Math 113 Notes

Kanyes Thaker

Spring 2020

0.1 Introduction

This document is an overview of Math 113, Abstract Algebra, at UC Berkeley. These notes are largely based off of *A First Course in Abstract Algebra* by John B. Fraleigh and lectures by Jeremy Lovejoy. This class does not require any prior mathematical knowledge outside of high school algebra; in fact, this course is entirely focused on constructing the key algebraic components that allow for high school algebra to fundamentally exist. These are not a replacement for lectures, labs, or discussions, but should provide a good enough overview to review for exams!

Contents

1 Introduction

We begin with some basic definitions. A **set** is, to put it simply, a collection of objects made of **elements**. If a is an element of S, we say that $a \in S$. Exactly one set exists with no elements; the **empty set** $\emptyset$.

A set can be given explicitly (person A, person B, person C) or be defined by a rule (the set of people in Math 113 over the age of 20). An explicit definition consists of a comma-separated list of elements enclosed in curly braces, i.e. $\{1, 2, 3\}$. If the set is defined by a rule $P(x)$ on its elements $x \in S$, we write $\{x|P(x)\}$.

A set is **well-defined**, meaning we know for sure whether or not an element is in S. We can't say that "S consists of a couple of numbers," since this doesn't give us a way to know whether or not a number is definitely in S.

For two sets B and A, B is a **subset** of A ($B \subseteq A$) if for every element in B is also in A. If $B \neq A$ but $B \subseteq A$, we say $B \subset A$ (B is then a proper subset of A). This means that $A \subseteq A$ and $\emptyset \subseteq A$.

Let A and B be sets. The **Cartesian product** of A and B is the set $A \times B = \{(a, b)|a \in A,\ b \in B\}$.

Some Common Sets

The set $\mathbb{Z}$ is the set of **integers**, i.e. positive and negative whole numbers and zero.

The set $\mathbb{Q}$ is the set of all **rational** numbers, i.e. numbers that can be expressed as quotients of m/n where $m \in \mathbb{Z}$ and $n \in \mathbb{Z}$, with $n \neq 0$.
$\mathbb{R}$ is the set of **real numbers**.

$\mathbb{Z}^+$, $\mathbb{Q}^+$, $\mathbb{R}^+$ are the set of all positive valued integers, rationals, and reals, respectively.

$\mathbb{C}$ is the set of all **complex** numbers.

$\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$are the set of all nonzero integers, rationals, reals, and complex numbers.

1.1 Set Relations

An element $a \in A$ **is related to** $b \in B$, if it (a, b) element of $\mathscr{R}$, where $a\mathscr{R}b$ describes the relation, and $\mathscr{R} \subseteq A \times B$.

Equality Relation

Every set S in this course possesses the **equality** relation, i.e. the subset

$$\{(x, x)|x \in S\}$$

of $S \times S$. Any relation between S and itself is a **relation on** S.

Example: Take the graph of the function $f(x) = x^3$, defined on $x \in \mathbb{R}$. Then $\{(x, x^3)|x \in \mathbb{R}\}$ is a relation on $\mathbb{R}$. This allows us to visualize "functions" as subsets of $\mathbb{R} \times \mathbb{R}$, i.e. a relation.

A **function** ϕ mapping from X to Y ($\phi : X \mapsto Y$) is a relation between X and Y such that each $x \in X$ is paired with exactly one $y \in Y$ in $(x, y) \in \phi$ (typically denoted $\phi(x) = y$). X is the **domain** of ϕ and Y is the **codomian** of ϕ. The ϕ is $\{\phi(x)|x \in X\}$.

1.2 Cardinality

The **cardinality** of a set is simply the number of elements in the set if the set is finite, denoted $|X|$. We are often interested if two sets have the same cardinality. If two sets have 5 or 6 elements, this is easy to see. How about $\mathbb{Z}$ and $\mathbb{Q}$? Or $\mathbb{Z}$ and $\mathbb{Z}^+$?

A function is **injective** or **one-to-one** if there exists a relation between X and Y such that if $(x_1, y_1) \in \mathscr{R} \subseteq X \times Y$ and $(x_2, y_2) \in \mathscr{R} \subseteq X \times Y$ and $x_1 = x_2$, then $y_1 = y_2$. Notice that this matches our definition of a function above; in simpler terms, if $\phi(x_1) = \phi(x_2)$ then $x_1 = x_2$. For example, $\phi(x) = x^2$ is not one-to-one, since we can reach $\phi(x) = 4$ from $x = 2$ and $x = -2$.

A function is **surjective** or **onto** if the range of ϕ is Y. For example, take $\phi(n) = \lfloor n/2 \rfloor$, with $\phi : \mathbb{Z} \mapsto \mathbb{Z}$. ϕ is not injective, since $n = 2$ and $n = 3$ yield the same $\phi(n) = 1$. However, it is surjective since the range of ϕ is $\mathbb{Z}$.

We combine both of these ideas: X and Y have the same cardinality if

there exists a function $\phi : X \mapsto Y$ such that ϕ is both injective and surjective (i.e. ϕ is **bijective**).

We still need a way to define the actual *size* of $\mathbb{Z}$. We denote $|\mathbb{Z}| = \aleph_0$. This class does not deal heavily with cardinalities of infinities, but $\aleph_0$ is used to denote the cardinality of the natural numbers (and $\mathbb{Z}$, and $\mathbb{Z}^+$, and $\mathbb{Q}$, and $\mathbb{Q}^+$ etc). Note that by Cantor's diagonalization argument (not covered here), $|\mathbb{R}| > \aleph_0$. An **infinite set** is one which has a proper subset of the same cardinality as the original set.

1.3 Partitions and Equivalence Relations

Two sets are **disjoint** if they have no common elements. A **partition** of a set S is a collection of nonempty, disjoint subsets of S such that every point in S is in one of these subsets, called **cells**. The cell containing element x is denoted $\bar{x}$; for example, if we partition $\mathbb{Z}$ into even and odd numbers (such that the partition has 2 cells), $\bar{6} = \{..., -2, 0, 2, ...\}$. In general, for each $n > 0 \in \mathbb{Z}$, we can partition $\mathbb{Z}^+$ into n cells by the remainder when a value is divided by n; these cells are then the **residuals modulo** $n \in \mathbb{Z}^+$**.**

There is an easy to see relation that arises as a result of this partitioning – $x\mathscr{R}y$ for $x, y \in S$ if and only if x and y are in the same cell of the partition ($(x, y) \in \mathscr{R} \subseteq S \times S$). This relation satisfies the properties below.

Equivalence Relations

An **equivalence relation** $\mathscr{R}$ on S satisfies the following three properties for $x, y, z \in S$.

1. (Reflexivity) $x\mathscr{R}x$.
2. (Symmetry) If $x\mathscr{R}y$ then $y\mathscr{R}x$.
3. (Transivity) If $x\mathscr{R}y$ and $y\mathscr{R}z$ then $x\mathscr{R}z$.

Congruence modulo n (i.e. $a \equiv b \mod n$) is an equivalence relation.

Equivalence Relations and Partitions

Let S be a nonempty set and let $\sim$ be an equivalence relation on S. Then $\bar{a} = \{x \in S | x \sim a\}$. Cells in a partition arising from an equivalence relation are known as **equivalence classes**.

2 Groups and Subgroups

In traditional calculus classes, we relate most concepts to the ideas of "addition" and "multiplication." Here, we abstract this concept to that of a **binary operation**, some operation involving two values. A binary operation on a set gives an algebra on that set, and we examine that algebra's structural properties.

To work through an example, we introduce **complex numbers** $\mathbb{C}$, where

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

We are especially interested in the polar coordinate form of complex numbers.

Euler's Formula

From the Taylor expansion of e^x, $\cos x$, and $\sin x$, we arrive at:

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

Define the **unit circle**

$$U = \{z \in \mathbb{C} | |z| = 1\}$$

as the circle in the Euclidian plane with center 0 and radius 1. Note that U is closed under multiplication (proof: if $z_1 \in U$ and $z_2 \in U$, then $|z_1 z_2| = |z_1||z_2| = 1$ therefore their product is in U). Using Euler's, we can relate z to a value θ in the half-open interval $[0, 2\pi)$, which we denote $\mathbb{R}_{2\pi}$. Note now that multiplying two complex numbers z_1 and z_2 results in an angle $\theta_1 + \theta_2 \pmod{2\pi}$. We see that multiplication on U and addition modulo 2π have the same algebraic properties; we call this an **isomorphism**.

Elements of the set $U_n = \{z \in \mathbb{C} | z^n = 1\}$ are the n^{th} **roots of unity**, and are of the form

$$\cos\left(m\frac{2\pi}{n}\right) + i\sin\left(m\frac{2\pi}{n}\right),\ m \in [0, n-1].$$

2.1 Binary Operations

In abstract algebra, we can generalize the notion of a 'binary operation'. Instead of being concerned with addition and multiplication, we define a binary operation as a function that takes in two values from the same set and

maps it into the set. More specifically, a **binary operation** $\star$ is a function $\star : S \times S \mapsto S$. $\forall (a, b) \in S \times S$, we denote $\star((a, b))$ as $a \star b$. We need a binary operation to be defined for *every* $(a, b) \in S \times S$.

Example: Let $M(\mathbb{R})$ to be the set of real-valued matrices. Matrix addition, $+$, is not a binary operation on this set, since if two matrices have different dimensions we cannot add them together.

Let $H \subseteq S$. A binary operation $\star$ is **closed on** H if $\forall (a, b) \in H \times H$, $a \star b \in H$. The binary operation $\star$ restricted to H is the **induced operation** of $\star$ on H.

A binary operation is **commutative** if $\forall a, b \in S$, $a \star b = b \star a$. A binary operation is **associative** if $\forall a, b, c \in S$, $(a \star b) \star c = a \star (b \star c)$.

2.2 Isomorphic Binary Structures

We are interested in studying how binary operations on sets of equal size give *structure* to those sets. A **binary algbraic structure** $\langle S, \star \rangle$ is a set S with a binary structure $\star$ on S.

Let $\langle S, \star \rangle$ and $\langle S', \star' \rangle$ be binary algebraic structures. An **isomorphism** of S with S' is a bijective function ϕ (one-to-one from S onto S') such that

$$\phi(x \star y) = \phi(x) \star' \phi(y), \ \forall x, y \in S.$$

If ϕ exists, we say that S and S' are **isomorphic binary structures**, so $S \simeq S'$. The relation above is known as the **homomorphism property**. A function is an isomorphism if it is both bijective and homomorphic.

