Abstract Algebra

Andreas Tsantilas
Professor Fengbo Hang

Fall, 2020

Contents

1 Sets and Functions

1.1 Sets

Naively, we can understand a "set" to simply mean something which contains unique objects. For instance,

$$\{1, 3, 4, 8, 6\}$$

is a set. Note that the contents of this set do not have to be in any particular order, and can be rearranged without distrubing the uniqueness of the set. That is, the set $\{1, 2, 3, 4\}$ is equivalent to the set $\{4, 1, 2, 3, 3\}$. A set is considered a type of object, so it is meaningful to talk about sets within sets.

For finite sets, it may suffice to put each object down in writing. For infinite sets, we are allowed to define a set that contains everything that obeys a certain property P:

$$A = \{x : P(x)\}.$$

If P is the property that $x > 0$, we have the set of positive numbers (the colon is to be read as "such that"). If x is contained in the set A, we call x and *element* or *member* of A, and denote it by the expression

$$x \in A.$$

Similarly, if x is not in A, we write

$$x \notin A.$$

This leads rise to the notion of set equality:

Definition 1.1.1 (Set equality)**.** A set A is equal to a set B if they have the same elements. That is $A = B$ if and only if whenever $x \in A$, $x \in B$, and whenever $y \in B$, $y \in A$.

We also have notions of combining sets, and finding common elements.

Definition 1.1.2 (Union and Intersection)**.** For sets A and B, we define the *union* of A and B to be

$$A \cup B = \{x : x \in A \text{ or } x \in B\}$$

and the *intersection* of A and B to be

$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$

This definition of sets extends easily into multiple, and perhaps infinitely many, sets. If $\mathcal{A} = \{A_1, A_2, \dots\}$ is a set of sets, then we define

$$\cup\mathcal{A} = \bigcup_{n=1}^{\infty} A_n = \{x : x \in A_i \text{ for some } A_i \in \mathcal{A}\}$$

and

$$\cap\mathcal{A} = \bigcap_{n=1}^{\infty} A_n = \{x : x \in A_i \text{ for every } A_i \in \mathcal{A}\}$$

Sets do not necessarily have to contain elements. We are free to define the *empty set*:

Definition 1.1.3 (Empty Set)**.** There exists a set $\emptyset$ known as the *empty set*. This set contains no elements; that is, for every x we have $x \notin \emptyset$. Moreover, this set is unique; if we have $\emptyset$ and another empty set $\emptyset'$, it follows from the contrapositive of Definition 1.1 that $\emptyset = \emptyset'$.

Certain sets appear to be larger than other sets. From this, we can describe the notion of subsets.

Definition 1.1.4 (Subset)**.** A set A is a *subset* of a set B, denoted $A \subseteq B$, if for any object x,

$$x \in A \Rightarrow x \in B.$$

If $A \subseteq B$ but $A \neq B$, then we say that A is a *proper subset* of B and we denote it $A \subset B$.

Definition 1.1.5 (Set Difference)**.** If A and B are sets, the *difference* of A and B is

$$A \setminus B = \{x : x \in A \text{ and } x \notin B\}.$$

For instance, if $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$, then $A \setminus B = \{1\}$.

Sometimes, if we are working with sets which are all subsets of a larger set U, we typically call U the *universe* in which we are working. When we work with sets of integers, U could be the set of all integers, $\mathbb{Z}$. If we are working in a fixed universe U, then it makes sense to define complements.

Definition 1.1.6. We define the *complement* A' (sometimes A^c or $\bar{A}$) of A by

$$A' = U \setminus A$$

We can now state the basic properties of sets, all of which may be proven from the definitions given in this section:

Claim (Properties of Sets)**.** Let A, B, C be sets and let X be a set containing A, B, C as subsets. Then the following properties hold:

1. $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$.
2. $A \cup X = X$ and $A \cap X = A$.
3. $A \cup A = A$ and $A \cap A = A$.
4. $A \cup B = B \cup A$ and $A \cap B = B \cap A$.
5. $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$.
6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (B \cup C)$.
7. $A \cup (X \setminus A) = X$ and $A \cap (X \setminus A) = \emptyset$.
8. $(A \cup B)' = A' \cap B'$, and $(A \cap B)' = A' \cup B'$.

Oftentimes in math, it is useful to consider the set of all possible subsets of a set X.

Definition 1.1.7 (Power Set)**.** The power set of X is the set of all possible subsets of X (including $\emptyset$ and X itself). It is denoted by

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

or sometimes by 2^X.

1.2 Relations

Foremost, we introduce the notion of an ordered pair, and equality between ordered pairs.

Definition 1.2.1 (Ordered Pair)**.** An *ordered pair* is an object of the form

$$(x, y)$$

which can equivalently be expressed in set-theoretic notation as

$$(x, y) \equiv \{\{x\}, \{x, y\}\}.$$

Two ordered pairs (x, y) and (x', y') are considered to be equal if and only if their components match. That is,

$$(x, y) = (x', y') \Leftrightarrow x = x' \text{ and } y = y'$$

Notice how the set theoretic expression has an element dedicated to defining the first element, and an element defining the second element in the pair.

Given two sets A and B, we can construct a new set consisting of ordered pairs of their elements.

Definition 1.2.2 (Cartesian Product)**.** Given two sets A and B, we define their Cartesian Product $A \times B$ to be:

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}.$$

We define the Cartesian Product of n sets to be

$$A_1 \times \cdots \times A_n = \{(a_1 \dots a_n) : a_i \in A_i\}.$$

The Cartesian Product of a set A with itself n times is often denoted

$$A^n = A \times \cdots \times A.$$

An ordered list of n objects is known as an n-tuple. This notion is consistent with the idea of vectors of the form $(x, y, z) \in \mathbb{R}^3$; each "slot" of the vector is an element of $\mathbb{R}$, and the order in which the components of a vector are listed matter.

Given this notion of Cartesian Products, we would like to be able to relate elements of a set X to one another.

Definition 1.2.3 (Relation)**.** A *relation* R on X is a subset of $X \times X$.

$$R \subseteq X \times X.$$

We say for $x, y \in X$ that xRy, or x is related to y, whenever

$$xRy \Leftrightarrow (x, y) \in R.$$

For instance, we can think of "greater than" to be a relation defined on $\mathbb{R} \times \mathbb{R}$. Thus, R will consist of ordered pairs (x, y) such that $x > y$. However, note that (y, x) and (x, x) are not an elements of R. Particularly interesting in math are relations which satisfy certain properties and can be thought of as a generalization of equality.

Definition 1.2.4 (Equivalence Relation)**.** The relation R on a set X is an equivalence relation on A if the following are satisfied:

1. $(x, x) \in R$ for all $x \in X$.
2. $(a, b) \in R \Leftrightarrow (b, a) \in R$.
3. $(a, b) \in R$ and $(b, c) \in R \Rightarrow (a, c) \in R$.

For a general binary relation $\sim$ on X, $\sim$ is an equivalence relation if for all $x, y, z \in X$:

1. $x \sim x$
2. $x \sim y \Rightarrow y \sim x$
3. $x \sim y$ and $y \sim z \Rightarrow x \sim z$.

These properties are called reflexivity, symmetry, and transitivity, respectively.

Definition 1.2.5 (Equivalence Class)**.** If X is a set and $\sim$ is an equivalence relation, then the *equivalence class* of x, denoted $[x]$, is

$$[x] := \{y \in X : x \sim y\}$$

Claim (Properties of Equivalence Classes)**.** The following are properties of equivalence classes. For a set X, a relation $\sim$, and $x_1, x_2 \in X$, the following are true:

1. $[x_1] = [x_2] \Leftrightarrow x_1 \sim x_2$.
2. $[x_1] \cap [x_2] \neq \emptyset \Leftrightarrow [x_1] = [x_2]$.

Proof. We will now prove both of these claims:

1. Since $x_1 \in [x_1]$, that implies $x_1 \in [x_2]$ since the sets are equal. Therefore $x_1 \in [x_2]$. For the backwards direction, we suppose $y \in [x_1]$. By transitivity, $y \sim x_1$ and $x_1 \sim x_2$ imply $y \sim x_2$, so $y \in [x_2]$. Since $y \in [x_1] \Rightarrow y \in [x_2]$, $[x_1] \subseteq [x_2]$. By symmetry, we can arrive at a similar conclusion for $[x_2] \subseteq [x_1]$, so $[x_1] = [x_2]$.
2. If we pick an $x_3 \in [x_1] \cap [x_2]$, that means $x_3 \sim x_1$ and $x_3 \sim x_2$, so $x_1 \sim x_2$ from transitivity, and their equivalence classes are equal. For the backwardsd direction, it is clear that equality between the calsses implies a nonempty intersection.

□

These equivalence classes form subsets of X, and seem to be either equal or completely disjoint. This leads to the notion of a partition.

Definition 1.2.6 (Partition)**.** A partition P on a set X is a subset of $\mathcal{P}(X)$ such that the following properties hold:

1. For all $A \in P$, $A \neq \emptyset$,
2. For all $A, B \in P$, $A \neq B \Rightarrow A \cap B = \emptyset$, and
3. $\bigcup_{A \in P} A = X$.

In plain English, it is a collections of disjoint subsets of X whose union equals X.

Definition 1.2.7 (Quotient Set of a Relation)**.** The *quotient set of the set X by a relation $\sim$* is denoted $X/\sim$ and is given by:

$$X/\sim := \{[x] : x \in X\}.$$

Note that $X/\sim \subset \mathcal{P}(X)$.

We will now demonstrate that the set of all equivalence classes given by $\sim$ form a very natural way to partition the set X. Indeed, all an equivalece relation is is a partition on X, and all a partition is is an equivalence relation.

Theorem 1.2.1 (The Quotient Set is a Partition)**.** Partitions and equivalence relations are equivalent. That is, every partition denotes an equivalence relation, defined by

$$x \sim y := \exists A \in P : x, y \in A,$$

and every equivalence relation $\sim$ forms a set $X/\sim$ that is a partition on X.

Proof. We show that every Partition is an equivalence relation, as defined in the previous theorem.

1. $x \sim x$, since we know from condition 3 of Definition 1.2.6 that there is an $A : x \in A$.
2. $x \sim y \Rightarrow \exists A \in P : x, y \in A \Rightarrow y \sim x$.
3. $x \sim y \Rightarrow \exists A \in P : x, y \in A$. $y \sim z \Rightarrow \exists B \in P : y, z \in B$. Therefore, $A \cap B \neq \emptyset$ so from condition 2, $A = B$. Therefore $x, z \in A$ so $x \sim z$.

Now we will demonstrate how the quotient set $X/\sim$ satisfies all 3 parts of Definition 1.2.6.

1. Clearly, $[x] \in X/\sim \neq \emptyset$ for all x, since $x \in [x]$.
2. Condition 2's contrapositive is $A \cap B \neq \emptyset \Rightarrow A = B$, which was proved previously.
3. Suppose $S = \bigcup_{[x] \in X/\sim} [x] \neq X$. Then that implies the existence of an $x' \notin S$. But since $x' \sim x'$, $[x'] \in X/\sim$, so it is in S.

□

1.3 Functions

Definition 1.3.1 (Function)**.** A *function* from a set X to a set Y is a subset f of $X \times Y$ such that

1. If $(x, y), (x, y') \in f$, then $y = y'$ and
2. If $x \in X$, then $(x, y) \in f$ for some $y \in Y$.

If $(x, y) \in f$, we define $f(x)$ to equal y. The first condition ensures that each element in x can be associated with a unique element in Y, and the second stipulates that f "captures" every element of X. Two functions $f : X \to Y$ and $g : X \to Y$ are said to be equal if and only if $f(x) = g(x)$ for every $x \in X$.

From the definition of a relation as a subset of $X \times Y$, functions are a special kind of relation.

Notation (Function)**.** If a function f is a subset of $X \times Y$, then we write

$$f : X \to Y$$

to denote the function f from X to Y. This notation can be used for any mapping from X to Y, but f almost always denotes a function.

Remark (Quotient Map)**.** Given a set X and a relation $\sim$, we call

$$\begin{aligned} \pi : X &\to X/\sim \\ : x &\mapsto [x] \end{aligned}$$

a quotient map.

Definition 1.3.2 (Image)**.** If $f : X \to Y$, and $S \subseteq X$, then we define the *image of S under f*, denoted $f(S)$, as

$$f(S) := \{f(x) : x \in S\}.$$

Definition 1.3.3 (Onto)**.** A function $f : X \to Y$ is said to be *onto* if

$$f(X) = Y.$$

That is, for every $y \in Y$, $y = f(x)$ for some $x \in X$. This condition is sometimes known as "surjectivity."

Definition 1.3.4 (One-to-one)**.** A function $f : X \to Y$ is said to be *one-to-one* if

$$x \neq x' \Rightarrow f(x) \neq f(x')$$

or, equivalently,

$$f(x) = f(x') \Rightarrow x = x'.$$

That is, different inputs have different outputs. This condition is sometimes known as "injectivity."

Definition 1.3.5 (Bijectivity)**.** A function $f : X \to Y$ is said to be *bijective* if it is both one-to-one and onto.

Definition 1.3.6 (Inverse of f)**.** If $f : X \to Y$ is a one-to-one function such that $f(X) = B \subseteq Y$, then we define the *inverse* of f denoted f^{-1}, where

$$f^{-1} : B \to X$$

such that

$$(y, x) \in f^{-1} \Leftrightarrow (x, y) \in f.$$

Definition 1.3.7 (Function Composition)**.** Given functions $f : X \to Y$ and $g : Y \to Z$, we define the *composition of g and f* to be

$$(g \circ f) : X \to Z$$

where

$$(g \circ f)(x) = g(f(x)).$$

2 The Integers

2.1 Constructing the Integers with Peano Arithmetic

Maybe omit?

2.2 Division Algorithms

Having constructed the integers, we can apply our familiar notions of division to them. Given a and $b \neq 0$, we may divide a by b to get a non-negative remainder r which is smaller than b. This intuitive notion can be summarized with the following theorem:

Theorem 2.2.1 (Division Algorithm)**.** Let a, b be integers, with $b \neq 0$. Then there exist unique integers q and r such that

$$a = bq + r \tag{2.2.1}$$

where $0 \leq r < b$.

Proof. proof here!!!! □

Definition 2.2.1 (Divisor, Common Divisor)**.** We say that $b \neq 0$ is a *divisor* a if $a = bk$ for some $k \in \mathbb{Z}$. We denote this

$$b|a$$

and read it as "b divides a." Note that this expression has a boolean output; that is, it is either true or false.

We say that an integer $d \neq 0$ is a *common divisor* of a and b if

$$d|a \text{ and } d|b$$

For any pair of integers, there is a common divisor that is larger than all others. This is an important concept.

Definition 2.2.2 (Greatest Common Divisor)**.** The *greatest common divisor* of two nonzero integers a and b is the positive integer d such that d is a divisor of a and b, and for and divisor d' of a and b, $d'|d$.

With this idea in mind, we can define the function $\gcd : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ which outputs the greatest common divisor of the given inputs.

Theorem 2.2.2 (gcd Theorem)**.** For nonzero integers a and b, then there exist integers m and n such that

$$\gcd(a, b) = ma + nb. \tag{2.2.2}$$

Moreover, the greatest common divisor is unique.

Proof. Proof here!!!!! □

Definition 2.2.3 (Relatively Prime)**.** We say two integers a and b are relatively prime if

$$\gcd(a, b) = 1. \tag{2.2.3}$$

From theorem 2.2.2, we can equivalently assert that if a and b are relatively prime, then there exist m and n such that

$$ma + nb = 1. \tag{2.2.4}$$

Another way to say this is that a and b share no factors in common.

With this in mind, Euclid formulated a procedural way to determine the greatest common divisor.

2.3 Prime Numbers

One of the most important concepts in all of mathematics is primality and prime numbers. Simply put, a prime number is a positive number not equal to 1 that can only be divided by 1 and itself.

Definition 2.3.1 (Prime Number)**.** An integer $p > 1$ is considered prime if its only divisors are ± 1 and $\pm p$.

Theorem 2.3.1. If a prime p divides the product ab, then $p|a$ or $p|b$.

Proof. Suppose p does not divide a. Then we will show that $p|b$. From equation (2.2.1), we have that

$$ab = qp$$

and because p does not divide a, $\gcd(p, a) = 1$. This is because the only factors of p are 1 and p, and we know that p and a don't share p in common, otherwise $p|a$. That means there are integers m and n such that

$$ma + np = 1.$$

Multiplying by b,

$$mab + nbp = b$$

into which we may substitute for ab:

$$mqp + nbp = b.$$

Notice how we get the equation

$$b = (mq + nb)p$$

therefore $p|b$, as desired. And by symmetry, if p divides ab but p does not divide b, then $p|a$. □

What follows is an important theorem in number theory.

Theorem 2.3.2 (Fundamental Theorem of Arithmetic)**.** Let n be an integer such that $n > 1$. Then

$$n = p_1 p_2 \cdots p_k \tag{2.3.1}$$

where $p_{1 \le i \le k}$ are prime numbers not necessarily distinct. Furthermore, this factorization is unique up to arrangement. If

$$n = q_1 q_2 \cdots q_l$$

where $q_{1 \le i \le k}$ are prime, then $l = k$ and for every p_i there is a unique corresponding q_j such that $p_i = q_j$. That is, the q_i's can be rearranged.

Proof. The proof proceeds by the principle of strong induction on n. Clearly, $n = 2$ is a product of primes, since 2 is prime. Now suppose the property holds for all integers r such that $1 < r < n$. If n is prime, then of course it is a product of primes. If it is not prime, then it can be written in the form $n = uv$, where uv are strictly less than n. Due to the principle of strong induction, $u = p_1^u \cdots p_m^u$ and $v = p_1^v \cdots p_l^v$. Therefore n is the product of these primes.

Next, we must prove that this factorization is unique for n. Again, we use strong induction. Clearly, for $n = 2$ there is only one way to decompose n into primes. Now assume that this uniqueness holds for all r in $1 < r < n$, and

$$n = p_1 \cdots p_k = q_1 \cdots q_l$$

where $p_1 \le p_2 \le \cdots \le p_k$ and $q_1 \le q_2 \le \cdots \le q_l$. By Theorem 2.3.1, we know that $p_1|q_i$ for some i such that $1 \le i \le l$, and $q_1|p_j$ for some j such that $1 \le j \le k$. Since all the p's and q's are prime, $p_1 = q_i$ and $q_1 = p_j$. Therefore, $p_1 = q_1$ since $p_1 \le p_j = q_1 \le q_i = p_1$. By the induction hypothesis,

$$n' = p_2 \cdots p_k = q_2 \cdots q_l$$

has a unique factorization. Thus $k = l$ and $q_i = p_i$ for $1 \le i \le k$. □

One might rightly ask how many primes there are. Since there are an infinite amount of numbers, one might reasonably expect there to be infinite primes.

Theorem 2.3.3 (Infinite Primes)**.** There exist an infinite number of primes.

