For any unit u, we have $ord_p(u) = 0$.*

Proof.

1. Suppose that q is an irreducible that is an associate of p. Fix a unit u with $q = pu$. Notice that if $p \mid u$, then since $u \mid 1$, we conclude that $p \mid 1$, which would imply that p is a unit, contradicting our definition of irreducible. Thus, $p \nmid u$, and so $ord_p(q) = 1$ by Lemma 11.5.8.
2. Suppose that q is an irreducible that is not an associate of p. Since q is irreducible, its only divisors are units and associates of q. Since p is not a unit nor an associate of q, it follows that $p \nmid q$. Therefore, $ord_p(q) = 0$.
3. This is immediate because if $p \mid u$, then since $u \mid 1$, we could conclude that $p \mid 1$ and hence p is unit, contradicting the definition of irreducible.

□

Proposition 11.5.11. *Let R be an integral domain. Let $a \in R$ and let $p \in R$ be prime. Suppose that $a = uq_1q_2 \cdots q_k$ where u is a unit and the q_i are irreducibles. We then have that exactly $ord_p(a)$ many of the q_i are associates of p.*

Proof. Since $p \in R$ is prime, Theorem 11.5.9 implies that

$$\begin{aligned} ord_p(a) &= ord_p(uq_1q_2 \cdots q_k) \\ &= ord_p(u) + \sum_{i=1}^{k} ord_p(q_i) \\ &= \sum_{i=1}^{k} ord_p(q_i). \end{aligned}$$

By Proposition 11.5.10, the terms on the right are 1 when q_i is an associate of p and 0 otherwise. The result follows. □

Theorem 11.5.12. *Let R be an integral domain. Suppose that the strict divisibility relation on R is well-founded (i.e. there does not exist $d_1, d_2, d_3, \ldots$ such that $d_{n+1} \parallel d_n$ for all $n \in \mathbb{N}^+$), and every irreducible in R is prime. We then have R is a UFD.*

Proof. Since the strict divisibility relation on R is well-founded, we can use Proposition 11.5.4 to conclude that every nonzero nonunit element of R can be written as a product of irreducibles. Suppose now that $q_1q_2 \cdots q_n = r_1r_2 \ldots r_m$ where each q_i and r_j are irreducible. Call this common element a. We know that every irreducible element of R is prime by assumption. Thus, for any irreducible $p \in R$, Proposition 11.5.11 (with $u = 1$) tells us that exactly $ord_p(a)$ many of the q_i are associates of p, and also that exactly $ord_p(a)$ many of the r_j are associates of p. Thus, for every irreducible $p \in R$, there are an equal number of associates of p on each side. Matching up the elements on the left with corresponding associates on the right tells us that $m = n$ and gives the required permutation. □

Of course, we are left with the question of how to prove that many natural integral domains have these two properties. Now in $\mathbb{Z}$, the proof of Proposition 2.5.6 (that irreducibles are prime) relied upon the existence of greatest common divisors. In the next chapter, we will attempt to generalize the special aspects of $\mathbb{Z}$ that allowed us to prove existence and some of the fundamental properties of GCDs.

Chapter 12

Euclidean Domains and PIDs

12.1 Euclidean Domains

Many of our results in Chapter 2 about $\mathbb{Z}$, and in particular Proposition 2.5.6, trace back to Theorem 2.3.1 about division with remainder. Similarly, in Corollary 9.3.11 we established an analog of division with remainder in the integral domain $F[x]$ of polynomials over a field F. Since this phenomenon has arisen a few times, we now define a class of integral domains that allow "division with remainder". One of ultimate hopes is that such integral domains will always be UFDs.

Definition 12.1.1. *Let R be an integral domain. A function $N\colon R\backslash\{0\} \to \mathbb{N}$ is called a Euclidean function on R if for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that*

$$a = qb + r$$

and either $r = 0$ or $N(r) < N(b)$.

Definition 12.1.2. *An integral domain R is a* Euclidean domain *if there exists a Euclidean function on R.*

Example 12.1.3. *As alluded to above, Theorem 2.3.1 and Corollary 9.3.11 establish the following:*

- *The function $N\colon \mathbb{Z}\backslash\{0\} \to \mathbb{N}$ defined by $N(a) = |a|$ is a Euclidean function on $\mathbb{Z}$, so $\mathbb{Z}$ is a Euclidean domain.*
- *Let F be a field. The function $N\colon F[x]\backslash\{0\} \to \mathbb{N}$ defined by $N(f(x)) = \deg(f(x))$ is a Euclidean function on $F[x]$, so $F[x]$ is a Euclidean domain.*

Notice that we do not require the uniqueness of q and r in our definition of a Euclidean function. Although it was certainly a nice perk to have some aspect of uniqueness in $\mathbb{Z}$ and $F[x]$, it turns out to be be unnecessary for the theoretical results of interest about Euclidean domains. Furthermore, although the above Euclidean function for $F[x]$ does provide true uniqueness, the one for $\mathbb{Z}$ does not since uniqueness there only holds if the remainder is positive (for example, we have $13 = 4 \cdot 3 + 1$ and also $13 = 5 \cdot 3 + (-2)$ where both $N(1) < N(3)$ and $N(-2) < N(3)$). We will see more natural Euclidean functions on integral domains for which uniqueness fails, and we want to be as general as possible.

The name *Euclidean domain* comes from the fact that any such integral domain supports the ability to find greatest common divisors via the Euclidean algorithm. Even more fundamentally, the notion of "size" given by a Euclidean function $N\colon R \to \mathbb{N}$ allows us to use induction to prove the existence of greatest common divisors. We begin with the following generalization of a simple result we proved about $\mathbb{Z}$ which works in any integral domain (even any commutative ring).

Proposition 12.1.4. *Let R be an integral domain. Let $a, b, q, r \in R$ with $a = qb + r$. For any $d \in R$, we have that d is a common divisor of a and b if and only if d is a common divisor of b and r, i.e.*

$$\{d \in R : d \text{ is a common divisor of } a \text{ and } b\} = \{d \in R : d \text{ is a common divisor of } b \text{ and } r\}.$$

Proof. Suppose first that d is a common divisor of b and r. Since $d \mid b$, $d \mid r$, and $a = qb + r = bq + r1$, it follows that $d \mid a$.