2.2.1 How to show Binary Structures are Isomorphic

Here is a set of steps to show that $\langle S, \star \rangle$ and $\langle S', \star' \rangle$ are isomorphic.

1. Define a function ϕ that gives the isomorphism of S with S'
2. Show that ϕ is one-to-one and onto S'
3. Show $\phi(x \star y) = \phi(x) \star' \phi(y)$.

2.2.2 How to show that Binary Structures are not Isomorphic

It is impossible to show that every possible one-to-one function S onto S'; the only time we can do this is when S and S' have different cardinalities. For example, $\mathbb{Q}$ is not isomorphic to $\mathbb{R}$ since $|\mathbb{Q}| = \aleph_0$ and $|\mathbb{R}| \neq \aleph_0$.

What about when S and S' have the same cardinality? Here we examine **structural properties**, properties that must be shared by any isomorphic structure. If $\langle S, \star \rangle$ has a structural property that $\langle S', \star' \rangle$ does *not* have, then S and S' are not isomorphic. We can show that $\mathbb{Q}$ and $\mathbb{Z}$ are not isomorphic. $\forall y \in \mathbb{Q}, \exists\ x \in \mathbb{Q} : x + x = y$. However, $\exists y \in \mathbb{Z} : x + x \neq y\ \forall x \in \mathbb{Z}$. $\mathbb{Q}$ has a structural property that $\mathbb{Z}$ does not have and therefore they are not isomorphic.

Identity Element

Let $\langle S, \star \rangle$ be a binary structure. $e \in S$ is an **identity element** for $\star$ if, $\forall s \in S$, $e \star s = s \star e = s$. Any binary structure has at most one identity element.

2.3 Groups

Groups

A **group** $\langle G, \star \rangle$ is a set G closed under $\star$ such that:

1. **Associativity of** $\star$ ($\mathscr{G}_1$):

$$\forall\ a, b, c \in G : (a \star b) \star c = a \star (b \star c)$$

2. **Identity** e **for** $\star$ ($\mathscr{G}_2$):

$$\exists\ e \in G : e \star x = x \star e = x \forall x \in G$$

3. **Inverse** ($\mathscr{G}_3$):

$$\forall a \in G\ \exists\ a' \in G : a \star a' = a' \star a = e.$$

A group G is **abelian** if its binary operation is commutative.

For example, $S \subset M_n(\mathbb{R})$ consisting of all invertible $n \times n$ matrices is a

group. All elements of S have an inverse by construction, and the identity element is I_n. It is closed under matrix multiplication since $\forall\ A, B \in S$, $(AB)(B^{-1}A^{-1} - A(BB^{-1})A^{-1} = AA^{-1} = I_n$. However, matrix multiplication is **not** commutative, and the group is **nonabelian**. The group mentioned here is the **general linear group of degree** n, denoted $GL(n, \mathbb{R}) \simeq GL(\mathbb{R}^n)$.

2.3.1 Elementary Properties of Groups

Left and Right Cancellation

If G is a group with binary operation $\star$, the **left and right cancellation laws** hold, i.e.

$$a \star b = a \star c \implies b = c$$

and

$$b \star a = c \star a \implies b = c.$$

The identity element is unique in a group; additionally, the inverse of each element in a group is unique. A **semigroup** is a set with an associative binary operation, and a **monoid** is a semigroup that also has an identity element. Every group is both a semigroup and a monoid.

2.4 Subgroups

In general, the symbol $+$ is used to denote addition, and is always commutative. Multiplication is traditionally just denoted by juxtaposing the two elements without a "$\cdot$," as ab. This is not necessarily commutative. The symbol 0 denotes additive identity and the symbol 1 denotes multiplicative identity. The multiplicative inverse is a^{-1} and the additive inverse is $-a$. The **order** of a group $|G|$ is the number of elements in G.

Subgroups

If $H \subseteq G$ is closed under the binary operation of G and if H with the induced operation from G is itself a group, then H is a **subgroup** of G ($H \leq G$). The subgroup consisting of G is an **improper subgroup**; all others are **proper subgroups**. $\{e\}$ is the **trivial subgroup**; all others are **nontrivial**.

There are two types of group structures of order 4; the group V known as the **Klein 4-group**, isomorphic to $U_4 = \{1, i, -1, -i\}$, consists of the elements $\{e, a, b, c\}$ where $a \star a = b \star b = c \star c = e$ and $a \star b = b \star a = c$, $b \star c = c \star b = a$, $a \star c = c \star a = b$. The Klein 4-group has three nontrivial proper subgroups, each of order 2: $\{a, e\}$, $\{b, e\}$, $\{c, e\}$.

The other group of order 4 is $\mathbb{Z}_4$, which only has one nontrivial proper subgroup, that is $\{0, 2\}$. Note $\{0, 3\}$ is not closed under addition, since $3+3 = 2$.

$H \leq G$ if and only if H is closed under $\star$, $e \in G \implies e \in H$, and $\forall\, a \in H,\ a^{-1} \in H$.

2.4.1 Cyclic Subgroups

Let G be a group and $a \in G$. Then

$$H = \{a^n | n \in \mathbb{Z}\}$$

is a subgroup of G and is the smallest subgroup of G containing a. This subgroup is known as the **cyclic subgroup** of G generated by a, denoted $\langle a \rangle$. $a \in G$ **generates** G and is a **generator for** G if $\langle a \rangle = G$. A group is **cyclic** if $\exists\, a \in G$ such that a generates G.

2.5 Cyclic Groups

Extending the previous concept of cyclic groups, we introduce basic properties of cyclic groups.

1. Every cyclic group is abelian
2. A subgroup of a cyclic group is cyclic
3. The cyclic subgroups of $\mathbb{Z}$ under addition are the groups $n\mathbb{Z}$ under addition

Greatest Common Divisor

Let $r, s \in \mathbb{Z}^+$. The positive generator d of the cyclic group

$$H = \{nr + ms | n, m \in \mathbb{Z}\}$$

is the **greatest common divisor** (GCD) of r and s. We write $d = GCD(r, s)$. Two values are relatively prime if their GCD is 1.

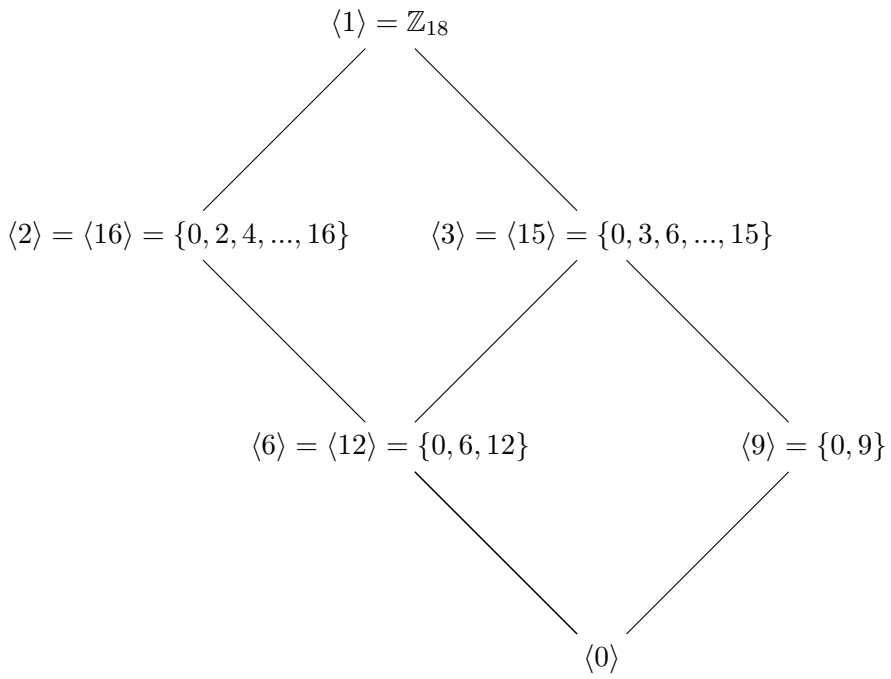
2.5.1 The Structure of Cyclic Groups

Let G be a cyclic group with generator a. If the order of G is infinite, then G is isomorphic to $\langle Z, + \rangle$. If G has finite order n, then G is isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$.

2.5.2 Subgroups of Finite Cyclic Groups

Let G be a cyclic group with n elements generated by a. Let $b \in G$ and let $b = a^s$. Then b generates a cyclic subgroup H of G containing n/d elements, where d is the greatest common divisor of n and s. $\langle a^t \rangle = \langle a^s \rangle$ if and only if $GCD(s, n) = GCD(t, n)$. If a is a generator of a finite cyclic group G of order n, then other generators in G are of the form a^r where r is relatively prime to n.

For a given group, we can draw the **subgroup diagram** as follows (here we choose $\mathbb{Z}_{18}$:



2.6 Generating Sets and Cayley Digraphs

Let G be a group with $a \in G$. We already discussed finding the smallest group containing a, which is $\langle a \rangle$. Suppose we want to find the smallest group containing both a and $b \in G$. We need to find the subgroup containing $a^n, b^m \forall\ m, n \in \mathbb{Z}$; a and b are generators of this subgroup, and if this subgroup is equal to G we say that the subgroup **generates** G. We extend this concept to arbitrarily sized **generating sets**. For example, the Klein 4-group $V = \{e, a, b, c\}$ is generated by $\{a, b\}$.

Intersection of Sets

Let $\{S_i | i \in I\}$ be a collection of sets over any set I of indices. The **intersection of sets** $\cap_{i \in I} S_i$ is the set of all the elements in all the sets S_i, i.e.

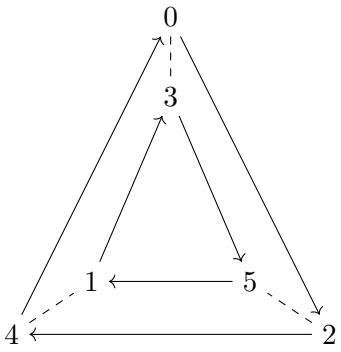
$$\bigcap_{i \in I} S_i = \{x | x \in S_i\} \forall i \in I\}.$$

The intersection of some H_i subgroups of G is a subgroup of G. Understand why this makes sense.

If G is a group and $a_i \in G,\ i \in I$ then the subgroup $H \leq G : H = \{a_i^n | i \in I, n \in \mathbb{Z}\}$ has as elements those elements of G that are finite products of integral powers of a_i.

2.6.1 Cayley Digraphs

A **Cayley digraph** (**directed graph**) consists of **vertices** and **arcs**, which are directed edges connecting vertices. Here is $\mathbb{Z}_6$ generated by $\{2, 3\}$; the solid lines represent increments of 2, and the dashes represent increments of 3 (these are their own inverse, and are as such have no arrows).



