Abstract Algebra

Muchang Bahng

Spring 2024

Contents

With set theory, we have established what sets, along with functions and relations are. Abstract algebra extends on this by studying *algebraic structures*, which are sets S with specific *operations* acting on their elements. This is a very natural extension and to be honest does not require much motivation. Let's precisely define what operations are.

Definition 0.1 (Operation)

A **p-ary operation**[a] $*$ on a set A is a map

$$* : A^p \longrightarrow A \tag{1}$$

where A^p is the p-fold Cartesian product of A. In specific cases,

1. If $p = 1$, then $*$ is said to be **unary**.
2. If $p = 2$, then $*$ is **binary**.

We can consider for $p > 2$ and even if p is infinite.

[a] or called an operation of arity p.

Definition 0.2 (Algebraic Structure)

An **algebraic structure** is a nonempty set A with a finite set of operations $*_1, \ldots, *_n$ and satisfying a finite set of axioms. It is written as $(A, *_1, \ldots, *_n)$.

If we consider functions between algebraic structures $f : A \to B$, there are some natural properties that we would like f to have.

Definition 0.3 (Preservation of Operation)

Given algebraic structures (A, μ_A), (B, μ_B), where μ_A and μ_B have the same arity p, a function $f : A \to B$ is said to **preserve the operation** if for all $x_1, \ldots, x_p \in A$,

$$f(\mu_A(x_1, \ldots, x_p)) = \mu_B(f(x_1), f(x_2), \ldots, f(x_p)) \tag{2}$$

Functions that preserve operations are generally called *homomorphisms*. However, given that preservation is defined with respect to each operation, a map may preserve one operation but not the other. Therefore, we will formally define homomorphisms for each class of algebraic structures we encounter.

1 Groups

1.1 Monoids and Semigroups

Now the endowment of some structures gives rise to the following. Usually, we will start with the most general algebraic structures and then as we endow them with more structure, we can prove more properties.

Definition 1.1 (Semigroup)

A **semigroup** $(S, *)$ is a set S with an associative binary operation.

Definition 1.2 (Monoid)

A **monoid** $(M, *)$ is a semigroup with an identity element $1 \in M$ such that given a $m \in M$

$$1 * m = m * 1 = m \tag{3}$$

Groupoids aren't necessarily that interesting, but there are cases in which semigroups and monoids come up.

Example 1.1 (Continuous Time Markov Chain)

Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and $(S, \mathcal{S})$ a measurable space. Then, a homogeneous continuous-time Markov chain is a stochastic process $\{X_t\}_{t \geq 0}$ taking values in S (i.e. $X_t : \Omega \rightarrow S$) satisfying the **Markov property**: for every bounded measurable f and and $t, s \geq 0$,

$$\mathbb{E}[f(X_{t+s}) \mid \{X_r\}_{r \leq t}] = \mathbb{E}[f(X_{t+s}) \mid X_t] = (P_s f)(X_t) \tag{4}$$

The set $\{P_t\}_{t \geq 0}$ is called the **Markov semigroup**.

Example 1.2 (Monoid of Transformations)

Given a set S, consider the set of all functions $f : S \rightarrow S$. This forms a monoid with the identity function $f(x) = x$ as the identity element. Proof of associativity is shown in my set theory notes.

Theorem 1.1 (Cardinality of Monoid of Transformations)

If $|S| = n$, then the monoid of transformations has cardinality n^n.

Example 1.3 ()

Let S be any nonempty set. Then $(2^S, \cup, \emptyset)$ and $(2^S, \cap, S)$ are monoids.

We first should ask whether the identity is unique in a monoid. It turns out it is.

Lemma 1.1 (Uniqueness of Monoid Identity)

The identity 1 of a monoid M is unique.

Proof.

Assume not, i.e. there are 2 identities $1 \neq 1'$. But then

$$1 = 11' = 1' \implies 1 = 1' \tag{5}$$

where the implication follows from transitivity of equivalence relations.

Definition 1.3 (Submonoid)

Given a monoid $(M, *)$, let $M' \subset M$. If the restriction of $*$ to $M' \times M'$ is closed in M', then we can define the **submonoid** $(M', *)$.

Theorem 1.2 (Identities of Submonoids)

If M' with identity $1'$ is a submonoid of M with identity 1, Then $1 = 1'$.

Proof.

Assume not. $1' \in M$, which means that

1.2 Groups

Definition 1.4 (Group)

A **group** $(G, *)$ is a set with binary operation $x * y$—also written as xy—having the following properties.[a]

1. *Closure.* $x, y \in G \implies xy \in G$[b]
2. *Associativity.* $\forall x, y, z \in G, x(yz) = (xy)z$
3. *Identity.* $\exists e \in G$ s.t. $\forall x \in G, xe = ex = x$
4. *Inverses.* $\forall x \in G\ \exists x^{-1} \in G$ s.t. $xx^{-1} = x^{-1}x = e$

[a] Note that this is a monoid with the additional property of inverses.

[b] but not necessarily $xy = yx$

This is an extremely simple structure, and the first thing we should prove is the uniqueness of the identity and inverses.

Lemma 1.2 (Uniqueness of Identity and Inverse)

The identity and the inverse is unique, and for any a, b, the equation $x * a = b$ has the unique solution $x = b * a^{-1}$.

Proof.

Assume that there are two identities of group $(G, *)$, denoted e_1, e_2, where $e_1 \neq e_2$. According to the properties of identities, $e_1 = e_1 * e_2 = e_2 \implies e_1 = e_2$.
As for uniqueness of a inverses, let a be an element of G, with its inverses a_1^{-1}, a_2^{-1}. Then,

$$\begin{aligned} a * a_1^{-1} = e &\implies a_2^{-1} * \left(a * a_1^{-1}\right) = a_2^{-1} * e \\ &\implies \left(a_2^{-1} * a\right) * a_1^{-1} = a_2^{-1} \\ &\implies e * a_1^{-1} = a_2^{-1} \end{aligned}$$

Since the inverse is unique, we can operate on each side of the equation $x * a = b$ to get $x * a * a^{-1} = b * a^1 \implies x * e = x = b * a^{-1}$. Clearly, the derivation of this solution is unique since the elements that we have operated on are unique.

At this point, we can see that for each group there is a corresponding "multiplication table" defined by the operation. For example, we can create a set of 6 elements $\{r_0, r_1, r_2, s_0, s_1, s_2\}$ and define the operation $\times$ as the following.

$\times$	r_0	r_1	r_2	s_0	s_1	s_2
r_0	r_0	r_1	r_2	s_0	s_1	s_2
r_1	r_1	r_2	r_0	s_1	s_2	s_0
r_2	r_2	r_0	r_1	s_2	s_0	s_1
s_0	s_0	s_2	s_1	r_0	r_2	r_1
s_1	s_1	s_0	s_2	r_1	r_0	r_2
s_2	s_2	s_1	s_0	r_2	r_1	r_0

Figure 1: Multiplication table for some random (or is it?) group. Note that we can only write such a table explicitly for a group of finite elements. But even for arbitrary groups, we should think of the operation completely defining a possibly "infinite" table.

Let's prove a little more about groups so that we have more tools for manipulation.

Lemma 1.3 (Properties of Group Operation)

Given $a, b, c \in G$,

1. $ab = cb \implies a = c$.
2. $\forall a \in G$, $(a^{-1})^{-1} = a$.
3. $(ab)^{-1} = b^{-1}a^{-1}$.

Proof.

TBD.

Definition 1.5 (Order of a Group)

The **order** of a group G is its cardinality, denoted $|G|$.

Definition 1.6 (Abelian Group)

An **abelian group** $(A, +)$ is a group where $+$ is commutative.[a]

[a] Note that I switched the notation from $*$ to $+$. By convention and to avoid confusion, $+$ denotes commutative operations.

It is clear that in an abelian group, the multiplication table must be symmetric across the diagonal.