Conversely, suppose that d is a common divisor of a and b. Since $d \mid a$, $d \mid b$, and $r = a - qb = a1 + b(-q)$, it follows that $d \mid r$. □

Theorem 12.1.5. *Let R be a Euclidean domain. Every pair of elements $a, b \in R$ has a greatest common divisor.*

Proof. Since R is a Euclidean domain, we may fix a Euclidean function $N \colon R\backslash\{0\} \to \mathbb{N}$. We first handle the special case when $b = 0$ since $N(0)$ is not defined. If $b = 0$, then the set of common divisors of a and b equals the set of divisors of a (because every element divides 0), so a satisfies the requirement of a greatest common divisor. We now use (strong) induction on $N(b) \in \mathbb{N}$ to prove the result.

- *Base Case:* Suppose that $b \in R$ is nonzero and $N(b) = 0$. Fix $q, r \in R$ with $a = qb + r$ and either $r = 0$ or $N(r) < N(b)$. Since $N(b) = 0$, we can not have $N(r) < N(b)$, so we must have $r = 0$. Therefore, we have $a = qb$. It is now easy to check that b is a greatest common divisor of a and b.
- *Inductive Step:* Suppose then that $b \in R$ is nonzero and we know the result for all pairs $x, y \in R$ with either $y = 0$ or $N(y) < N(b)$. Fix $q, r \in R$ with $a = qb + r$ and either $r = 0$ or $N(r) < N(b)$. By (strong) induction, we know that b and r have a greatest common divisor d. By Proposition 12.1.4, the set of common divisors of a and b equals the set of common divisors of b and r. It follows that d is a greatest common divisor of a and b.

□

As an example, consider working in the integral domain $\mathbb{Q}[x]$ and trying to find a greatest common divisor of the following two polynomials:

$$f(x) = x^5 + 3x^3 + 2x^2 + 6 \qquad g(x) = x^4 - x^3 + 4x^2 - 3x + 3.$$

We apply the Euclidean Algorithm as follows (we suppress the computations of the long divisions):

$$\begin{aligned} x^5 + 3x^3 + 2x^2 + 6 &= (x+1)(x^4 - x^3 + 4x^2 - 3x + 3) + (x^2 + 3) \\ x^4 - x^3 + 4x^2 - 3x + 3 &= (x^2 - x + 1)(x^2 + 3) + 0. \end{aligned}$$

Thus, the set of common of $f(x)$ and $g(x)$ equals the set of common divisors of $x^2 + 3$ and 0, which is just the set of divisors of $x^2 + 3$. Therefore, $x^2 + 3$ is a greatest common divisor of $f(x)$ and $g(x)$. Now this is not the only greatest common divisor because we know that any associate of $x^2 + 3$ will also be a greatest common divisor of $f(x)$ and $g(x)$ by Proposition 11.1.11. The units in $\mathbb{Q}[x]$ are the nonzero constants, so other greatest common divisors are $2x^2 + 6$, $\frac{5}{6}x^2 + \frac{5}{2}$, etc. We would like to have a canonical choice for which to pick, akin to choosing the nonnegative value when working in $\mathbb{Z}$.

Definition 12.1.6. *Let F be a field. A* monic *polynomial in $F[x]$ is a nonzero polynomial whose leading term is* 1.

Notice that every nonzero polynomial in $F[x]$ is an associate with a unique monic polynomial (if the leading term is $a \neq 0$, just multiply by a^{-1} to get a monic associate, and notice that this is the only way to multiply by a nonzero constant to make it monic). By restricting to monic polynomials, we get a canonical choice for a greatest common divisor.

Definition 12.1.7. *Let F be a field and let $f(x), g(x) \in F[x]$ be polynomials. If at least one of $f(x)$ and $g(x)$ is nonzero, we define* $\gcd(f(x), g(x))$ *to be the unique monic polynomial which is a greatest common divisor of $f(x)$ and $g(x)$. Notice that if both $f(x)$ and $g(x)$ are the zero polynomial, then* 0 *is the only greatest common divisor of $f(x)$ and $g(x)$, so we define* $\gcd(f(x), g(x)) = 0$.

Now $x^2 + 3$ is monic, so from the above computations, we have

$$\gcd(x^5 + 3x^3 + 2x^2 + 6, x^4 - x^3 + 4x^2 - 3x + 3) = x^2 + 3$$

We end this section by showing that the Gaussian Integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ also form a Euclidean domain. In order to show this, we will use the following result.

Proposition 12.1.8. *The subring $\mathbb{Q}[i] = \{q + ri : q, r \in \mathbb{Q}\}$ is a field.*

Proof. Let $\alpha \in \mathbb{Q}[i]$ be nonzero and write $\alpha = q + ri$ where $q, r \in \mathbb{Q}$. We then have that either $q \neq 0$ or $r \neq 0$, so

$$\begin{aligned}
\frac{1}{\alpha} &= \frac{1}{q + ri} \\
&= \frac{1}{q + ri} \cdot \frac{q - ri}{q - ri} \\
&= \frac{q - ri}{q^2 + r^2} \\
&= \frac{q}{q^2 + r^2} + \frac{-r}{q^2 + r^2} \cdot i.
\end{aligned}$$

Since both $\frac{q}{q^2+r^2}$ and $\frac{-r}{q^2+r^2}$ are elements of $\mathbb{Q}$, it follows that $\frac{1}{\alpha} \in \mathbb{Q}[i]$. Therefore, $\mathbb{Q}[i]$ is a field. $\square$

Definition 12.1.9. *We define a function $N \colon \mathbb{Q}[i] \to \mathbb{Q}$ by letting $N(q + ri) = q^2 + r^2$. The function N is called the* norm *on the field $\mathbb{Q}[i]$.*

Proposition 12.1.10. *For the function $N(q + ri) = q^2 + r^2$ defined on $\mathbb{Q}[i]$, we have the following:*

1. *$N(\alpha) \geq 0$ for all $\alpha \in \mathbb{Q}[i]$.*
2. *$N(\alpha) = 0$ if and only if $\alpha = 0$.*
3. *$N(q) = q^2$ for all $q \in \mathbb{Q}$.*
4. *$N(\alpha) \in \mathbb{N}$ for all $\alpha \in \mathbb{Z}[i]$.*
5. *$N(\alpha\beta) = N(\alpha) \cdot N(\beta)$ for all $\alpha, \beta \in \mathbb{Q}[i]$.*