Proof. Suppose there were a finite number of primes, $\{p_1, \ldots, p_k\}$, where p_k is the largest prime. Then consider the following number

$$Q = p_1 \cdots p_k + 1$$

If Q is prime, then we have found a prime larger than p_k, and so we have a contradiction. If Q is not prime, then because of the fundamental theorem of arithmetic, there must be a p such that $p|Q$. But because p is in $p_{1 \leq i \leq k}$, that means that p must divide $Q - p_1 \cdots p_k = 1$, which is impossible. Therefore we have found a prime p that is not in the original list of primes, so we contradict the premise that the primes may be contained in a finite list. Therefore, there are an infinite number of primes. □

2.4 Modular Arithmetic

When we divide numbers, sometimes we are left with a remainder r. We can group numbers together if, when divided by a number n, they share the same r. This is an equivalence relation.

Definition 2.4.1 (Congruence Modulo n)**.** Let $n > 0$ be a fixed integer. We say two integers a and b are equivalent modulo n if $n|(a - b)$. Note how this is equivalent to saying that a and b have the same remainder r when divided by n. This is called *congruence modulo* n and is denoted by

$$a \equiv b \pmod{n}.$$

Lemma 2.4.1. The basic properties of this congruence are as follows:

1. Congruence modulo n defines an equivalence relation on the set of integers.
2. This relation has n distinct equivalence classes.
3. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.
4. If $ab \equiv ac \pmod{n}$, and a is relatively prime to n, then $b \equiv c \pmod{n}$.

Theorem 2.4.2 (Fermat's Little Theorem)**.** If p is a prime number, then for any integer a,

$$a^p \equiv a \pmod{p}. \tag{2.4.1}$$

Proof. The proof proceeds by induction on a. For $a = 0$, it is trivial that $0^p \equiv 0 \pmod{p}$. Suppose the identity holds for a. Then we can expand the expression

$$(a + 1)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} + 1.$$

However, notice how the middle terms each have a factor of p from the binomeal coefficient (since p is prime, it cannot be divided by the terms in the denominator). And by the induction hypothesis, since $a^p \equiv a \pmod{p}$, and $1 \equiv 1 \pmod{p}$, modulo p the expression becomes

$$(a + 1)^p \equiv a + 1 \pmod{p},$$

completing the proof. □

3 Groups

Having taken care of the preliminaries, we are now able to discuss the subject of this course. By delineating very simple axioms, we get surprisingly complex algebraic structures. In a certain sense, these structures should be seen as generalizations of set operations that are already familiar to us, such as numbers, matricies, and the like.

3.1 Definitions and Lemmae

Definition 3.1.1 (Group)**.** A *group* $(G, \cdot)$ is a set G equipped with an operation $\cdot : G \times G \to G$ such that the following axioms hold:

1. (Associativity.) $a, b, c \in G$ implies that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
2. (Identity element.) There exists an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$.
3. (Inverse elements.) If $a \in G$, then there exists an $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Often times, when the operation is clear from context, we simply say G is a group and simply denote the product between a and b as ab. Moreover, notice how the second condition exlcudes the possibilty of having an empty set as a group, since there must be at least one element in a group. Lastly, the product may not necessarily commute; that is, it is not necessarily the case that $ab = ba$. We have a special name for the groups whose elements commute:

Definition 3.1.2 (Abelian Group)**.** A group G is said to be *abelian* (or *commutative*) if for every $a, b \in G$, $a \cdot b = b \cdot a$.

Groups which do not commute are called *non-abelian* or *non-commutative*. One prominent such example is the group of $n \times n$ matrices with nonzero determinants (why?) over $\mathbb{R}$, under the canonical product. This group is denoted as $GL_n(\mathbb{R})$, where $AB \neq BA$, in general.

Now, we will go over some useful lemmas.

Lemma 3.1.1. If G is a group, then the following hold:

1. The identity element in G is unique.
2. Every $a \in G$ has a unique inverse in G.
3. For every $a \in G$, $(a^{-1})^{-1} = a$.
4. For all $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof.

1. Suppose we have two identity elements, e and e'. Then by the definition of an identity, $e = e'e = e'$, so $e = e'$.
2. Suppose a had two inverses, b and c. Then $(ab)c = b(ac)$, since the inverse commutes and the product is associative. But then we get $ec = be$, so $c = b$.
3. First, we prove something stronger, which is that we can cancel from the same side in a group. That is, $ax = ay \Rightarrow x = y$. We know that each $a \in G$ has a unique inverse, so we see that $a^{-1}ax = a^{-1}ay$. By the associative law, $(a^{-1}a)x = (a^{-1}a)y$, so $ex = ey$. Therefore, by the definition of the identity element, $x = y$. In this instance, we have that $a^{-1}(a^{-1})^{-1} = e = a^{-1}a$. Multiplying on the left by a, we get that $(a^{-1})^{-1} = a$.
4. We have that $b^{-1}a^{-1}(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = e$, and that $(ab)b^{-1}a^{-1} = a(bb^{-1})a^{-1} = aea^{-1} = e$.

□

We can state the cancellation result in the following lemma.

Lemma 3.1.2 (Cancellation Laws)**.** If G is a group, then the following are true for $a, x, y \in G$:

$$ax = ay \Rightarrow x = y$$

and

$$xa = ya \Rightarrow x = y.$$

Proof. We proved the first one in the previous lemma, and the proof for the second one follows similarly. □

We now give definitions and lemmae concerning repeated applications of the product in G.

Definition 3.1.3. For a group $(G, \cdot)$, we can define a^m, where $a \in G$ and $m \in \mathbb{Z}$:

1. If $m > 0$, then $a^m := a \cdot a \cdot \ldots \cdot a$, (i.e., a composed with itself m times).
2. If $m = 0$, then $a^m := e$.
3. If $m < 0$, then $a^m := (a^{-1})^{|m|}$.

It should be verified that $a^k a^\ell = a^{k+\ell}$, and that $(a^k)^\ell = a^{k\ell}$.

Now we define operations on subsets of groups.

Definition 3.1.4 (Subset Operations)**.** Let $A, B, C \subseteq G$. Then we define the following sets:

$$A \cdot B = \{a \cdot b : a \in A, b \in B\}.$$

$$A^{-1} = \{a^{-1} : a \in A\}.$$

It should be verified that the following properties hold:

1. $A(BC) = (AB)C$,
2. $(A^{-1})^{-1} = A$
3. $(AB)^{-1} = B^{-1}A^{-1}$.

3.2 Subgroups

Much like a set has subsets, or vector space has subspaces, a group has a smaller groups contained within it.

Definition 3.2.1 (Subgroup)**.** We say that H is a subgroup of $(G, \cdot)$ if

1. $H \subseteq G$, and
2. H is a group under the product in G.

Immediately from this definition, we know that every group G has at least two subgroups, known as the "trivial" subgroups. These are $\{e\}$ and G itself. Now we introduce the following lemma, which can serve as a criterion for determining whether H is a subgroup of G.

Lemma 3.2.1 (Subgroup Criteria)**.** A *nonempty* subset H of G is a subgroup of G if and only if

1. (Inverse Elements.) $a \in H \Rightarrow a^{-1} \in H$.

2. (Closure.) $a, b \in H \Rightarrow ab \in H$.

Proof. The hypothesis that H is nonempty is very important, since otherwise all the statements are vacuously true; but since $\emptyset$ does not contain an identity element, $\emptyset$ is not a subgroup. Now we prove the above.

If H is a subgroup of G, then clearly 1 and 2 hold.

Suppose 1 and 2 hold. Then all that needs to be verified is that the associative law holds and that $e \in H$. But since $H \subseteq G$, and the associative law holds for every element G, then clearly it holds for every element in H. Moreover, since $a \in H$, then from 1, $a^{-1} \in H$. From 2, we also see that $aa^{-1} = e \in H$, which completes the proof. □

These two criteria can be condensed down into one pithy requirement, namely that for a nonempty subset H of G, $a, b \in H \Rightarrow ab^{-1} \in H$. Moreover, if H is finite and nonempty, then all that needs to be shown is that H is closed under multiplication.

Notation. If H is a subgroup of G, then we denote it by

$$H \leq G.$$

Lemma 3.2.2 (Subgroup Intersection)**.** Suppose $\forall \alpha \in \Lambda$, $H_\alpha \leq G$. Then

$$S = \bigcap_{\alpha \in \Lambda} H_\alpha \leq G.$$

Proof. In order to show this is a subgroup, we invoke the subgroup critera lemma. Clearly, this is nonempty since $e \in H_\alpha$ for all $\alpha \in \Lambda$, so $e \in S$. Now we use the criterion that $x, y \in H \Rightarrow xy^{-1} \in H$ is equivalent to H is a subgroup. We have that

$$x, y \in S \Rightarrow x, y \in H_\alpha \forall \alpha \in \Lambda \Rightarrow xy^{-1} \in H_\alpha \forall \alpha \in \Lambda \Rightarrow xy^{-1} \in S.$$

Therefore, S is a subgroup of G. □

Notice how this lemma made no mention on the size of Λ, so this lemma applies to both the infinite case and all finite cases.

Claim. For a group G and a nonempty subset $A \subseteq G$, there exists a unique subgroup H of G such that

1. $A \subseteq H$
2. For $K \leq G$, if $A \subseteq K$, we have that $H \subseteq K$.

That is, for a subset A, there exists an H which is the smallest subgroup containing A, and H is unique.

Proof.

1. (Existence.) Let $\alpha \in \Lambda$, and $\forall \alpha, A \subseteq K_\alpha$. Then, from Lemma 3.2.2,

   $$H = \bigcap_{\alpha \in \Lambda} K_\alpha.$$

   This satisfies property 1, since for all $\alpha, A \subseteq K_\alpha$ so $A \subseteq H$. Moreover, since we took the intersection of all the K such that $A \subseteq K$, then since H is their intersection, $H \subseteq K_\alpha \forall \alpha \in \Lambda$, so property 2 is satisfied. Moreover, H is a subgroup by Lemma 3.2.2.

2. (Uniqueness.) Suppose H and H' are two sets satisfying the above property. Then from property 2, $H \subseteq H'$ since $A \subseteq H'$. However, we also have that $H' \subseteq H$. Therefore $H = H'$.

□

3.3 Cyclic Groups

Definition 3.3.1 (Subgroup Generated by a Set)**.** Given $A \neq \emptyset$ and $A \subseteq G$, we define the subgroup generated by A to be

$$\langle A \rangle = \{a_1^{m_1} a_2^{m_2} \cdots : a_i \in A, m_i \in \mathbb{Z}\}.$$

This is the smallest subgroup of G containing A.

Proof. Clearly, $\langle A \rangle$ is a group containing A. Therefore, $H \subseteq \langle A \rangle$.

Next, we see that if $A \subseteq H \leq G$, then $\langle A \rangle$. Since H contains A, we know that $a_1 \in H$. However, since H is a group, we have that $a_1^k \in H, \forall k \in \mathbb{Z}$. This holds for all elements $a_i \in A$, so $a_1^{m_1}, \ldots, a_i^{m_i} \in H$. Since H is a group, then it must be closed under product. Therefore, we have $a_1^{m_1} a_2^{m_2} \cdots \in H$ for all $m_i \in \mathbb{Z}$. However, this is just $\langle A \rangle$. Therefore, $\langle A \rangle \subseteq H$.

Thus $H = \langle A \rangle$. □

Notation. If we want to find the group generated by the singleton $\{a\}$, then we write

$$\langle a \rangle := \langle \{a\} \rangle.$$

Definition 3.3.2 (Cyclic Group)**.** Let G be a group. Then we say G is *cyclic* if $\exists a \in G : G = \langle a \rangle$. We also say that a *generates* G. We also define the *order* of a, sometimes denoted $o(a)$, to be the smallest positive integer n such that

$$a^n = e.$$

We then say $|a| = n$ if n is finite, and if n is infinite we say $|a| = \infty$.

Theorem 3.3.1 (Cyclic Groups are Abelian)**.** If G is a cyclic group generated by a, then it is abelian.

Proof. We have that for any two elements $x, y \in G$, that $x = a^r$ and $y = a^s$. Therefore,

$$xy = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = yx.$$

□

Theorem 3.3.2 (Subgroup of a Cyclic Group)**.** Let $H \leq G$, and G be a cyclic group generated by a. Then any subgroup of G is cyclic.

Proof. Let $\langle a \rangle$ be the parent cyclic subgroup, and let H be our subgroup. Let k be the smallest positive integer such that $a^k \in H$. Because H is a subgroup, H is closed under the product. Thus, we have

$$a^{nk} \in H, n \in \mathbb{Z}.$$

Now suppose there were an element $a^\ell \in \langle a \rangle$ such that $a^\ell \neq a^{nk}$ for all $n \in \mathbb{Z}$. Then by the division algorithm, there exists an $q \in \mathbb{Z}$ such that

$$\ell = kq + r, \text{ where } 0 < r < k.$$

Therefore, we have that

$$a^\ell = a^{kq} a^r.$$

Again, because H is closed, this implies that $a^r \in H$. But since $0 < r < k$, that would contradict the premise that k is the smallest positive integer such that $a^k \in H$. Therefore, all elements in H are generated by a^k, so

$$H = \langle a^k \rangle$$

so H is cyclic. □

Corollary 3.3.3. All subgroups of $(\mathbb{Z}, +)$ are cyclic, and can be expressed as $H = n\mathbb{Z}$ for $n \in \mathbb{N}$.

3.4 Homomorphisms

Just like we have maps from sets to sets, or linear transformations from one vector space to another, we would like to be able to relate groups to one another. We can do this by using special maps called homomorphisms.

Definition 3.4.1 (Homomorphism)**.** Let G and H be groups. Let $\phi : G \to H$ such that $\forall x, y \in G$,

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

Then, we refer to ϕ as a homomorphism (sometimes "group" homomorphism) from G to H. Moreover, we denote the following set to be the set of all homomorphisms from G to H:

$$\hom(G, H) = \{\phi : \phi : G \to H, \text{ and } \phi(xy) = \phi(x)\phi(y) \forall x, y \in G\}.$$

It should be noted that the product between x and y in $\phi(xy)$ denotes the product in G, and $\phi(x)\phi(y)$ is actually a product between two elements in H.

Example. Let G be a group. Then we have that $\phi : (\mathbb{Z}, +) \to (G, \cdot)$ where $x \mapsto a^x$ for some x is a homomorphism, since $\phi(x + y) = a^{x+y} = a^x \cdot a^y = \phi(x) \cdot \phi(y)$.

Example. The determinant of a matrix is a homomorphism from $GL_n(\mathbb{R}) \to \mathbb{R}^* = \mathbb{R} \setminus \{0\}$. This is true since

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

Definition 3.4.2 (Isomorphism)**.** If a homomorphism ϕ is bijective, then it is known as an isomorphism.

Lemma 3.4.1 (Properties of Homomorphisms)**.** Let $\phi : G \to H$ be a homomorphism. Then

1. $\phi(e_G) = e_H$.
2. $\phi(a^m) = \phi(a)^m$.
3. $\phi(a^{-1}) = \phi(a)^{-1}$.

Proof.

1. $\phi(e_G x) = \phi(e_G)\phi(x) = \phi(x)$. Therefore, $\phi(e_G)$ is the identity element in H, or e_H.
2. We have that $\phi(a^m) = \phi(aa \cdots a) = \phi(a)\phi(a) \cdots \phi(a)$, where the product is repeated m times. Therefore, $\phi(a)\phi(a) \cdots \phi(a) = \phi(a)^m$ since this is just a repeated product in H.
3. $\phi(aa^{-1}) = \phi(e_G) = e_H = \phi(a)\phi(a^{-1})$. Therefore, $\phi(a^{-1}) = \phi(a)^{-1}$.

□

Lemma 3.4.2. Let $\phi \in \hom(G, H)$, and let $A, B \subseteq G$. Then

1. $\phi(AB) = \phi(A)\phi(B)$.
2. $\phi(A^{-1}) = \phi(A)^{-1}$.

Proof.

1. $\phi(AB) = \{\phi(ab) : a \in A, b \in B\} = \{\phi(a)\phi(b) : a \in A, b \in B\} = \phi(A)\phi(B)$.
2. $\phi(A^{-1}) = \{\phi(a^{-1}) : a \in A\} = \{phi(a)^{-1} : a \in A\} = \phi(A)^{-1}$.

□

Now we will prove a lemma about the image of subgroups under homomorphisms.

Lemma 3.4.3 (Subgroups and Homomorphisms)**.** Suppose $\phi \in \hom(G, H)$, and that $K \leq G$ and $L \leq H$. Then

1. $K \leq G \Rightarrow \phi(K) \leq H$
2. $L \leq H \Rightarrow \phi^{-1}(H) \leq G$.

Proof.

1. We have that $K \neq \emptyset \Rightarrow \phi(K) \neq \emptyset$. Suppose we have $x, y \in \phi(K)$. Then that means that $x = \phi(a)$ and $y = \phi(b)$ for some $a, b \in K$. Now we use the subgroup criterion to show that $xy^{-1} \in \phi(K)$. But we have that $ab^{-1} \in K$ so $\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = xy^{-1} \in \phi(K)$. So $\phi(K) \leq H$.
2. Clearly, $\phi^{-1}(H)$ is nonempty, since $e_H \in L$ so $\phi^{-1}(e_H) = e_G$, so $e_G \in \phi^{-1}(L)$. Now we use the subgroup criterion. If $a, b \in \phi^{-1}(L)$, this implies that $\phi(a), \phi(b) \in L$. therefore, $\phi(a)\phi(b)^{-1} \in L$, so $\phi(ab^{-1}) \in L$. Therefore, $ab^{-1} \in \phi^{-1}(L)$. Therefore, $\phi^{-1}(L) \leq G$.

□

Due to the previous lemma, we have that $\phi(G) \leq H$. We sometimes call this the *image of G under ϕ*. That is, we write that $\phi(G) = \text{Im}(\phi)$. Moreover, we have that since $\{e\} \leq H$, $\phi^{-1}(\{e\}) \leq G$. This subgroup has a special name.

Definition 3.4.3 (Kernel)**.** Let $\phi \in \hom(G, H)$. Then we say the *kernel* of ϕ is simply the set of all $a \in G$ such that $\phi(a) = e$.

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

The kernel of G is a subgroup of G by the previous lemma.

Example. We know that $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$. We have that $\text{Im}(\det) = \mathbb{R}*$, and $\ker(\det) = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\} = SL_n(\mathbb{R})$. Therefore, $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$.

We have a natural homomorphism $\phi \in \hom(\mathbb{Z}, G) : k \mapsto a^k$ for some $a \in G$. Therefore, $\Im(\phi) = \{a^k : k \in \mathbb{Z}\}$, but this just equals the subgroup generated by a, $\langle a \rangle$. We also know that $\ker \phi \leq G$. However, we know that all subgroups of $\mathbb{Z}$ are cyclic. Therefore, $\ker \phi$ is either $\{0\}$ or $\ker \phi = n\mathbb{Z}$ for some $n \in \mathbb{N}$. In the first case, this implies that if $a^k = a^\ell$, then $a^{k-\ell} = 0$ so $k = \ell$. Thus, we have $\phi(k) = \phi(\ell) \Rightarrow k = \ell$, or ϕ is an injection. In turn, this implies that $|\{a^k : k \in \mathbb{Z}\}| = |\langle a \rangle| = \infty$.