Example 1.4 (Abelian Groups)

Here are some examples.

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are all abelian groups with respect to addition. $\mathbb{Q}^* \equiv \mathbb{Q} \setminus \{0\}$ and $\mathbb{R}^* \equiv \mathbb{R} \setminus \{0\}$ are abelian groups with respect to multiplication.
2. The set of all functions on a given interval $[a, b]$ is abelian with respect to addition, defined as

$$(f+g)(x) \equiv f(x) + g(x).$$

We can construct groups a simpler forms of more complex algebraic structures, which we will see later. If you know about rings and fields, it is trivially true that for a ring $(R, +, \times)$ or field $(F, +, \times)$, $(R, +)$ and so $(F, +)$ is a group. We can also construct a group with the multiplication operation.

Example 1.5 (Group of Units in a Ring)

Given a ring $(R, +, \times)$, let R^* be the set of units.

$$R^* := \{r \in R \mid r^{-1} \in R\} \tag{6}$$

Then, $(R^*, \times)$ is a group, called the **group of units** of R. We can see that $a, b \in R^* \implies ab \in R^*$ since $(ab)^{-1} = b^{-1}a^{-1}$, which exists by closure. Associativity is inherited from R to R^*. The identity is a unit and thus is in R^*. Finally for inverses, given $a \in R$ is a unit, a^{-1} exists and is also a unit since $(a^{-1})^{-1} = a$.

Since a field F is a ring, it is immediately true that $(F^*, \times) = (F \setminus \{0\}, \times)$ is a group.

Definition 1.7 (Subgroup)

Given group $(G, *)$ and $(G', *)$ with the same operations, G' is a **subgroup** of G if $G' \subset G$.

1.3 Generating Sets and Group Presentations

A group G may be very abstract and complicated, and so working with all its elements can be a bit painful. It would be more useful to work with a smaller subset S of G that can completely characterize G.[1] We would like to formalize this notion, which will be very useful later on. For now, let's start off with a simple element $a \in G$, and perhaps we can consider the elements

$$\ldots, a^{-2}, a^{-1}, a^0 = e, a^1, a^2, \ldots \tag{7}$$

It may or may not be the case that a may cycle back to itself for some n, i.e. $a = a^n$.

Definition 1.8 (Order of an Element)

The **order** of a group element $a \in G$ is the minimum number $n \in \mathbb{N}$ s.t. $a = a^n$, denoted $|a|$ or $\text{ord}(a)$.[a]

[a] Note that this is different from the order of a group. This is confusing, I know.

Now the set of all multiples of a may or may not be the group, but if we take a certain subset of these elements and take all multiples of all combinations of them, we may have better coverage of the group.

Definition 1.9 (Word)

A **word** is any written product of group elements and inverses. They are generally in the form

$$s_1^{\epsilon_1} s_2^{\epsilon_2} s_3^{\epsilon_3} \ldots s_k^{\epsilon_k}, \text{ where} e_i \in \mathbb{Z} \tag{8}$$

e.g. given a set $\{x, y, z\}$, $xy, xz^{-1}yyx^{-2}, \ldots$ are words.

[1] Note that this is similar to the basis that generates a topology.

Definition 1.10 (Generating Set)

The **generating set** $\langle S \rangle$ of a group G is a subset of G such that every element of the group can be expressed as a word of finitely many elements under the group operations. The elements of the generating set are called **generators**.

Definition 1.11 (Free Group)

The **free group** F_S over a given set S consists of all words that can be built from elements of S.

Now for notational convenience, one method of specifying a group is to put it in the form

$$\Big\langle \, S \mid R \, \Big\rangle \tag{9}$$

where S is the generating set and R is a set of relations. This is called the *group presentation*.

Example 1.6 (Group Presentations)

The cyclic group of order n could be presented as

$$\Big\langle \, a \mid a^n = 1 \, \Big\rangle \tag{10}$$

Dih (8), with r representing a rotation by 45 degrees in the direction of the orientation and f representing a flip over any axis, is presented by

$$\Big\langle \, \{r, f\} \mid r^8 = 1, f^2 = 1, (rf)^2 = 1 \, \Big\rangle \tag{11}$$

A lot of groups fall into one or more categories depending on what properties they have. We will proceed to just define these categories and introduce the groups as needed.

1.4 Group Homomorphisms

At this point, we would like to try and classify groups (e.g. can we find *all* possible groups of a finite set?). But consider the two groups.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

+	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Figure 2: Two isomorphic groups.

These groups have different elements, but the operation behaves in exactly the same way between them (it may be a little harder if I relabeled the elements or permuted the rows/columns). Since we can trivially make arbitrary sets there really isn't much meaning to having two versions of the same group (at least in the algebraic sense). Therefore, these groups should be labeled "equivalent" in some way, and we will precisely define this notion now.

Definition 1.12 (Group Homomorphism)

Let $(G, \circ)$ and $(H, *)$ be two groups. The mapping $f : (G, \circ) \longrightarrow (H, *)$ is a **group homomorphism** if for all $a, b \in G$,

$$f(a \circ b) = f(a) * f(b) \tag{12}$$

Furthermore,

1. A **group isomorphism** is a bijective group homomorphism, and we call groups M, N **isomorphic**, denoted $M \simeq N$, if there exists an isomorphism between them.
2. An **endomorphism** is a homomorphism from a group to itself.
3. An **automorphism** is a isomorphism from a group to itself.

It turns out that from the simple property that $f(ab) = f(a)f(b)$, it also maps identities to identities, and inverses to inverses!

Lemma 1.4 (Homomorphisms Maps Identities/Inverses to Identities/Inverses)

Given a homomorphism $f : (G, *) \to (H, \times)$ and $a \in G$,

$$f(e_G) = e_H, \qquad f(a^{-1}) = f(a)^{-1} \tag{13}$$

Proof.

Let $a \in G$. Then

$$f(a) = f(ae_G) = f(a)f(e_G) \implies e_H = f(a)^{-1}f(a) = f(a)^{-1}f(a)f(e_G) = f(e_G) \tag{14}$$

To prove inverses, we see that

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(e_G) = e_H \tag{15}$$

from above, and this implies that $f(a^{-1}) = f(a)^{-1}$. We can also do this with right hand side multiplication.

Example 1.7 (Exponential Map)

The map $a \mapsto 2^a$ is an isomorphism between $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \times)$ since

$$2^{a+b} = 2^a \times 2^b \tag{16}$$

which is proved in my real analysis notes when constructing the exponential map on the reals.

Example 1.8 (Determinant)

The determinant $\det : \mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}^*$ is a homomorphism because of the product rule for determinants.

Therefore, we can see that an isomorphism is really just a “renaming” of the elements, which aligns with our view of equivalence as above. Not only does it renamee the elements, but it preserves all the algebraic properties of the group and each element.

Theorem 1.3 (Preservation of Properties in Isomorphism)

If $f : G \to H$ is an isomorphism, then
1. f^{-1} is also an isomorphism.
2. $|G| = |H|$.
3. $\forall a \in G$, $\mathrm{ord}(a) = \mathrm{ord}(f(a))$.
4. G is abelian $\implies$ H is abelian.

Proof.

Listed.

1. Since f is bijective by definition, f^{-1} is well-defined and bijective as well. Now we show that f^{-1} is a group homomorphism. Given $c, d \in H$, take
$$f\big(f^{-1}(c), f^{-1}(d)\big) = f\big(f^{-1}(c)\big)\, f\big(f^{-1}(d)\big) = cd \tag{17}$$
where the first equality follows since f is a homomorphism, and the second since f^{-1} is the inverse mapping. Now mapping both sides through f^{-1}, we get
$$f^{-1}(c) f^{-1}(d) = f^{-1}(cd) \tag{18}$$
and so f^{-1} is a homomorphism.
2. This is trivial by bijectivity.
3. TBD.
4. Let $c, d \in H$. Then $c = f(a), d = f(b)$ for some $a, b \in G$, and so $cd = f(a)f(b) = f(ba) = f(b)f(a) = dc$.