Proof. The first four are all immediate from the definition. Let $\alpha, \beta \in \mathbb{Q}[i]$ be arbitrary, and write $\alpha = q + ri$ and $\beta = s + ti$ where $q, r, s, t \in \mathbb{Q}$. We have

$$\begin{aligned}
N(\alpha\beta) &= N((q + ri)(s + ti)) \\
&= N(qs + rsi + qti - rt) \\
&= N((qs - rt) + (rs + qt)i) \\
&= (qs - rt)^2 + (rs + qt)^2 \\
&= q^2s^2 - 2qsrt + r^2t^2 + r^2s^2 + 2rsqt + q^2t^2 \\
&= q^2s^2 + r^2s^2 + q^2t^2 + r^2t^2 \\
&= (q^2 + r^2) \cdot (s^2 + t^2) \\
&= N(q + ri) \cdot N(s + ti) \\
&= N(\alpha) \cdot N(\beta).
\end{aligned}$$

□

Corollary 12.1.11. $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

Proof. Notice that $\{1, -1, i, -i\} \subseteq U(\mathbb{Z}[i])$ because $1^2 = 1$, $(-1)^2 = 1$, and $i \cdot (-i) = 1$. Suppose conversely that $\alpha \in U(\mathbb{Z}[i])$ and write $\alpha = c + di$ where $a, b \in \mathbb{Z}$. Since $\alpha \in U(\mathbb{Z}[i])$, we can fix $\beta \in \mathbb{Z}[i]$ with $\alpha\beta = 1$. We then have $N(\alpha\beta) = N(1)$, so $N(\alpha) \cdot N(\beta) = 1$ by the previous proposition. Since $N(\alpha), N(\beta) \in \mathbb{N}$, we conclude that $N(\alpha) = 1$ and $N(\beta) = 1$. We then have $c^2 + d^2 = N(\alpha) = 1$. It follows that one of c or d is 0, and the other is ± 1. Thus, $\alpha = c + di \in \{1, -1, i, -i\}$. □

Theorem 12.1.12. *$\mathbb{Z}[i]$ is a Euclidean domain with Euclidean function $N(a + bi) = a^2 + b^2$.*

Proof. Notice $\mathbb{Z}[i]$ is an integral domain because it is a subring of $\mathbb{C}$. Let $\alpha, \beta \in \mathbb{Z}[i]$ be arbitrary with $\beta \neq 0$. When we divide α by β in the field $\mathbb{Q}[i]$ we get $\frac{\alpha}{\beta} = s + ti$ for some $s, t \in \mathbb{Q}$. Fix integers $m, n \in \mathbb{Z}$ closest to $s, t \in \mathbb{Q}$ respectively, i.e. fix $m, n \in \mathbb{Z}$ so that $|m - s| \leq \frac{1}{2}$ and $|n - t| \leq \frac{1}{2}$. Let $\gamma = m + ni \in \mathbb{Z}[i]$, and let $\rho = \alpha - \beta\gamma \in \mathbb{Z}[i]$. We then have that $\alpha = \beta\gamma + \rho$, so we need only show that $N(\rho) < N(\beta)$. Now

$$\begin{aligned}
N(\rho) &= N(\alpha - \beta\gamma) \\
&= N(\beta \cdot (s + ti) - \beta \cdot \gamma) \\
&= N(\beta \cdot ((s + ti) - (m + ni)) \\
&= N(\beta \cdot ((s - m) + (t - n)i) \\
&= N(\beta) \cdot N((s - m) + (t - n)i) \\
&= N(\beta) \cdot ((s - m)^2 + (t - n)^2) \\
&\leq N(\beta) \cdot \left(\frac{1}{4} + \frac{1}{4}\right) \\
&= \frac{1}{2} \cdot N(\beta) \\
&< N(\beta),
\end{aligned}$$

where the last line follows because $N(\beta) > 0$ (since $\beta \neq 0$). □

We work out an example of finding a greatest common divisor of $8 + 9i$ and $10 - 5i$ in $\mathbb{Z}[i]$. We follow the above proof to find quotients and remainders. Notice that

$$\begin{aligned}
\frac{8 + 9i}{10 - 5i} &= \frac{8 + 9i}{10 - 5i} \cdot \frac{10 + 5i}{10 + 5i} \\
&= \frac{80 + 40i + 90i - 45}{100 + 25} \\
&= \frac{35 + 130i}{125} \\
&= \frac{7}{25} + \frac{26}{25} \cdot i.
\end{aligned}$$

Following the proof (where we take the closest integers to $\frac{7}{25}$ and $\frac{26}{25}$), we should use the quotient i and determine the remainder from there. We thus write

$$8 + 9i = i \cdot (10 - 5i) + (3 - i).$$

Notice that $N(3-i) = 9+1 = 10$ which is less than $N(10-5i) = 100+25 = 125$. Following the Euclidean algorithm, we next calculate

$$\begin{aligned}\frac{10-5i}{3-i} &= \frac{10-5i}{3-i} \cdot \frac{3+i}{3+i} \\ &= \frac{30+10i-15i+5}{9+1} \\ &= \frac{35-5i}{10} \\ &= \frac{7}{2} - \frac{1}{2} \cdot i.\end{aligned}$$

Following the proof (where we now have many choices because $\frac{7}{2}$ is equally close to 3 and 4 and $-\frac{1}{2}$ is equally close to -1 and 0), we choose to take the quotient 3. We then write

$$10 - 5i = 3 \cdot (3-i) + (1-2i).$$

Notice that $N(1-2i) = 1+4 = 5$ which is less than $N(3-i) = 9+1 = 10$. Going to the next step, we calculate

$$\begin{aligned}\frac{3-i}{1-2i} &= \frac{3-i}{1-2i} \cdot \frac{1+2i}{1+2i} \\ &= \frac{3+6i-i+2}{1+4} \\ &= \frac{5+5i}{5} \\ &= 1+i\end{aligned}$$