3 Permutations, Cosets, and Direct Products

3.1 Groups of Permutations

Permutations

A **permutation of a set** A is a function $\phi : A \mapsto A$ that is both one-to-one and onto.

$$1 \mapsto 3$$
$$2 \mapsto 1$$
$$3 \mapsto 6$$
$$4 \mapsto 2$$
$$5 \mapsto 5$$
$$6 \mapsto 4$$

3.1.1 Permutation Groups

The **function composition** $\circ$ is a binary operation on the collection of all permutations of a set A. This operation is also known as *permutation multiplication*. For simplicity, we omit the actual $\circ$ symbol; the operation $\sigma\tau(x) = \sigma \circ \tau(x) = \sigma(\tau(x))$.

As an example, for the set $A = \{1, 2, 3, 4, 5\}$ define

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

and let

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

Then

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

Let A be a nonempty set and let S_A be the collection of all permutations of A. Then S_A is a group under permutation multiplication.

When A is the finite set $\{1, 2, ..., n\}$, then the group of all permutations of A is known as the **symmetric group on** n **letters**. Note that $|S_n| = n!$.

3.1.2 Dihedral Groups

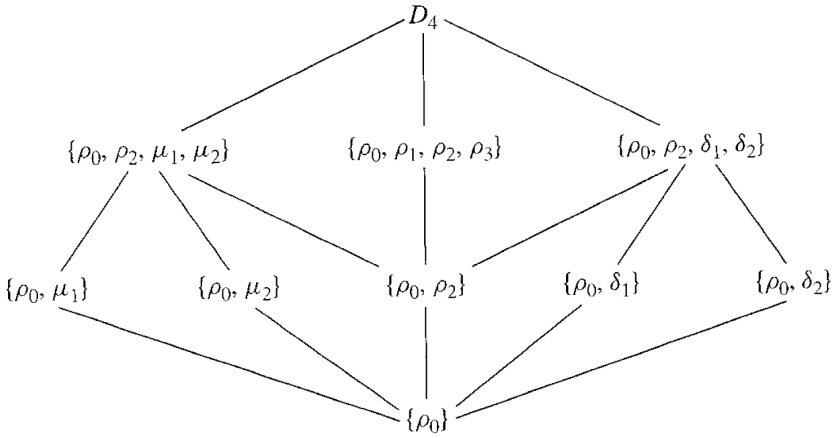
Let's assign some geometry to the above notion. Take the symmetric group on 3 letters S_3. Imagine if each of the values in $A = \{1, 2, 3\}$ were the labels of the vertices of an equilateral triangle. Then the elements of S_3 are the different ways we could overlay the same triangle on itself, namely including rotations and reflections. The group of symmetries of a regular polygon (i.e. rotations and reflections) is known as a **dihedral group**. For n dimensions, we call this the n**th dihedral group** D_n. Note that this is isomorphic to the symmetric group (they are not the same group, since we can't change connectivity (i.e. the edges of the polygon have to stay connected in D_n)). D_4 is the group of symmetries of the square, also known as the **octic group**.

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \qquad \delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \qquad \delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$



Cayley's Theorem

From the above we arrive at an interesting conclusion. For S_G (the group of all permutations of G) every group G is isomorphic to a subgroup of S_G. In other words, every group is isomorphic to a group of permutations.

Image

Let $f : A \mapsto B$ be a function and let $H \subseteq A$. The **image of** H **under** f is $\{f(h)|h \in H\}$ and is denoted by $f[H]$.

Furthermore, let G and G' be groups and let $\phi : G \mapsto G'$ be a one-to-one function such that $\phi(xy) = \phi(x)\phi(y),\ \forall\ x, y \in G$. Then $\phi[G]$ is a subgroup of G' and ϕ provides an isomorphism of G with G'.

Here's a brief proof of Cayley's Theorem.

Proof: Let G be a group. Define a one-to-one function $\phi : G \mapsto S_G$ such that $\phi(x, y) = \phi(x)\phi(y)$. Define $\lambda_x(g) = xg\ \forall\ x \in G$. Since $\forall\ c \in G,\ \lambda_x(x^{-1}c) = c$, we see that λ_x is onto G. Additionally, for $a, b \in G$, if $\lambda_x(a) = \lambda_x(b)$ then $a = b$, so λ_x is a one-to-one and a permutation. Now let $\phi(x) = \lambda_x\ \forall x \in G$. Then $\phi(x)$ is one-to-one since $\phi(x) = \phi(y) \implies \lambda_x(e) = \lambda_y(e) \implies xe = ye \implies x = y$. We then see that $(\lambda_x\lambda_y)(g) = \lambda_x(\lambda_y(g)) = \lambda_x(yg) = xyg = (xy)g = \lambda_{xy}(g)$, therefore $\phi(x)\phi(y) = \phi(xy)$ and thus ϕ provides an isomorphism of G with S_G. □

Note that in the above proof we could have substituted λ_x with $\rho_x(g) = gx$ and used the map $\mu : G \mapsto S_G$ with $\mu(x) = \rho_{x^{-1}}$. Here, ϕ is the **left rectangular representation** of G and μ is the **right rectangular representation** of G.

3.2 Orbits, Cycles, and the Alternating Groups

Orbits

Let σ be a permutation of A. The equivalence classes defined by the equivalence relation:

$$\forall\ a, b \in A,\ a \sim b \iff b = \sigma^n(a),\ n \in \mathbb{Z}$$

are the **orbits** of σ.

Cycles

A permutation $\sigma \in S_n$ is a **cycle** if it contains at most one orbit with more than one element. The number of elements in its largest orbit is the **length** of the cycle.

Since cycles are permutations themselves, it makes sense that we can multiply them. We also use a shorthand notation to describe cycles, where the elements "point" to each other in left-to-right order. For example:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} = (1\ 3\ 6)(2\ 8)(4\ 7\ 5).$$

Note that the cycles above are **disjoint**, i.e. no element appears in more than one cycle. Multiplication of disjoint cycles is commutative.

A cycle of length 2 is known as a **transposition**. Any cycle is a product of transpositions, and every permutation is the product of disjoint cycles. No permutation in S_n can be expressed as the product of an odd number of transpositions and an even number of transpositions. If it can be expressed by an odd number of transpositions, the permutation is **odd**, else it is **even**.

If $n \geq 2$, then the collection of all even permutations of $\{1, 2, 3, ..., n\}$ forms a subgroup of order $n!/2$ of the symmetric group S_n.

Alternating Groups

The subgroup of S_n consisting of the even permutations of n letters is the **alternating group A_n on n letters**.

3.3 Cosets and the Theorem of Lagrange

Let H be a subgroup of G. Then if we define $\sim_L$ such that $a \sim_L b \iff a^{-1}b \in H$ and $\sim_R$ such that $a \sim_R b \iff ab^{-1} \in H$ then $\sim_L$ and $\sim_R$ are equivalence relations on H.

Cosets

Let H be a subgroup of G. The subset $aH = \{ah | h \in H\}$ of G is the **left coset** of H containing a and the subset $Ha = \{ha | h \in H\}$ of G is the **right coset** of H containing a. For a subgroup H of an abelian group G, the partition of G into left cosets of H and the partition into right cosets are the same.

Theorem of Lagrange

Let H be a subgroup of G. Then the order of H is a divisor of the order of G. As a consequence, every group of prime order is cyclic. Likewise, the order of an element of a finite group divides the order of the group.

Proof: Let n be the order of G, and let H have order m. Every coset of a subgroup has the same number of elements as that subgroup, so every coset of H has m elements. Let r be the number of cells in the partition of G into left cosets of H. Then $n = rm$, so m is a factor of n. □

Index

Let H be a subgroup of a group G. The number of left cosets of H in G is the **index of H in G** and is denoted $(G : H)$. Suppose H and K are subgroups of a group G such that $K \leq H \leq G$ and suppose $(H : K)$ and $(G : H)$ are finite. Then $(G : K)$ is finite and $(G : K) = (G : H)(H : K)$.

3.4 Direct Products and Finitely Generated Abelian Groups

Here we show how we can use known groups as building blocks for more groups.

Cartesian Product

The **Cartesian product of sets** $S_1, S_2, ..., S_n$ is the set of all ordered n-tuples $(a_1, a_2, ..., a_n)$, where $a_i \in S_i$ for $i = 1, 2, ..., n$. The Cartesian product is denoted

$$\prod_{i=1}^{n} S_i.$$

Let $G_1, ..., G_n$ be groups. For $(a_1, a_2, ..., a_n)$ and $(b_1, b_2, ..., b_n)$ in $\prod_{i=1}^{n} G_i$, define $(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n)$ to be the element $(a_1b_1, a_2b_2, ..., a_nb_n)$. Then $\prod_{i=1}^{n} G_i$ is a group, the **direct product of the groups** G_i, under this binary operation. If the operation is commutative, we sometimes use additive notation and refer to $\prod_{i=1}^{n} G_i$ as the **direct sum of groups**, and denote this as $\oplus_{i=1}^{n} G_i$.

The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime. To generalize, $\prod_{i=1}^{n} Z_{m_i}$ is cyclic and isomorphic to $\mathbb{Z}_{m_1 m_2 ... m_n}$ if and only if $m_1, m_2, ..., m_n$ are such that they are all relatively prime.

Least Common Multiple

Let $r_1, ..., r_n \in \mathbb{Z}_{>0}$. Their **least common multiple** or lcm is the positive generator of the scyclic group of all common multiples of the r_i; that is, the cyclic group of all integers divisible by each r_i.

Let $(a_1, a_2, ..., a_n) \in \prod_{i=1}^{n} G_i$. If a_i is of finite order r_i in G_i, then the order of $(a_1, a_2, ..., a_n)$ in $\prod_{i=1}^{n} G_i$ is equal to the lcm of all the r_i.

Example: We use the above to find the order of $(8, 4, 10)$ in $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$. The gcd of 8 and 12 is 4; then 8 is of order $12/4 = 3$ in $\mathbb{Z}_{12}$. Following a similar procedure, the order of 4 in $\mathbb{Z}_{60}$ is 15 and the order of 10 in $\mathbb{Z}_{24}$ is 12. Then the lcm of 3, 15, 12 is 60, so $(8, 4, 10)$ is of order 60 in $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$.