A trivial example is the identity map, which is an automorphism. But can we generalize this a bit better?

Theorem 1.4 ()

Let G be a group with $a \in G$. Then the following is an automorphism on G.
$$\phi : G \longrightarrow G,\ \phi(x) = axa^{-1} \tag{19}$$

Proof.

The map $\psi : G \longrightarrow G,\ \psi(x) = a^{-1}xa$ is clearly the inverse of ϕ, with $\phi\psi = \psi\phi = I$ for all $x \in G \implies \phi$ is bijective. Secondly, $\phi(x)\phi(y) = axa^{-1}aya^{-1} = a(xy)a^{-1} = \phi(xy) \implies \phi$ preserves the group structure.

Definition 1.13 (Kernel)

Given group homomorphism $f : G \to H$, the **kernel** of f is defined
$$\ker(f) \coloneqq \{g \in G \mid f(g) = e_H\} \tag{20}$$
That is, it is the preimage of the identity.

Theorem 1.5 (Kernels are Subgroup)

Given a group homomorphism $f : G \to H$,

1. $\ker(f)$ is a subgroup of G.
2. f is injective $\iff \ker(f) = \{e_G\}$.

Proof.

For the first part, we prove the properties of a group. To show closed, consider $a, b \in \ker(f)$. Then $f(ab) = f(a)f(b) = e_H e_H = e_H \implies ab \in \ker(f)$. Since $f(e_G) = e_H$, $e_G \in \ker(f)$. If $a \in \ker(f)$, then $f(a^{-1}) = f(a)^{-1} = e_H^{-1} = e_H \implies a^{-1} \in \ker(f)$. Finally associativity follows from associativity of the supgroup.

For the second part, we prove bidirectionally.

1. $(\rightarrow)$. Since f is injective, $f(a) = f(b) \implies a = b$. Let $a \in \ker(f)$. Then $f(a) = e_H$, and so $f(e_G) = e_H = f(a)$. By injectivity, $a = e_G$, and so $\ker(f) = \{e_G\}$.
2. $(\leftarrow)$. Let $a, b \in G$ s.t. $f(a) = f(b)$. Then $f(a)f(b)^{-1} = e_H \implies af(a)f(b^{-1}) = f(ab^{-1}) = e_H \implies ab^{-1} \in \ker(f)$. But by hypothesis $\ker(f) = \{e_G\} \implies ab^{-1} = e_G \implies a = b$.

Example 1.9 (Projection onto Unit Circle)

Given $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ with × and $S^1 = \{x \in \mathbb{C} \mid |x| = 1\}$ (which is a group under multiplication), the map $f : \mathbb{C}^* \rightarrow S^1$ defined $f(z) = z/|z|$ is a group homomorphism since

$$f(z_1 z_2) = \frac{z_1 z_2}{|z_1 z_2|} = \frac{z_1 z_2}{|z_1||z_2|} = f(z_1)f(z_2) \tag{21}$$

Theorem 1.6 (Tip)

To prove a group homomorphism, show that every element of G and H can be written as a word of certain g_i's in G and then h_i's in H, and map the g_i's to h_i's.

1.5 Some Types of Groups

At this point we are ready to start identifying some types of groups. We will introduce the following (non-exclusive) categories: cyclic groups, symmetric groups, symmetry groups[2], and Lie groups. There is one other category called the dicyclic group but I omit it. Just know that the group of quaterions of order 8 is one such dicyclic group that doesn't fit into any other categories. Here is a table of all known groups of small orders. We will prove this theorem as we go along.

Theorem 1.7 (Classification of Simple Groups of Small Order)

The following are the only groups of order n. You can notice that it is dominated by direct products of cyclic groups, since they exist for every order, while the other types increase in order very fast.

n	**Abelian Groups**	**Non-Abelian Groups**
1	$\{e\}$ (trivial group)	None
2	$\mathbb{Z}_2 = S_2 = \text{Dih}(1)$	None
3	$\mathbb{Z}_3 = A_3$	None
4	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 = \text{Dih}(2)$	None
5	$\mathbb{Z}_5$	None
6	$\mathbb{Z}_6 = \mathbb{Z}_3 \times \mathbb{Z}_2$	$S_3 = \text{Dih}(3)$
7	$\mathbb{Z}_7$	None
8	$\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$D_4 = \text{Dih}(4)$, Q_8 (quaternion)
9	$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$	None
10	$\mathbb{Z}_{10} = \mathbb{Z}_5 \times \mathbb{Z}_2$	$D_5 = \text{Dih}(5)$
11	$\mathbb{Z}_{11}$	None
12	$\mathbb{Z}_{12} = \mathbb{Z}_4 \times \mathbb{Z}_3$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$	A_4, $D_6 = \text{Dih}(6)$, $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ (dicyclic)

Figure 3: Classification of groups up to order 12.

[2] confusing name, I know

1.5.1 Cyclic Groups

Definition 1.14 (Cyclic Group)

A **cyclic group**, denoted Z_n, is a group generated by a single element. In a **finite cyclic group**, there exists a $k \in \mathbb{N}$ such that $g^k = g^0 = 1$ (or in additive notation, $kg = 0g = 0$), where g is the generator. A **finitely generated group** is a group generated by a finite number of elements. In **infinite cyclic groups**, all elements are distinct for distinct k.

Example 1.10 (Cyclic Groups)

Here are some examples of cyclic groups.

1. $(\mathbb{Z}_n, +)$, the integers mod n, is a cyclic group of order n, generated by 1.[a]
2. The nth roots of unity in $\mathbb{C}$ is a cyclic group of order n, generated by the counterclockwise rotation $e^{2\pi/n}$.
3. The set of discrete angular rotations in $SO(2)$, in the form of

$$R = \left\{ \begin{pmatrix} \sin\theta & \cos\theta \\ \cos\theta & -\sin\theta \end{pmatrix} \;\middle|\; \theta \in \left\{ \frac{2\pi}{n} k \right\}_{k=0}^{n-1} \right\} \tag{22}$$

4. $(\mathbb{Z}, +)$ is an infinite cyclic group.

[a] In fact, the generator of $\mathbb{Z}_n$ can be any integer relatively prime to n and less than n.

That's really it for cyclic groups, and to make things simpler, there is a complete characterization of them.

Theorem 1.8 (Cyclic Groups are Unique up to Order)

Given a cyclic group, Z or Z_n

1. If it is finite, then $(Z_n, +) \simeq (\mathbb{Z}_n, +) \simeq \langle 1 \rangle$.
2. If it is infinite, then $(Z, +) \simeq (\mathbb{Z}, +) \simeq \langle 1 \rangle$.

Proof.

Therefore, we have completely characterized all cyclic groups! However, note that there can be isomorphisms from a cyclic group to a subgroup.

Example 1.11 (Integers to Even Integers)

Let $2\mathbb{Z}$ denote the set of all even integers with addition. Then we can verify that this is a group, and

$$\mathbb{Z} \simeq 2\mathbb{Z} \tag{23}$$

1.5.2 Symmetric and Alternating Groups

Notice that given any set S, we can define the set of all functions $f : S \to S$ as a monoid. What if we consider the set of all invertible functions? This by definition means bijective functions, and so consider this subset.

Definition 1.15 (Symmetric/Transformation Group)

Given a set S, the **transformation group**, or **symmetric group**, of S is the group of all bijective maps from S to itself.

This exists for all sets S, and if S is finite, we call it a **permutation group**, since the set of bijective transformations of it is a permutation of its elements.

Definition 1.16 (Permutation Group)

The **permutation group** is the set of all bijective transformations from any set X to the same set, denoted either $\text{Sym}(X)$ or S_n. If $X = \{1, 2, 3, ..., n\}$, known as the set of all permutations of X, with cardinality $n!$.