Therefore, we have

$$3 - i = (1+i) \cdot (1-2i) + 0.$$

Putting together the various divisions, we see the Euclidean algorithm as:

$$\begin{aligned}8+9i &= i \cdot (10-5i) + (3-i) \\ 10-5i &= 3 \cdot (3-i) + (1-2i) \\ 3-i &= (1+i) \cdot (1-2i) + 0\end{aligned}$$

Thus, the set of common divisors of $8+9i$ and $10-5i$ equals the set of common divisors of $1-2i$ and 0, which is just the set of divisors of $1-2i$. Since a greatest common divisor is unique up to associates and the units of $\mathbb{Z}[i]$ are $1, -1, i, -i$, it follows the set of greatest common divisors of $8+9i$ and $10-5i$ is

$$\{1-2i, -1+2i, 2+i, -2-i\}.$$

In a Euclidean domains with a “nice” Euclidean function, say where $N(b) < N(a)$ whenever $b \parallel a$, one can mimic the inductive argument in $\mathbb{Z}$ to prove that every element is a product of irreducibles. For example, it is relatively straightforward to prove that our Euclidean functions on $F[x]$ and $\mathbb{Z}[i]$ satisfy this, and so every (nonzero nonunit) element factors into irreducibles. In fact, one can show that every Euclidean domain has a (possibly different) Euclidean function N with the property that $N(b) < N(a)$ whenever $b \parallel a$. However, rather than develop this interesting theory, we approach these problems from another perspective.

12.2 Principal Ideal Domains

We chose our definition of a Euclidean domain to abstract away the fundamental fact about $\mathbb{Z}$ that we can always divide in such a way to get a quotient along with a "smaller" remainder. As we have seen, this ability allows us to carry over to these integral domains the existence of greatest common divisors and the method of finding them via the Euclidean Algorithm.

Recall back when we working with $\mathbb{Z}$ that we had another characterization of (and proof of existence for) a greatest common divisor in Theorem 2.4.13. We proved that the greatest common divisor of two nonzero integers a and b was the least positive number of the form $ma + nb$ where $m, n \in \mathbb{Z}$. Now the "least" part will have no analogue in a general integral domain, so we will have to change that. Perhaps surprisingly, it turns out that the way to generalize this construction is to think about ideals. The reason why is that $\{ma + nb : m, n \in \mathbb{Z}\}$ is simply the ideal $\langle a, b\rangle$. As we will see, in hindsight, what made this approach to greatest common divisors work in $\mathbb{Z}$ is the fact that every ideal of $\mathbb{Z}$ is principal (from Proposition 10.4.7). We give the integral domains which have this property a special name.

Definition 12.2.1. *A* principal ideal domain*, or* PID*, is an integral domain in which every ideal is principal.*

Before working with these rings on their own terms, we first prove that every Euclidean domains is a PID so that we have a decent supply of examples. Our proof generalizes the one for $\mathbb{Z}$ (see Proposition 10.4.7) in the sense that instead of looking for a smallest positive element of the ideal, we simply look for an element of smallest "size" according to a given Euclidean function.

Theorem 12.2.2. *Every Euclidean domain is a PID.*

Proof. Let R be a Euclidean domain, and fix a Euclidean function $N\colon R\backslash\{0\} \to \mathbb{N}$. Suppose that I is an ideal of R. If $I = \{0\}$, then $I = \langle 0\rangle$. Suppose then that $I \neq \{0\}$. The set

$$\{N(a) : a \in I\backslash\{0\}\}$$

is a nonempty subset of $\mathbb{N}$. By the well-ordering property of $\mathbb{N}$, the set has a least element m. Fix $b \in I$ with $N(b) = m$. Since $b \in I$, we clearly have $\langle b\rangle \subseteq I$. Suppose now that $a \in I$. Fix $q, r \in R$ with

$$a = qb + r$$

and either $r = 0$ or $N(r) < N(b)$. Since $r = a - qb$ and both $a, b \in I$, it follows that $r \in I$. Now if $r \neq 0$, then $N(r) < N(b) = m$ contradicting our minimality of m. Therefore, we must have $r = 0$ and so $a = qb$. It follows that $a \in \langle b\rangle$. Since $a \in I$ was arbitrary, we conclude that $I \subseteq \langle b\rangle$. Therefore, $I = \langle b\rangle$. □

Corollary 12.2.3. *$\mathbb{Z}$, $F[x]$ for F a field, and $\mathbb{Z}[i]$ are all PIDs.*

Notice also that all fields F are also PIDs for the trivial reason that the only ideals of F are $\{0\} = \langle 0\rangle$ and $F = \langle 1\rangle$. In fact, all fields are also trivially Euclidean domain via absolutely any function $N\colon F\backslash\{0\} \to \mathbb{N}$ because we can always divide by a nonzero element with zero as a remainder. It turns out that there are PIDs which are not Euclidean domains, but we will not construct examples of such rings now.

Returning to our other characterization of greatest common divisors in $\mathbb{Z}$, we had that if $a, b \in \mathbb{Z}$ not both nonzero, then we considered the set

$$\{ma + nb : m, n \in \mathbb{Z}\}$$

and proved that the least positive element of this set was the greatest common divisor. In our current ring-theoretic language, the above set is the ideal $\langle a, b\rangle$ of $\mathbb{Z}$, and a generator of this ideal is a greatest common divisor. With this change in perspective/language, we can carry this argument over to an arbitrary PID.

Theorem 12.2.4. *Let R be a PID and let $a, b \in R$.*

1. *There exists a greatest common divisor of a and b.*

2. *If d is a greatest common divisor of a and b, then there exists $r, s \in R$ with $d = ra + sb$.*

Proof.

1. Let $a, b \in R$. Consider the ideal

$$I = \langle a, b \rangle = \{ra + sb : r, s \in R\}.$$

Since R is a PID, the ideal I is principal, so we may fix $d \in R$ with $I = \langle d \rangle$. Since $d \in \langle d \rangle = \langle a, b \rangle$, we may fix $r, s \in R$ with $ra + sb = d$. We claim that d is a greatest common divisor of a and b.

First notice that $a \in I$ since $a = 1a + 0b$, so $a \in \langle d \rangle$, and hence $d \mid a$. Also, we have $b \in I$ because $b = 0a + 1b$, so $b \in \langle d \rangle$, and hence $d \mid b$. Thus, d is a common divisor of a and b.