In the second case, we have that $\ker \phi = n\mathbb{Z}$. Since $n \in \ker \phi$, we have that $a^n = 0$. If we consider the subgroup generated by a, we know that $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$. From the division algorithm, however, we have that $k = n\ell + r$, where $0 \leq r < n$, so $\langle a \rangle = \{a^r : 0 \leq r < n\}$. This is just the set of elements $\{e, a, a^2, \ldots, a^{n-1}\}$, whose elements are mutually distinct, since of $a^r = a^s$, then $n|r - s$. Since $|r - s| < n$, then $|r - s| = 0$ so $r = s$. Therefore, $|\langle a \rangle| = n$.

This suggests an alternate framing of the order of a subgroup of the integers.

Definition 3.4.4. If $a \in \mathbb{Z}$, then we can express the order of a $o(a)$ of $\langle a \rangle$ as

$$o(a) = \begin{cases} n & \text{if } \ker \phi = n\mathbb{Z} \\ \infty & \text{if } \ker \phi = \{0\}. \end{cases}$$

3.5 Lagrange's Theorem

3.5.1 The First Counting Argument

Definition 3.5.1. For a subgroup $H \leq G$, and for any element $a \in G$, we call the set

$$aH = \{ah : h \in H\}$$

a *left coset* of H in G. Similarly, a *right coset* of H in G. is $Ha = \{ha : h \in H\}$.

Lemma 3.5.1. Let G be a group and $H \leq G$. Then

$$L = \{aH : a \in G\}$$

that is, the set of left cosets of H is a partition of G. Moreover,

$$R = \{Ha : a \in G\}$$

is also a partition of G.

Proof. We will only prove this for left cosets. Suppose $\alpha \in L$. Then $\alpha = aH$ for some $a \in G$. Moreover, $\alpha \neq \emptyset$ since H is a subgroup and therefore $ae = a \in aH$. In order to show that this is a partition, we have to show that

$$G = \bigcup_{\alpha \in L} \alpha.$$

Clearly, this is the case, since $ae = a \in aH$ for all $a \in G$, therefore $G \subseteq \bigcup \alpha$. Moreover, since G is closed under the product, we have that every $aH \subseteq G$, so $\bigcup \alpha \subseteq G$. This proves that the union is equal to G.

Next, we have to show that for $\alpha, \beta \in L$, if $\alpha \cap \beta \neq \emptyset \Rightarrow \alpha = \beta$. Suppose $\alpha = aH$ and $\beta = bH$ for $a, b \in G$. If $x \in \alpha \cap \beta$, then $x = ah_1 = bh_2$ for $h_1, h_2 \in H$. This implies that $ah_1H = bh_2H$. However, $h_1H = H = h_2H$, since H is closed under multiplication. Therefore, $aH = bH$, so $\alpha = \beta$.

Therefore L is a partition on G. □

We usually denote ${}^{G}\!/_{H} = L$, which is read as G modulus H. Since every partition is an equivalence relation, then let $\sim$ be the equivalence relation of L. Then

$$x \sim y \iff \exists \alpha \in L : x, y \in \alpha \iff \exists a \in G : x, y \in aH.$$

Claim. $x \sim y \iff x^{-1}y \in H$.

Proof. First, we have that $x \sim y \Rightarrow x^{-1}y \in H$:

$$\begin{aligned} x, y \in aH &\Rightarrow x = ah_1, y = ah_2 \\ &\Rightarrow y = xh_1^{-1}h_2 \\ &\Rightarrow x^{-1}y = h_1^{-1}h_2 \in H. \end{aligned}$$

Next, we prove the reverse direction:

$$\begin{aligned} x^{-1}y \in H &\Rightarrow x^{-1}yH = H \\ &\Rightarrow xH = yH \\ &\Rightarrow x \in xH, y \in xH = yH \\ &\Rightarrow x \sim y. \end{aligned}$$

This proves the claim. □

Now we have that $G\backslash \sim = G \setminus H$, with the mapping

$$\pi : G \to G \setminus H : x \mapsto [x] = xH.$$

For right cosets, we have that $x \sim y$ if $xy^{-1} \in H$.

Claim. There is a bijection between left and right cosets.

Proof. We have that $\alpha \mapsto \alpha^{-1}$ is a bijection, since

$$\alpha = aH \Rightarrow \alpha^{-1} = H^{-1}a^{-1} = Ha^{-1} \Rightarrow \alpha^{-1} \in R.$$

□

If we have the bijection $\phi : \alpha \mapsto \alpha^{-1}$, then we can make another bijection from the set of right cosets to left cosets, namely $\psi : \beta \mapsto \beta^{-1}$. We have that

$$(\psi \circ \phi)(\alpha) = \psi(\alpha^{-1}) = \alpha = (\phi \circ \psi)(\alpha)$$

Therefore, ψ, ϕ are bijections since they have well-defined inverses, and moreover, $\phi^{-1} = \psi$. If two sets have a bijection between them, then they have the same number ov elements.

Definition 3.5.2 (Index of H)**.** Let L be the set of left cosets in G, and R be the set of right cosets. Then we define the index of H in G to be

$$[G : H] := |L| = |R|.$$

Now, let us consider the first counting argument.

Proposition 3.5.2. We have that L is a partition. Thus

$$|G| = \sum_{\alpha \in L} |\alpha|.$$

However, we know $\alpha = aH \Rightarrow |\alpha| = |H|$. This is because the map f from H to aH where $x \mapsto ax$ is a bijection. Clearly, f is one-to-one because of the cancellation law in H; it is also onto since by definition, members of aH are of the form ah for some $h \in H$. Therefore we have $ah = f(h)$ for some $h \in H$. Therefore,

$$|G| = \sum_{\alpha \in L} |\alpha| = \sum_{\alpha \in L} |H| = [G : H]|H| = |L||H|.$$

This proposition gives rise to an important theorem in group theory.

Theorem 3.5.3 (Lagrange's Theorem)**.** If G is a finite group and H is a subgroup of G, then

$$[G : H]|H| = |G|.$$

In particular, $|H|$ is a divisor of $|G|$.

Warning. Note that we cannot omit the hypothesis that G is finite from the theorem, since we can have a group of infinite order such that $|H|$ is finite; then $|H|$ does not divide $|G|$. Moreover, the converse of Lagrange's theorem is false. That is, a group G does not have to have a subgroup of order m if m divides $|G|$. Take S_4; this has no subgroup of order 6.

Lagrange's theorem also provides an interesting corollary pertaining to cyclic subgroups.

Corollary 3.5.4. If G is a finite group, then $\forall a \in G$, we have that

$$o(a)|o(G) = |G|.$$

Hence,

$$a^{|G|} = e.$$

3.5.2 The Second Counting Argument

Proposition 3.5.5. Let G be a finite group, and let $H, K \leq G$. Then

$$HK \leq G \iff HK = KH$$

where

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

Proof. The first direction is true, since we have that $(HK)^{-1} = HK = K^{-1}H^{-1} = KH$.

Next, we have that $HK = KH$. Then HK is nonempty, since $e \in HK$. Moreover, if $a, b \in HK$, then $(HK)(HK)^{-1} = HKK^{-1}H^{-1} = HKKH = HKH = HHk = HK$, so $ab^{-1} \in HK$. □

Theorem 3.5.6. Let G be a group, and $H, K \leq G$ such that H, K are finite. Then

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

Proof. FILL IN PROOF. □

Corollary 3.5.7. If G is a finite group with subgroups H, K, then if $|H| > \sqrt{|G|}$ and $|K| > \sqrt{|G|}$, then

$$\exists x \in H \cap K : x \neq e.$$

3.6 Normal Subgroups

Recall from the previous section that if we have a subgroup G, then we can define the set G/H to be the set of all left cosets of H in G, denoted L. A reasonable question to ask could be if there is any possible group structure on G/H, since as of now it is just a set.

Since L is a partition of G, then this admits a natural quotient map from G to the equivalence classes of this partition,

$$\pi : G \to G/H : a \mapsto aH.$$

We hope that this map $\pi \in \hom(G, G/H)$, in order to [WHY???]. Therefore, our task will lie in analyzing which requirements need to be put on H in order for this to occur.

Given an $h \in H$, and $a, b \in G$, and the map π is a homomorphism, we have that

$$\pi(a)\pi(b) = \pi(ah)\pi(b) = \pi(ahb) = \pi(ab),$$

since $\pi(ah) = ahH = aH$. Therefore,

$$\begin{aligned} abH &= ahbH \\ bH &= hbH \\ H &= b^{-1}hbH \\ &\Rightarrow b^{-1}hb \in H. \end{aligned}$$

In other words, $b^{-1}Hb \subseteq H$. However, this implies that $Hb \subseteq bH \Rightarrow H \subset bHb^{-1} \Rightarrow H \subseteq (b^{-1})^{-1}Hb^{-1}$, so $H \subseteq b^{-1}Hb$, so $H = b^{-1}Hb$ for all $b \in G$. In particular, we have that the left and right cosets are equal, $Hb = bH$.

Definition 3.6.1. Let G be a group, and let $N \leq G$ such that

$$gN = Ng, \ \forall g \in G.$$

Then we say that N is a normal subgroup of G, and denote it by

$$N \trianglelefteq G.$$

Corollary 3.6.1.

1. G always has two normal subgroups, $\{e\}$ and G.
2. If G is an abelian group, then every subgroup is normal.

There are multiple equivalent definitions of normality, the proofs of which will not be presented.

Theorem 3.6.2 (Equivalent Conditions for Normality)**.** That a subgroup N of G is normal is equivalent to the following. Let L be the set of all left cosets of G. For all $g \in G$ and $n \in N$,

1. $gng^{-1} \in N$
2. $gNg^{-1} \subset N$
3. $gNg^{-1} = N$
4. $gN = Ng$.
5. $\alpha, \beta \in L \Rightarrow \alpha\beta \in L$.

The last condition is extremely suggestive; it implies that the set of left cosets G/N is closed under multiplication. Therefore, a natrual question to ask would be if G/N has a group structure. The answer is indeed yes.

Theorem 3.6.3 (G/N is a Group)**.** Let G be a group and let N be a normal subgroup of G. Then the construction G/N, the group of left cosets of N, is a group under the set product. This is referred to as forming a *quotient structure*.

Proof.

1. (Identity). We claim that N is the identity element in G/N. This is clear because $\alpha = aN$, then $\alpha N = aNN = aN = \alpha$, and $N\alpha = NaN = aNN = aN = Na = \alpha$.
2. (Inverses). If $\alpha = aN$, then we can consider $\alpha^{-1} = a^{-1}N$, since $aNa^{-1}N = aa^{-1} = N$, and $a^{-1}NaN = a^{-1}aN = N$.
3. (Closure). One of the equivalent conditions for normality is closure, since

$$aNbN = a(Nb)N = a(bN)N = abNN = abN$$

which is also a left coset.

□

Following the previous discussion, we showed that

Lemma 3.6.4. If $\pi : G \to G/N$, and $\pi \in \hom(G, G/H)$ where N is a subgroup of G, then we must have that $N \trianglelefteq G$.

Definition 3.6.2. If the only normal subgroups of G are $\{e\}$ and G, then we say that G is a simple group.

One of the biggest struggles in the 20th century was to find and classify all finite simple groups. Now we prove the following theorem:

Theorem 3.6.5 (Group of Prime Order)**.** Let G be a group of prime order; that is, $|G| = p$. Then

1. G is cyclic.

2. G is simple.

Proof.

1. Let $a \in G \setminus e$. Thus, $o(a)|p = |G|$. But since p is prime, this means $o(a) = 1$ or $o(a) = p$. But we know that $o(a) \neq 1$, since $a \neq e$. Therefore, $o(a) = p$ and $|\langle a \rangle| = p = |G|$, so $\langle a \rangle = G$.

2. Again, if there were a normal subgroup $N \trianglelefteq G$, we would have that $|N||p = |G|$. Therefore, $|N| = 1$ or $|N| = p$; so the only normal subgroups are $\{e\}$ or G, so G is simple.

□

A natural question might be is

Theorem 3.6.6. If $\pi : G \to {}^{G}\!/_{N}$, where N is a subgroup of G, then

$$\pi : a \mapsto aN \in \hom(G, {}^{G}\!/_{N}) \iff N \trianglelefteq G.$$

Proof. We already proved the first direction, by from lemma [NAME LEMMA]. Now suppose N is normal. Then we have $\alpha, \beta \in {}^{G}\!/_{N}$, such that $\alpha = aN$ and $\beta = bN$ for some $a, b \in G$. Then we have $\alpha\beta = (ab)N$ Therefore, $\pi(ab) = abN = aNb = aNNb = aNbN = \pi(a)\pi(b)$, so π is a homomorphism. □

Moreover, it is interesting to look at the kernel of π.

Lemma. Let N be a normal subgroup, and $\pi : G \to G/N$. Then

$$\ker \pi = N.$$

Proof. We have that

$$\begin{aligned} \ker \pi &= \{a \in G : \pi(a) = N\} \\ &= \{a \in G : aN = N\} \\ &= \{a \in G : a \in N\} \\ &= N. \end{aligned}$$

□

Theorem 3.6.7 (Kernel is Normal)**.** Let $\phi \in \hom(G, H)$. Then $\ker \phi \trianglelefteq G$.

Proof. According to one of the equivalent conditions, N is normal if $aNa^{-1} \subset N$ for all $a \in G$. Then we have $g \in G$ and $n \in \ker \phi$. Then

$$\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g^{-1}) = \phi(g)e_H\phi(g)^{-1} = e_H$$

so $gng^{-1} \in \ker \phi$. Therefore, $\ker \phi$ is a normal subgroup of G. □

3.7 Isomorphisms

In the previous sections, we discussed maps between groups that preserved the group structure (homomorphisms). Now, we want to find a stronger way to relate groups.

Definition 3.7.1 (Isomorphic)**.** Given two groups G and H, we say that G is isomorphic to H (and vice versa) if we can find a group isomorphism between them. That is, there exists a bijective map from G to H (H to G) such that the map is also a homomorphism. If this is true, we denote the statement G is isomorphic to H by

$$G \cong H.$$

If this is true, then we can say that G and H are basically the same thing; every action you do in G has a unique corresponding action in H. This is incredibly useful if we don't know a lot about a certain group, but do know a good deal about another one; if the two groups are isomorphic, then we can more easily study the other one. This begs the question; how do we go about finding an isomorphism? We first look at a typical problem in algebra.

3.7.1 A Typical Problem

Let G and H be groups, and let ϕ be a homomorphism from G to H. Moreover, let G_1 be a group such that there exists an onto homomorphism π from G to G_1 (this is sometimes known as an epimorphism). It might be convenient to express this in terms of a diagram:

$$\begin{array}{ccc} G & \xrightarrow{\phi} & H \\ {\scriptstyle\pi}\downarrow & & \\ G_1 & & \end{array}$$

Now we want to ask if there is a homomorphism from G_1 to H, say ψ, such that ψ is a homomorphism. Moreover, we want $\psi \circ \pi = \phi$. That

$$\begin{array}{ccc} G & \xrightarrow{\phi} & H \\ {\scriptstyle\pi}\downarrow & \overset{\exists\psi?}{\nearrow} & \\ G_1 & & \end{array}$$

If we can find such a $\psi \circ \pi = \phi$, then we say that the diagram commutes. This essentially means that we can get to H by way of ϕ or by $\psi \circ \pi$, which should be the same. Now let's state a theorem.

Theorem 3.7.1. Let G, H, G_1 be groups, and let $\phi \in \hom(G, H)$, let $\pi \in \hom(G, G_1)$. If $\ker \pi \subseteq \ker \phi$, then there exists a unique $\psi \in \hom(G_1, H)$ such that $\psi \circ \pi = \phi$ (the diagram commutes).

Remark. The condition $\ker \pi \subseteq \ker \phi$ seems to be natural, since if we could find such a ψ, then $\psi \circ \pi = \phi$. Thus, if $a \in \ker \pi$, then $\phi(a) = \psi(\pi(a)) = \psi(e) = e$. Therefore, we put this in our assumption for the theorem, but this theorem shows us that this condition is enough.

Proof. In our assumption, we have that $\ker \pi \subseteq \ker \phi$. First we show existence. Given $a_1 \in G_1$, we know that because we assume π to be onto, that $\pi(a) = a_1$. Thus, define $\psi(a_1) = \phi(a)$. Now we want to show that ψ is well-defined. That is, if $a_1 = \pi(a) = \pi(b)$, we need to show that $\psi(a_1) = \phi(a) = \phi(b)$. Thus, suppose we have $\pi(a) = \pi(b)$. This is equivalent to saying that $\pi(ab^{-1}) = e$. Therefore, $ab^{-1} \in \ker \pi$. But by assumption, this is also contained in $\ker \phi$, so $\phi(ab^{-1}) = e$, which is equivalent to saying $\phi(a) = \phi(b)$.

Now that we have shown that ψ is a well-defined map, we want to check that $\psi \in \hom(G_1, H)$. Given $a_1, b_1 \in G_1$, we know that $a_1 = \pi(a)$ and $b_1 = \pi(b)$ for some $a, b \in G$. Thus, $\psi(a_1 b_1) = \phi(ab) = \phi(a)\phi(b)$. However, by the way we defined ψ, we know that $\phi(a)\phi(b) = \psi(a_1)\psi(b_1)$. Therefore, $\psi \in \hom(G_1, H)$. Now we want to show that $\psi \circ \pi = \phi$. For $a \in G$, we have that $\psi(\pi(a)) = \phi(a)$. Therefore $\psi \circ \pi = \phi$, so the diagram commutes.

Next, we show uniqueness. Suppose we have ψ and $\widetilde{\psi}$, such that $\psi \circ \pi = \phi = \widetilde{\psi} \circ \pi$. We know that there exists an $a \in G$ such that $\pi(a) = a_1$. Therefore, we have $\psi(a_1) = \phi(a) = \psi(a_1)$. Therefore, since this is true for all $a_1 \in G_1$, $\psi = \widetilde{\psi}$. □

This theorem gives us one way to construct homomorphisms between groups to complete the diagram. If we are lucky, this homomorphism may also be an isomorphism as well.

3.7.2 First Isomorphism Theorem

We know from a few sections ago that $\ker\phi$ is a normal subgroup. Therefore, we can make a quotient group $G/\ker\phi$. We don't really understand what this is, but if we can find an isomprphism from this group to something we do know, then we can say they are essentially the same. Indeed, this is true, and we call it the first isomprphism theorem.