3.4.1 The Structure of Finitely Generated Abelian Groups

The Fundamental Theorem of Finitely Generated Abelian Groups

Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \ldots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z},$$

where p_i are primes (not necessarily distinct) and the r_i are positive integers. The direct product is unique except for possible rarrangement of hte factors; that is, the number of factors $\mathbb{Z}$ is unique (the **Betti number of** G) and the prime powers $(p_i)^{r_i}$ are unique.

Example: We find all abelian groups up to isomorphism of order 360. This means that any abelian group of order 360 should be structurally identical to one of the groups listed. We express 360 as a product of prime powers as $2^3 3^2 5$. Then using the FTFGAG, we can express this as:

1. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
2. $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
3. $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
4. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
5. $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
6. $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

These are the 6 different abelian groups up to isomorphism of order 360.

3.4.2 Applications

Decomposable versus Indecomposable Groups

A group G is **decomposable** if it is isomorphic to a direct product of two proper nontrivial subgroups. Else it is **indecomposable**.

Various Theorems

The finite indecomposable abelian groups are exactly the cyclic groups with order a power of a prime.

If m divides the order of a finite abelian group G, then G has a subgroup of order m.

If m is a square free integer (m is not divisible by the square of any prime), then every abelian group of order m is cyclic.

4 Homomorphisms and Factor Groups

4.1 Homomorphisms

For two groups G and G', we're interested in maps between the groups that relate the structure of the former to the structure of the latter. These maps are useful because knowing the properties of one group gives us information about properties of the other. An isomorphism $\phi : GG'$ is an example of such a map. Here we introduce a more general set of maps. In our early definition of an isomorphism, we required that the maps be one-to-one and onto. These conditions have nothing to do with the binary operations on the sets – however, these binary operations are the thing we care most about in our more abstract focus on the *algebra* on the sets.

Homomorphism

A map ϕ of G into a group G' is a **homomorphism** if the homomorphism property

$$\phi(ab) = \phi(a)\phi(b)$$

holds $\forall\ a, b \in G$. In the above idea, the product ab on the left hand side takes place in G, while the product $\phi(a)\phi(b)$ takes place in G'.

For any groups G and G', there is at least one homomorphism; the **trivial homomorphism** $\phi(g) = e'$ for $g \in G$ with $e' \in G'$. This then reduces the above homorphism property to $e' = e'e'$ which is true. As an example for why this is important, take the homomorphism ϕ from G *onto* G'. We can show that if G is abelian, then G' is abelian! This arrives from the above property; $\forall a, b \in G,\ ab = ba$. Since ϕ is onto, $\exists\ a, b\ \in\ G : \phi(a) =$

$a' \in G', \phi(b) = b' \in G'$. From here, we see that $a'b' = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = b'a'$ therefore G' is abelian.

Evaluation Homomorphism

For F, the additive group of all functions $\mathbb{R} \mapsto \mathbb{R}$, where $\mathbb{R}$ is the additive group of reals, and $c \in \mathbb{R}$, the **evaluation homomorphism** is $\phi_c : F \mapsto \mathbb{R}$ with $\phi_c(f) = f(c)$.

As another example, take $\mathbb{R}^n$, the additive group of n-dimensional column vectors (isomorphic to $\prod_{i=1}^{n} \mathbb{R}$). Then $\phi : R^n \mapsto \mathbb{R}^m$ is $\mathbf{Av}$ for an $m \times n$ dimensional matrix $\mathbf{A}$ with $\mathbf{v} \in \mathbb{R}^n$. ϕ is a homomorphism.

Reduction Modulo n

Let γ be the natural map of $\mathbb{Z} \mapsto \mathbb{Z}_n$ given by $\gamma(m) = r$, where r is the remainder of the division algorithm when m is divided by n. Then γ is a homomorphism.

4.1.1 Properties of Homomorphisms

Image and Range

Let ϕ be a mapping of X into Y, and let $A \subseteq B$ and $B \subseteq Y$. Then the **image** $\phi[A]$ of A in Y under ϕ is $\{\phi(a)|a \in A\}$. The set $\phi[X]$ is the **range** of ϕ. The **inverse image** $\phi^{-1}[B]$ of B in X is $\{x \in X|\phi(x) \in B\}$.

Let ϕ be a homomorphism of G into G'.

1. If e is the identity element in G then $\phi(e)$ is the identity element e' in G'.
2. If $a \in G$ then $\phi(a^{-1}) = \phi(a)^{-1}$
3. If H is a subgroup of G, then $\phi[H]$ is a subgroup of G'
4. If K' is a subgroup of G', then $\phi^{-1}[K']$ is a subgroup of G.

Kernel

Let $\phi : G \mapsto G'$ be a homorphism of groups. The subgroup $\phi^{-1}[\{e'\}] = \{x \in G|\phi(x) = e'\}$ is the **kernel** of ϕ, denoted $\mathrm{Ker}(\phi)$.

For a group homomorphism $\phi : G \mapsto G'$, let H =Ker(ϕ). For $a \in G$, the set

$$\phi^{-1}[\{\phi(a)\}] = \{x \in G | \phi(x) = \phi(a)\}$$

is the left coset aH of H, and is also the right coset Ha of H. In other words, the partitions of G into left and right cosets of H are the same.

Trivial Kernel

A group homorphism $\phi : G \mapsto G'$ is a one-to-one if and only if Ker(ϕ) = $\{e\}$.

From this, we can easily show that ϕ is an isomorphism by showing that it is a homomorphism, showing it has a trivial kernel, and then showing that it maps G onto G'.

Normal Groups

A group is **normal** if its left and right cosets coincide, that is, if $gH = Hg$, $\forall g \in G$. All subgroups of abelian groups are normal. If $\phi : G \mapsto G'$ is a homomorphism, then Ker(ϕ) is a normal subgroup of G.

4.2 Factor Groups

Factor Groups

Let $\phi : G \mapsto G'$ be a group homomorphism with kernel H. Then the cosets of H form a **factor group**, G/H, where $(aH)(bH) = (ab)H$. Also, the map $\mu : G/H \mapsto \phi[G]$ defined by $\mu(aH) = \phi(a)$ is an isomorphism. Both coset multiplication and μ are well-defined, independent of the choices a and b from the cosets. We sometimes refer to G/H as "G modulo H."

As an example, take $\mathbb{Z}/5\mathbb{Z}$. For the remainder function $\gamma : \mathbb{Z} \mapsto \mathbb{Z}_n$ where $\gamma(m)$ is the remainder when m is divided by m, we see that Ker(γ) = $n\mathbb{Z}$. The cosets of $n\mathbb{Z}$ are the **residuals** modulo n; the cosets of Ker(γ) for $n = 5$ are $\{m + 5n | m \in \{1, ..., 5\}, n \in \mathbb{Z}\}$. For $\mathbb{Z}_5$, we take the isomorphism $\mu : \mathbb{Z}/5\mathbb{Z} \mapsto \mathbb{Z}_5$, which assigns, to each coset of $5\mathbb{Z}$, its smallest nonnegative element. For example, $\mu(5\mathbb{Z}) = 0$, and $\mu(1 + 5\mathbb{Z}) = 1$. For a factor group G/H, two elements are **congruent modulo** H if they are in the same coset of H.

4.2.1 Factor Groups from Normal Subgroups

So far we've obtained factor groups from homomorphisms. However, in general, the left and right cosets need not be the same. We can define a binary operation

$$(aH)(bH) = (ab)H$$

to define left coset multiplication, if and only if H is a normal subgroup of G. Additionally, if H is a normal subgroup of G, then the cosets of H form a group G/H under the binary operation $(aH)(bH) = (ab)H$. The group G/H here is the **factor group** or **quotient group** of G by H.

As an example, consider $\mathbb{R}$ under addition (which is abelian), and let $c \in \mathbb{R}^+$. Every coset of $\langle c \rangle$ has exactly one element between 0 and c (i.e. $\{..., -c, 0, c, ...\}, \{..., -c+1, 1, c+1, ...\}, \{..., -c+2, 2, c+2, ...\}$). Choose these elements to represent the entire coset. If we add these 'representatives,' we're actually computing the sum modulo c. The group $\mathbb{R}_c$ is isomorphic to $\mathbb{R}/\langle c \rangle$ under an operation $\phi(x) = x + \langle c \rangle$ for $x \in \mathbb{R}_c$. $\mathbb{R}/\langle c \rangle$ is then also isomorphic to the unit circle U of complex numbers under multiplication.

4.2.2 The Fundamental Homomorphism Theorem

Every homomorphism $\phi : G \mapsto G'$ gives rise to a natural factor group $G/\text{Ker}(\phi)$. We can now show the other side of this argument; that G/H gives rise to a homomorphism with kernel H.

If H is a normal subgroup of G (i.e. $gH = Hg$ for all $g \in G$) then this is true; $\gamma : G \mapsto G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H.

Proof: $\gamma(xy) = (xy)H = (xH)(yH) = \gamma(x)\gamma(y)$ so γ is a homomorphism; since $xH = H$ if and only if $x \in H$, the kernel of γ is H. □

The Fundamental Homomorphism Theorem

Let $\phi : G \mapsto G'$ be a group homomorphism with kernel H. Then $\phi[G]$ is a group, and $\mu : G/H \mapsto \phi[G]$ given by $\mu(G/H) = \phi(g)$ is an isomorphism. If $\gamma : G \mapsto G/H$ is the homomorphism given by $\gamma(g) = gH$, then $\phi(g) = \mu\gamma(g)$ for each g in G.

In summary, every homomorphism with domain G gives rise to a factor group G/H, and every factor group G/H gives rise to a homomorphism mapping G into G/H.

As an example, we can classify the group $(\mathbb{Z}_4 \times \mathbb{Z}_2)/(\{0\} \times \mathbb{Z}_2)$ according to the FTFGAG. The map $\pi_1 : \mathbb{Z}_4 \times \mathbb{Z}_2 \mapsto \mathbb{Z}_4$ with $\pi_1(x, y) = x$ is a homomorphism of $\mathbb{Z}_4 \times \mathbb{Z}_2$. Note the kernel of π_1 is $\{0\} \times \mathbb{Z}_2$, so the factor group given is isomorphic to $\mathbb{Z}_4$.

4.2.3 Normal Subgroups and Inner Automorphisms

We want a better way to check whether subgroups are normal without having to find both the left and right subgroups.

Conditions for Normal Subgroups

The following are three equivalent conditions for a subgroup H of G to be a normal subgroup of G.

1. $ghg^{-1} \in H \; \forall \; g \in G$ and $h \in H$
2. $gHg^{-1} = H \; \forall \; g \in G$
3. $gH = Hg \; \forall \; g \in G$

Automorphisms

An isomorphism $\phi : G \mapsto G$ of a group G with itself is an **automorphism** of G. The automorphism $i_g : G \mapsto G$, where $i_g(x) = gxg^{-1}$, $\forall g \in G$ is the **inner automorphism of G by g**. Performing i_g on x is called **conjugation of x by g**.