Lemma 1.5 ()

Every element in finite S_n can be decomposed into a partition of cyclic rotations.

Example 1.12 ()

Listed.

1. (12) is a mapping $1 \to 2,\ 2 \to 1$.
2. (123) is a mapping $1 \to 2,\ 2 \to 3,\ 3 \to 1$.
3. $(123)(45)$ is a mapping $1 \to 2,\ 2 \to 3,\ 3 \to 1,\ 4 \to 5,\ 5 \to 4$.

Definition 1.17 ()

The **conjugacy class** of S_n correspond to the cycle structures of S_n. Two elements of S_n are conjugate in S_n if and only if they consist of the same number of disjoint cycles of the same lengths.

Example 1.13 ()

1. $(123)(45)$ is conjugate to $(143)(25)$.
2. $(12)(45)$ is not conjugate to $(143)(25)$.

Theorem 1.9 (Transpositions)

The set of all **transpositions** forms a generating set of S_n.

Definition 1.18 ()

The **signature** of a permutation is a homomorphism

$$\text{sgn} : S_n \longrightarrow \{1, -1\} \tag{24}$$

Lemma 1.6 ()

The signature of a permutation changes for every transposition that is applied to it.

Now the reason that symmetric groups are nice is that we can embed a group into its symmetric group.

Theorem 1.10 (Cayley's Theorem)

Every group G is isomorphic to a subgroup of its symmetric group. If G is finite, then so is $\text{Sym}(G)$, so every finite group is a subgroup of S_n, for some n.

Proof.

Let $H = \text{Sym}(G)$. We define the map

$$\phi : G \longrightarrow H \tag{25}$$

by the following rule. For $a \in G$, map it to permutation $\sigma = \phi(a) \in H$ defined as $\sigma(g) = ag$ for all $g \in G$. Note that given an $a \in G$, ag must also be in G, meaning that a corresponding $\sigma \in H$ exists. It is sufficient to prove that ϕ is an isomorphism onto its image. We first prove injectivity. Given $a \neq b \in G$, $\phi(a) = \sigma, \phi(b) = \tau$. Assume $\sigma = \tau \implies a = ae = \sigma(e) = \tau(e) = be = b \implies a = b$, a contradiction. We now check that $\phi(ab) = \phi(a)\phi(b)$. Given $g \in G, \phi(a)\phi(b)(g) = \phi(a)(bg) = a(bg) = (ab)g = \phi(ab)(g)$.

Definition 1.19 (Alternating Group)

The **alternating group** of order n is the set of all **even permutations** (permutations that have signature 1) of $\{1, 2, ..., n\}$. It is denoted A_n or $\text{Alt}(n)$ and its cardinality is $\frac{1}{2}n!$. Note that the set of odd permutations do not form a group, since the composition of two odd permutations (each having signature -1 is an even permutation.

Example 1.14 (Low Order Symmetric Groups)

1. S_0 is the set of all permutations on the **null set**. S_1 is the set of all permutations on the **singleton set**. Both sets have cardinality 1 and the element is **trivial**. Note that $S_1 = A_1$.
2. S_2 is a cyclic, abelian group of order 2 consisting of the identity permutation and the transposition of two elements.
3. S_3 is the first cyclic, nonabelian group, with order $6.S \simeq \text{Dih}(3)$, which can be seen as the group of rotations and reflections on the equilateral triangle, and the elements of S_3 equate to permuting the vertices on the triangle.

In lecture, we talked about the number of all finite set is e. Since $n!$ is the order of permutation groups, i.e. the order of automorphism groups, we can sum their inverses over all $n \in \mathbb{N}$ to get e.

1.5.3 Symmetry Groups of Geometric Objects

Definition 1.20 (Polytope)

A **polytope** in n-dimensions is a geometrical object with "flat sides, " called an n-polytope. It is a generalization of a polygon or a polyhedron to an arbitrary number of dimensions.

Definition 1.21 (Simplex)

A **n-simplex** is a n-polytope which is the n-dimensional convex hull of its $n+1$ vertices. Moreover, the $n+1$ vertices must be **affinely independent**, meaning that

$$\{u_1 - u_0, u_2 - u_0, ..., u_n - u_0 | \{u_i\}_{i=0}^n \text{ vertices}\} \tag{26}$$

are linearly independent vectors that span the n-dimensional space.

Definition 1.22 (Symmetry Group)

The **symmmetry group** of a geometrical object is the group of all transformations in which the object is invariant. Preserving all the relevant structure of the object.

Definition 1.23 (Dihedral Group)

A common example of such groups is the **dihedral group** of order $2n$, with the group presentation

$$\text{Dih}(n) := \langle r, f \mid r^n = f^2 = e, rfr = f \rangle \tag{27}$$

, denoted $\text{Dih}(n)$ of order $2n$, which is the group of symmetries of a n-simplex, which includes rotations and reflections.

Example 1.15 (Dih(3) on Triangle)

The group of rotations and flips you can do on a equilateral triangle is called the Dihedral Group $\text{Dih}(3)$. It is not abelian.

	r_0	r_1	r_2	s_0	s_1	s_2
r_0	r_0	r_1	r_2	s_0	s_1	s_2
r_1	r_1	r_2	r_0	s_1	s_2	s_0
r_2	r_2	r_0	r_1	s_2	s_0	s_1
s_0	s_0	s_2	s_1	r_0	r_2	r_1
s_1	s_1	s_0	s_2	r_1	r_0	r_2
s_2	s_2	s_1	s_0	r_2	r_1	r_0

Figure 4: Multiplication table for D_3.

Example 1.16 (Groups of Order 3)

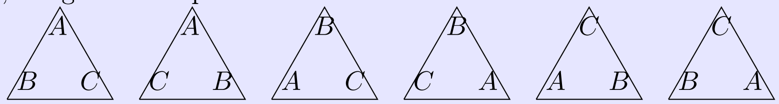
$\text{Dih}(3) \simeq S_3$, since permutations of the vertices of a triangle are isomorphic to a permutations of a 3-element set.

However, S_4 is not isomorphic to the symmetry group of a square. It is however, isomorphic to that of a tetrahedron, i.e. $\text{Dih}(4)$.

Example 1.17 (Low Order Dihedral Group)

We introduce some low order Dihedral groups.

1. $\text{Dih}(3)$ is the group of all rotations and reflections that preserve the structure of the equilateral triangle in $\mathbb{R}^2$, a regular 2-simplex.



2. $\text{Dih}(4)$ is the group of all rotations and reflections that preserve the structure of the regular tetrahedron in $\mathbb{R}^3$. An incorrect, yet somewhat useful, way of visualizing this group is to imagine a square in $\mathbb{R}^2$. However, the points are not pairwise equidistant and therefore does not preserve symmetry between all points.
3. $\text{Dih}(n)$ is similarly the group of all rotations and reflections that preserve the structure of a regular $(n-1)$-simplex in $\mathbb{R}^{n-1}$.

Example 1.18 (Klein 4 Group)

The **Klein 4-Group** can be described as the symmetry group of a non-square rectangle. With the three non-identity elements being horizontal reflection, vertical reflection, and 180-degree rotation.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Figure 5: Multiplication table for the Klein 4-group (V_4)

Example 1.19 (Groups of Order 4)

There are only 2 groups of order 4.

C_4	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

(a) Cyclic group C_4

V	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(b) Klein four-group V

Figure 6: Cayley tables for the two groups of order 4

1.5.4 Lie Groups

Definition 1.24 (General Linear Group)

The **general linear group**, denoted $\text{GL}(V)$, is the set of all bijective linear mappings from V to itself. Similarly, $\text{GL}_n(\mathbb{F})$, or $\text{GL}\ (n, \mathbb{F})$ is the set of all nonsingular $n \times n$ matrices over the field $\mathbb{F}$. Due to the same dimensionality of the following spaces, it is clear that $\text{GL}(V) \simeq \text{GL}(\mathbb{F}^n) \simeq \text{GL}_n(\mathbb{F})$. The **special linear group**, denoted $\text{SL}_n(\mathbb{F})$ or $\text{SL}(n, \mathbb{F})$, is the set of $n \times n$ matrices a with determinant 1. $\text{SL}_n(\mathbb{F})$ is a subgroup of $\text{GL}_n(\mathbb{F})$, which is a subset of the ring of all $n \times n$ matrices over field $\mathbb{F}$, denoted $\mathbb{L}_n(\mathbb{F})$.