Theorem 3.7.2 (First Isomorphism Theorem)**.** Let G, H be groups and let $\phi \in \hom(G, H)$. Then

$$G/_{\ker\phi} \cong \operatorname{Im}\phi.$$

Proof. We have already been given a special way to construct homomorphisms between groups, and now we want to construct an isomorphism. Let π be the natural map between G and $G/\ker\phi$. That is, $\pi : g \mapsto g\ker\phi$ for $g \in G$. Therefore, consider the diagram

$$\begin{array}{ccc} G & \xrightarrow{\quad\phi\quad} & \operatorname{Im}\phi \\ {\scriptstyle\pi}\downarrow & \nearrow_{\exists\psi?} & \\ G/_{\ker\phi} & & \end{array}.$$

From this, it is clear that π is onto, since by definition a coset is of the form $g\ker\phi$ for $g \in G$. However, we also know that $\ker\pi = \ker\phi$, since for any quotient group of a normal subgroup, the kernel is simply the normal subgroup. From the previous theorem, there is a unique homomorphism $\psi : G/\ker\phi \to H$, such that $\psi \circ \pi = \phi$. Now we have that

$$\operatorname{Im}\psi = \psi(G/\ker\phi) = \psi(\pi(G)) = \phi(G) = \operatorname{Im}\phi.$$

Therefore, we claim that $\psi : G/\ker\phi \mapsto \operatorname{Im}\phi$ is an isomorphism. We have shown that ψ is onto, since we showed that $Ima\psi = \operatorname{Im}\phi$. We only need to show that ψ is one-to-one. Suppose $\psi(\alpha) = \psi(\beta)$. Therefore, $\psi(\pi(a)) = \psi(\pi(b))$, so $\phi(a) = \phi(b)$. This implies that $\phi(ab^{-1}) = e$, so $ab^{-1} \in \ker\phi = \ker\pi$, so $ab^{-1} \in \ker\pi$. Therefore, $\pi(ab^{-1}) = e$, so $\pi(a) = \pi(b)$, and thus $\alpha = \beta$. Thus, ψ is an isomorphism, so

$$G/_{\ker\phi} \cong \operatorname{Im}\phi.$$

□

Theorem 3.7.3. Let $\phi \in \hom(G, H)$. Then we have that

$$\phi \text{ is one-to-one} \iff \ker\phi = \{e\}.$$

Proof. Let's show the first direction. If ϕ is one-to-one, then we have that $a \in \ker\phi$ implies $\phi(a) = e = \phi(e)$. Since ϕ is one-to-one this implies $a = e$. Therefore, $\ker\phi \subset \{e\}$. Clearly, e is also in $\ker\phi$. So $\ker\phi = \{e\}$.

The other direction shows us that ϕ is one to one. Suppose $\phi(a) = \phi(b)$. Then $\phi(ab^{-1}) = e$, so $ab \in \ker\phi$. However, since $\ker\phi = e$, then $ab^{-1} = e$ so $a = b$. □

Corollary 3.7.4. Let G be a group, and let $a \in G$ such that $o(a) = \infty$. Then

$$\langle a\rangle \cong \mathbb{Z}.$$

Proof. Let $\phi : \mathbb{Z} \to G$ where $k \mapsto a^k$. We know that ϕ is a homomorphism and one-to-one, since if $\phi(k) = e$, we have $a^k = e$. Since $o(a) = \infty$, this forces $k = 0$. Therefore, $\ker\phi = \{0\}$. Clearly, this map is also onto $\langle a\rangle$. Therefore ϕ is an isomprphism. □

Corollary 3.7.5. Let G be a group, and let $a \in G$ such that $o(a) = n < \infty$. Then

$$\langle a \rangle \cong \mathbb{Z}_n.$$

Proof. Consider $\phi : k \mapsto a^k$. We have that $\ker \phi = n\mathbb{Z}$, since a raised to any multiple of n is just e. Moreover, $\operatorname{Im} \phi = a$. By the first isomorphism theorem, $\mathbb{Z}/\ker \phi = \mathbb{Z}_n$ is isomorphic to $\operatorname{Im} \phi$, so

$$\langle a \rangle \cong \mathbb{Z}_n.$$

□

Hence, we have shown that all cyclic groups are essentially the same as $\mathbb{Z}$ or $\mathbb{Z}_n$.

3.7.3 Second Isomorphism Theorem

Theorem 3.7.6. Let G be a group, and $H \leq G$, and $N \trianglelefteq G$. Then,

1. $HN \leq G$
2. $H \cap N \trianglelefteq H$
3. $HN/N \cong H/(H \cap N)$.

Proof.

1. We have that $HN = NH$, since N is normal. Therefore, $HN \leq G$.
2. Let $\pi : H \to HN/N$, where $aN \mapsto aN$. We claim that $\operatorname{Im} \pi = HN/N$. We only have to show that $HN/N \subseteq \operatorname{Im} \pi$, since the other way is obvious. Let $\alpha \in HN/N$. Then any $\alpha \in HN/N$ is just anN for $a \in H$ and $n \in N$. Thus, $anN = aN$, which is just the image of π. Now we claim that $\ker \pi = H \cap N$. We have

$$\begin{aligned} \ker \pi &= \{a \in H : aN = N\} \\ &= \{a \in H : a \in N\} \\ &= H \cap N. \end{aligned}$$

   But since the kernel of any homomorphism is always normal, this tells us that $H \cap N \trianglelefteq H$.

3. Moreover, we have that

$$H/\ker \pi = H/H \cap N \cong \operatorname{Im} \pi = HN/N.$$

□

Now we turn to some useful theorems

Theorem 3.7.7. Let G be a group. Let $\phi \in \hom(G, G_1)$ such that ϕ is onto. The following are true:

1. The set $\{H \leq G : \ker \phi \subseteq H\} \cong \{H_1 : H_1 \leq G_1\}$.
2. For $N \trianglelefteq G$, and $\ker \phi \subseteq N$, then $\phi(N) \trianglelefteq G_1$.
3. If $N \trianglelefteq G$, and $\ker \phi \subseteq N$, then $G/N \cong G_1/\phi(N)$.

Proof.

1. Clearly, the map $\psi : H \mapsto \phi(H)$ works since if $\ker \phi \subseteq H$, $\phi(H)$ is a subgroup.

2. For $a_1 \in G_1$, we have that $a_1 = \phi(a)$ for some $a \in G$. Therefore, consider $a_1\phi(n)a_1^{-1}$. This is just $\phi(a)\phi(n)\phi(a)^{-1} = \phi(ana^{-1}) = \phi(n')$ for some $n' \in N$. Therefore $a_1\phi(n)a_1^{-1} \in \phi(N)$, so $\phi(N) \trianglelefteq G_1$.

3. Let $\pi : G_1 \mapsto G_1/\phi(N)$, since $\phi(N)$ is a normal subgroup of G_1. Therefore, we have that $\pi \circ \phi \in \hom(G, G_1/\phi(N))$. This is clear since ϕ is onto and π is onto, since π is just the canonical quotient map. We note that $\ker \pi \circ \phi = \{a \in G : \pi(\phi(a)) = \phi(N)\}$, or just $\{a \in G : a \in N\}$. Therefore, from the first isomorphism theorem, $G/\ker \pi \circ \phi$ is isomprphic to its image, which is just $G_1/\phi(N)$. Thus,

$$G/N \cong G_1/\phi(N).$$

□

It is important to think of homomorphisms and quotient groups together. Homomorphisms relate groups together, and quotients somehow make groups smaller. Now with this in mind, quotients help us a lot in proving new results.

3.8 Cauchy and Sylow Theorems for Finite Abelian Groups

Theorem 3.8.1 (Cauchy)**.** Suppose G is a finite abelian group. Supose $p| \ |G|$, where p is prime. Then there exists an $a \in G$ such that $o(a) = p$.

Recall that for any $x \in G$, $o(x)| \ |G|$. However, the converse of Lagrange's theorem is not true. Consider $\mathbb{Z}_2 \times Z_2$. There is no element here that is of order 4.

Proof. We do this by inductio on G. The base case is that $|G| = p$. If this is so, then $\forall a \neq e$, we have $o(a) = p$.

Now assume the theorem is true for all $|G| < n$. Now we show it is true for $|G| = n$. We have that $p|||G|$. If we have a $b \in G$ such that $p|o(b)$, say $o(b) = pm$, then $o(b^m) = p$. Now pick $b \in G \setminus \{e\}$.

Case 1: If $p|o(b)$, then there exists an $a \in G$ such that $o(a) = p$.

Case 2: Of p does not divide $o(b)$, then p does not divide $|\langle b\rangle|$. Therefore, since G is abelian, and all subgroups are normal, consider $\pi : G \to G/\langle b\rangle$. We have that $|G/\langle b\rangle| = |G|/o(b) < n$. Moreover, the group $G/\langle b\rangle$ is also abelian. Because of the fundamental theorem of arithmetic, we have that p divides $|G|$, and p does not divide $o(b)$; so p divides $|G/\langle b\rangle|$. Therefore, by the induction hypothesis, $\exists \gamma \in G/\langle b\rangle$ such that $o(\gamma) = p$. Therefore, since the quotient map π is onto, $\gamma = \pi(x)$ for some $x \in G$.

We would like to make one further observation, which is that if ϕ is a homomorphism, then $o(\phi(x))|o(x)$. This is because if $x^k = e$, then $\phi(x)^k = e$; therefore $o(\phi(x))|o(x)$. We also know that $o(\gamma)|o(x)$, since π is a homomorphism. Therefore, $p|o(x)$. Now we know from our first observation that $o(x) = pm$ for some m, so $x^m = a$. Therefore, there exists an $a \in G$ such that $o(a) = p$. □

Theorem 3.8.2. Let G be an Abelian group and p be prime. If $p^k| \ |G|$, then there exists a subgroup $|H| = p^k$.

Proof. The base case is $k = 1$, which follows as a direct result of Cauchy's theorem.

Now suppose this is true for $k < n$. We want to show it works for $k = n$. Now we have $p^n \ |G|$. First, $p| \ |G|$, so $o(a) = p$ for some p. Now we have a quotient map $\pi : G \to G/\langle a\rangle$. Therefore, we have that $|G/\langle a\rangle| = |G|/p$. Therefore, $p^{n-1}| \ |G/\langle a\rangle|$. Sine $G/\langle a\rangle$ is abelian, there exists a subgroup $|L| = p^{n-1}$ by the induction hypothesis. Let $H = \pi^{-1}(L)$. This is a subgroup of G since onto maps preserve subgroups. Now we can consider π restricted to the subgroup H, or $\pi|_H : H \to L$, which is also onto. We therefore have that $\ker \pi|_H = \langle a\rangle$. This tells us that

$$H/\langle a\rangle \cong L.$$

Therefore, since $|L| = p^{n-1}$, and $o(a) = p$, then $|H| = p^n$. This concludes the proof. □

Theorem 3.8.3. Suppose G is a group such that $p^m \mid |G|$, but p^{m+1} does not divide $|G|$. Then there exists a unique subgroup $P \leq G$ such that $|P| = p^m$.

Proof. We have that $|G| = pk$, where $0 \leq k < p$. By the previous theorem, we know that there exists a group P of order m. Now we prove uniqueness. Suppose there are two subgroups of G such that $|P| = p^m = |P'|$. We know that the set PP' is also a subgroup of G, since $PP' = P'P$. From the first counting argument, we have that

$$|PP'| = \frac{|P||P'|}{|P \cap P'|} = \frac{p^{2m}}{|P \cap P'|}.$$

From Lagrange's theorem, we know that $|P \cap P'| \mid |P|$. Therefore, $|P \cap P'| = p^k$, so $|PP'| = p^{2m-k}$. However, since PP' is a subgroup, we have that $|PP'| \mid |G|$. This forces $k = m$, since p^{m+1} does not divide $|G|$. Since $|P \cap P'| = p^m$, we know that $P = P'$. Therefore, this is unique. □

3.9 Automorphisms

Definition 3.9.1. If $\phi \in \hom(G, G)$, and ϕ is an isomorphism, then we call ϕ an Automorphism of G. The set of all automorphisms of G are denoted as

$$\mathrm{Aut}(G).$$

Lemma 3.9.1. Let G be a group. Then $\mathrm{Aut}(G)$ is a group under function composition.

Proof. First, $\mathrm{Aut}(G)$ is nonempty since the identity map $e(x) : x \mapsto x$ is in $\mathrm{Aut}(G)$.

Next, suppose $\phi, \psi \in \mathrm{Aut}(G)$. Then consider $\phi\psi^{-1}$. Since ψ is a bijection, so is ψ^{-1}. However, bijections are stable under composition. Therefore $\phi\psi^{-1} \in \mathrm{Aut}(G)$. □

Definition 3.9.2. Let $c_g(x)$ denote conjugation by an element in G. Therefore, we have that

$$c_g(x) = gxg^{-1} \in \mathrm{Aut}(G).$$

Proof. This is an automorphism and it is simple to prove. □

4 The Sylow Theorems

4.1 Applications of Sylow Theorems

The Sylow theorems give us some constraints on the subgroups of finite groups. Hopefully with this extra information, we will be able to completely characterize certain finite groups. These theorems are not a silver bullet; as we will see in later chapters, we will encounter more tools in our analysis of finite groups.

This section should be studied closely in order to understand the various techniques we can employ in order to classify (or partially classify) finite groups.

Example. Suppose $|G| = 6$. I claim that either $G \cong \mathbb{Z}_6$ or $G \cong S_3$ (of course, $\mathbb{Z}_6 \ncong S_3$ since the former is abelian.) This is a problem known as a classification problem, where we find all the groups of order 6 up to isomorphism.

Proof. Since $|G| = 2 \times 3$, we see that $n_2|3$, and $n_2 \equiv 1 \pmod 2$. Thus, $n_2 = 1, 3$. Now we consider n_3. We see that $n_3|2$ and $n_3 \equiv 1 \pmod 3$. Thus $n_3 = 1$. Now we have two cases:

1. $(n_2 = 1, n_3 = 1)$. Now we have that P_2 is a Sylow-2 subgroup, and the only one at that. Since all Sylow-p subgroups are conjugate to one another, this means that $P_2 \trianglelefteq G$, since $aP_2a^{-1} = P_2$ for all $a \in G$. The same logic applies to P_3, since it is the only Sylow-3 subgroup; moreover, its index is 2 in G, and all subgroups of index 2 are normal (exercise). Now we can find an isomorphism from G to $\mathbb{Z}_6$. We know that P_2 must be generated by elements of order 2, since 2 is prime and all subgroups of prime order are cyclic. We have that

$$P_2 = \langle a \rangle,\ o(a) = 2$$
$$P_3 = \langle b \rangle,\ o(b) = 3.$$

   Now we want to reason that $o(ab) = 6$. If we can prove that, then we will have a cyclic, abelian group of order 6, which is patently isomorphic to $\mathbb{Z}_6$. We first show that $ab = ba$. This is because if we look at the commutator $[a, b] = aba^{-1}b^{-1}$, we see that $(aba^{-1})b^{-1} \in P_3$, since P_3 is a normal subgroup and is closed under conjugation and multiplication. Similarly, we have that $a(ba^{-1}b^{-1}) \in P_2$. This means that $a, b \in P_2 \cap P_3$. But $P_2 \cap P_3 = \{e\}$, since the order of elements in P_2 divides 2, and the order of elements in P_3 divides 3. Since they are relatively prime, we have that the only possible member of their intersection is the identity. Therefore, $[a, b] = e$ so $ab = ba$. From here, we can argue that $o(ab) = 6$. We have that $(ab)^k = a^k b^k = e$ for some k, since a, b commute. This implies that $a^k = b^{-k} \in P_2 \cap P_3 = \{e\}$. Thus $a^k = e$, and $b^{-k} = e \Rightarrow b^k = e$. Therefore $2|k$ and $3|k$. Thus $o(ab) = 6$ since 6 is the least number that accomplishes this. Thus $|\langle ab \rangle| = 6 = |G|$. Then

$$G = \langle ab \rangle \cong \mathbb{Z}_6.$$

   In any abelian group, every Sylow-p subgroup must be unique, a fact covered in the Sylow theorems for abelian groups (also obviois from the conjugacy condition).

2. $(n_2 = 3, n_3 = 1)$. Now we want to show that $G \cong S_3$. We have to construct an explicit isomorphism between the two. We have that $P_3 \trianglelefteq G$. Moreover, $P_2 \ntrianglelefteq G$. If we look at the set $|G/P_2| = 3$, we have that G acts on G/P_2 by $a \cdot \alpha = a\alpha$ for all $a \in G$, and $\alpha \in G/P_2$. Hence we have the homomorphism

$$\rho : G \to \Sigma_{G/P_2} \cong S_3.$$

We will show that this ρ is an isomorphism. Looking at the kernel of ρ, we have that

$$\begin{aligned} a \in \ker\rho &\iff \forall \alpha \in G/P_2,\ a\alpha = \alpha \\ &\iff \forall b \in G,\ abP_2 = bP_2 \\ &\iff \forall b \in G,\ b^{-1}abP_2 = P_2 \\ &\iff \forall b \in G,\ b^{-1}ab \in P_2 \\ &\iff \forall b \in G,\ a \in bP_2b^{-1}. \end{aligned}$$

Thus we have that $\ker\rho \leq P_2 \Rightarrow \ker\rho = \{e\}$ or $\ker\rho = P_2$. But the latter is impossible, since the kernel is always normal but $P_2 \not\trianglelefteq G$. Therefore we accept that $\ker\rho = \{e\}$, and because Σ_{G/P_2} is finite, we actually have an isomprphism between the two. Thus

$$G \cong \Sigma_{G/P_2} \cong S_3.$$

□

In the previous example, we classified all groups of order 6. In general, it is not true that we can classify all groups. We can consider the example of groups of order 77.

Example. Initially, this number 77 might seem a little contrived. That's because it is; we claim that all groups of order 77 are isomorphic to $\mathbb{Z}_{77}$.

Proof. We have that $|G| = 7 \times 11$. Thus $n_7|11$, so $n_7 = 1, 11$. However, $n_7 \equiv 1 \pmod 7$. This means that $n_7 = 1$. Similarly, we can see that $n_{11} = 1$. Thus $P_7, P_{11} \trianglelefteq G$. Now we hope to find an element in G whose order is 77. Again, since all groups of prime order are cyclic,

$$\begin{aligned} P_7 &= \langle a \rangle,\ o(a) = 7 \\ P_{11} &= \langle b \rangle,\ o(b) = 11. \end{aligned}$$

Again, we hope to show that $o(ab) = 77$. We can use the same commutator trick as in case 1 of the previous example to show that $ab = ba$. Again, we can show that $o(ab) = 77$, and thus showing that $G = \langle ab \rangle \cong \mathbb{Z}_{77}$. By proceeding exactly as in case 1 of the previous example,

$$\begin{aligned} (ab)^k &= e = a^k b^k \\ &\Rightarrow a^k = b^{-k} \in P_7 \cap P_1 1 = \{e\} \\ &\Rightarrow a^k = e, b^{-k} = e \\ &\Rightarrow 7|k,\ 11|k \\ &\Rightarrow 77|k. \end{aligned}$$

Hence $o(ab) = 77$ since 77 is the least common multiple of 7 and 11. □

Example. Now let's consider groups of order 20449. We claim that all groups of this order are abelian. Later on, we will classify *all* finite abelian groups using new tools. Again, the harder parts of group theory are when we consider non-abelian groups. Note that simply determining that groups of this order are abelian, we don't fully classify it in terms of isomorphisms. That is for later sections.

Proof. We have that $|G| = 20449 = 11^2 \times 13^2$. Therefore, $n_{11} = 1, 13, 13^2$, but the only solution that satisfies this is $n_{11} = 1$. Next we do the same for n_{13} and find out that $n_{13} = 1$. Now we have that $P_{11}, P_{13} \trianglelefteq G$. Thus $|P_{11}| = 11^2$ means that P_{11} is abelian, since all groups of order p^2 are abelian.