Suppose now that c is a common divisor of a and b. Fix $m, n \in R$ with $a = cm$ and $b = cn$. We then have

$$\begin{aligned} d &= ra + sb \\ &= r(cm) + s(cn) \\ &= c(rm + sn). \end{aligned}$$

Thus, $c \mid d$. Putting it all together, we conclude that d is a greatest common divisor of a and b.

2. For the d in part 1, we showed in the proof that there exist $r, s \in R$ with $d = ra + sb$. Let d' be any other greatest common divisor of a and b, and fix a unit u with $d' = du$. We then have

$$d' = du = (ra + sb)u = (ru)a + (su)b.$$

□

It is possible to define a greatest common divisor of elements $a_1, a_2, \dots, a_n \in R$ completely analogously to our definition for pairs of elements. If we do so, even in the case of a nice Euclidean domain, we can not immediately generalize the idea of the Euclidean Algorithm to many elements without doing a kind of repeated nesting that gets complicated. However, notice that we can very easily generalize our PID arguments to prove that greatest common divisors exist and are unique up to associates by following the above proofs and simply replacing the ideal $\langle a, b \rangle$ with the ideal $\langle a_1, a_2, \dots, a_n \rangle$. We even conclude that it possible to write a greatest common divisor in the form $r_1a_1 + r_2a_2 + \dots + r_na_n$. The assumption that all ideals are principal is extremely powerful.

With the hard work of the last couple of sections in hand, we can now carry over much of our later work in $\mathbb{Z}$ which dealt with relatively prime integers and primes. The next definition and ensuing two propositions directly generalize corresponding results about $\mathbb{Z}$.

Definition 12.2.5. *Let R be a PID. Two elements $a, b \in R$ are* relatively prime *if 1 is a greatest common divisor of a and b.*

Proposition 12.2.6. *Let R be a PID and let $a, b, c \in R$. If $a \mid bc$ and a and b are relatively prime, then $a \mid c$.*

Proof. Fix $d \in R$ with $bc = ad$. Fix $r, s \in R$ with $ra + sb = 1$. Multiplying this last equation through by c, we conclude that $rac + sbc = c$, so

$$\begin{aligned} c &= rac + s(bc) \\ &= rac + s(ad) \\ &= a(rc + sd). \end{aligned}$$

It follows that $a \mid c$. □

Proposition 12.2.7. *Suppose that R is a PID. If p is irreducible, then p is prime.*

Proof. Suppose that $p \in R$ is irreducible. By definition, p is nonzero and not a unit. Suppose that $a, b \in R$ are such that $p \mid ab$. Fix a greatest common divisor d of p and a. Since $d \mid p$, we may fix $c \in R$ with $p = dc$. Now p is irreducible, so either d is a unit or c is a unit. We handle each case:

- *Case 1:* Suppose that d is a unit. We then have that 1 is an associate of d, so 1 is also a greatest common divisor of p and a. Therefore, p and a are relatively prime, so as $p \mid ab$ we may use Proposition 12.2.6 to conclude that $p \mid b$.

- *Case 2:* Suppose that c is a unit. We then have that $pc^{-1} = d$, so $p \mid d$. Since $d \mid a$, it follows that $p \mid a$.

Therefore, either $p \mid a$ or $p \mid b$. It follows that p is prime. □

Excellent. We've developed enough theory of PIDs to prove that GCDs always exist, and used that to prove that irreducibles are always prime in PIDs. However, there is still the question on why $\parallel$ is well-founded in PIDs. Now that we no longer have a notion of size of elements, this seems daunting. Notice that the the defining property of PIDs is a condition on the ideals, so we first rephrase the $\parallel$ relation in terms of ideals.

Proposition 12.2.8. *Suppose that R is an integral domain and $a, b \in R$. We have $a \parallel b$ if and only if $\langle b \rangle \subsetneq \langle a \rangle$.*

Proof. Immediate from Proposition 11.1.8 and Corollary 11.1.9. □

Thus, if we want to prove that $\parallel$ is well-founded, i.e. if we want to prove that there is no infinite descending sequence of strict divisibility, then we can instead prove that there is no infinite ascending chain of ideals. Commutative rings that have this property are given a special name in honor of Emmy Noether.

Definition 12.2.9. *A commutative ring R is said to be* Noetherian *if there is no strictly increasing sequence of ideals*

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$$

Equivalently, whenever

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

is a sequence of ideals, there exists $N \in \mathbb{N}^+$ such that $I_k = I_N$ for all $k \geq N$.

Immediately from the definition, we obtain the following result.

Proposition 12.2.10. *Let R be a Noetherian integral domain. We have that $\parallel$ is a well-founded relation on R, and hence every nonzero nonunit element of R can be written as a product of irreducibles.*

Proof. Let R be a Noetherian integral domain. We need to prove that $\parallel$ is well-founded on R. Suppose instead that we have a sequence $a_1, a_2, a_3, \dots$ such that $a_{n+1} \parallel a_n$. Letting $I_n = \langle a_n \rangle$ for all n, it follows from Proposition 12.2.8 that $I_n \subsetneq I_{n+1}$ for all $n \in \mathbb{N}^+$. Thus, we have

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$$

which contradicts the definition of Noetherian. Therefore, $\parallel$ is well-founded on R. The last statement now following from Proposition 11.5.4. □

This is all well and good, but we need a "simple" way to determine when a commutative ring R is Noetherian. Fortunately, we have the following.

Theorem 12.2.11. *Let R be a commutative ring. The following are equivalent:*

1. *R is Noetherian.*
2. *Every ideal of R is finitely generated (i.e. for every ideal I of R, there exist $a_1, a_2, \dots, a_m \in R$ with $I = \langle a_1, a_2, \dots, a_m \rangle$).*

Proof. Suppose first that every ideal of R is finitely generated. Let

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

be a sequence of ideals. Let

$$J = \bigcup_{k=1}^{\infty} I_k = \{r \in R : r \in I_k \text{ for some } k \in \mathbb{N}^+\}$$

We claim that J is an ideal of R.