Definition 1.25 (Translation Group)

The group of all translations in the space V is denoted $\text{Tran}\, V$. Its elements are usually denoted as t_u, where u is the vector that is being translated by. It can also be interpreted as shifting the origin by $-u$. It is clear that $\text{Tran}\, V \simeq V$.

Definition 1.26 (General Affine Group)

The **general affine group** is the pair of all transformations

$$\text{GA}(V) \equiv \text{Tran}(V) \times \text{GL}(V) \tag{28}$$

Definition 1.27 (Isometries)

The **Euclidean group** of **isometries** in the Euclidean space $\mathbb{E}^n$ (with the Euclidean norm), denoted $\text{Isom}\, \mathbb{E}^n$ or $\mathbb{E}(n)$, consists of all distance-preserving bijections from $\mathbb{E}^n$ to itself, called **motions** or **rigid transformations**. It consists of all combinations of rotations, reflections, and translations. The **special Euclidean group** of all isometries that preserve the **handedness** of figures is denoted

$\mathbb{SE}(n)$, which is comprised of all combinations rotations and translations called **rigid motions** or **proper rigid transformations**.

Definition 1.28 (Orthogonal Group)

The **orthogonal group**, denoted $\mathrm{O}(n)$, consists of all isometries that preserve the origin, i.e. consists of rotations and reflections. The **special orthogonal group**, denoted $\mathrm{SO}(n)$, is a subgroup of $\mathrm{O}(n)$ consisting of only rotations. We can see that

$$\mathrm{O}(n) = \frac{\mathrm{Isom}\,\mathbb{E}^n}{\mathrm{Tran}\,V} \tag{29}$$

Definition 1.29 (Transitive)

A transformation group G is called **transitive** if for any $x, y \in X$, there exists a $\phi \in G$ such that $y = \phi(x)$.

Example 1.20 ()

$\mathrm{Tran}(V)$ and $\mathrm{GA}(V)$ are transitive groups.

Definition 1.30 (Congruence Classes)

Let X be a set and G its transformation group on X. The way we define G determines the **geometry** of X. More specifically, a figure $F_1 \subset X$ is **equivalent** or **congruent** to $F_2 \subset X$ iff there exists $\phi \in G$ such that $F_2 = \phi(F_1)$ (or equivalently, $F_1 = \phi(F_2)$). This is an equivalence relation since

1. $F \sim F$.
2. $F \sim H \implies H \sim F$.
3. $F \sim H, H \sim K \implies F \sim K$

Two figures that are in the same equivalence class are known to be **congruent** with respect to the geometry of X induced by G.

Clearly, if two figures are congruent in Euclidean geometry, then they are congruent in Affine geometry, since $\mathrm{E}(n) \subset \mathrm{GA}(n)$.

1.6 Subgroups

We have seen a few examples of subgroups, but we will heavily elaborate on here. We know that given a set, we can define an equivalence relation on it to get a quotient set. Now if we have a group, defining any such relation may not be compatible with the group structure. Therefore, it would be nice to have some principles in which we can construct such compatible equivalence classes. Fortunately, we can do such a thing by taking a subgroup $H \subset G$ and "shifting" it to form the cosets of G, which are the equivalence classes.

Definition 1.31 (Coset)

Given a group G, $g \in G$, and subgroup H,

1. A **left coset** is $gH \coloneqq \{gh \mid h \in H\}$.
2. A **right coset** is $Hg \coloneqq \{hg \mid h \in H\}$.
3. If G is abelian, then the **coset** is $gH \coloneqq \{g + h \mid h \in H\}$.

This divides the group into equivalence classes $g \mapsto [g] = gH$, and we write (for left cosets)

$$a \equiv b \pmod{H} \iff a = bh \text{ for some } h \in H \tag{30}$$

Proof.

We show that this indeed forms an equivalence class.

With this partitioning scheme in mind, the following theorem on the order of such groups becomes very intuitive, and has a lot of consequences.

Theorem 1.11 (Lagrange's Theorem)

Let G be a finite group and H its subgroup. Then

$$|G| = [G : H]|H| \tag{31}$$

where $[G : H]$, called the **index of** H, is the number of cosets in G. Therefore, the order of a subgroup of a finite group divides the order of the group.

Proof.

The union of the $[G : H]$ disjoint cosets is all of G. On the other hand, every H is in one-to-one correspondence with each coset aH, so every coset has $|H|$ elements. Therefore, there are $[G : H]|H|$ elements altogether.

However, the converse is usually false, as there is a group of order 12 having no subgroup of order 6.

Corollary 1.1 ()

The order of any element of a finite group divides the order of the group.

Proof.

Take any $a \in G$ and construct the cyclic subgroup $\langle a \rangle \subset G$. Then by Lagrange's theorem, $|a| = |\langle a \rangle|$ divides $|G|$.

Corollary 1.2 ()

Every finite group of a prime order is cyclic.

Proof.

Let $a \in G$ be any element other than the identity e, and consider $\langle a \rangle \subset G$. The order must divide $|G|$ which is prime, so $|a| = 1$ or $|G|$. But $|a| \neq 1$ since we did not choose the identity, so $|a| = |G| \implies \langle a \rangle = G$.

Corollary 1.3 ()

If $|G| = n$ and $a \in G$ is arbitrary, then $a^n = e$.

Proof.

Let $|a| = k$. Then $k \mid n$, and so $a^n = a^{kl} = (a^k)^l = e^l = e$.

Corollary 1.4 (Fermant's Little Theorem)

Let p be a prime number. The multiplicative group $\mathbb{Z}_p \setminus \{0\}$ of the field $\mathbb{Z}_p$ is an abelian group of order $p-1 \implies g^{p-1} = 1$ for all $g \in \mathbb{Z}_p \setminus \{0\}$. So,

$$a^{p-1} \equiv 1 \iff a^p \equiv a \pmod{p} \tag{32}$$

Definition 1.32 (Normal Subgroups)

A subgroup $N \subset G$ is a **normal subgroup** iff the left cosets equal the right cosets. That is, $\forall b \in G, h \in H$.

$$b^{-1}hb \in H \tag{33}$$

Every subgroup of an abelian group is normal.

The concept of normal subgroups allow us to endow on the quotient set a group structure.

Definition 1.33 (Quotient Group)

Given a group G and a normal subgroup H, the **quotient group** G/H is the set of left cosets aH with the operation

$$aH\,bH = abH \tag{34}$$

Lemma 1.7 ()

A subgroup $H \subset G$ is normal if and only if there exists a group homomorphism $\phi : G \to G'$ with $\ker \phi = H$.

Proof.

We prove bidirectionally.

1. $(\to)$. Since H is normal, we can form the quotient group G/H. Let $\phi : G \to G/H$ be defined $\phi(a) = aH$. Then,

$$\begin{aligned} \ker \phi = \phi^{-1}(eH) &= \{a \in G \mid aH = eH = H\} && (35) \\ &= \{a \in G \mid a \in H\} && (36) \end{aligned}$$

   Therefore, ϕ is a homomorphism because $\phi(ab) = abH = (aH)(bH)$.

Theorem 1.12 (Quotient Maps are Homomorphisms)

The map $\pi : G \to G/H$ is a group homomorphism, and the **quotient group** is the set of left cosets with

Proof.

Corollary 1.5 ()

If $|G| = n$, then $g^n = e$ for all $g \in G$.