Similarly, P_{13} is abelian. Thus $P_{11}P_{13} \leq G$ since they are both normal subgroups, and the product of two normal subgroups is a subgroup. We claim $P_{11}P_{13}$ is abelian. Using the counting argument,

$$|P_{11}P_{13}| = \frac{|P_{11}| \cdot |P_{13}|}{|P_{11} \cap P_{13}|} = \frac{11^2 \cdot 13^2}{1}$$

Since $|P_{11} \cap P_{13}|$ divides both 11^2 and 13^2. This implies that $G = P_{11}P_{13}$. If we consider $x \in P_{11}$ and $y \in P_{13}$, we can use the same commutator trick to show that $xy = yx$. We're not done; if we have an $a, b \in G$, we can represent $a = xy$ and $b = x'y'$. Thus

$$ab = xyx'y' = xx'yy' = x'xy'y = x'y'xy = ba.$$

Therefore G is abelian. □

Now recall the definition of a simple group. If G is simple, then its only normal subgroups are $\{e\}$ and G itself. We call it "simple" since it cannot be further reduced by taking the quotient with a non-trivial normal subgroup. It was a great effort over the 20th century, spilling into the 21st, to classify all finite simple groups.

Example. We claim that if $|G| = 12$, then G is not simple (i.e., it has a non-trivial normal subgroup).

Proof. We have that $|G| = 2^2 \times 3$. Then we apply the standard analysis to show that $n_2 = 1, 3$, and $n_3 = 1, 4$. If Clearly, if n_2 or $n_3 = 1$, then we're finished. Now we consider the case when $n_3 = 4$; we claim that n_2 must necessarily be 1. Let us denote the Sylow-3 subgroups as H_1, H_2, H_3, H_4. Then we have that $(H_i \setminus \{e\}) \cap (H_j \setminus \{e\}) = \emptyset$ for $i \neq j$. Otherwise, we would have that if $a \in H_j \cap H_j$, we have that $o(a) = 3$ so $\langle a \rangle = H_i = H_j$ so $i = j$, a contradiction. Then we have that the set

$$\{H_1 \setminus \{e\}, H_2 \setminus \{e\}, H_3 \setminus \{e\}, H_4 \setminus \{e\}\}$$

is a partition of the set of order 3 elements in G. This is because if we have $a \in G$, and $o(a) = 3$, then $\langle a \rangle = H_i$ for some i. Thus the number of order 3 elements is $2 \times 4 = 8$. Now let P_2 be a Sylow-2 subgroups. Then $P_2 \subseteq G \setminus \{\text{order 3 elements}\}$. However, we know that $|P_2| = 4$ and $|G \setminus \{\text{order 3 elements}\}| = 4$. Thus

$$P_2 = G \setminus \{\text{order 3 elements}\}.$$

This means that there is a unique Sylow-2 subgroup, since there is only one set of elements not of order 3. Moreover, if there were 3 Sylow-2 subgroups, then there would be $3 \times 3 = 9$ elements of order 2. There cannot simultaneously be 8 elements of order 3 and 9 of order 2, since the total order of G is 12. Thus $n_2 = 1$ and

$$P_2 \trianglelefteq G,$$

so groups of order 12 are not simple. □

As a final example, we can look at how to leverage the properties of group actions in order to classify groups.

Example. We claim that groups G of order $72 = 2^3 \times 3^2$ are not simple.

Proof. We have that $n_3 = 1, 4$. We want to show that if $n_3 = 4$, then $n_2 = 1$. A way to construct a normal subgroup is to consider the kernel of some homomorphism; and a way to naturally obtain a homomorphism is by considering a group action. We have that the order of any Sylow-3 subgroup is 9. Thus, let $\mathrm{Syl}_3(G) = \{Sylow3-subgroups\}$. $|\mathrm{Syl}_3(G)| = 4$. Then we can say that G acts on $\mathrm{Syl}_3(G)$ by $a \cdot P = aPa^{-1}$. This group action is transitive (i.e., it has only one orbit: $\mathrm{Orb}(P_3) = \mathrm{Syl}_3(G)$. Therefore, by the class equation,

$$4 = |\mathrm{Orb}(P_3)| = [G : \mathrm{Stab}(P_3)] = [G : N_G(P_3)]$$

Where $N_G(P_3)$ are the normalizers of P_3 in G. Now we define $H := N_G(P_3) \Rightarrow [G : H] = 4$. But the normalizers themselves form a normal subgroup. Therefore let G act on G/H by left multiplication, where $a \cdot \alpha = a\alpha$ for $a \in G$ and $\alpha \in G/H$. This gives rise to the homomorphism

$$\rho : G \to \Sigma_{G/H}.$$

We have that the kernel $\ker \rho \subseteq H \Rightarrow \ker \rho \neq G$. Now we want to show that $\ker \rho \neq \{e\}$. Then, since the kernel is always normal, we will have found a nontrivial normal subgroup.

If $\ker \rho = \{e\}$, them the group $G/\{e\} \cong \mathrm{Im}(\rho)$, or $G \cong \mathrm{Im}(\rho)$. But since $\mathrm{Im}(\rho) \leq \Sigma_{G/H}$, we have that $|G| = |\mathrm{Im}(\rho)|$, and in turn $\mathrm{Im}(\rho)| \; |24$. Thus $|G||24$ which is impossible. Therefore, there exists a normal subgroup of G that is not G or $\{e\}$. Hence groups of order 72 are not simple. □

The gist of this example is if we have large subgroups we will be able to find non-trivial normal subgroups. If we look at action on the left cosets, then the kernel will be a normal subgroup; if the kernel were $\{e\}$ then the order of the group (which is large) would divide the order of the permutation group (which is small), and hence produce a contradiction.

5 Finite Abelian Groups

The problem of classification can be boiled down to trying to create a table of groups such that (a) None of the groups in the table are isomorphic to one another, and (b) any given finite group is isomorphic to one member in the table. In the area of mathematics called surface theory, we can classify all surfaces by their genus, or the number of holes. In order to do this, we will need to consider the tool of direct products.

5.1 Direct Products

DO LATER

6 Ring Theory

Our aim in this chapter will be to do some basic ring theory. A ring is another algebraic structure. A ring is a set with two operations, which are compatible with one another. The main reason we are interested in ring theory is because we want to study polynomials.

6.1 Definitions

Definition 6.1.1 (Ring)**.** A *ring* is a set R endowed with two operations, $+$ and $\cdot$, such that

1. $(R, +)$ is an abelian group. The unit element is denoted by 0
2. For every $x, y, z \in R$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
3. For every $x, y, z \in R$,

$$x \cdot (y + z) = x \cdot y + x \cdot z (y + z) \cdot x \qquad = y \cdot x + z \cdot x. \tag{6.1.1}$$

Usually, we write the product $x \cdot y$ as xy. Moreover, the additive inverse of a is represented as $a^{-1} = -a$.

Example. The most basic example of a ring is $(\mathbb{Z}, +, \cdot)$.

Definition 6.1.2 (Commutative Ring)**.** We say a ring $(R, +, \cdot)$ is commutative if $\forall x, y \in R$, we have that

$$x \cdot y = y \cdot x.$$

We generally reserve the term "abelian" for groups.

Definition 6.1.3 (Ring with Unit)**.** If $(R, +, \cdot)$ is a ring, and there is an element $1 \in R$ such that

$$1 \cdot r = r \cdot 1 = r, \ \forall r \in R,$$

then we say that 1 is the unit element in R, and we say that R is a group with unit.

Lemma 6.1.1 (The unit is unique)**.** *Proof.* Suppose 1 and $1'$ are both units. Then we have

$$1 = 1 \cdot 1' = 1' \cdot 1 = 1'.$$

□

Example. We have that $(\mathbb{Z}, +, \cdot)$ is a commutative ring with unit. However, if you look at the even integers, $(2\mathbb{Z}, +, \cdot)$, this is a commutative ring without unit. This is because if ther there is a unit u, then we have that $2u = 2$ so $u = 1$, but $1 \notin 2\mathbb{Z}$.

Moreover, the rationals $\mathbb{Q}$ is a commutative ring.

Example. Recall that $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{[a] : a \in Z\}$. This is a commutative ring with unit:

1. $(\mathbb{Z}, +)$ is an abelian group;
2. $\alpha(\beta\gamma) = (\alpha\beta)\gamma$;
3. $\alpha\beta = \beta\alpha$

4. Let $\alpha = [a]$, $\beta = [b]$, and $\gamma = [c]$. Then

$$\begin{aligned}\alpha(\beta+\gamma) &= [a][b+c] \\ &= [a(b+c)] \\ &= [ab+ac] \\ &= [ab]+[ac] \\ &= [a][b]+[a][c] \\ &= \alpha\beta+\alpha\gamma.\end{aligned}$$

This is the first nontrivial example of a commutative ring with unit.

Example. Let x be a variable. We denote the ring of polynomials with real coefficients by

$$\mathbb{R}[x] = \{a_0 + a_1x + \cdots + a_mx^m : a_i \in \mathbb{R}, m \in \mathbb{N}\}.$$

We can add and multiply polynomials and group like terms. We have that $(R[x], +, \cdot)$ is a commutative ring with unit (the polynomial where $a_i = \delta_{0,i}$).

If we wanted to have polynomials with multiple variables, we would write

$$\mathbb{R}[x, y] = \{\sum_{i,j} a_{ij}x^iy^j : a_{ij} \in \mathbb{R}\}.$$

This is also a polynomial ring with unit.

Now, let's look at an example that is not commutative.

Example. We consider the ring of matrices $\mathcal{M}_n(\mathbb{R}) = \mathbb{R}^{n\times n}$. Its unit is the identity matrix I, and for $n \geq 2$, the product in the matrix ring does not commute. We can provide counterexamples to this effect.

We also have that $\mathcal{M}_n(\mathbb{C})$ and $\mathcal{M}_n(\mathbb{Z})$ are non-commutative rings.

Example. Let V be a vector space over $\mathbb{C}$, and consider $\mathcal{L}(V, V)$ which is the set of all linear transformations from V to V. We have that for $S, T \in \mathcal{L}(V, V)$, $S+T \in \mathcal{L}(V, V)$ and $S\circ T \in \mathcal{L}(V, V)$. It should be verified that $(\mathcal{L}(V, V), +, \circ)$ is a ring.

Example. Let $C([0, 1], \mathbb{R})$ be the set of continuous functions from $[0, 1]$ to $\mathbb{R}$. We define the product to be $(f \cdot g)(t) = f(t)g(t)$ and the addition to be $(f + g)(t) = f(t) + g(t)$. We have that $(C([0, 1], \mathbb{R})), +, \cdot)$ is a ring with unit. Likewise, all C^1 functions from $[0, 1]$ to $\mathbb{R}$.

Lemma 6.1.2. For any ring, we have that

$$a \cdot 0 = 0 \cdot a = 0.$$

Proof. We have that $a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0$. Therefore $a \cdot 0 = 0$; we can prove the other equality similarly. □

Definition 6.1.4 (Zero Divisors)**.** Let R be a ring. We say that a, b are zero divisors if we have $a, b \neq 0$ and

$$a \cdot b = 0$$

for some $a, b \in R$.

Definition 6.1.5 (Integral Domain)**.** If $(R, +, \cdot)$ is a commutative ring that has no zero divisors, then we call R an integral domain. Equivalently, we can say that an integral domain is a ring such that

$$ab = 0 \Rightarrow a = 0 \text{ or } b = 0.$$

Example. We can show that $(C([0,1],\mathbb{R}),\cdot)$ is not an integral domain. We can define two continuous functions that are 0 at the points where the other is nonzero; thus $fg = 0$ but $f, g \neq 0$.

Integral domains are expecially useful since the left and right cancellation laws hold in the integral domain.

Lemma 6.1.3. If R is an integral domain, then we have

$$ab = ac,\ a \neq 0 \Rightarrow b = c.$$

Proof. We can rearrange this to be $a(b-c) = 0$. By assumption, $a \neq 0$. Therefore $b - c = 0$, so $b = c$. Note that this doesn't work in a non-integral domain, since we have nonzero b that can satisfy $ab = a0 = 0$. □

Definition 6.1.6 (Degree of a polynomial)**.** The degree of a polynomial is the highest power of x that appears in a polynomial $f(x)$ with nonzero coefficeint. We denote this by $\deg(f)$. Sometimes we define the degree of the 0 polynomial to be $\deg(0) = -\infty$.

Example. The polynomial ring $\mathbb{R}[x]$ is an integral domain. If we have two polynomials $f, g \in \mathbb{R}[x]$, and $f, g \neq 0$, then we need to show $f \cdot g \neq 0$.

Proof. Let $f(x) = a_0 + a_1x + \cdots + a_mx^m, a_m \neq 0$. We define $g(x) = b_0 + b_1x + \cdots + b_nx^n, b_n \neq 0$. Now we gather the highest-order terms, which will be $a_mb_nx^{m+n}$. This is nonzero, therefore the product $f \cdot g \neq 0$. Therefore $\mathbb{R}[x]$ is an integral domain. □

Corollary 6.1.4. For any two nonzero polynomias $\deg(f \cdot g) = \deg(f) + \deg(g)$. If f or $g = 0$, then by the convention that $\deg(0) = -\infty$, this still holds.

Definition 6.1.7. Let R be aring with unit $1 \neq 0$. Then we say $a \in R$ is invertible if there exists a $b \in R$ such that

$$ab = ba = 1.$$

Such an element b is unique, and we denote it as a^{-1}.

Proof. We have uniqueness since $b = bab' = b'$. □

Definition 6.1.8 (Invertible Elements of a Ring)**.** We denote the set of all invertible elements in a ring $(R, +, \cdot)$ as

$$R^\times = \{a \in R : \exists a^{-1}\}.$$

Lemma 6.1.5. If R is a ring with unit $1 \neq 0$. The group of units $R^\times$ is a group. With the product $\cdot$.

Proof.

1. $R^\times \neq 0$ since $1 \in R^\times$.
2. $a, b \in R^\times \Rightarrow ab \in R^\times$ and $(ab)^{-1} = b^{-1}a^{-1}$.
3. If $a \in R^\times$, then $\exists b \in R$ such that $ab = ba = 1$. Then this implies that $b \in R^\times$.
4. The product is associative since it is associative in R.

□

Example. We have that $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, and $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$.
For matrices, $\mathcal{M}_n(\mathbb{R})^\times = \{A \in \mathcal{M}_n(\mathbb{R}) : \det(A) \neq 0\}$.

Definition 6.1.9 (Division Ring)**.** If R is a ring with unit, such that every nonzero element is invertible (i.e., $R^\times = R \setminus \{0\}$), then we say that R is a division ring.

Definition 6.1.10 (Field)**.** A commutative division ring is known as a field.

Example. As discussed above, some examples of fields are

1. $(\mathbb{Q}, +, \cdot)$
2. $(\mathbb{R}, +, \cdot)$
3. $(\mathbb{C}, +, \cdot)$.

Example. Consider $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. This is a field. Let $\alpha = a_1 + a_2\sqrt{2}$, and let $\beta = b_1 + b_2\sqrt{2}$.

1. Suppose $\alpha, \beta \in \mathbb{Q}[\sqrt{2}]$. Then $\alpha - \beta(a_1 - b_1) + (a_2 - b_2)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$.
2. The product $\alpha\beta = a_1b_1 + a_1b_2\sqrt{2} + a_2b_1\sqrt{2} + 2a_2b_2$. This clearly belongs to $\mathbb{Q}[\sqrt{2}]$. Needless to say, the product is commutative and associative, since real numbers commute and associate under the product.
3. Now we show that if $\alpha \in \mathbb{Q}[\sqrt{2}] \setminus \{0\}$. Then we write the inverse of the element $\alpha = a + b\sqrt{2}$ as
$$\frac{1}{\alpha} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} \in \mathbb{Q}[\sqrt{2}]$$

This proves that $\mathbb{Q}[\sqrt{2}]$ is a field.

Example. We denote the set of quaternions as $\mathbb{H}$. This is a division ring, but not commutative. We have that
$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}.$$
We set up the following rules for the product:

1. $i^2 = j^2 = k^2 = -1$
2. $ij = k = -ji$
3. $jk = i = -kj$,
4. $ki = j = -ik$.

This is a very important example of a division ring that does not commute. For $\alpha = a+bi+cj+dk \in \mathbb{H}$, then we have
$$\alpha^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}.$$

Lemma. Every field is an integral domain.

Proof. Assume $ab = 0$. If $a = 0$, we are done. If $a \neq 0$, then a^{-1} exists and $a^{-1}ab = b = a^{-1}0 = 0$. □

Theorem 6.1.6 (Wederburn's Theorem)**.** Any finite integral domain is a field.

Proof. Let R be a finite integral domain. We need to show that there exists a unit element $1 \neq 0$, and that every nonzero element is invertible.

Suppose we pick $a \in R \setminus \{0\}$. Let $f_a : R \to R : x \mapsto ax$. We can show that f_a is one-to-one, since

$$f_a(x) = f_a(y) \Rightarrow ax = ay \Rightarrow x = y$$

since the cancellation law holds in integral domains. Since R is finite, we know that since f_a is one-to-one that f_a is also onto. This implies that $\exists 1 \in R$ such that $a = f_a(1)$, so for all $x \in R$, $ax = ax \cdot 1 \Rightarrow x = x \cdot 1$. This implies $1 \neq 0$ and is a unit element in R. If $a \in \mathbb{R} \setminus \{0\}$, then there is a b such that $f_a(b) = 1 \to ab = 1$, so a is invertible.

Hence, R is a field □

Theorem 6.1.7. If $n \geq 2$, then

$$\mathbb{Z}_n \text{ is an integral domain} \iff n \text{ is prime.}$$

Proof. ($\Rightarrow$). Suppose $n = k\ell$, $k, \ell \in \mathbb{N}$. This implies that $[n] = [k][\ell] = 0$. This implies that $[k] = [0]$ or $[\ell] = [0]$. Say $[k] = [0]$; this means that $n|k$, so $n \leq k$. But we also know that $n \geq k$, since $k|n$. Therefore, $n = k$ so $\ell = 1$. Therefore, n is prime.

($\Leftarrow$). Suppose n is prime. Let $\alpha, \beta \in \mathbb{Z}_n$ and $\alpha \cdot \beta = [0]$. Then let $\alpha = [a]$ and $\beta = [b]$. If we have $[ab] = [0]$, then $n|ab$. But n is prime, so that means that $n|a$ or $n|b$. Then $\alpha = [0]$ or $\beta = [0]$. □

Corollary 6.1.8. If $n \geq 2$, then

$$\mathbb{Z}_n \text{ is a field} \iff n \text{ is prime.}$$

Definition 6.1.11 (Characteristic of a Ring)**.** Let F be a field, with an identity element $u \in F$. Define $ku = u + \cdots + u$ where addition is repeated $k \in \mathbb{N}$ times. Consider the set

$$H = \{k \in \mathbb{N} : ku = 0\} \leq (\mathbb{Z}, +).$$

If $H = \{0\}$, then we say that $\text{char}(F) = 0$. If $H \neq \{0\}$, then we have that $\text{char}(F) = \min(H)$.