From the above, we see that $gH = Hg$ only if $i_g[H] = H$ for all $g \in G$, i.e. H is **invariant** under all inner automorphisms of G. Note that this doesn't mean that $i_g(h) = h \; \forall h \in H$; i_g may perform a nontrivial

permutation on H. The normal subgroups of G are those invariant under all inner automorphisms. A subgroup $K \leq G$ is a **conjugate subgroup** of H if $K = i_g[H]$ for some $g \in G$.

4.2.4 The Center and Commutator Subgroups

Every nonabelian group G has two important normal subgroups. The first is the **center** $Z(G)$ (Z comes from the German *Zentrum* for "center"), the set of elements of G which commute with all elements of G, or

$$Z(G) = \{z \in G | zg = gz, \ \forall g \in G\}.$$

$Z(G)$ is an abelian subgroup of G. If G is abelian, then $Z(G) = G$.

The second important normal subgroup is the **commutator**. Earlier, we discussed some properties of finitely generated abelian groups. For non-abelian groups, it might be useful to to try and form an abelian group as similar to G as possible (to *abelianize* it). This means our new group would have $ab = ba \ \forall a, b \in G'$ where G' is our "abelianized" group. Alternatively, we could say $aba^{-1}b^{-1} = e$. An element $aba^{-1}b^{-1} \in G$ with $a, b \in G$ is a **commutator** of G. Then we can turn G into an abelian group by turning all commutators in G to e. The set of all commutators is the **commutator subgroup** denoted C. If N is a normal subgroup of G, then G/N is abelian if and only if $C \leq N$.

4.3 Group Action on a Set

We've seen some examples of groups *acting* on things, like D_3 the group of symmetries of the triangle, the general linear group acting on $\mathbb{R}^n$, etc. We generalize this here.

Group Action

Let X be a set and G a group. An **action of G on X** is the map $\star : G \times X \mapsto X$ such that

1. $ex = x, \ \forall x \in X$
2. $(g_1 g_2)(x) = g_1(g_2 x), \ \forall x \in X, \ \forall g_1, g_2 \in G$

X here is known as a **G-set**. Additionally, for each $g \in G$, the function $\sigma_g : X \mapsto X = \sigma_g(x) = gx$ is a permutation of X. The map $\phi : G \mapsto S_X = \phi(g) = \sigma_g$ is a homomosphism as $\phi(g)(x) = gx$.

The subset of G that leaves every element of X fixed is a normal subgroup N of G, and then X is a G/N-set. The action of gN on X is $(gN)x = gx$. If $N = \{e\}$, i.e. only the identity leaves all X fixed, then G **acts faithfully** on X. If $\forall x_1, x_2 \in X,\ \exists g \in G : gx_1 = x_2$ then G is **transitive** on X.

4.3.1 Isotropy Subgroups

For a G-set X, define the following:

$$X_g = \{x \in X | gx = x\} \quad G_x = \{g \in G | gx = x\}.$$

For each $x \in X$, $G_x \leq G$. For a particular $x \in X$, the subgroup G_x is known as the **isotropy subgroup** of x, the subgroup of G that sends x to itself under $\star$.

5 Rings and Fields

So far we've dealt with sets with a single binary operation. However, this isn't natural for us. We're used to dealing with sets with *two* binary operations defined on it (i.e. $\mathbb{Z}$ and $\mathbb{R}$ with multiplication and addition).

5.1 Rings and Fields

The most general algebraic structure with two binary operations is a ring.

Rings

A **ring** $\langle R, +, \cdot \rangle$ is a set R with two binary operations $+$ and $\cdot$, called *addition* and *multiplication*, defined on R that satisfies the following axioms:

1. $\langle R, + \rangle$ is an abelian group
2. Multiplication is associative
3. $\forall\ a, b, c \in R$, the **left distributive law** $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and the **right distributive law** $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ hold

From here forward in these notes, $\mathbb{Z}, \mathbb{C}, \mathbb{Q}, \mathbb{R}$ refer to the *rings* defined by the same sets, not the groups. Additionally, for a cyclic group $\langle \mathbb{Z}_n, + \rangle$, if we define for $a, b \in \mathbb{Z}_n$ the product ab to be $ab \mod n$, then $\langle \mathbb{Z}_n, +, \cdot \rangle$ is a ring.

If $R_1, ..., R_n$ are rings, then we can define the ring of ordered $n-$tuples $(r_1, ..., r_n)$ from $R_1 \times ... \times R_n$ the **direct product of rings**.

If a ring has additive identity 0, then for all $a, b \in R$:

1. $0a = a0 = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$

5.1.1 Ring Homomorphisms and Isomorphisms

Ring Homomorphism

For rings R and R', a map $\phi : R \mapsto R'$ is a **homomorphism** if the following two conditions are satisfied for all $a, b \in R$:

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a)\phi(b)$

Note that condition (1) establishes that ϕ is a group homomorphism, and therefore all group homomorphism properties apply. ϕ is one-to-one if and only if its **kernel** $\text{Ker}(\phi) = \{a \in R | \phi(a) = 0'\}$ is the subset $\{0\} \in R$. We use the symbol F to denote the ring of all functions mapping $\mathbb{R}$ into $\mathbb{R}$. The **evaluation homomorphism** $\phi_a : F \mapsto \mathbb{R}$ is defined as $\phi_a(f) = f(a)$, $\forall f \in F$.

Ring Isomorphism

An **isomorphism** $\phi : R \mapsto R'$ from a ring R to a ring R' is a homomorphism that is one-to-one and onto R'. The rings are then **isomorphic**.

5.1.2 Fields

Rings are defined by their first binary operator being abelian and the second associative. A ring in which the second binary operator is commutative is a **commutative ring**. A ring is not guaranteed an identity element (take $2\mathbb{Z}$ as an example). A ring with an identity element is called a **ring with unity**, and the identity element 1 is called **unity**. Note that if a ring has

an identity element, that identity element is unique. In the **zero ring** $\{0\}$, 0 is both the multiplicative and additive identity.

For integers r, s where $\gcd(r, s) = 1$, the rings $\mathbb{Z}_{rs}$ and $\mathbb{Z}_r \times \mathbb{Z}_s$ are isomorphic. Additively they are cyclic abelian groups of order rs generated by 1 and $(1, 1)$ respectively, and $\phi : \mathbb{Z}_{rs} \mapsto \mathbb{Z}_r \times \mathbb{Z}_s$ defined by $\phi(n \cdot 1) = n \cdot (1, 1)$ is an additive group isomorphism. In a ring R with unity 1, the set of nonzero elements R^* will be a multiplicative group if multiplicative inverses exist and the group is closed under ring multiplication. A **multiplicative inverse** of $a \in R$ with unity 1 is an element $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Field

Let R be a ring with unity 1. An element $u \in R$ is a **unit** of R if it has a multiplicative inverse in R. If every nonzero element of R is a unit, then R is a **skew field** (or **division ring**). A **field** is a commutative skew field. A noncommutative skew field is called a **strictly skew field**.

A **subring** is a subset of a ring that is a ring under the induced operations from the whole ring, and a **subfield** is defined analgously as a subset of a field. More generally, for any set with a given algebraic structure, any subset that maintains the same algebraic structure is a **substructure**.

5.2 Integral Domains

In a traditional number system, the product of two numbers ab can only equal 0 if either $a = 0$ or $b = 0$. This is not necessarily true when we deal with finite sets. For instance, $6 \times 2 = 0$ in $\mathbb{Z}_{12}$.

0 Divisors

If a and b are two nonzero elements of a ring R such that $ab = 0$ then a and b are **divisors of 0**.

In $\mathbb{Z}_n$, the divisors of 0 are precisely those elements of $\mathbb{Z}_n$ that are *not* relatively prime to n. Likewise, this means that if p is prime then $\mathbb{Z}_p$ has no divisors of 0.

Within a ring, we have **cancellation laws**. Since all rings are groups under addition (i.e. if $\langle R, +, \cdot \rangle$ is a ring then $\langle R, + \rangle$ is a group), the additive cancellation law holds. The multiplicative cancellation law holds in a ring if

$ab = ac$ or $ba = ca$, $a \neq 0 \implies b = c$. The cancellation laws hold in a ring R if and only if R has no divisors of 0.

Integral Domains

An **integral domain** D is a commutative ring with unity containing no divisors of zero. The most basic integral domain is $\mathbb{Z}$.

Every field F is an integral domain. Every finite integral domain is a field. If p is a prime, then $\mathbb{Z}_p$ is a field.

5.2.1 The Characteristic of a Ring

Characteristic

If for a ring R a positive integer n exists with $n \cdot a = 0$ for all $a \in R$, then the least such positive integer is the **characteristic of** R. If no such integer exists, then R is of **characteristic 0**.

If R is as ring with unity, then the characteristic of R is the smallest n such that $n \times 1 = 0$ for some $n \in \mathbb{Z}$. If no such n exists, the ring has characteristic 0.

5.3 Fermat's Theorem and Euler's Theorem

Fermat's Little Theorem

If $a \in \mathbb{Z}$ and p is a prime not dividing a, then p divides $a^{p-1} - 1$, that is $a^{p-1} \equiv 1 \mod p$ for $a \not\equiv 0$.

As an example, we can prove that $2^{11,213} - 1$ is not divisible by 11. By Fermat's Theorem, $2^{10} \equiv 1 \mod 11$ therefore $2^{11,213} - 1 \equiv (2^{10})^{1,121} 2^3 - 1 \equiv 7 \mod 11$. Primes of the form $2^p - 1$ where p is prime are known as **Mersenne primes**.

Euler generalized Fermat's theorem. His generalization follows from the principle that the set G_n of nonzero elements of $\mathbb{Z}_n$ that are not 0 divisors forms a group under multiplication modulo n. We define the **Euler phi-function** $\varphi : \mathbb{Z}^+ \mapsto \mathbb{Z}^+$ as $\varphi(n)$ equaling the number of nonzero elements of $\mathbb{Z}_n$ that are not divisors of 0.

Euler's Theorem

If a is an integer relatively prime to n, then $a^{\varphi(n)} \equiv 1 \mod n$.

We can derive several key insights from this.