Definition 1.34 (Euler's Totient Function)

Euler's Totient Function, denoted $\varphi(n)$, consists of all the numbers less than or equal to n that are coprime to n.

Theorem 1.13 (Euler's Theorem)

For any n, the order of the group $\mathbb{Z}_n \setminus \{0\}$ of invertible elements of the ring $\mathbb{Z}_n$ equals $\varphi(n)$, where φ is Euler's totient function. In other words with $G = \mathbb{Z}_n \setminus \{0\}$,

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \text{ where } a \text{ is coprime to } n \tag{37}$$

Example 1.21 ()

In $\mathbb{Z}_{125} \setminus \{0\}$, $\varphi(125) = 125 - 25 = 100 \implies 2^{100} \equiv 1 \pmod{125}$

Definition 1.35 ()

Let G be a transformation group on set X. Points $x, y \in X$ are equivalent with respect to G if there exists an element $g \in G$ such that $y = gx$. This has already been defined through the equivalence of figures before. This relation splits X into equivalence classes, called **orbits**. Note that cosets are the equivalence classes of the transformation group G; oribits are those of X. We denote it as

$$Gx \equiv \{gx \mid g \in G\} \tag{38}$$

By definition, transitive transformation groups have only one orbit.

Definition 1.36 ()

The subgroup $G_x \subset G$, where $G_x \equiv \{g \in G | gx = x\}$ is called the **stabilizer** of x.

Example 1.22 ()

The orbits of $O(2)$ are concentric circles around the origin, as well as the origin itself. The stabilizer of the point $p \neq 0$ is the identity and the reflection across the line ??. The stabilizer of 0 is the entire $O(2)$.

Example 1.23 ()

The group S_n is transitive on the set $\{1, 2, ..., n\}$. The stabilizer of $k, (1 \leq k \leq n)$ is the subgroup $H_k \simeq S_{n-1}$, where H_k is the permutation group that does not move k at all.

Theorem 1.14 ()

There exists a 1-to-1 injective correspondence between an orbit G_x and the set G/G_x of cosets, which maps a point $y = gx \in Gx$ to the coset gG_x.

Definition 1.37 ()

The **length of an orbit** is the number of elements in it.

Corollary 1.6 ()

If G is a finite group, then

$$|G| = |G_x||Gx| \tag{39}$$

In fact, there exists a precise relation between the stabilizers of points of the same orbit, regardless of G being finite or infinite:

$$G_{gx} = gG_xg^{-1} \tag{40}$$

1.7 Products and Extensions of Groups

1.7.1 Direct Products

Definition 1.38 (Direct Product)

The **direct product** of two groups G and H is denoted

$$G \times H \equiv \{(g,h) \mid g \in G, h \in H\} \tag{41}$$

Note that the product need not be binary (nor must it be of finite arity).

Example 1.24 ()

The **general affine group** is defined

$$\mathrm{GA}(V) \equiv \operatorname{Tran} V \times \mathrm{GL}(V) \tag{42}$$

Example 1.25 ()

The **Galileo Group** is the transformation group of spacetime symmetries that are used to transform between two reference frames which differ only by constant relative motion within the constructs of Newtonian physics. It is denoted

$$\operatorname{Tran} \mathbb{R}^4 \times H \times \mathrm{O}(3) \tag{43}$$

where H is the group of transformations of the form

$$(x,y,z,t) \longmapsto (x+at, y+bt, z+ct, t) \tag{44}$$

Example 1.26 ()

The **Poincaré Group** is the symmetry group of spacetime within the principles of relativistic mechanics, denoted

$$G = \operatorname{Tran} \mathbb{R}^4 \times \mathrm{O}_{3,1} \tag{45}$$

where $\mathrm{O}_{3,1}$ is the group of linear transformations preserving the polynomial

$$x^2 + y^2 + z^2 - t^2 \tag{46}$$

1.7.2 Semidirect Products

1.7.3 Group Extensions

1.8 Group Actions

Definition 1.39 (Group Action)

Let G be a group, X a set. Then, a (left) group action of G on X is a function:

$$\varphi : G \times X \longrightarrow X,\ (g, x) \longmapsto \varphi(g, x) \tag{47}$$

satisfying two axioms:

1. Identity. $\forall x \in X, \varphi(e, x) = x$.
2. Compatibility. $\forall g, h \in G$ and $\forall x \in X, \varphi(gh, x) = \varphi(g, \varphi(h, x))$.

The group G is said to **act on** X. X is called a **G-set**. The two axioms, furthermore, imply that for every $g \in G$, the function that maps $x \in X$ to $\varphi(g, x) \in X$ is a bijective map, since the inverse is the function mapping $x \mapsto \varphi(g^{-1}, x)$.

(g, x) can be interpreted as the element g in the transformation group G acting on an element x in X.

Example 1.27 ()

$\operatorname{Isom}\mathbb{R}^3$ acts on $\mathbb{R}^3$ since every element $g \in \operatorname{Isom}\mathbb{R}^3$ acts on the entire space $\mathbb{R}^3$.

Example 1.28 ()

S_n acts on $\{1, 2, ..., n\}$by permuting its elements.

Example 1.29 ()

The $\text{GA}(V)$ acts transitively on the points of an affine space.

Equivalent Interpretation of Group Actions Note that this group action G on space X identifies a group homomorphism into the group of automorphisms of that space. Given an abstract group element $g \in G$, $\varphi(g, \cdot) : X \longrightarrow X$ is defined accordingly, where $\varphi(g, \cdot) \in \text{Aut}(X)$. So alternatively, we can interpret a group action as a homomorphism from G to $\text{Aut}(X)$.

$$\phi : G \longrightarrow \text{Aut}(X),\ g \mapsto \phi(g) = \varphi(g, \cdot) \tag{48}$$

Definition 1.40 (Representation)

A group action on a finite-dimensional vector space X is called a **representation** of that group.

1.9 Abelian Groups

First, note that the successive addition of elements of an additive abelian group can be represented by integer multiplication.

$$x + x + ... + x = nx,\ n \in \mathbb{Z} \tag{49}$$

Similarly, we can take the integer power of an element to represent successive multiplication in a multiplicative abelian group.

Lemma 1.8 ()

It is easy to check that in an additive abelian group A, with $a, b \in A$ and $k, l \in \mathbb{Z}$,

$$k(a+b) = ka + kb \tag{50}$$
$$(k+l)a = ka + la \tag{51}$$
$$(kl)a = k(la) \tag{52}$$

which implies

$$k(a-b) = ka - kb, \; (k-l)a = ka - la \tag{53}$$

Definition 1.41 ()

For any subset $S \subset A$, the collection of all linear combinations

$$k_1 a_1 + k_2 a_2 + ... + k_n a_n, \; k_i \in \mathbb{Z}, a_i \in S \tag{54}$$

is the smallest subgroup of A containing S, called the **subgroup generated by** S and denoted $\langle S \rangle$. If $\langle S \rangle = A$, then we say that A is **generated** by S, or that S is a **generating set** of A.

Definition 1.42 ()

An abelian group that has a finite generating set is called **finitely generated**. Finitely generated abelian groups are similar to finite dimensional vector spaces.

Definition 1.43 ()

A system $\{a_1, a_2, ..., a_n\}$ of elements of a group A is called **linearly independent** if $k_1 a_1 + k_2 a_2 + ... + k_n a_n = 0 \implies k_1, k_2, ..., k_n = 0$. A system of linear independent elements that generates A is called a **basis**.

Note that every finite dimensional vector has a basis, but not every finitely generated abelian group has one. For example, $(\mathbb{Z}_n, +)$ is generated by one element, but it has no basis since every element $a \in \mathbb{Z}_n$ satisfies the nontrivial relation $na = 0$.

Definition 1.44 ()

A finitely generated abelian group is **free** if it has a basis.

Theorem 1.15 ()

All bases of a free abelian group L contain the same number of elements.