- First notice that $0 \in I_1 \subseteq J$.
- Let $a, b \in J$ be arbitrary. Fix $k, \ell \in \mathbb{N}^+$ with $a \in I_k$ and $b \in I_\ell$. We then have $a, b \in I_{\max\{k,\ell\}}$, so $a + b \in I_{\max\{k,\ell\}} \subseteq J$.
- Let $a \in J$ and $r \in R$ be arbitrary. Fix $k \in \mathbb{N}^+$ with $a \in I_k$. We then have that $ra \in I_k \subseteq J$.

Since J is an ideal of R, and we are assuming that every ideal of R is finitely generated, we may fix $a_1, a_2, \dots, a_m \in R$ with $J = \langle a_1, a_2, \dots, a_m \rangle$. For each i, fix $k_i \in \mathbb{N}$ with $a_i \in I_{k_i}$. Let $N = \max\{k_1, k_2, \dots, k_m\}$. We then have that $a_i \in I_N$ for each i, hence $J = \langle a_1, a_2, \dots, a_m \rangle \subseteq I_N$. Therefore, for any $n \geq N$, we have

$$I_N \subseteq I_n \subseteq J \subseteq I_N$$

hence $I_n = I_N$.

Suppose conversely that some ideal of R is not finitely generated and fix such an ideal J. Define a sequence of elements of J as follows. Let a_1 be an arbitrary element of J. Suppose that we have defined $a_1, a_2, \dots, a_k \in J$. Since J is not finitely generated, we have that

$$\langle a_1, a_2, \dots, a_n \rangle \subsetneq J$$

so we may let a_{k+1} be some (any) element of $J \backslash \langle a_1, a_2, \dots, a_k \rangle$. Letting $I_n = \langle a_1, a_2, \dots, a_n \rangle$ for each $n \in \mathbb{N}^+$, we then have

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$$

so R is not Noetherian. □

Corollary 12.2.12. *Every PID is Noetherian.*

Proof. This follows immediately from Theorem 12.2.11 and the fact that in a PID every ideal is generated by one element. □

Corollary 12.2.13. *Every PID is a UFD, and thus every Euclidean domain is a UFD as well.*

Proof. Let R be a PID. By Corollary 12.2.12, we know that R is Noetherian, and so $\|$ is well-founded by Proposition 12.2.10. Furthermore, we know that every irreducible in R is prime by Proposition 12.2.7. Therefore, R is a UFD by Theorem 11.5.12. □

Finally, we bring together many of the fundamental properties of elements and ideals in any PID.

Proposition 12.2.14. *Let R be a PID and let $a \in R$ with $a \neq 0$. The following are equivalent.*

1. *$\langle a\rangle$ is a maximal ideal.*

2. *$\langle a\rangle$ is a prime ideal.*

3. *a is prime.*

4. *a is irreducible.*

Proof. We have already proved much of this, so let's recap what we know.

- (1) $\Rightarrow$ (2) is Corollary 10.5.6.
- (2) $\Leftrightarrow$ (3) is Proposition 11.4.4.
- (3) $\Rightarrow$ (4) is Proposition 11.4.3.
- (4) $\Rightarrow$ (3) is Proposition 12.2.7.

To finish the equivalences, we prove that (4) $\Rightarrow$ (1).

Suppose that $a \in R$ is irreducible, and let $M = \langle a\rangle$. Since a is not a unit, we have that $1 \notin \langle a\rangle$, so $M \neq R$. Suppose that I is an ideal with $M \subseteq I \subseteq R$. Since R is a PID, there exists $b \in R$ with $I = \langle b\rangle$. We then have that $\langle a\rangle \subseteq \langle b\rangle$, so $b \mid a$ by Proposition 11.1.8. Fix $c \in R$ with $a = bc$. Since a is irreducible, either b is a unit or c is a unit. In the former case, we have that $1 \in \langle b\rangle = I$, so $I = R$. In the latter case we have that b is an associate of a so $I = \langle b\rangle = \langle a\rangle = M$ by Corollary 11.1.9. Thus, there is no ideal I of R with $M \subsetneq I \subsetneq R$. □

It is natural to misread the previous proposition to conclude that in a PID every prime ideal is maximal. This is almost true, but pay careful attention to the assumption that $a \neq 0$. In a PID R, the ideal $\{0\}$ is always a prime ideal, but it is only maximal in the trivial special case of when R is a field. In a PID, every *nonzero* prime ideal is maximal.

Corollary 12.2.15. *If R is a PID, then every nonzero prime ideal is maximal.*

12.3 Quotients of $F[x]$

We have now carried over many of the concepts and proofs that originated in the study of the integers $\mathbb{Z}$ over to the polynomial ring over a field $F[x]$ (and more generally any Euclidean Domains or even PID). One construction we have not focused on is the quotient construction. In the integers $\mathbb{Z}$, we know that every nonzero ideal has the form $n\mathbb{Z} = \langle n\rangle$ for some $n \in \mathbb{N}^+$ (because after all $\mathbb{Z}$ is a PID and we have $\langle n\rangle = \langle -n\rangle$). The quotients of $\mathbb{Z}$ by these ideals are the now very familiar rings $\mathbb{Z}/n\mathbb{Z}$.

Since we have so much in common between $\mathbb{Z}$ and $F[x]$, we would like to study the analogous quotients of $F[x]$. Now if F is a field, then $F[x]$ is a PID, so for every nonzero ideal of $F[x]$ equals $\langle p(x)\rangle$ for some $p(x) \in F[x]$. Suppose then that $p(x) \in F[x]$ and let $I = \langle p(x)\rangle$. Given $f(x) \in F[x]$, we will write $\overline{f(x)}$ for the coset $f(x) + I$ just like we wrote $\overline{k}$ for the coset $k + n\mathbb{Z}$. As long as we do not change the ideal I (so do not change $p(x)$) in a given construction, there should be no confusion as to which quotient we are working in. When dealing with these quotients, our first task is to find unique representatives for the cosets as in $\mathbb{Z}/n\mathbb{Z}$ where we saw that $\overline{0}, \overline{1}, \dots, \overline{n-1}$ served as distinct representatives for the cosets.