- Let m be a positive integer and let $a \in \mathbb{Z}_m$ be relatively prime to m. For each $b \in \mathbb{Z}_m$, the equation $ax = b$ has a unique solution in $\mathbb{Z}_m$. Likewise, the congruence $ax \equiv b \mod m$ has as solutions all integers in precisely one residue class modulo m.
- Let m be a positive integer and let $a, b \in \mathbb{Z}_m$. Let d be the gcd of a and m. The equation $ax = b$ has a solution in $\mathbb{Z}_m$ if and only if d divides b. When d divides b, the equation has exactly d solutions in $\mathbb{Z}_m$. More specifically, the solutions are the integers in exactly d distinct residue classes modulo m.

5.4 The Field of Quotients in an Integral Domain

Not every integral domain is a field. Here we attempt a construction that places every integral domain within a *field of quotients of the integral domain*. This construction is a generalization of the construction of $\mathbb{Z}$ to $\mathbb{Q}$. We examine how to enlarge an integral domain D into a field of quotients F.

1. We define what the elements of F are. We use a constrained form of the Cartesian product

   $$S = \{(a, b) | a, b \in D, b \neq 0\}$$

   where the ordered pair (a, b) represents **formal quotient** a/b and $S \subseteq D \times D$. S is still not our field, since different ordered pairs can represent the same number (i.e. $(2, 4)$ and $(3, 6)$ represent the same number $\frac{1}{2}$). To represent the fact that these ordered pairs are the same, we define the equivalence relation $(a, b) \sim (c, d)$ if $ad = bc$. We let $[(a, b)]$ denote the equivalence class containing (a, b). F is the set of all equivalence classes $[(a, b)]$ for all $(a, b) \in S$.

2. We now define the binary operations of addition and multiplication in F. We take inspiration for these definitions from $\mathbb{Z}$ transformed into $\mathbb{Q}$, where the ordered pair (a, b) represents $a/b \in \mathbb{Q}$. Then

   $$[(a, b)] + [(c, d)] = [(ad + bc, bd)].$$

$$[(a,b)][(c,d)] = [(ac, bd].$$

3. We can then check the field axioms for F. This means that addition and multiplication are both commutative and associate in F. $[(0,1)]$ and $[(1,1)]$ are the additive and multiplicative identities in F respectively. $[(-a,b)]$ is the additive inverse, and $[(b,a)]$ is the multiplicative inverse so long as (a,b) is not the additive identity. All the distributive laws hold in F.

4. We conclude by showing F contains D. We show that there is an isomorphism $i : D \mapsto F$ given by $i(a) = [(a,1)]$. i here is an isomorhpism of D with a subring of F. In other words, i is an isomorphism of D with $i[D]$, and $i[D]$ is a subdomain of F. From here, we can conclude that any integral domain D can be embedded in a field F such that every element in F is the quotient of two elements in D (the field of quotients).

Uniqueness of the Field of Quotients

Let F be a field of quotients of D and let L be a field containing D. Then there exists a map $\psi : F \mapsto L$ that gives an isomorphism of F with a subfield of L such that $\psi(a) = a$ for $a \in D$. Therefore, every field L containing D contains a field of quotients of D, further implying that any two fields of quotients of D are isomorphic.

5.5 Rings of Polynomials

From basic algebra, we have a general understanding of addition and multiplication with respect to polynomials. We use the notation $R[x]$ to denote the set of all polynomials with coefficients in a ring R. We refer to x as an **indeterminate** (not a variable). We also refrain from writing expressions such as $x^2 - 4 = 0$ since $x^2 - 4$ is not the zero polynomial in $\mathbb{Z}[x]$.

Polynomials

Let R be a ring. Then a **polynomial** $f(x)$ with coefficients in R is an **infinite formal sum**

$$\sum_{i=0}^{\infty} a_i x^i$$

where $a_i \in R$ and $a_i = 0$ for all but a finite number of values of i. The largest value of i such that $a_i \neq 0$ is the **degree** of the polynomial, and the values of a_i are the **coefficients** of the polynomial. If $\forall i,\ a_i = 0$ the polynomial has undefined degree.

We are already familiar with how polynomials are added and multiplied. The set $R[x]$ in an indeterminate x is a ring under polynomial addition and multiplication, and inherits properties of commutativity and unity from R.

We can also have polynomials in multiple indeterminates. For two indeterminates x and y, $(R[x])[y]$ represents the polynomials in y with coefficients in $R[x]$. $(R[x])[y]$ is isomorphic to $(R[y])[x]$ and we generally write this as $R[x, y]$. We similarly define **the ring $R[x_1, ..., x_n]$ of polynomials in the n indeterminates x_i with coefficients in R.**

If an D is an integral domain then so is $D[x]$. Likewise, if F is a field then $F[x]$ is an integral domain (note that $F[x]$ is not a field, but since it is an integral domain we can construct a field of quotients $F(x)$ of $F[x]$). $F(x_1, ..., x_n)$ is the field of quotients of $F[x_1, ..., x_n]$ and is called **the field of rational functions in n indeterminates over F.**

Evaluation Homomorphism for Field Theory

Let F be a subfield of E, $\alpha \in E$, with indeterminate x. Then the map $\phi_\alpha : F[x] \mapsto E$ is a homorphism (known as **evaluation at** α) defined by

$$\phi_\alpha \left(\sum_{i=0}^{n} a_i x^i \right) = \sum_{i=0}^{n} a_i \alpha^i$$

We now discuss what it means to find a zero of a polynomial. Let F be a subfield of a field E, and let α be an element of E. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be in $F[x]$ and let ϕ_α be the evaluation homomorphism. Let $f(\alpha)$ denote $\phi_a lpha(f(x))$. If $f(\alpha) = 0$, then α is a **zero** of $f(x)$.

5.6 Factorization of Polynomials over a Field

Solving the polynomial zero problem can be complex. We aim here to unravel a common way of reducing the zero-finding problem. Given two fields F and E with $F \leq E$, suppose $f(x) \in F[x]$ factors in $F[x]$ so that $g(x)h(x) = f(x)$ for $g(x), h(x) \in F[x]$, and let $\alpha \in E$. By the evaluation homomorphism we have

$$f(\alpha) = \phi_\alpha(f(x)) = \phi_\alpha(g(x)h(x)) = \phi_\alpha(g(x))\phi_\alpha(h(x)) = g(\alpha)h(\alpha).$$

Thus either $g(\alpha) = 0$ or $h(\alpha) = 0$, reducing the problem of finding a zero of $f(x)$.

The Division Algorithm

Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0$$

be two elements in $F[x]$, $a_n, b_m \in F$, $m > 0$. Then there are unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$, with $r(x)$ is of degree less than m. We can form this factorization from standard long division as in elementary algebra.

Factor Theorem

$a \in F$ is a factor of $f(x) \in F[x]$ if and only if $x-a$ is a factor of $f(x)$. A nonzero polynomial $f(x) \in F[x]$ of degree n can have at most n zeros in F. Finally, if G is a finite subgroup of the multiplicative group $\langle F^*, \cdot \rangle$ of F, then G is cyclic; more specifically, the multiplicative group of all nonzero elements of a finite field is cyclic.

5.6.1 Irreducible Polynomials

A non-constant polynomial $f(x) \in F[x]$ is **irreducible over** F (equivalently an **irreducible polynomial over** $F[x]$) if it cannot be expressed as a product $g(x)h(x)$ of two polynomials, each with degree lower than f. Let $f(x) \in F[x]$, and let $f(x)$ be quadratic or cubic. $f(x)$ is reducible over F if and only if it has a zero in F.

The Gauss Lemma

If $f(x) \in \mathbb{Z}[x]$, then f factors into two polynomials in $\mathbb{Q}[x]$ (of degrees r and s), if and only if it can also be factored into two polynomials in $\mathbb{Z}[x]$, also of degrees r and s. For a polynomial $f(x) = a_n x^n + \ldots + a_0$, with $a_0 \neq 0$, if f has a zero in $\mathbb{Q}$, then it must have a zero in m, where m divides a_0.

Eisenstein Criterion

Let $p \in \mathbb{Z}$ be prime. Suppose $f(x) = a_n x^n + ... + a_0$ is in $\mathbb{Z}[x]$. $f(x)$ is irreducible over $\mathbb{Q}$ if the following 3 conditions hold:

1. $a_n \not\equiv 0 \mod p$
2. $a_i \equiv 0 \mod p$, $\forall i < n$
3. $a_0 \not\equiv 0 \mod p^2$

As an corollary of the Eisenstein criterion, we can determine that the following polynomial, known as the p**th cyclotomic polynomial**, is irreducible over $\mathbb{Q}$, where

$$\Phi_p(x) = \frac{x^p - 1}{x - 1}.$$

5.6.2 Uniqueness of Factorization in $F[x]$

Polynomials in $F[x]$ can be factored into a product of irreducible polynomials, which are unique except for order and unit.

5.7 Noncommutative Examples - Endomorphisms, Weyl Algebra, Quaternions

We have only so far discussed one noncommutative ring, $M_n(F)$, the ring of $n \times n$ matrices with entries in F. Here we briefly discuss some more examples that occur naturally in algebra.

Endomorhpisms

A homomorphism of an abelian group A into itself is known as an **endomorphism**. The set of all endomorphisms of A is denoted $\mathrm{End}(A)$. $\mathrm{End}(A)$ forms a ring under homomorphism addition and function compositon. However, it is not generally commutative.

We illustrate noncommutativity with an example; take the abelian group $\langle \mathbb{Z} \times \mathbb{Z}, + \rangle$. Take two elements of $\mathrm{End}(\langle \mathbb{Z} \times \mathbb{Z}, + \rangle)$; we can take

$$\phi((m,n)) = (m+n, 0),$$

which expands $(m,n) \in \mathbb{Z} \times \mathbb{Z}$ into the first factor of (m,n); and

$$\psi((m,n)) = (0,n),$$

which collapses the first factor entirely. Then

$$(\phi\psi)(m,n) = (n,0)$$
$$(\psi\phi)(m,n) = (0,0).$$

Weyl Algebra

Let F have characteristic 0, and let $\langle F[x], + \rangle$ be the additive group of the ring of polynomials with coefficients in F. Consider $X \in \mathrm{End}(F[x])$, such that $X(f(x) \in F[x]) = xf(x)$. Further consider $Y \in \mathrm{End}(F[x])$ such that $Y(f(x) \in F[x]) = \frac{d}{dx} f(x)$.

$$YX = \frac{d}{dx} xf(x) = f(x) + xY(f(x))$$

$$XY = xY(f(x))$$

The subring generated by X and Y is the called **Weyl algebra**.

Group Algebra

Let G be a multiplicative group $\{g_i | i \in I\}$, and let R be a commutative ring with unity. Then define RG as the set of all $\sum_{i \in I} a_i g_i$. $\langle RG, +, \cdot \rangle$ is a ring, and is known as the **group ring of G over R**. If F is a field, FG is the **group algebra of G over F**.