Definition 1.45 ()

The **rank** of a free abelian group L is the number of elements in its basis. It is denoted rk$L$. The zero group is regarded as a free abelian group of rank 0.

Theorem 1.16 ()

Every free abelian group L of rank n is isomorphic to the group $\mathbb{Z}^n$ of integer rows of length n.

Theorem 1.17 ()

Every subgroup n of a free abelian group l of rank n is a free abelian group of rank $\leq n$.

Note that unlike a vector space, a free abelian group of positive rank contains subgroups of the same rank that do not conside with the whole group. For example, the subgroup $m\mathbb{Z} \subset \mathbb{Z}, m > 0$ has rank 1, just as the whole group.

Moreover, a free abelian group of rank n can be embedded as a subgroup into an n-dimensional Euclidean vector space E^n. To do this, let $\{e_1, e_2, ..., e_n\}$ be a basis of E^n. Then, the subgroup generated by these basis vectors is the set of vectors with integer components, which is a free abelian group of rank n. This subgroup obtained as such is called a **lattice** in E^n.

Definition 1.46 ()

A subgroup $L \subset E^n$ is **discrete** if every bounded subset of E^n contains a finite number of elements in L. Clearly, every lattice is discrete, and a subgroup generated by a linearly independent system of vectors (i.e. a lattice in a subspace of E^n) is discrete.

Lemma 1.9 ()

A subgroup $L \subset E^n$ is discrete if and only if its intersection with any neighborhood of 0 consists of 0 itself.

Theorem 1.18 ()

Every discrete subgroup $L \subset E^n$ is generated by a linearly independent system of vectors of E^n.

Corollary 1.7 ()

A discrete subgroup $L \subset E^n$ whose linear span coincides with E^n is a lattice in E^n.

Lattices in E^3 play an important role in crystallography since the defining feature of a crystal structure is the periodic repetition of the configuration of atoms in all three dimensions. More explicitly, let Γ be the symmetry group of the crystal structure and let $\mathcal{L}$ be the group of all vectors a such that the parallel translation $t_a \in \Gamma$. Then, $\mathcal{L}$ is a discrete subgroup of E^n and thus, is a lattice in E^3. More specifically, we can present

$$\Gamma \equiv \operatorname{Dih} C \times \mathcal{L} \tag{55}$$

where $\operatorname{Dih} C$ is the Dihedral group of the crystal structure that preserves its lattices.

Definition 1.47 ()

An **integral elementary row transformation** of a matrix is a transformation of one of the following three types:

1. adding a row multiplied by an integer to another row
2. interchanging two rows
3. multiplying a row by -1

An **integral elementary column transformation** is defined similarly.

Lemma 1.10 ()

Every integral rectangular matrix $C = (c_{ij})$ can be reduced by integral elementary row transformations to the diagonal matrix $\text{diag}(u_1, ..., u_p)$, where $u_1, u_2, ..., u_p \geq 0$ and $u_i | u_{i+1}$ for $i = 1, 2, ..., p-1$.

Example 1.30 ()

The following matrix can be reduced (with a few steps now shown) to the stated form.

$$\begin{pmatrix} 2 & 6 & 2 \\ 2 & 3 & 4 \\ 4 & 2 & 4 \end{pmatrix} \rightarrow \begin{pmatrix} 2 & 3 & 4 \\ 0 & -3 & 2 \\ 4 & 2 & 4 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 14 \\ 0 & 8 & 12 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 20 \end{pmatrix} \tag{56}$$

where $1|2$ and $2|20$.

Note that for $n \times 1$ or $1 \times n$ matrices, this procedure is precisely the Euclidean algorithm that produces the GCD of n integers.

Lemma 1.11 ()

Given square integral matrix C with reduced form $\text{diag}(u_1, ..., u_p)$,

$$u_i = \frac{d_i}{d_{i-1}} \tag{57}$$

where d_i is the GCD of the minors of order i of the original matrix C. Recall that a minor of a matrix is the determinant of the matrix with one of its rows and columns removed. d_0 is assumed to equal 1. This implies that the numbers $u_1, u_2, ..., u_p$, along with the reduced form, are uniquely determined by C.

Theorem 1.19 ()

For any subgroup N of a free abelian group L of rank n, there exists a basis $\{e_1, ..., e_n\}$ of L and natural numbers $u_1, ..., u_m$, $(m \leq n)$, such that $\{u_1 e_1, ..., u_m e_m\}$ is a basis fo the group N and $u_i | u_{i+1}$ for $i = 1, 2, ..., m-1$.

2 Rings

Definition 2.1 (Ring)

A **ring** is a set $(R, +, \times)$ equipped with two operations, called addition and multiplication. It has properties:

1. R is an abelian group with respect to $+$, where we denote the additive identity as 0 and the additive inverse of x as $-x$.
2. R is a monoid with respect to $\times$, where we denote the multiplicative identity as 1, also known as the **unity**.
3. $\times$ is both left and right distributive with respect to addition $+$

$$a \times (b + c) = a \times b + a \times c \tag{58}$$
$$(a + b) \times c = a \times c + b \times c \tag{59}$$

for all $a, b, c \in \mathbb{R}$.

If $\times$ is associative, R is called an **associative ring**, and if $\times$ is commutative, R is called a **commutative ring**.

In fact, in some cases the existence of the multiplicative identity is not even assumed, though we will do it here.[3]

Lemma 2.1 ()

Additive inverses are unique and $-1 \times a$ is the additive inverse of a.

Proof.

We can see that

$$\begin{aligned} -1 + 1 = 0 &\implies (-1 + 1) \times a = 0 \times a && (60) \\ &\implies -1 \times a + 1 \times a = 0 && (61) \\ &\implies -1 \times a + a = 0 && (62) \end{aligned}$$

and therefore by definition $-1 \times a$ must be the additive inverse.

Note that we do not assume that there exists multiplicative inverses in a ring. However, there may be some elements for which multiplicative inverses do exist, i.e. $a, b \in R$ where $ab = 1$.

Definition 2.2 (Unit)

A **unit** of a ring R is an element $u \in R$ that has a multiplicative inverse in R. That is, there exists a $v \in R$ s.t. $uv = vu = 1$.

The next property that we would like to talk about is a zero divisor, which is the property that nonzero $a, b \in R$ satisfy $ab = 0$.

Definition 2.3 (Left, Right Zero Divisor)

An element a of a ring R is called a **left zero divisor** if there exists a nonzero x such that $ax = 0$ and a **right zero divisor** if there exists a nonzero x such that $xa = 0$.

Another property that we would desire is some sort of decomposition of ring elements as other ring elements.

[3] If a multiplicative identity is not assumed, then this is called an *rng*, or a *rung*.

Definition 2.4 (Left, Right Divisor)

Let $a, b \in R$ a ring.

1. If there exists an element $x \in R$ with $ax = b$, we say a is a **left divisor** of b.
2. If there exists an element $y \in R$ with $ya = b$, we say a is a **right divisor** of b.
3. We say a is a **two-sided divisor** if it is both a left divisor and a right divisor of b. Note that the x and y are not required to be equal.

It turns out that the existence of units and zero divisors classify rings into subcategories, which we will elaborate on. That is, we will start with the most general theory on rings, and then shrink down into subcategories of rings.

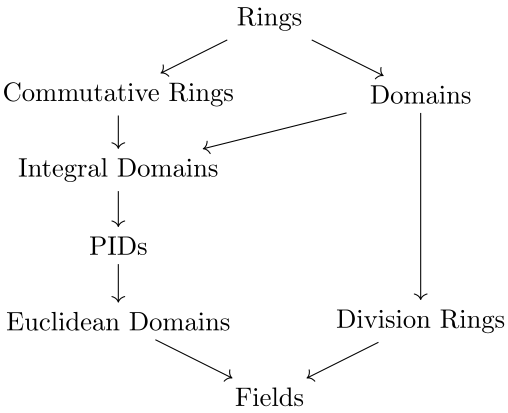


Figure 7: Basic hierarchy of rings.