Proposition 12.3.1. *Let F be a field and let $p(x) \in F[x]$ be nonzero. Let $I = \langle p(x)\rangle$ and work in $F[x]/I$. For all $f(x) \in F[x]$, there exists a unique $h(x) \in F[x]$ such that both:*

- $\overline{f(x)} = \overline{h(x)}$
- *Either $h(x) = 0$ or $\deg(h(x)) < \deg(p(x))$*

In other words, if we let

$$S = \{h(x) \in F[x] : h(x) = 0 \text{ or } \deg(h(x)) < \deg(p(x))\}$$

then the elements of S provide unique representatives for the cosets in $F[x]/I$.

Proof. We first prove existence. Let $f(x) \in F[x]$. Since $p(x) \neq 0$, we may fix $q(x), r(x)$ with

$$f(x) = q(x)p(x) + r(x)$$

and either $r(x) = 0$ or $\deg(r(x)) < \deg(p(x))$. We then have

$$p(x)q(x) = f(x) - r(x)$$

Thus $p(x) \mid (f(x) - r(x))$ and so $f(x) - r(x) \in I$. It follows from Proposition 10.1.6 that $\overline{f(x)} = \overline{r(x)}$ so we may take $h(x) = r(x)$. This proves existence.

We now prove uniqueness. Suppose that $h_1(x), h_2(x) \in S$ (so each is either 0 or has smaller degree than $p(x)$) and that $\overline{h_1(x)} = \overline{h_2(x)}$. Using Proposition 10.1.6, we then have that $h_1(x) - h_2(x) \in I$ and hence $p(x) \mid (h_1(x) - h_2(x))$. Notice that every nonzero multiple of $p(x)$ has degree greater than or equal to $\deg(p(x))$ (since the degree of a product is the sum of the degrees in $F[x]$). Now either $h_1(x) - h_2(x) = 0$ or it has degree less than $\deg(p(x))$, but we've just seen that the latter is impossible. Therefore, it must be the case that $h_1(x) - h_2(x) = 0$, and so $h_1(x) = h_2(x)$. This proves uniqueness. $\square$

Let's look at an example. Suppose that we are working with $F = \mathbb{Q}$ and we let $p(x) = x^2 - 2x + 3$. Consider the quotient ring $R = \mathbb{Q}[x]/\langle p(x)\rangle$. From above, we know that every element in this quotient is represented uniquely by either a constant polynomial or a polynomial of degree 1. Thus, some distinct elements of R are $\overline{1}$, $\overline{3/7}$, $\overline{x}$, and $\overline{2x - 5/3}$. We add elements in the quotient ring R by adding representatives as usual, so for example we have

$$\overline{4x - 7} + \overline{2x + 8} = \overline{6x + 1}$$

Multiplication of elements of R is more interesting if we try to convert the resulting product to one of our chosen representatives. For example, we have

$$\overline{2x + 7} \cdot \overline{x - 1} = \overline{(2x + 7)(x - 1)} = \overline{2x^2 + 5x - 7}$$

which is perfectly correct, but the resulting representative isn't one of our chosen ones. If we follows the above proof, we should divide $2x^2 + 5x - 7$ by $x^2 - 2x + 3$ and use the remainder as our representative. We have

$$2x^2 + 5x - 7 = 2 \cdot (x^2 - 2x + 3) + (9x - 13)$$

so

$$(2x^2 + 5x - 7) - (9x - 13) \in \langle p(x)\rangle$$

and hence

$$\overline{2x^2 + 5x - 7} = \overline{9x - 13}$$

It follows that in the quotient we have

$$\overline{2x + 7} \cdot \overline{x - 1} = \overline{9x - 13}$$

Here's another way to determine that the product is $\overline{9x - 13}$. Notice that for any $f(x), g(x) \in F[x]$, we have

$$\overline{f(x)} + \overline{g(x)} = \overline{f(x) + g(x)} \qquad \overline{f(x)} \cdot \overline{g(x)} = \overline{f(x) \cdot g(x)}$$

by definition of multiplication in the quotient. Now $p(x) = x^2 - 2x + 3$, so in the quotient we have $\overline{x^2 - 2x + 3} = \overline{0}$. It follows that

$$\overline{x^2} + \overline{-2x+3} = \overline{0}$$

and hence

$$\overline{x^2} = \overline{2x-3}$$

Therefore

$$\begin{aligned}
\overline{2x+7} \cdot \overline{x-1} &= \overline{2x^2+5x-7} \\
&= \overline{2} \cdot \overline{x^2} + \overline{5x-7} \\
&= \overline{2} \cdot \overline{2x-3} + \overline{5x-7} \\
&= \overline{4x-6} + \overline{5x-7} \\
&= \overline{9x-13}
\end{aligned}$$

For another example, consider the ring $F = \mathbb{Z}/2\mathbb{Z}$. Since we will be working in quotients of $F[x]$ and too many equivalence classes begins to get confusing, we will write $F = \{0, 1\}$ rather than $F = \{\overline{0}, \overline{1}\}$. Consider the polynomial $p(x) = x^2+1 \in F[x]$. We then have that the elements of $F[x]/\langle x^2+1\rangle$ are represented uniquely by either a constant polynomial or a polynomial of degree 1. Thus, the distinct elements of $F[x]/\langle x^2+1\rangle$ are given by $\overline{ax+b}$ for $a, b \in F$. Since $|F| = 2$, we have two choices for each of a and b, and hence the quotient has four elements. Here is the additional and multiplication tables for $F[x]/\langle x^2+1\rangle$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{1}$	$\overline{x+1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x+1}$	$\overline{0}$

The addition table is fairly straightforward, but some work went into constructing the multiplication table. For example, we have

$$\overline{x} \cdot \overline{x+1} = \overline{x^2+x}$$

To determine which of our chosen representatives gives this coset, we notice that $\overline{x^2+1} = \overline{0}$ (since clearly $x^2+1 \in \langle x^2+1\rangle$), so $\overline{x^2} + \overline{1} = \overline{0}$. Adding $\overline{1}$ to both sides and noting that $\overline{1} + \overline{1} = \overline{0}$, we conclude that $\overline{x^2} = \overline{1}$. Therefore

$$\begin{aligned}
\overline{x} \cdot \overline{x+1} &= \overline{x^2+x} \\
&= \overline{x^2} + \overline{x} \\
&= \overline{1} + \overline{x} \\
&= \overline{x+1}
\end{aligned}$$

The other entries of the table can be found similarly. In fact, we have done all the hard work because we now know that $\overline{x^2} = \overline{1}$ and we can use that throughout.