5.7.1 The Quaternions

The **quaternions** are an example of a strictly skew field, that is, a noncommutative division ring. We let the set $\mathbb{H}$ (after mathematician Sir William Rowan Hamilton) be $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$. We reduce our discussion of $\mathbb{H}$ to 4 key elements: these are

$$1 = (1,0,0,0) \qquad i = (0,1,0,0)$$
$$j = (0,0,1,0) \qquad k = (0,0,0,1)$$

We allow for scalar multiplication here, i.e.

$$a_1 = (a_1, 0, 0, 0) \qquad a_2 i = (0, a_2, 0, 0)$$
$$a_3 j = (0, 0, a_3, 0) \qquad a_4 k = (0, 0, 0, a_4)$$

We define addition on this group using component-wise addition. For multiplication we use the trick of the following sequence:

$$i, j, k, i, j, k.$$

That is to say, the product of left-to-right adjacent elements is the next element to the right. The product of right-to-left adjacent elements is the *negative* of the element to the left. This arises from the standard cross product from calculus. In other words,

$$ij = k \qquad jk = i \qquad ki = j \qquad kj = -i \qquad ji = -k \qquad ik = -j$$

Our definition of a product of quaternions is then simply our normal distributive definition of multiplication. Quaternions are isomorphic to a subring of $M_2(\mathbb{C})$, so multiplication is associative; however, it is (obviously) not commutative from our definition of multiplication above. The quaternions form a **strictly skew field**, as it can be shown that every element of $\mathbb{H}$ has a multiplicative inverse.

Wedderburn's Theorem

Every finite division ring is a field.

5.8 Ordered Rings and Fields

Omitted for now.

6 Ideals and Factor Rings

6.1 Homomorphisms and Factor Rings

Recall our discussion of ring homomorphisms from earlier, and our definition of the evaluation homomorphism for rings. Here we explore some more examples in-depth, and go over the properties of homomorphisms for rings. Note that all these properties are analogous to those of groups that we discussed much earlier.

Projection Homomorphism

Let $R_1, ..., R_n$ be rings. For each R_i, the map $\pi_i : R_i \times ... \times R_n \mapsto R_i$ defined by $\pi_i(r_1, ..., r_n) = r_i$ is the **projection homomorphism onto the ith component**.

All the properties of homomorphisms for groups translate to rings as well. For a homomorphism ϕ of R into R', if 0 is in R then $\phi(0) = 0'$ is 0 in R'. Additionally, $\phi(-a) = -\phi(a)$. If $S \leq R$, then $\phi(S) \leq R'$; likewise, if $S' \leq R'$, then $\phi^{-1}[S'] \leq R$. The main difference: if R has unity 1, then the unity of R' is $\phi(1)$.

Again analogous to groups, the subring

$$\phi^{-1}[0'] = \{r \in R | \phi(r) = 0'\}$$

is the **kernel** of ϕ. If we let $H = \text{Ker}(\phi)$, we see that $\phi^{-1}(\phi(a)) = a + H = H + a$, where $H + a$ is the coset containing a of the abelian additive group $\langle H, + \rangle$.

The additive cosets of the kernel H of a ring R form a ring R/H where $(a + H) + (b + H) = (a + b) + H$ and $(a + H)(b + H) = (ab) + H$.

Ideals

An additive subgroup N of a ring R such that

$$aN \subseteq N \qquad\qquad Nb \subseteq N$$

is known as an **ideal**; this condition is the **ideal property**. For example, $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$ since we know $n\mathbb{Z}$ is a subring, and for all $s, m \in \mathbb{Z}$, $s(nm) = (nm)s = n(sm) \in n\mathbb{Z}$. An ideal is the analogue of a "normal subgroup" for rings.

Let N be an *ideal* of R. Then the additive cosets of N form the ring R/N with

$$(a + N) + (b + N) = (a + b) + N$$

$$(a + N)(b + N) = (ab) + N.$$

This is the **factor ring** or **quotient ring** of R by N.

Fundamental Homomorphism Theorem (for Rings)

Let N be an ideal of a ring R. Then $\gamma : R \mapsto R/N$ given by $\gamma(x) = x + N$ is a ring homomorphism with kernel N. Let $\phi : R \mapsto R'$ be a ring homomorphism with kernel N. Then $\phi[R]$ is a ring, and the map $\mu : R/N \mapsto \phi[R]$ given by $\mu(x + N) = \phi(x)$ is an isomorphism, and we have $\phi(x) = \mu\gamma(x)$.

6.2 Prime and Maximal Ideals

The ring $\mathbb{Z}_p$, isomorphic to $\mathbb{Z}/p\mathbb{Z}$, is a field for p a prime (it is an example of a **finite field** or **Galois Field**, denoted $GF(p)$). Thus, a factor of an integral domain may be a field.

Every nonzero ring R has at least two ideals, the **improper ideal** R and the **trivial ideal** $\{0\}$. The factor rings are R/R, which has one element, and $R/\{0\}$, which is isomorphic to R. All other ideals are called **proper nontrivial ideals**. If a ring has unity, and N contains a unit, then $N = R$; note that this means that a field has no proper nontrivial ideals.

Maximal Ideals

A **maximal ideal** of R is an ideal M different from R such that there is no proper ideal N of R properly containing M. Additionally, if R is a commutative ring with unity, then M is a maximal ideal of R if and only if R/M is a field. Furthermore, a commutative ring with unity is a field if and only if it has no proper nontrivial ideals.

As an example, we can show that $\mathbb{Z}_p$ is maximal in $\mathbb{Z}$. Assume that $\mathbb{Z}_p$ is contained within an ideal N of $\mathbb{Z}$. Then there is some $x \in N$ which is not in $\mathbb{Z}_p$, i.e. there is an x in N which is not a multiple of p. Then $\gcd(x, p) = 1$, so $\exists\, r, s \in \mathbb{Z} : rx + sp = 1$. Since p and x are both contained within N, the RHS of the equation is also in N, since $(aN)(bN) = (ab)N$. Then 1 is in N, which means $N = \mathbb{Z}$. Therefore $\mathbb{Z}_p$ is a maximal ideal. To show an ideal is maximal, we assume it is contained within another ideal, then show that that ideal is equal to the whole ring.

Prime Ideals

An ideal $N \neq R$ is a **prime ideal** if $ab \in N$ implies that either $a \in N$ or $b \in N$ for $a, b \in R$. R/N is an integral domain if and only if N is a prime ideal of R.

As an example, prime ideals in the integers correspond to the prime numbers. Take the ideal $p\mathbb{Z}$ in $\mathbb{Z}$. Then if $ab \in p\mathbb{Z}$, then $p|ab$ so $p|a$ or $p|b$, which means $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$, so $p\mathbb{Z}$ is a prime ideal. For composite n, the ideal $n\mathbb{Z}$ is *not* prime, since if $n = rs$ but neither r nor s is n, then $rs \in n\mathbb{Z}$ but neither r nor s is in $n\mathbb{Z}$. In summary:

1. An ideal M of R is maximal if and only if R/M is a field.
2. An ideal N of R is prime if and only if R/N is an integral domain.
3. Every maximal ideal of R is a prime ideal.

6.2.1 Prime Fields

For any ring R with unity 1, there is a simple homomorphism from $\mathbb{Z}$ to R:

$$\phi(n) = n \cdot 1, \quad n \in \mathbb{Z}.$$

Suppose R has characteristic $n > 0$; then the kernel of ϕ is $n\mathbb{Z}$ and is an ideal. The kernel of a ring homomorphism is an ideal because the kernel of a ring homomorphism is a subring of R, and for $s \in \text{Ker}(\phi)$, $r \in R$, $\phi(rs) = 0'$ in R. The image $\phi[\mathbb{Z}] \leq R$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$. From here, we can determine that a ring with unity and nonzero characteristic n, it is isomorphic to $\mathbb{Z}_n$; if the characteristic of the ring is 0, then it is isomorphic to $\mathbb{Z}$.

If the characteristic of a field F is nonzero, then F contains a subring isomorphic to $\mathbb{Z}_n$. If n is not prime, then F would have zero divisors, which is impossible; therefore n must be prime. If F is of characteristic zero, it must contain a subring isomorphic to $\mathbb{Z}$. More specifically, F contains a field of quotients of this subring that is isomorphic to $\mathbb{Q}$, which we determine from the uniqueness of the field of quotients. We can conclude that every single field contains a subfield isomorphic to $\mathbb{Z}_p$ for prime p or a subfield isomorphic to $\mathbb{Q}$; in other words, all fields are built from $\mathbb{Z}_p$ and $\mathbb{Q}$. We call these the **prime fields**.

6.2.2 Ideal Structure in $F[x]$

If R is a commutative ring with unity and $a \in R$, the ideal $\{ra | r \in R\}$ is known as the **principal ideal generated by** a denoted $\langle a \rangle$. An ideal is a principal ideal if $N = \langle a \rangle$ for some $a \in R$. If F is a field, every ideal in $F[x]$ is principal. This is analogous to the theorem that if G is a cyclic group, every subgroup of G is cyclic.

Proof: Let N be an ideal of $F[x]$. Suppose $N \neq \{0\}$. Then let $g(x)$ be an element of N of minimal degree. If the degree of $g(x)$ is 0, then $N = \langle 1 \rangle$ and is principal. If the degree of $g(x)$ is greater than 0, we can let $f(x)$ be in N. By the properties of polynomials, $f(x) = g(x)q(x) + r(x)$, where the degree of r is less than the degree of g. Since $f, g \in N$, $f(x) - g(x)q(x) = r(x)$ is also in N. Since g has minimal degree in N, $r(x) = 0$. Then $f(x) = g(x)q(x)$ thus $N = \langle g(x) \rangle$. □
Additionally, an ideal $\langle p(x) \rangle \neq \{0\}$ of $F[x]$ is maximal if and only if $p(x)$ is irreducible over F.

6.3 Gröbner Bases for Ideals

Omitted for now.

7 Extension Fields

7.1 Introduction to Extension Fields

We are at the point now where we can determine that every nonconstant polynomial has a zero, an incredibly important (and not trivial) pillar of algebra. A field E is an **extension field** of F if $F \leq E$.

Kronecker's Theorem

Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there exists an extension field E of F and $\alpha \in E$ such that $f(\alpha) = 0$.