In other words, the characteristic of a ring is the order of the unit element with respect to $+$.

Theorem 6.1.9. Every field with nonzero characteristic has prime characteristic.

Proof. Let $m = \text{char}(F) \neq 0$. Suppose $m = k\ell$, and $k, \ell \in \mathbb{N}$. Then we have that $0 = mu = ku \cdot \ell u$. This means that $ku = 0$ or $\ell u = 0$; thus $m|k$ or $m|\ell$, since m is the smallest number with this property. This implies that $k = m$ or $\ell = m$, since we have that $k|m$ and $\ell|m$. Therefore, $\ell = 1$ or $k = 1$, so m is prime. □

Example. Define the set

$$\mathbb{R}(x) := \left\{ \frac{p(x)}{q(x)} : p, q \in \mathbb{R}[x], q \neq 0 \right\}$$

6.2 Ring Homomorphisms

When we studied groups, we did not study them as isolated objects, but also their connections. Similarly, we will study the mappings between rings. In order to define a ring homomorphism, we want to preserve both of the products.

Definition 6.2.1. Let R, S be rings, and let $\phi : R \to S$. Moreover, let $r_1, r_2 \in R$. If ϕ satisfies

1. $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$
2. $\phi(r_1 r_1) = \phi(r_1)\phi(r_2)$,

then we say that ϕ is a ring homomorphism from R to S.

Example. Consider $c : \mathbb{C} \to \mathbb{C}$ given by

$$c(z) = \overline{z}.$$

This is a ring homomorphism, since $c(z+w) = \overline{z+w} = \overline{z} + \overline{w} = c(z) + c(w)$. Moreover, for the product, $c(zw) = \overline{z \cdot w} = \overline{z} \cdot \overline{w} = c(z)c(w)$.

Example. Let $\pi : \mathbb{Z} \to \mathbb{Z}_n$ given by

$$k \mapsto [k].$$

Example. Let us identify all ring homomorphisms from Z to Z. If ϕ is a ring homomorphism, then we use the fact that ϕ is a group homomorphism with respect to addition:

$$\phi(k) = \phi(k \cdot 1) = \phi(1 + \cdots + 1) = k\phi(1).$$

Next, we have that $\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1)$. Thus $\phi(1) = 1$ or 0. This means that $\phi(k) = k \forall k$, or $\phi(k) = 0 \forall k$.

Therefore, $\phi = \text{id}$ or $\phi = 0$.

Example. We established that $\mathbb{Q}[\sqrt{2}]$ is a field. Then we define the ring homomorphism $\phi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]$ given by

$$\phi(\alpha) = a - b\sqrt{2}.$$

We have that $\alpha + \beta = (a_1 + b_1) + (a_2 + b_2)\sqrt{2}$, and so

$$\phi(\alpha + \beta) = (a_1 + b_1) - (a_2 - b_2)\sqrt{2} = a_1 - a_2\sqrt{2} + b_1 - b_2\sqrt{2} = \phi(\alpha) + \phi(\beta).$$

Next, it can be shown that this is a homomorphism with respect to the product. This is akin to complex conjugation.

Lemma 6.2.1. If ϕ is a homomporphism from R to S, then

1. $\phi(0) = 0$.
2. $\phi(-a) = -\phi(a)$.
3. If R is an integral domain, then $\phi(1) = 1$.

Proof.

1. $\phi(0) = \phi(0 + 0) = \phi(0) + \phi(0) \Rightarrow \phi(0) = 0$.
2. $\phi(a - a) = \phi(a) + \phi(-a) = 0 \Rightarrow \phi(-a) = -\phi(a)$.
3. In this case, we have the left and right cancellation laws, so

$$\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1) \Rightarrow \phi(1) = 1.$$

□

When defining the kernel for a ring homomorphism, we have two operations to choose from. Built into the idea of a ring is that $(R, +)$ is an abelian group. The ring multiplication was less restricted, so we give more emphasis to the addition operation.

Definition 6.2.2 (Kernel of Ring Homomorphism)**.** Let ϕ be a ring homomorphism from R to S. Then we define the kernel of ϕ to be

$$\ker \phi := \{r \in R : \phi(r) = 0\}$$

where 0 is the additive identity.

Definition 6.2.3. If R and S are two rings, and $\phi : R \to S$ is a bijective ring homomorphism, then we say that ϕ is a (ring) isomorphism from R to S. If such a ϕ exists, then we say that R and S are isomorphic.

Example. Let V be a vector space over $\mathbb{R}$, and let $\dim(V) = n$. Select a basis $u_1, \ldots, u_n$. Consider the ring $\mathcal{L}(V, V)$.

On the other hand, consider the ring of $n \times n$ matricies. Then we claim that

$$\mathcal{L}(V, V) \cong \mathbb{R}^{n \times n}.$$

For all $T \in \mathcal{L}(V, V)$, let A be the matrix of T with respect to $u_1, \ldots, u_n$. Then let

$$A = \begin{bmatrix} T(u_1) & T(u_2) & \ldots & T(u_n). \end{bmatrix}$$

Then the homomorphism $\phi : T \mapsto A$ is a ring isomorphism.

6.3 Ideals and Quotient Rings

When dealing with groups, we realized that there were important objects called subgroups. In particular, we discussed the importance of normal subgroups. These allowed us to make a quotient group. Similarly, we can define a subring and a so-called ideal—a structure far more important than a subring.

Definition 6.3.1 (Subring)**.** Let $(R, +, \cdot)$ be a ring. If $S \subseteq R$ is a subset which is closed under $+, \cdot$, and $(S, +, \dot{c})$ is a ring, then we say that S is a subring of R.

Remark. In order to check that $S \subseteq R$ is a subring, we need to show that

1. S is a subgroup of $(R, +)$.
2. S is closed under $\cdot$.

Example. Recall $\mathbb{Z}[\sqrt{2}] = \{k + \ell\sqrt{2} : k, \ell \in \mathbb{Z}\}$. We now demonstrate that it is a subring of $\mathbb{R}$.

1. We know that $\mathbb{Z}[\sqrt{2}] \neq \emptyset$ since $0 \in \mathbb{Z}[\sqrt{2}]$. Moreover, if $\alpha = k_1 + \ell_1\sqrt{2}$ and $\beta = k_2 + \ell_2\sqrt{2}$, them $\alpha - \beta = (k_1 - k_2) + (\ell_1 - \ell_2)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Therefore $\mathbb{Z}[\sqrt{2}]$ is a subgroup of $(\mathbb{R}, +)$.
2. $\alpha \cdot \beta = k_1k_2 + k_1\ell_2\sqrt{2} + k_2\ell_1\sqrt{2} + 2\ell_1\ell_2$ is still in $\mathbb{Z}[\sqrt{2}]$.

Therefore, $\mathbb{Z}[\sqrt{2}]$.

Lemma 6.3.1. Let $\phi : R \to S$ be a ring homomorphism. Suppose $R' \subset R$ is a subring of R. Then $\phi(R') \subset S$ is a subring of S.

Proof. Since $0 \in \phi(R')$, we have that $\phi(R')$ is nonempty. Next, if $\alpha, \beta \in \phi(R')$, then $\alpha = \phi(x)$ and $\beta = \phi(y)$ where $x, y \in R'$. Then $\alpha - \beta = \phi(x) - \phi(y) = \phi(x - y) \in \phi(R')$. Lastly, $\alpha \cdot \beta = \phi(xy) \in \phi(R')$. Therefore the image $\phi(R')$ is a subring of S. □

Lemma 6.3.2 (Kernel is a Subring)**.** Let $\phi : R \to S$ be a ring homomorphism. Then $\ker \phi$ is a subring of R.

Proof. We have that $0 \in \ker \phi$. Then suppose $a, b \in \ker \phi$. This means that $\phi(a - b) = \phi(a) - \phi(b) = 0$. Therefore $a - b \in \ker \phi$. Lastly, we have that $\phi(ab) = \phi(a)\phi(b) = 0$, so $ab \in \ker \phi$.

Therefore, the kernel is a subring. □

However, we were able to do something with the kernel, which is to "mod out" some of the structure of a group. Indeed, the kernel satisfies something far more than simply being a subring; it is the ring analogue of a normal subgroup, known as an ideal.

Definition 6.3.2 (Ideal)**.** Let R be a ring. $I \subset R$ is an ideal of R if:

1. I is a subgroup of $(R, +)$.
2. For all $r \in R$ and $a \in I$, then $ra, ar \in I$. Equivalently stated, $rI \subseteq I$ and $Ir \subseteq I$.

Clearly, I is also a subring of R. If only multiplcation from the left implies that $ra \in I$, then we call I a left ideal. Similarly, we call I a right ideal if only $Ir \subseteq I$ is guaranteed.

Lemma 6.3.3. The kernel of a ring homomorphism $\phi : R \to S$ is an ideal.

Proof. We showed that $\ker \phi$ was a subgroup of $(R, +)$. In order to show the second property, note that if $a \in \ker \phi$ and $r \in R$, then

$$\phi(ra) = \phi(r)\phi(a) = \phi(r) \cdot 0 = 0$$

and similarly for the right. □

Example. Let's consider all the ideals of $(\mathbb{Z}, +, \cdot)$. This means that I is a subgroup of $(\mathbb{Z}, +)$. But in section [section], we showed that all subgroups are of the form $m\mathbb{Z}$ where $m \in \mathbb{N}$. But any element $ma \in m\mathbb{Z}$ means that for all $b \in \mathbb{Z}$ we have $bma = mba \in m\mathbb{Z}$, and $mab \in m\mathbb{Z}$.

Example. For $n \geq 2$, consider $\mathcal{M}_n(\mathbb{R})$. Consider the set

$$L = \{[u, 0, \ldots, 0] : u \in \mathbb{R}^n\}.$$

For any $A \in \mathcal{M}_n(\mathbb{R})$, we have $A[u, 0, \ldots, 0] = [Au, 0, \ldots, 0] \in L$. L is a left ideal, but not necessarily an ideal. In fact, this leads to a theorem:

Theorem 6.3.4. For $n \geq 2$, the ring $\mathcal{M}_n(\mathbb{R}) = \mathbb{R}^{n \times n}$ has no non-trivial ideals; that is, the only ideals are $I = \{0\}$ or $I = \mathbb{R}^{n \times n}$.

Proof. We only consider the case where $n = 2$. The other cases are similar. For $A \in \mathbb{R}^{2\times 2}$, and A is invertible, then $A \in I$ where I is an ideal. We also know that $\exists A^{-1} \in \mathbb{R}^{2\times 2}$, such that

$$AA^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in I.$$

Thus, $\forall B \in \mathbb{R}^{2\times 2}$, $id \cdot B \in I$, so $\mathbb{R}^{2\times 2} \subseteq I$. Since $I \subseteq \mathbb{R}^{2\times 2}$, we have that $I = \mathbb{R}^{2\times 2}$.

If A is not invertible, $A \in I, A \neq 0$, we can perform a series of elementary row and column operations on A to obtain

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

That is, $\exists P, Q \in \mathbb{R}^{2\times 2}$ such that

$$PAQ = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in I.$$

Then

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in I$$

And thus

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \text{id} \in I$$

Thus, by the same argument above, $I = \mathbb{R}^{2\times 2}$. Therefore, if I is an ideal of $\mathbb{R}^{2\times 2}$, then $I = \{0\}$ or $I = \mathbb{R}^{2\times 2}$. □

Lemma 6.3.5. If R is a ring, $\forall \alpha \in \Lambda$, I_α is an ideal of R implies that

$$E = \bigcap_{\alpha \in \Lambda} I_\alpha$$

is an ideal of R.

Proof.

1. $\forall \alpha \in \Lambda$, $0 \in I$. This implies that $0 \in E$.
2. Since $\forall \alpha \in \Lambda$, I_α is a subgroup of $(R, +)$, so is E by the previous chapter.
3. Suppose $r \in R$ and $a \in E$. Then $\forall \alpha \in \Lambda$, we have that $ra, ar \in I_\alpha$ so $ra, ar \in E$ so E is an ideal.

□

Just like we had the concepts of generating subsets, we can effectively generate

Definition 6.3.3 (Subring Generated by a Set)**.** Let $X \subset R$. We denote the ideal generated by X to be

$$(X) := \bigcap_{I : X \subset I} I.$$

This is the smallest ideal containing X.

Lemma 6.3.6. If R is a ring with unit 1, and $X \subset R$, and X is nonempty, then

$$(X) = \{r_1 x_1 s_1 + \cdots + r_m x_m s_m : r_i, s_i \in R, x_i \in X\}$$

Proof. Let I be the right hand side. Then I is an ideal of R, which is easy to verify. Now suppose $\alpha \in I$. Then $\alpha = r_1 x_1 s_1 + \cdots + r_m x_m s_m$. Each $r_i x_i s_i \in (X)$, so $\alpha \in (X)$. Hence $I = (X)$. □

Remark. If R is a commutative ring with unit 1, and $X \subset R$, then

$$(X) = \{r_1 x_1 + \cdots + r_m x_m : r_i \in R, x_i \in X\}.$$

Definition 6.3.4 (Quotient Ring)**.** Let R be a ring and I be an ideal. We define the quotient ring to be

$$R/I := \{a + I : a \in R\}.$$

This is an abelian group with respect to $+$. Moreover, we can define the product of two elements $\alpha, \beta \in R/I$. Let $\alpha = a + I$ and let $\beta = b + I$. Then

$$\alpha \cdot \beta := (ab + I).$$

It should be verified that $(R/I, +, \cdot)$ is a ring. This admits a quotient map $\pi : a \mapsto a + I$, which is also a homomorphism. We sometimes denote $a + I$ to be $[a]$.

Like we discussed earlier, when we had this "quotient" operation for groups and normal subgroups, this gave rise to the first isomorphism theorem. We can state a similar theorem for rings. The problem is making the diagram commute:

$$\begin{array}{ccc} R & \xrightarrow{\phi} & S \\ {\scriptstyle\pi}\downarrow & \nearrow_{\exists! \psi} & \\ T & & \end{array}$$

Where $\ker\pi \subseteq \ker\phi$ and where $\psi \circ \pi = \phi$.

Theorem 6.3.7. For rings R, S, T, if we have a homomorphism $\phi : R \to S$, and an onto homomorphism $\pi : R \to T$, and $\ker\pi \subseteq \ker\phi$, then there exists a unique homomorphism $\psi : T \to S$ such that $\psi \circ \pi = \phi$.

Theorem 6.3.8 (First Isomorphism Theorem for Rings)**.** If $\phi : R \to S$ is a ring homomorphism, then

1. $\ker\phi$ is an ideal, and
2. $R/\ker\phi \cong \mathrm{Im}(\phi)$.

Example. Consider the homomorphism $\phi : C([0,1],\mathbb{R}) \to \mathbb{R}$ given by

$$\phi : f \mapsto f(1/2).$$

The kernel of this is

$$\ker\phi = \{f \in C([0,1],\mathbb{R}) : f(1/2) = 0\}$$

And $\mathrm{Im}\,\phi = R$. Therefore,

$$C([01,],\mathbb{R})/\ker\phi \cong \mathbb{R}.$$

Example. Suppose R, S are rings, and $\pi : R \to S$ is an onto ring homomorphism. Then $\ker\pi \subset R$ is an ideal. Now we look at all the ideals in S. We claim that there is a one-to-one correspondence.

$$\{\text{ideals in } S\} \sim \{I : I \subset R \text{ is an ideal such that } \ker\pi \subset I\}.$$

This is given by

$$J \to \pi^{-1}(J)$$
$$\pi(I) \leftarrow I$$

This gives a bijection. The reason we showed this is made clear in the next example:

Example. Let R be a ring, and $I_0 \subset R$ is an ideal. We have the natural quotient map $\pi : R \to R/I_0$. Thus we claim

$$\{I : I \subset R \text{ is an ideal, } I_0 \subset I\} \cong \{J : J \text{ is an ideal of } R/I_0\}$$

This is the map given by

$$I \to \pi(I) = I/I_0$$
$$\pi^{-1}(J) \leftarrow J$$

Next, we want to understand when the quotient R/I_0 is a field? A field is much simpler than an arbitrary field. First, we make the following observation.

Theorem 6.3.9. Suppose R is a commutative ring with unit $1 \neq 0$. Then

$$R \text{ is a field } \iff \text{ any ideal of } R \text{ is either } 0 \text{ or } R.$$

Proof. Suppose $I \subset R$ is an ideal. If $I = 0$, we're done. If there is a nonzero element in I that is not 0, then this implies $\exists a \in I \setminus \{0\}$. Since we are in a field, then a^{-1} is also in the field. For any $r \in R$, we have that $(ra^{-1})a \in I$ since I is an ideal. This implies that for any $r \in I$, this implies that $R \subset I$. But we also have $I \subset R$. Therefore $R = I$.

Now suppose every ideal is either the whole thing or the trivial one. Now suppose $a \in R \setminus \{0\}$. We need to show that a is invertible. If we look at $(a) = \{ra : r \in R\}$, we know that this must be equal to all of R. This implies that $1 = ra$ for some $r \in R$. Therefore a is invertible. □

Now suppose R is a commutative ring with unit 1, and let $M \subset R$ be a propper ideal, or $M \neq R$ ($1 \notin M$). Then we have the map

$$\pi : R \to R/M$$

where the unit correspondsto $\pi(1) = [1] \neq [0]$. We showed before that

$$\{I : I \subset R \text{ is an ideal, } M \subset I\} \cong \{\text{ideals of } R/M\}$$

We have the correspondences

$$M \leftrightarrow 0$$
$$R \leftrightarrow R/M.$$

Definition 6.3.5. Let R be a ring with unit $1 \neq 0$, and let $M \subset R$ be a proper ideal. If

$$M \subset I \Rightarrow I = R \text{ or } I = M$$

then we say that M is a maximal ideal of R.

We have the following important theorem:

Theorem 6.3.10.

$$R/M \text{ is a field} \iff (M \text{ is a maximal ideal.}$$

Proof. This is our way of saying that the only ideals of R/M correspond to the ideals I where $M \subset I$. Clearly, if $M \subset I$ only for $I = R, M$, then $\pi(M) = 0$ and $\pi(R) = R/M$. Since these are the only two ideals in R/M, we know that R/M must be a field. □

Example. We went over the example where we had the evaluation map $\phi : f \mapsto f(1/2)$. We considered the set

$$\ker \phi = \{f \in C([0,1], \mathbb{R}) : f(1/2) = 0\}.$$

We also showed that

$$C([0,1], \mathbb{R})/\ker \phi \cong \mathbb{R}.$$

but $\mathbb{R}$ is a field. Therefore M must be a maximal ideal. As a matter of fact, we can do the same $\forall 0 \leq t \leq 1$.

Theorem 6.3.11. If M is a maximal ideal of $C([0,1], \mathbb{R})$, then for some $0 \leq t \leq 1$,

$$M = \{f \in C([0,1], \mathbb{R}) : f(t) = 0\}.$$

This is a very useful fact in the study of functional analysis.

6.4 Constructing Quotient Fields

First we discussed quotient rings, and then the first isomorphism theorem, and now we discussed when the quotient field is a ring.