Suppose instead that we work with the polynomial $p(x) = x^2 + x + 1$. Thus, we are considering the quotient $F[x]/\langle x^2+x+1\rangle$. As above, since $\deg(x^2+x+1) = 2$, we get unique representatives from the elements $ax+b$ for $a, b \in \{0, 1\}$. Although we have the same representatives, the cosets are different and the multiplication table changes considerably:

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

For example, let's determine $\overline{x} \cdot \overline{x+1}$ in this situation. Notice first that $\overline{x^2+x+1} = \overline{0}$, so $\overline{x^2} + \overline{x} + \overline{1} = 0$. Adding $\overline{x} + \overline{1}$ to both sides and using the fact that $\overline{1} + \overline{1} = \overline{0}$ and $\overline{x} + \overline{x} = \overline{0}$, we conclude that

$$\overline{x^2} = \overline{x} + \overline{1} = \overline{x+1}$$

Therefore, we have

$$\begin{aligned}\overline{x} \cdot \overline{x+1} &= \overline{x^2+x} \\ &= \overline{x^2} + \overline{x} \\ &= \overline{x} + \overline{1} + \overline{x} \\ &= \overline{1}\end{aligned}$$

Notice that every nonzero element of the quotient $F[x]/\langle x^2+x+1\rangle$ has a multiplicative inverse, so the quotient in this case is a field. We have succeeded in constructing of field of order 4. This is our first example of a finite field which does not have prime order.

The reason why we obtained a field when taking the quotient by $\langle x^2+x+1\rangle$ but not when taking the quotient by $\langle x^2+1\rangle$ is the following. It is the analogue of the fact that $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is prime (equivalently irreducible) in $\mathbb{Z}$.

Proposition 12.3.2. *Let F be a field and let $p(x) \in F[x]$ be nonzero. We have that $F[x]/\langle p(x)\rangle$ is a field if and only if $p(x)$ is irreducible in $F[x]$.*

Proof. Let $p(x) \in F[x]$ be nonzero. Since F is a field, we know that $F[x]$ is a PID. Using Proposition 12.2.14 and Theorem 10.5.5, we conclude that

$$\begin{aligned}F[x]/\langle p(x)\rangle \text{ is a field} &\Longleftrightarrow \langle p(x)\rangle \text{ is a maximal ideal of } F[x] \\ &\Longleftrightarrow p(x) \text{ is irreducible in } F[x]\end{aligned}$$

□

When $F = \{0,1\}$ as above, we see that x^2+1 is not irreducible (since 1 is a root of $x^2+1 = (x+1)(x+1)$) but x^2+x+1 is irreducible (because it has degree 2 and neither 0 nor 1 is a root). Generalizing the previous constructions, we get the following.

Proposition 12.3.3. *Let F be a finite field with k elements. If $p(x) \in F[x]$ is irreducible and $\deg(p(x)) = n$, then $F[x]/\langle p(x)\rangle$ is a field with k^n elements.*

Proof. Since $p(x)$ is irreducible, we know from the previous proposition that $F[x]/\langle p(x)\rangle$ is a field. Since $\deg(p(x)) = n$, we can represent the elements of the quotient uniquely by elements of the form

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1x + a_0}$$

where each $a_i \in F$. Now F has k elements, so we have k choices for each value of a_i. We can make this choice for each of the n coefficients a_i, so we have k^n many choices in total. □

It turns out that if $p \in \mathbb{N}^+$ is prime and $n \in \mathbb{N}^+$, then there exists an irreducible polynomial in $\mathbb{Z}/p\mathbb{Z}[x]$ of degree n, so there exists a field of order p^n. However, directly proving that such polynomials exist is nontrivial. It is also possible to invert this whole idea by first proving that there exists fields of order p^n, working to understand their structure, and then using these results to prove there there exist irreducible polynomials in in $\mathbb{Z}/p\mathbb{Z}[x]$ of each degree n. In addition, we will prove every finite field has order some prime power, and any two finite fields of the same order are isomorphic, so this process of taking quotients of $\mathbb{Z}/p\mathbb{Z}[x]$ by irreducible polynomials suffices to construct all finite fields (up to isomorphism).

Finally, we end this section with one way to construct the complex numbers. Consider the ring $\mathbb{R}[x]$ of polynomials with real coefficients. Let $p(x) = x^2 + 1$ and notice that $p(x)$ has no roots in $\mathbb{R}$ because $a^2 + 1 \geq 1$ for all $a \in \mathbb{R}$. Since $\deg(p(x)) = 2$, it follows that $p(x) = x^2 + 1$ is irreducible in $\mathbb{R}[x]$. From above, we conclude that $\mathbb{R}[x]/\langle x^2 + 1\rangle$ is a field. Now elements of the quotient are represented uniquely by $\overline{ax + b}$ for $a, b \in \mathbb{R}$. We have $\overline{x^2 + 1} = \overline{0}$, so $\overline{x^2} + \overline{1} = \overline{0}$ and hence $\overline{x^2} = \overline{-1}$. It follows that $\overline{x}^2 = \overline{-1}$, so $\overline{x}$ can play the role of "i". Notice that for any $a, b, c, d \in \mathbb{R}$ we have

$$\overline{ax + b} + \overline{cx + d} = \overline{(a + c)x + (b + d)}$$

and

$$\begin{aligned}
\overline{ax + b} \cdot \overline{cx + d} &= \overline{acx^2 + (ad + bc)x + bd} \\
&= \overline{acx^2} + \overline{(ad + bc)x} + \overline{bd} \\
&= \overline{ac} \cdot \overline{x^2} + \overline{(ad + bc)x} + \overline{bd} \\
&= \overline{ac} \cdot \overline{-1} + \overline{(ad + bc)x} + \overline{bd} \\
&= \overline{(ad + bc)x + (bd - ac)}.
\end{aligned}$$

Notice that this multiplication is the exact same as when you treat the complex numbers as having the form $b + ai$ and "formally add and multiply" using the rule that $i^2 = -1$. One advantage of our quotient construction is that we do not need to verify all of the field axioms. We get them for free from our general theory.