Proof: We know any polynomial $f(x) \in F[x]$ can be factored into irreducible polynomials. We can sufficiently find E containing α such that $p(\alpha) = 0$, where $p(x)$ is an irreducible factor of f. From this, we know that

$\langle p(x)\rangle$ is a maximal ideal, meaning $F[x]/\langle p(x)\rangle$ is a field. We construct a map from F into $F[x]/\langle p(x)\rangle$,

$$\psi(a) = a + \langle p(x)\rangle.$$

This mapping ψ is a bijective homomorphism. We consider $E = F[x]/\langle p(x)\rangle$ as an extension field of F. Let $\alpha = x + \langle p(x)\rangle$, meaning $\alpha \in E$. Using the evaluation homomorphism, we can evaluate $p(\alpha)$ as

$$\phi_\alpha(p(x)) = \sum_{i=0}^{n} a_i(x + \langle p(x)\rangle)^i$$

Note, however, that we are computing in $F[x]/\langle p(x)\rangle$. Computation in a quotient field, where x is a member of the coset α, means that $(x+\langle p(x)\rangle)^i = x^i + \langle p(x)\rangle$. This is because, by the binomial theorem, all the intermediate terms of the polynomial expansion will be multiples of $p(x)$. Thus

$$p(\alpha) = p(x) + \langle p(x)\rangle = 0$$

□

Algebraics and Trascendentals

An element α of an extension field F is **algebraic over** F if $f(\alpha) = 0$ for a nonzero $f(x)$. If this condition is not met, α is **transcendental over** F. In a more traditional context, an element of $\mathbb{C}$ that is algebraic over $\mathbb{Q}$ is called an **algebraic number**. An element of $\mathbb{C}$ that is transcendental over $\mathbb{Q}$ is a **transcendental number**.

For an extension field E of F, let $\alpha \in E$ be algebraic over F. Then there is a unique, irreducible monic polynomial $p(x)$ in $F[x]$ such that $p(\alpha) = 0$. A **monic polynomial** is one whose leading coefficient is 1. Additionally, if $f(\alpha) = 0$, then $p(x)|f(x)$. We denote this irreducible polynomial as $\text{irr}(\alpha, F)$. The degree of this polynomial is $\deg(\alpha, F)$.

As an example, take $\alpha = \sqrt{1+\sqrt{3}} \in \mathbb{C}$. In order to get all coefficients in $\mathbb{Q}$, we can get $\alpha^2 = 1+\sqrt{3}$ so $\alpha^4 - 2\alpha^2 + 1 = 3$ and $\text{irr}(\alpha, \mathbb{Q}) = x^4 - 2x^2 - 2$, and $\deg(\alpha, \mathbb{Q}) = 4$.

7.1.1 Simple Extension Fields

Suppose α is algebraic in F. Then $\langle \text{irr}(\alpha, F)\rangle$ is the kernel of the evaluation homomorphism ϕ_α from $F[x]$ into E. We know that the kernel of a

homomorphism is a maximal ideal. Then, $F[x]/\langle \text{irr}(\alpha, F)\rangle$ is a field, and $F[x]/\langle \text{irr}(\alpha, F)\rangle \simeq \phi_\alpha[F[x]] \leq E$. This subfield is the smallest subfield of E containing F and α,denoted as $F(\alpha)$.

Now suppose α is transcendental in F. Then the evaluation homomorphism is an isomorphism of $F[x]$ with some subdomain of E. Then $\phi_\alpha[F[x]]$ is not a field, but it is an integral domain, denoted $F[\alpha]$. Thus E contains a field of quotients of $F[\alpha]$, which is also denoted $F(\alpha)$ as above.

We illustrate the above with an example. π is transcendental over $\mathbb{Q}$, so $\mathbb{Q}(\pi)$ is isomorphic to $\mathbb{Q}(x)$, the field of rational functions over the indeterminate x.

An extension field is a **simple extension** of F if $E = F(\alpha)$ for some $\alpha \in E$. If $\deg(\alpha, F) \geq 1$, then every element β of the simple extension field E can be expressed, for $b_i \in F$, as $\beta = \sum_{i=0}^{n-1} b_i \alpha^i$.

7.1.2 Algebraic Construction of $\mathbb{C}$ from $\mathbb{R}$

Take the polynomial $p(x) = x^2 + x + 1$ in $\mathbb{Z}_2[x]$, which is irreducible. There is an extension field E which contains a zero α of $p(x)$. The elements of $\mathbb{Z}_2(\alpha)$ are $0+0\alpha$, $1+0\alpha$, $0+1\alpha$, and $1+1\alpha$. This forms a field $0, 1, \alpha, 1+\alpha$, the **finite field of four elements**, also the **Galois field of 4 elements** denoted $GF(4)$. Then in $\mathbb{Z}_2(\alpha)$, $(1+\alpha)^2 = 1 + \alpha^2 = 1 + \alpha + 1 = \alpha$, since $\alpha^2 + \alpha + 1 = 0$. $1 + \alpha^2$ is irreducible in $\mathbb{R}[x]$, and is thus a maximal ideal in $mathbbR[x]$, making $\mathbb{R}[x]/\langle x^2 + 1\rangle$ an extension field of $\mathbb{R}$. Let

$$\alpha = x + \langle x^2 + 1\rangle.$$

Then $\mathbb{R}[x]/\langle x^2 + 1\rangle = \mathbb{R}(\alpha)$, which consists of all elements $a + b\alpha$ where $a, b \in \mathbb{R}$. Since $\alpha^2 + 1 = 0$, we know that α is equivalent to $i \in \mathbb{C}$, and therefore $\mathbb{R}(\alpha) \simeq \mathbb{C}$, completing the construction of $\mathbb{C}$ from $\mathbb{R}$ using quotient fields.

7.2 Vector Spaces

Here we briefly introduce the notion of vector spaces, with relevance to field theory.

Vector Space

A **vector space** over a field F consists of an abelian group V under addition with the operation of left scalar multiplication such that $\forall a, b \in F$, and $\forall \alpha, \beta \in V$

1. $a\alpha \in V$
2. $a(b\alpha) = (ab)\alpha$
3. $(a+b)\alpha = a\alpha + b\alpha$
4. $a(\alpha+\beta) = a\alpha + a\beta$
5. $1\alpha = \alpha$

We call the elements of F **scalars** and the elements of V **vectors**.

Using this (rather general) definition, we can see that $F[x]$ is a vector space over F (which follows from intuition we've seen in linear algebra). More importantly, an extension field E of F is a vector space over F, with addition and scalar multiplication defined as usual. The field of scalars is then a subset of the vector space.

We also have the following vector space properties, which you may recognize from analysis classes. If V is a vector space over F, then $0\alpha = \alpha 0 = 0$, and $(-a)\alpha = a(-\alpha) = -(a\alpha)$.

Linear Independence and Bases

Suppose we have a subset $S = \{\alpha_i | i \in I\}$ of a vector space V. S **spans** V if, for all $\beta \in V$,

$$\beta = \sum_{j=1}^{n} a_j \alpha_{i_j}.$$

Such a vector β is a **linear combination** of the α_{i_j}. If there is a finite subset of V which spans V, then V is **finite-dimensional**. The vectors in S are **linearly independent** over F if the sum $\sum_{j=1}^{n} a_j \alpha_{i_j} = 0$ only when every a_j is 0. A subset of V that spans V and is linearly independent is a **basis** for V. The number of elements in a basis is the **dimension** of V.

We now connect this linear algebra theory to field theory. Let E be an extension field of F, with $\alpha \in E$ algebraic over F. If $\deg(\alpha, F) = n$, then $F(\alpha)$ is an n-dimensional vector space over F with basis $\{1, \alpha, ..., \alpha^{n-2}, \alpha^{n-1}\}$. Every element β of $F(\alpha)$ is algebraic over F, and $\deg(\beta, F) \leq \deg(\alpha, F)$.

7.3 Algebraic Extensions

Finite Extension

An extension field E of F is an **algebraic extension** of F if every element in E is algebraic over F. Additionally, if E is of finite dimension as a vector space over F with dimension n, then E is a **finite extension** of degree n over F. Here, we use the notation that the degree of E over F is $[E : F] = n$. A finite extension field E over F is an algebraic extension of F.

If K is a finite extension of E, and E is a finite extension of F, then $[K : F] = [K : E][E : F]$. This comes naturally from linear algebra; if $\{\alpha_i\}_{i=0}^{n}$ is a basis for E over F, and $\{\beta_i\}_{i=0}^{m}$ is a basis for K over E, then the basis for K over F will be $\{\alpha_i\beta_j\}$ which has mn elements. In general,

$$[F_r : F_1] = \prod_{i=0}^{r-2} [F_{r-i} : F_{r-i-1}].$$

Additionally, if $\beta \in F(\alpha)$, where $\alpha \in E$ is algebraic over F, then $F \leq F(\beta) \leq F(\alpha)$ and therefore $[F(\alpha) : F] = [F(\alpha) : F(\beta)][F(\beta) : F]$ and $\deg(\beta, F)$ divides $\deg(\alpha, F)$.

Algebraic Closure

Let E be an extension field of F. Then

$$\bar{F}_E = \{\alpha \in E | \alpha \text{ algebraic over} F\}$$

is a subfield of E called the **algebraic closure of F in E**. From here, we can easily see that the set of all algebraic numbers is a field, since this set is the closure of $\mathbb{Q}$ in $\mathbb{C}$.

A field F is **algebraically closed** if every nonconstant polynomial in $F[x]$ has a zero in F; equivalently, F is algebraically closed if and only if every nonconstant polynomial in $F[x]$ factors into *linear* factors. This further implies that F has no proper algebraic extensions (if it did, it would

$\text{irr}(\alpha, f) = x - \alpha$ for $\alpha \in E$ to maintain the property of linear factors, which would mean $\alpha \in F$).

The Fundamental Theorem of Algebra

The field $\mathbb{C}$ of complex numbers is an algebraically closed field.

Proof: Let $f(z) \in \mathbb{C}[z]$ have no zero in $\mathbb{C}$. Then $1/f(z)$ is analytic everywhere. If $f \notin \mathbb{C}$, then

$$\lim_{|z| \to \infty} |f(z)| = \infty$$

This is also intuitive from calculus; if a polynomial has no zeroes then at its limits it must tend to either positive or negative infinity. Therefore

$$\lim_{|z| \to \infty} |1/f(z)| = 0,$$

meaning f is bounded in the plane. Liouville's theorem from complex analysis determines every bounded entire function must be constant (not covered in this course); therefore $1/f(z)$ is constant and $f(z)$ is constant. Thus every nonconstant polynomial in $\mathbb{C}[z]$ just have a zero in $\mathbb{C}$, and $\mathbb{C}$ is algeraically closed. $\square$