Now consider the integral domain $\mathbb{Z}$. The most remarkable fact of $\mathbb{Z}$ is the fundamental theorem of arithmetic, or that every integer has a prime number decomposition. We want to see if any other integral domains have such a property, a "prime number decomposition" of sorts. This is a useful generalization since we want to eventually study polynomials. In particular, we will show that $\mathbb{R}[x_1, \ldots, x_m]$ and $\mathbb{C}[x_1, \ldots, x_m]$ are unique factorization domains. We will show this for so-called Euclidean domains (e.g., $\mathbb{R}[x]$).

The first step is to do the following. Suppose D is an integral domain. We'll discuss a so-called "embedding" theorem, which shows that we can find a field F such that D is a subring of F. For

instance, $\mathbb{Z} \subset \mathbb{Q}$. Another example is $\mathbb{R}[x] \subset \mathbb{R}(x)$, where $\mathbb{R}(x)$ is the rational functions. The remarkable fact is that this can be done for any integral domain D!

Let D be our integral domain, where D is a commutative ring $D \neq 0$ and $ab = 0 \Rightarrow a$ or $b = 0$.

But notice how in the example $\mathbb{Z} \to \mathbb{Q}$, we have that $5/3 = 10/6 = 25/15$. Therefore it makes sense to define an equivalence class in the quotient ring.

Define the relation $\sim$ on $D \times (D \setminus \{0\})$ given by

$$(a_1, a_2) \sim (b_1, b_2) \iff a_1 b_2 = a_2 b_1.$$

Claim. We claim that $\sim$ is an equivalence relation. The new field F will be $D \times (D \setminus \{0\})/\sim$. This is a very typical way of constructing new mathematical objects from old ones; we define an equivalence relation and take a quotient.

Proof.

1. (Reflexivity.) We have that for $(a_1, a1)$, $a_1 a_2 = a_2 a_1$, but this is true since D is commutative.
2. (symmetry.) This is also true since we can say $a_2 b_1 = a_1 b_2$.
3. (Transitivity.) Suppose $(a_1, b_1) \sim (a_2, b_2) \sim (a_3, b_3)$. Then

$$\begin{aligned} a_1 b_2 &= a_2 b_2 \\ a_2 b_3 &= a_3 b_2. \end{aligned}$$

   If we look at

$$\begin{aligned} a_1 b_2 b_3 &= a_2 b_1 b_3 \\ &= a_2 b_3 b_1 \\ &= a_3 b_2 b_1. \end{aligned}$$

   That is, $(a_1 b_3) b_2 = (a_3 b_1) b_2$. But $b_2 \neq 0$. Therefore this gives us $a_1 b_3 = a_3 b_1$ as desired.

□

Thus, let $F = D \times (D \setminus \{0\})/\sim$. The equivalence class of $(a, b) = [a, b]$. Next, we want to define operations on F so that F is a field.

1. For $\alpha_1, \alpha_2 \in F$, then we define

$$\alpha_1 + \alpha_2 = [a_1, b_1] + [a_2, b_2] = [a_1 b_2 + a_2 b_1, b_1 b_2].$$

2. For $\alpha_1, \alpha_2 \in F$, then we define

$$\alpha_1 \cdot \alpha_2 = [a_1, b_1] \cdot [a_2, b_2] = [a_1 a_2, b_1 b_2].$$

Claim. We need to show that $+, \cdot$ are well defined operations.

Proof. Let $\alpha_1 = [a_1, b_1] = [a_1', b_1']$. Let $\alpha_2 = [a_2, b_2] = [a_2', b_2']$. We have that $a_1 b_1' = a_1' b_1$, and $a_2 b_2' = a_2' b_2$. Then we need to have the equality

$$(a_1 b_2 + a_2 b_1) b_1 b_2' = (a_1' b_2' + a_2' b_1') b_1 b_2$$

which we can show from the equivalence relation formulas. Similar process for showing that multiplication is well defined. □

Notice how the equivalence relation is very reminiscent of how fractions work; indeed, $[5,3] = [10,6]$ in this case. In general, for any integral domain D, we have the following simplifications:

1. $[a,b] = [ac,bc],\ c \neq 0$.
2. $[a_1,b] + [a_2,b] = [a_1 + a_2, b]$.

Where the first implies the second. This is very similar to when two fractions have a common denominator. Now we have to show the field properties.

Theorem 6.4.1. The set $F = D \times (D \setminus \{0\})/\sim$ is a field with the operations

$$[a_1,b_1] + [a_2,b_2] = [a_1b_2 + a_2b_1, b_1b_2]$$
$$[a_1,b_1] \cdot [a_2,b_2] = [a_1a_2, b_1b_2].$$

Proof.

1. First, we show that F is a commutative ring with unit. We have that $(F,+)$ is an abelian group. The additive identity element is just $0 = [0,b], \forall b \in D \setminus \{0\}$. Note that for any $b_1, b_2 \in D \setminus \{0\}$, that $[0,b_1] = [0,b_2]$. Then if we have $\alpha = [a,b]$, then we can represent 0 as $[0,b]$, so we can simply add the first slot to get $\alpha + 0 = [a,b] + [0,b] = [a,b] = \alpha$. The fact that $+$ is commutative is clear since D is commutative. Moreover, every element has an inverse with respect to $+$; $-\alpha = [-a,b]$. Moreover, $+$ is associative which can be proven by expanding. Thus, $(F,+)$ is an abelian group.

2. We now show that product $\cdot$ is associative and commutative. This is simple, since

$$(\alpha_1\alpha_2)\alpha_3 = [(a_1a_2)a_3, (b_1b_2)b_3] = [a_1(a_2a_3), b_1(b_2b_3)] = \alpha_1(\alpha_2\alpha_3).$$

and

$$\alpha_1\alpha_2 = [a_1a_2, b_1b_2] = [a_2a_1, b_2b_1] = \alpha_2\alpha_1.$$

3. In order to prove the distributive laws, we can do the trick where we make the two elements have the same common denominator.

4. The unit element is $1 = [b,b]$ for all $b \neq 0$. This is well defined since $[b_1,b_1] = [b_2,b_2]$. Moreover, $\alpha \cdot 1 = [a,b] \cdot [b,b] = [ab,bb] = [a,b] = \alpha$. Clearly, this unit element is also not equal to 0. Indeed, $(F,+,\cdot)$ is a ring with unit.

5. We now show that every nonzero element is invertible. Given $\alpha = [a,b]$, we have that $a \neq 0$ and $b \neq 0$, since $\alpha \neq 0$. Thus, we claim that $\alpha^{-1} = [b,a]$ does the job, since $\alpha\alpha^{-1} = [ab,ab] = 1$. Therefore, $(F,+,\cdot)$ is a field.

□

Now we show that there can be an imbedding (a one-to-one ring homomorphism) between D and F.

Theorem 6.4.2 (Embedding Theorem)**.** For an integral domain D, we can find an injective ring homomorphism

$$\phi : D \to F$$

i.e., we can view D as a subring of F.

Proof. For $a \in D$, then $\forall b_2, b_2 \in D \setminus \{0\}$,

$$[ab_1, b_1] = [ab_2, b_2].$$

The reason we don't let $b_1, b_2 = 1$ is because D may not have a unit element. Then we define

$$\phi(a) = [ab, b], \ \forall b \in D \setminus \{0\}.$$

We can show that ϕ is a ring homomorphism:

1. $\phi(a_1 + a_2) = [(a_1 + a_2)b, b] = [a_1 b + a_2 b, b] = [a_1, b] + [a_2, b] = \phi(a_1) + \phi(a_2)$.
2. $\phi(a_1)\phi(a_2) = [a_1 b, b][a_2 b, b] = [a_1 a_2 b^2, b^2] = [a_1 a_2 b, b] = \phi(a_1 a_2)$.

Now demonstrate ϕ is one-to-one. Suppose $a \in \ker \phi$. Then $\phi(a) = 0 = [0, b]$. Thus $ab^2 = 0$; but since d is an integral domain and $b \neq 0$, then $a = 0$. □

This whole process is very powerful. We start with an integral domain, and can turn it most naturall into a field. As a matter of fact, we can show that this F is in some sense the smallest field that contains D!

Theorem 6.4.3. Let $D \subset K$ where K is a field. Then K has a subfield that is isomorphic to F.

Proof. Consider the map $\phi : F \to K$ given by for $[a, b] \in F$,

$$\phi : [a, b] \mapsto ab^{-1} \in K.$$

The claim is that by ϕ, $F \cong \operatorname{Im} \phi$, where $D \subset \operatorname{Im} \phi \subset K$. Clearly, for all $d \in D$, $d = \phi([d, 1])$, so $D \subset \operatorname{Im} \phi$. Next, we show that ϕ is a ring homomorphism:

1. $\phi([a, b] + [c, d]) = \phi([ad + bc, bd]) = ad(bd)^{-1} + bc(bd)^{-1} = \phi([ad, bd]) + \phi([bc, bd])$. This is because $(a, b) \sim (ad, bd)$ for $d \neq 0$.
2. $\phi([a, b][c, d]) = \phi([ac, bd]) = ac(bd)^{-1} = ab^{-1}cd^{-1} = \phi([a, b])\phi([c, d])$.

Next, we verify that ϕ is injective. If we can do this, then $\operatorname{Im} \phi$ is isomorphic to F.

Suppose $\phi([a, b]) = \phi([c, d])$. This means that $ab^{-1} = cd^{-1}$. Then $ad = bc$; but by $\sim$, this implies that $(a, b) \sim (c, d)$. Thus $[a, b] = [c, d]$. By the first isomorphism theorem for rings, this means that $\ker \phi = [0, d]$ and that

$$F / \ker \phi = F \cong \operatorname{Im} \phi.$$

□

In some sense, this means that we have done the bare minimum to embed D into a field, which is powerful.

6.5 Unique Factorization Domains

What was reason we went throguh lengths to prove that we can embed an integral domain in a field? If you recall our main goal, we wanted to generalize the fundamental theorem of arithmetic to certain integral domains. In particular, we wanted to do this for polynomial rings over integral domains, $D[x]$.

Definition 6.5.1. Suppose $a, b \in D$ where D is an integral domain, and $a \neq 0$. We say that $a|b$ if $b = ac$ for some $c \in D$.

However, though we had that $(a|b \wedge b|a) \Rightarrow a = b)$, we may not have the same in integral domains, since they may differ up to a sign.

Definition 6.5.2. For $a, b \in D$, we say that $a \sim b$ if $\exists u \in D^\times$ (u is invertible) such that

$$a = bu.$$

It is easy to check that this is an equivalence relation. We say a and b only differ by an invertible element. The reason we defined this is for the following fact:

Lemma 6.5.1. If $a, b \in D \setminus \{0\}$, and $a|b$ and $b|a$, then $a \sim b$.

Proof. We have $b = ac$ and $a = bd$. Thus $a = bd = acd = a \cdot 1$. Thus $cd = 1$, so $c, d \in D^\times$. Thus $a \sim b$. □

For $a \in D$, $a = (au)u^{-1} \forall u \in D^\times$. But this is a trivial way to write a, much like for primes, $p = p(x/x)$ where x is invertible is the only way to factor p. Thus, we provide an analogous definition for integral domains.

Definition 6.5.3 (Irreducible Elements)**.** If $p \in D \setminus \{0\}$, and p is not invertible, and

$$p = ab \Rightarrow aD^\times \text{ or } b \in D^\times$$

then we say p is an irreducible element in D.

Example. The polynomial $3x+10 \in \mathbb{R}[x]$ is irreducible. It's nonzero since only constant polynomials are invertible in $\mathbb{R}[x]$. Now suppose $3x + 1 = fg$. This implies that $\deg(f) + \deg(g) = 1$. But $\deg(f), \deg(g) \geq 0$. Thus $\deg(f)$ or $\deg(g) = 0$. Thus f or g is invertible. In general, degree 1 polynomials are irreducible, and degree 2 polynomials may not be.

Lemma 6.5.2. If $p \in D$ is irreducible, and $p \sim q$, then q is also irreducible.

Proof. If $q = pu$, where $u \in D^\times$, then $q \neq 0$. This also shows that $q \notin D^\times$, since we would have $puq^{-1} = 1$ so p would be invertible, a contradiction. Thus, if $q = ab$, then $pu = ab$ so $p = abu^{-1}$. This implies that $a \sim 1$ or $bu^{-1} \sim 1$. Then this implies that $a \sim 1$ or $b \sim 1$, which is equivalent to saying either a or b is invertible. □

Definition 6.5.4. Let D be an integral domain with unit $1 \neq 0$. If for every $a \in D$, $a \neq 0$, and $a \notin D^\times$, then

1. $a = p_1 p_2 \cdots p_r$ where p_i are irreducible, and
2. If $a = p_1 \cdots p_r = q_1 \cdots q_s$, where p_i, q_j are prime, then $r = s$, and $p_1 \sim q_i$ after permutation,

then we say that D is a unique factorization domain (UFD).

Example. $\mathbb{Z}$ is a unique factorization domain.

6.5.1 Polynomial Rings Revisited

In order to discuss implications, we discuss polynomial rings briefly. Recall that for a commutative ring R, we let

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n : a_i \in R, n \in \mathbb{N}\}$$

and the degree of f is $\deg(f)$. Moreover, $(R, +, \cdot)$ is also a ring.

Lemma 6.5.3. If D is an integral domain, then so is $D[x]$. Moreover, for $f, g \in D[x]$, we have that if $f, g \neq 0$, then $\deg(fg) = \deg(f) + \deg(g)$.

Example. For a polynomial ring $\mathbb{R}[x, y] = \mathbb{R}[x][y]$. The reason is that we can regroup it so that we isolate the degrees of y; we can consider any two variable polynomial as having coefficients in $\mathbb{R}[x]$. This helps us for the following fact:

Corollary 6.5.4. If D is an integral domain, then so is $D[x_1, \ldots, x_n]$.

Proof. We can do this inductively. We proved that $D[x_1]$ is an integral domain if D is an integral domain. □

In particular, if K is a field (which is an integral domain), then so is $K[x_1, \ldots, x_n]$.

6.6 Euclidean Domains

We initiated our study of unique factorization domain in order to generalize the structure of the integers. We now turn to a particular example of unique factorization domains, known as Euclidean Domains (EUD).

Definition 6.6.1. Suppose D is an integral domain, and $D \neq \{0\}$. If there exists a function $d : D \setminus \{0\} \to \mathbb{N}$ which satisfies

1. $a, b \in D \setminus \{0\} \Rightarrow d(a) \leq d(ab)$.
2. If $a \in D$, $b \in D \setminus \{0\} \Rightarrow \exists q, r \in D$ such that

$$a = bq + r$$

with $r = 0$ or $r \neq 0$ and $d(r) < d(b)$

then we say D is a Eulidean Domain.

Notice how we define the function d with the degree of polynomials in mind.

Example. Suppose $D = \mathbb{Z}$, and $d(a) = |a|$. We can verify that this is a Euclidean domain:

1. $d(ab) = |ab| = |a||b| \geq |a| = d(a)$.
2. Since $|a|$ may lie between integer multiples of $|b|$, we can always find q such that $|a - qb| < |b|$. Then let $r = a - qb$; then $a = bq + r$, and $r = 0$ or $d(r) = |r| < |b| = d(b)$.

The next example is very important.

Example. Let K be a field, and consider $K[x]$, where $f \in K[x] \setminus \{0\}$. Let $d(f) = \deg(f) \in \mathbb{N}$.

1. Suppose $f, g \in K[x] \setminus \{0\}$. Then we have that

$$d(fg) = d(f) + d(g) \geq d(f).$$

2. $f \in K[x]$, $g \in K[x] \setminus \{0\}$. Then

$$f = gh + r$$

where $h, r \in K[x]$ and $r = 0$ or $\deg(r) < \deg(h)$. This is by the long division formula we learned for polynomials in high school which eventually yields a remainder term.

Example. We denote $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ as the Gaussian Integers. We will now prove that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$, and that it is therefore an integral domain. Suppose $\alpha, \beta \in \mathbb{Z}[i]$. Let $\alpha = a_1 + b_1 i$, and $\beta = a_2 + b_2 i$. Then $\alpha - \beta = (a_1 - a_2) + (b_1 - b_2)i \in \mathbb{Z}[i]$. Thus $\mathbb{Z}[i]$ is a subgroup of $(\mathbb{C}, +)$.

Now we show that they are closed under product. Then $\alpha\beta = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i$. Thus $\mathbb{Z}[i]$ is subring of $\mathbb{C}$, so it is an integral domain.

In order to show that it is a Euclidean Domain, we define $d(\alpha) = a^2 + b^2$.

1. For $\alpha, \beta \in \mathbb{Z}[i]$, we have that

$$d(\alpha\beta) = |\alpha\beta|^2 = (|\alpha||\beta|)^2 = d(\alpha)d(\beta) \geq d(\alpha).$$

2. Suppose $\alpha \in \mathbb{Z}[i]$ and $\beta \in \mathbb{Z}[i] \setminus \{0\}$. The quantity $\alpha/\beta \in \mathbb{C}$. If we visualize the Gaussian Integers, it can be thought of as a grid pattern with each α at an intersection. Then $\exists \gamma \in \mathbb{Z}[i]$ such that $|\alpha/\beta - \gamma| < 1$, or $|\alpha - \beta\gamma| < |\beta|$. Then let $r = \alpha - \beta\gamma$. Then $\alpha = \beta\gamma + r$, and either $r = 0$ or
$$d(r) = |r|^2 < |\beta|^2 = d(\beta).$$
Thus $\mathbb{Z}[i]$ is a Euclidean Domain.

Remark. It is worth noting that the remainder term r and the quotient term q may not even be unique. For instance, in the previous example, there were a few selections we could make of γ.

6.7 Principal Ideal Domains

In this section, we show the result that every ideal can be generated by a single element in a Euclidean Domain.

Definition 6.7.1 (Principal Ideal Domain)**.** If D is an integral domain with unit $1 \neq 0$ such that every ideal is generated by one element, then we say that D is a principal ideal domain (PID).

Theorem 6.7.1 (EUDs are PIDs)**.** Suppose D is a Euclidean Domain, and $I \subset D$ is a nonzero ideal. Then $\exists a_0 \in I$ such that
$$I = (a_0) = \{a_0 b : b \in D\}.$$

Proof. We know that $\exists a_0 \in I$ such that $d(a_0) \leq d(a)$, $\forall \in I \setminus \{0\}$. THen the claim is that $I = (a_0)$. Clearly, $(a_0) \subset I$; next we need to show the other direction.

If $a \in I, a \neq 0$, then $a = a_0 q + r$, $q, r \in D$. Here, either $r = 0$ or $r \neq 0$ but $d(r) < d(a)$. We claim that $r = 0$. If not, then $r = a - a_0 b \in I$, so $d(r) < d(a_0)$ which contradicts our choice of a_0 as having the smallest d-value. Then $r = 0$ and thus $a \in (a_0)$. Therefore $I = (a_0)$. □

Theorem 6.7.2. If D is a Euclidean domain, then D has a unit element $1 \neq 0$.

Proof. D itself is a nonzero ideal. Then there is an $a_0 \in D$ such that $D = (a_0)$. Now we know that $a_0 \neq 0$, since otherwise $D = 0$. Thus $a_0 = a_0 u$ for some $u \in D$. For $a \in D$, we have $a_0 u a = a_0 a$. This implies that $ua = a$. This tells us that u is the unit element in D. □

In fact, principal ideal domains are unique factorization domains, a fact we will not prove here.

Example. Some examples are $\mathbb{Z}$, $\mathbb{Z}[i]$, and $\mathbb{F}[x]$.

Example. A counter example to aomething that is not a PID (and hence not an EUD) is $\mathbb{R}[x, y]$. Let I be an ideal, and $I = \{p \in \mathbb{R}[x, y] : p(0, 0) = 0\}$; then I is not a principal ideal.

Proof. If I is a principal ideal, so $I = (p)$; this implies that $x \in I$ implies that $x = pq$. Then recall that any $f \in \mathbb{R}[x, y]$ as $R[x][y]$. Then $\deg_y(x) = \deg_y(p) + \deg_y(q)$. But $\deg_y(x)$ is just 0, which implies that $\deg_y(p) = 0$. That means that there is no y term in p. Now for $y \in I$, we can do the same and get that $\deg_x(p) = 0$. This means that p is a constant polynomial which is nonzero, since $I \neq \{0\}$. But this contradicts how we constructed I, since we said that $p(0, 0) = 0$. Therefore I is not principal ideal. □

Now we show that $EUD \subset UFD$. This means we can do similar things like we can do for integers. This doesn't mean that it will be easy for us to find the unique factorization, even though we know it exits. But there may be some special cases in which we can compute the irreducibles that form an element.

Theorem 6.7.3 (EUDs are UFDs)**.** If $D \neq 0$ is a Euclidean domain, then D is also a unique factorization domain.

Proof. Let D be an EUD. If $a, b \in D \setminus \{0\}$, and b is not invertible, then $d(a) < d(ab)$. If $d(a) = d(b)$, then $a = (ab)c + r$. The claim is that $r = 0$. If $r \neq 0$, then from the d inequality we have that $d(r) < d(ab) = d(a)$, so $r = a - ab = a(1 - bc) \neq 0$, so $d(r) \geq d(a)$ which is a contradiction. Then $r = 0$. Thus we have $a = abc$, so $bc = 1$. Thus b is invertible, which is a contradiction. Thus $d(a) < d(ab)$. If $a \sim b$ by an invertible element, then $d(a) = d(b)$.

Every $a \in D \setminus \{0\}$, a is not invertible, then we prove that $a = p_1 \cdots p_m$, where p_i are prime elements. This is proved by induction, like the fundamental theorem of arithmetic. Assume if a is not the product of finitely many irreducible elements, then a is not irreducible. Thus $a = a_1 b_1$, and a_1, b_1 are not invertible. Then either a_1 or b_1 is not the product of finitely many prime elements. Without loss of generality, we say a_1 is not the product of finitely many irreducible elements. Then a_1 is not prime; $a - 1 = a_2 b_2$ where a_2 or b_2 are not invertible and one of them (say a_2) is not the product of irreducibles. This process repeats. Then we have a sequence of elements, none of which are a product of primes. Then by the above, we have that $d(a) > d(a_1)$. Then we have the chain of inequality

$$d(a) > d(a_1) > d(a_2) > \ldots, \ d(a_i) \geq 0$$

which is a contradiction, since d is always an integer value, the inequalities are strict, and $d(a)$ is finite. Therefore, all Euclidean domains are unique factorization domains. □

Corollary 6.7.4. If D is a Euclidean Domain, and $a, b \in D \setminus \{0\}$, if b is not invertible, then

$$d(a) < d(ab).$$

Theorem 6.7.5 (Uniqueness of Decomposition)**.** *Proof.* If $a, b \in D$ where D is a unique factorization domain. Then consider (a, b). Since every EUD is a PID, then $(a, b) = (c)$, where $c \neq 0$ and is not necessarily unique. Then suppose $(c_1) = (c_2) = (a, b)$. Then $c_1 \sim c_2$. Now $c|a$ and $c|b$, and let $d|a$ and $d|c$. Hence we call c the greatest common divisor of a and b, denoted $c = \gcd(a, b)$. Now suppose p is an irreducible, and $p \not| a$. Then $\gcd(p, a) \sim 1$. This is because $\gcd(p, a)|p$, so $\gcd(p, a) \sim p$ or $\gcd(p, a) \sim p$, so it can only be the first one.

Assume $a|bc$, and $\gcd(a, b) \sim 1$. Then $a|c$ since $r_1 a + r_2 b = 1 \Rightarrow c = r_1 ac + r_2 bc$. Thus $a|r_1 ac, a|r_2 bc$. Thus $a|c$.

Now suppose $a \in D \setminus \{0\}$ which si not invertible. Let

$$a = p_1 \cdots p_m = q_1 \cdots q_n.$$

Then $m = n$ and after permutation, $p_i \sim q_i$.

We do induction on m; if $m = 1$, then we have $p_1 = q_1 \cdots q_n$. This implies $n = 1$; if not, then since p_1 is irreducible, then it must be that $q_2 \cdots q_n \sim 1$. This implies that q_2 is invertible, which is a contradiction.

Now assume it is true for $m < M >\geq$. Now for $m = M$, Then we have $p_1 \cdots p_M = q_1 \cdots q_n$. Then $p_M | q_1 \cdots q_n$. Then $\exists i : p_M \sim q_i$. If not, then $\gcd(p_M, q_n) \sim 1 \Rightarrow p_M | q_1 \cdots q_{n-1} \Rightarrow p_M | q_1 \cdots q_{n-2}$, and so on, intil we get that $p_M | 1$, which means that p_M is invertible, a contradiction. By reordering, assume $p_M \sim q_n$. Then $p_1, \cdots p_{M-1} = q_1 \cdots q_{n-1} u$ where u is invertible. This tells us that $n \geq 2$. By the induction hypothesis, we get that $M - 1 = n - 1$; then $m = n$. Then we get that after reordering, $p_i \sim q_i$ for $1 \leq i \leq M - 1$. Hence we have proved the same for M, so $p_M \sim q_M$. □

Remark. For $a, b \in D \setminus \{0\}$, then we can use the Euclidean algorithm which tells us

$$\gcd(a, b) = \gcd(b, r).$$

This procdedure must halt, because otherwise we will get the infinite inequality like we did before.

Now we turn to our main focus, converning polynomials. Some applications of this will be that if F is a field, then $F[x]$ is a UFD; and then so is $F[x_1][x_2] = F[x_1, x_2]$, and for any number of variables.

Theorem 6.7.6. If D is a UFD, then so is $D[x]$.

Before we prove it, we make the following remark:

Remark. If D is a UFD, and $a_1, \ldots, a_m \in D$ are not all 0's, we have that the $\gcd(a_1, \ldots, a_m)$ exists.

From now on, we always assume that D is a UFD. For $f \in D[x] \setminus \{0\}$, then we make the following observations:

1. If f is invertible in $D[x]$, then it is a constant polynomial. This can be proven using the degrees.
2. $f(x) = a_n x^n + \cdots + a_0$, where $a_n \neq 0$. We define the content of f to be
$$C(f) := \gcd(a_n, a_{n-1}, \ldots, a_0).$$
If $C(f) = 1$, then we call f a primitive polynomial.

Lemma 6.7.7 (Gauss)**.** If $f, g \in D[x] \setminus \{0\}$, then
$$C(fg) = C(f)C(g).$$
In particular, if $C(f), C(g) = 1$ then $C(fg) = 1$.

Proof. Let $f = a_m x^m + \cdots + a_0$, and let $g = b_n x^n + \cdots + b_0$, where $a_n, b_n \neq 0$. Then $f \cdot g$ is a polyonomial $fg = d_{m+n}x^{m+n} + \cdots + d_0$. We need that $\gcd(d_{m+n}, \ldots, d_0)$. We need to show that we cannot find an irreducible element p dividing all the coefficients.

Given p irreducible, then p must not divide some a_k, b_ℓ since $C(f) = C(g) = 1$. Then look at $d_{k+\ell}$, wich is $\sum_{i+j=k+\ell} a_i b_j$. Then $p \not| a_k b_\ell$, but $p | a_{k+1} b_{\ell-1}$, and $p | a_{k+2} b_{\ell-2}$, etc. Thus $p \not| d_{k+\ell}$. Then $\gcd(d_{m+n}, \ldots, d_0) = 1$, or $C(fg) = 1$.

To complete the proof, if you look at $f = C(f) \cdot f_1$, where $C(f_1) = 1$, and $g = C(g) \cdot g_1$, where $C(g_1) = 1$, then $fg = C(f)C(g)f_1 g_1$, thus $C(fg) = C(f)C(g)C(f_1 g_1) = C(f)C(g)$. □

Once we have this, we have the following. Since D is a UFD, then $D \subset F$ is the quotient field of D which we constructed. Suppose $f \in F[x] \setminus \{0\}$. Then
$$f = \frac{a_n}{b_n} x^n + \cdots + \frac{a_0}{b_0}$$
where $a_i, b_i \in D$. We can multiply and divide f by $1/b = 1/(b_n \cdot b_0)$, and then take out $C(f) = a$ so we can get a polynomial
$$f = \frac{a}{b} f_1$$
where $C(f_1) = 1$. We can also assume that $\gcd(a, b) = 1$. Then we have the following:

Lemma 6.7.8. Let $f \in D[x] \setminus \{0\}$, and $C(f) = 1$. Then
$$f \text{ is prime in } D[x] \text{ which is a UFD (may not be EUD)} \iff f \text{ is prime in } F[x] \text{ (EUD)}.$$
where $F[x]$ is the ring of polynomials over the quotient field F of D.

Proof. Suppose f is prime in $D[x]$, and $f = gh$, where $g, h \in F[x]$. Then we can write
$$g = \frac{a_1}{b_1} g_1, \ g_1 \in D[x], \ C(g_1) = 1$$
$$h = \frac{a_2}{b_2} h_1, \ h_1 \in D[x], \ C(h_1) = 1.$$

This means that

$$f = \frac{a_1 a_2}{b_1 b_2} g_1 h_1$$

from which we get the equality $b_1 b_2 f = a_1 a_2 g_1 h_1$. Then $c(b_1 b_2 f) = c(a_1 a_2 g_1 h_1)$, so $b_1 b_2 \sim a_1 a_2$. Then $a_1 a_2 = b_1 b_2 u$ where u is invertible. Thus

$$f = u g_1 h_1 = (u g_1) h_1 \in D[x].$$

but f is prime in $D[x]$. This means that g_1 or h_1 are invertible. This tells us that, WLOG, $\deg(g_1) = 0 \Rightarrow \deg(g) = 0$ so g is invertible in $F[x]$, so f is prime in $F[x]$.

Suppose f is a prime polynomial in $F[x]$. Suppose $f(x) = g(x)h(x)$. We hope to show that one of them must be invertible in $F[x]$. Let's say that g is invertible; this means that g must be a constant polynomial, and so $\deg(g) = 0$. Then $g(x) = a \in D \setminus \{0\}$. Then $f(x) = ah(x)$. Because the content of f is equivalent to 1, this tells us that $a \in D^\times$. Therefore, we have proven that if f is prime in $F[x]$, it is prime in $D[x]$. □

Now we are able to prove the main theorem:

Theorem 6.7.9. If D is a UFD, then $D[x]$ is a UFD.

Proof. Suppose $f \in D[x] \setminus \{0\}$. Suppose that f is not invertible. Then $f \notin D[x]^\times = D^\times$. If $\deg(f) = 0$, then $f = p_1 p_2 \cdots p_m, p_i \in D$ are irreducible. Then p_i's are also prime in $D[x]$.

If $\deg(f) >)$, then $f = C(f) f_1$ where f_1 is primitive, and $f_1 \in D[x]$. Now we can do prime decomposition in D. We know that $f_1 \in F[x]$, and $f_1 = g_1 \cdots g_m, g_i \in F[x]$ and g are irreducible and rational coefficients;

$$g_i = \frac{a_i}{b_i} h_i,\ h_i \in D[x],\ C(h_i) = 1,\ a_i, b_i \in D \setminus \{0\}.$$

This implies that h_i is irreducible in $F[x]$, since it differs from the irreducible g by invertible elements in F. Thus h_i is prime in $F[x]$, and by the above lemma, it is also prime in $D[x]$. Then

$$f_1 = \frac{a}{b} h_1 h_2 \dots h_m$$

we can rearrange this to

$$b f_1 = a h_1 \cdots h_m$$

The content of both sides,

$$C(b f_1) \sim C(a h_1 \cdots h_m)$$

Thus $a = bu$ where $u \in D^\times$. Then $f_1 = u h_1 \cdots h_m$. But this means that f has a prime composition in $D[x]$ too.

Now we need to prove uniqueness of this decomposition. Suppose $f \in D \setminus \{0\}$, and f is not invertible. Then $f \sim g_1 \cdots g_m \sim h_1 \cdots h_n$. Then if $\deg(f) = 0$, then $\deg(g_i) = 0 = \deg(h_i)$. We know that g_i, h_i are prime in D. therefore, $m = n$ and $g_i \sim h_i$ after permutation.

If $\deg(f) \geq 1$, then we write $f \sim a_1 \cdots a_r g_1 \cdots g_m \sim b_1 \cdots b_s h_1 \cdots h_n$. Where $a_i \in D$ is irreducible, and $g_i \in D[x]$ are irreducible, and $\deg(g_i) \geq 1$, and similarly $b_i \in D$ are irreducible and $h_i \in D[x]$ are irreducible and $\deg(h_i) \geq 1$. Thus g_i must be primitive, and so is h_i. The content of both sides means that $a_1 \cdots a_r \sim b_1 \dots b_s$. WLOG, we can assume that $a_1 \cdots a_r = b_1 \cdots b_s$ since you can move the invertible elements somewhere. Since all of these are prime, $r = s$ and $a_i \sim b_i$ after permutation. This means that g_i, h_i are also prime in $F[x]$. This tells us $m = n$ and $g_i \sim h_i$ after permutation in $F[x]$. This tells us

$$g_i(x) = \frac{a}{b} h_i(x),\ a, b \in D \setminus \{0\}.$$

Then we get $a h_i = b g_i$, so by taking the content of both sides, $a \sim b$, so $a = bu$. This means that $g_i(x) = u h_i(x)$. □

Example. If $\mathbb{Z}$ is a EUD, then $\mathbb{Z}[x]$ is a UFD. Since $\mathbb{Q}$ is a field, then we have that $\mathbb{Q}[x], \mathbb{Q}[x,y]$ are UFD, and similarly $\mathbb{C}[x], \mathbb{C}[x,y]$ are UFD. This does not mean we can easily know which polynomials are prime, although there are some cases when we can easily find it out.

Theorem 6.7.10. In $\mathbb{C}[x]$, a polynomial is prime if and only if it is of degree 1.

Proof. If p is prime in $\mathbb{C}[x]$, and $\deg(p) \geq 1$. Then we can split the polynomial into $p(x) = c_n(x-\rho_1)(x-\rho_2)\cdots(x-\rho_n)$, $\rho_j \in \mathbb{C}$. This implies that $n = 1$ otherwise it would be the product of polynomials.

Conversely, if $\deg(p) = 1$, then $p = gh$, so we get that $\deg(g) + \deg(h) = 1$ which implies that $\deg(g) = 0$ or $\deg(h) = 0$. Thus p is an irreducible. □

What are prime polynomials in $\mathbb{R}[x]$? It's easy to check that degree 1 polynomials are. Moreover, so are quadratic polynomials with no real roots (i.e., $x^2 + bx + c, b^2 - 4ac < 0$). However, these are all of them. If its degree is greater than or equal to 3, we can derive a contradiction. There is always the nontrivial factorization of

$$p = (x-\alpha)(x-\overline{\alpha})q$$

where $\alpha \in \mathbb{C} \setminus \mathbb{R}$, and q has degree ≥ 1.

Things become much harder for $\mathbb{Q}[x]$. A special example is a minor case but is also crucial.

Theorem 6.7.11 (Eisenstein Criterion)**.** Let $f \in \mathbb{Z}[x]$, and suppose $f = a_n x^n + \cdots + a_0$. Suppose p is a fixed prime such that $p \not| a_n$, $p|a_i$ where $0 \leq i \leq n-1$, but $p^2 \not| a_0$. Then this f is prime in $\mathbb{Q}[x]$.

Proof. Assume f is primitive, since we can pull out common divisors. Then we only need to show that f is prime in $\mathbb{Z}[x]$. Now we do it by contradiction.

If f is not prime in $\mathbb{Z}[x]$, and $f(x) = g(x)h(x)$, and g, h are not invertible in $\mathbb{Z}[x]$. Then this implies that $\deg(g), \deg(h) \geq 1$. If not, then if $\deg(g) = 0$, since f is primitive, then $g = \pm 1$, which would mean that g is invertible in $\mathbb{Z}[x]$, a contradiction. We write

$$g(x) = b_r x^r + \cdots + b_0$$
$$h(x) = c_S x^s + \cdots + c_0$$

and write their product as $a_n x^n + \cdots + a_0$. Moreover, $a_0 = b_0 c_0$. Since p divides a_0, then $p|b_0$ or $p|c_0$. Say $p|b_0$; since $p^2 \not| a_0$, then $p \not| c_0$. On the other hand, $a_n = b_r c_s$, but $p \not| a_n$, so $p \not| b_r$. We can go through, and let $p \not| b_k$, where $k \leq r$ be the least such k. Then $a_k = b_k + b_{k-1}c_1 + \cdots + b_0 c_k$. Therefore, we have that $p \not| a_k$, and $k \leq r < r + s$. But this means that $k < n$, so $p|a_k$. This gives us a contradiction. □

Corollary 6.7.12. IF p is a prime number, $m \in \mathbb{N}$, then

$$x^m - p$$

is irreducible in $\mathbb{Q}[x]$.

Proof. $p \not| 1$, and $p|0$, $p|-p$, and $p^2 \not| p$. Thus $x^m - p$ is irreducible. □

This next example is very important for when we're learning field theory.

Lemma 6.7.13. Let p be a fixed prime number. Then

$$1 + x + x^2 + \cdots + x^{p-1}$$

is prime in $\mathbb{Q}[x]$.

Proof. Looking at the geometric series, we can make it equal to

$$1 + x + x^2 + \cdots + x^{p-1} = \frac{x^p - 1}{x - 1}.$$

Executing a change of variables, let $x - 1 = y$. Then

$$\begin{aligned}\frac{(y+1)^p - 1}{y} &= \frac{y^p + \binom{p}{1}y^{p-1} + \cdots + \binom{p}{p-1}y + 1 - 1}{y} \\ &= y^{p-1} + \binom{p}{1}y^{p-2} + \cdots + \binom{p}{p-1}.\end{aligned}$$

Then since $\mathbb{Q}[x]$ and $\mathbb{Q}[y]$ are integral domains, we know that they are isomorphic via $x \mapsto y - 1$. Then we have the Eisenstein criteron, since $p \not| 1$, but $p|\binom{p}{k}$, and $p^2 \not| \binom{p}{p-1}$. Then this tells us that the polynomial is prime in $\mathbb{Q}[y]$, so it is also prime in $\mathbb{Q}[x]$ since they are isomorphic. □