Example 2.1 (Integers, Rationals, Reals, Complexes)

The fields $\mathbb{Z}, \mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are rings with:

1. Sets:
   - $\mathbb{Q}$: rational numbers $\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$
   - $\mathbb{R}$: real numbers
   - $\mathbb{C}$: complex numbers $\{a + bi : a, b \in \mathbb{R}\}$
2. Standard addition and multiplication
3. Additive identity 0
4. Multiplicative identity 1

These form commutative rings with unity where every non-zero element has a multiplicative inverse.

Example 2.2 (Continuous Functions)

The set of all continuous functions $f : \mathbb{R} \to \mathbb{R}$ is a ring under point-wise addition and multiplication.

Example 2.3 (Matrices)

The ring $M_n(R)$ of $n \times n$ matrices over a ring R consists of:

1. $n \times n$ arrays of elements from R
2. Matrix addition (entry-wise):

$$(A + B)_{ij} = A_{ij} + B_{ij} \tag{63}$$

3. Matrix multiplication:

$$(AB)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj} \tag{64}$$

4. Zero matrix as additive identity
5. Identity matrix I_n as multiplicative identity

This forms a non-commutative ring for $n > 1$, even when R is commutative.

Example 2.4 (Power Set)

Given a set X, let 2^X be its power set, that is the set of all subsets of X. Then, 2^X is a commutative associative ring with respect to the operations of symmetric difference (i.e. the set of elements which is in exactly one of the sets)

$$M \triangle N \equiv (M \setminus N) \cup (N \setminus M) \tag{65}$$

and intersection $\cap$, taken for addition an multiplication, respectively. We will not prove all of the axioms of the ring, but we can state some important facts about this structure. The additive identity is $\emptyset$ and the multiplicative identity is X. Finally, it is clear that

$$\begin{aligned}
&M \triangle N \equiv (M \setminus N) \cup (N \setminus M) \equiv N \triangle M \\
&M \cap N = N \cap M \\
&M \cap N \cap P = (M \cap N) \cap P = M \cap (N \cap P)
\end{aligned}$$

Definition 2.5 (Characteristic Number)

The **characteristic** of ring R, denoted $\text{char}(R)$, is the smallest number of times one must successively add the multiplicative identity 1 to get the additive identity 0.

$$1 + 1 + ... + 1 = 0 \tag{66}$$

If no such number n exists, then $\text{char}(R) = 0$.

Theorem 2.1 (Freshman's Dream)

Given a field F with $\text{char}(F) = p$,

$$(a+b)^p = a^p + b^p \tag{67}$$

Proof.

We have

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k \tag{68}$$

It is clear that

$$\binom{p}{k} = \frac{p(p-1)...(p-k+1)}{k!} \tag{69}$$

is divisible by p for all $k \neq 0, p$, so all the middle terms must cancel out to 0.

2.1 Commutative Rings

Note that for commutative rings, distinguishing left and right divisors are meaningless, and so we can talk about just *divisors*.

Lemma 2.2 (Left=Right Divisors)

In a commutative ring R, a is a left divisor of b iff a is a right divisor of b. In this case, we just say that a is a **divisor** of b, written $a|b$.

Proof.

a is a right divisor of $b \iff \exists x(xa = b) \iff \exists x(ax = b) \iff a$ is a left divisor.

Definition 2.6 (Prime and Compositive Elements)

In a commutative ring R, an element $p \in R$ is said to be **prime** if it is not 0, not a unit, and has only divisors 1 and p.

Lemma 2.3 (Euclid)

If p is prime, then $p|ab \implies p|a$ or $p|b$.

Lemma 2.4 ()

Let R be a commutative ring and $a, b, d \in R$. If $d|a$ and $d|b$, then $d|(ma + nb)$ for any $m, n \in R$.

Definition 2.7 (Greatest Common Divisor)

The **greatest common divisor** of elements a and b, denoted $\gcd(a, b)$ of an commutative ring R is a common divisor of a and b divisible by all their common divisors. That is, it is the element $d \in R$ satisfying

1. $d \mid a$ and $d \mid b$
2. if $k \mid a$ and $k \mid b$, then $k \mid d$.

If $\gcd(a, b) = 1$, then a and b are said to be **relatively prime**.

Note that in an arbitrary commutative ring, the gcd of two elements always exists since we can at least identify 1, but there may not be a *unique* gcd.

2.2 Domains

We can see that domains behave similarly to the integers, but with the missing property that $\times$ is commutative. This motivates the following definition of an integral domain, which can be seen as a generalization of the integers.

Definition 2.8 (Domain)

A ring R with no zero divisors for every element is called a **domain**. An **integral domain** is a commutative domain R.[a]

[a] Almost always, we work with integral domains so we will default to this.

Example 2.5 (Domains vs Integral Domains)

We show some examples of integral domains.

1. The ring $\mathbb{Z}$ of integers.
2. The field $\mathbb{R}$.

3. The ring $\mathbb{Z}[x]$ of polynomials of one variable with integer coefficients.

We show examples of domains that are not integral domains.

1. Quaternions $\mathbb{H}$ are not commutative but are a domain.

Theorem 2.2 (Fields are Integral Domains)

Every field is an integral domain.

Proof.

Theorem 2.3 (Polynomial Integral Domains)

Rings of polynomials are an integral domain if the coefficients come from an integral domain.

Proof.

Factorization of polynomials over $\mathbb{C}$ into linear factors and polynomials over $\mathbb{R}$ into linear and quadratic factors is similar to the factoring of the integers to prime numbers. In fact, such a factorization exists for polynomials over any field F, but their factors can be of any degree. Moreover, there exists no general solution for the factoring of polynomials over any field.

Example 2.6 ()

$\mathbb{Z}$ and $F[x]$ over field F are integral domains. Any field F is also an integral domain.

Example 2.7 ()

The quotient ring $\mathbb{Z}_n$ is not an integral domain when n is composite.

Example 2.8 ()

A product of two nonzero commutative rings with unity $R \times S$ is not an integral domain since $(1,0) \cdot (0,1) = (0,0) \in R \times S$.

Example 2.9 ()

The ring of $n \times n$ matrices over any nonzero ring when $n \geq 2$ is not an integral domain. Given matrices A, B, if the image of B is in the kernel of A, then $AB = 0$.

Example 2.10 ()

The ring of continuous functions on the interval is not an integral domain. To see why, notice that given the piecewise functions

$$f(x) = \begin{cases} 1 - 2x & x \in [0, \frac{1}{2}] \\ 0 & x \in [\frac{1}{2}, 1] \end{cases}, \quad g(x) = \begin{cases} 0 & x \in [0, \frac{1}{2}] \\ 2x - 1 & x \in [\frac{1}{2}, 1] \end{cases} \tag{70}$$

$f, g \neq 0$, but $fg = gf = 0$.

Theorem 2.4 ()

An integral domain is a ring that is isomorphic to a subring of a field.

Theorem 2.5 ()

The characteristic of an integral domain is either 0 or a prime number.

Definition 2.9 (Regular Elements)

An element r of a ring R is **regular** if the mapping

$$\rho : R \longrightarrow R, \qquad x \mapsto xr \tag{71}$$

is injective for all $x \in R$.

Theorem 2.6 ()

An integral domain is a commutative associative ring where every element is regular.

While we have shown that gcd's exist in commutative rings, we can say a bit more when working in Euclidean domains.

Definition 2.10 (Associate Elements)

Elements a and b are **associated**, denoted $a \sim b$ if either of the following equivalent conditions holds

1. $a|b$ and $b|a$
2. $a = cb,$ where c is invertible

The two conditions are equivalent because c and c^{-1} are both in A.

Theorem 2.7 (GCD's in a Euclidean Domain)

Any two distinct gcd's of a, b in a Euclidean domain must be associate elements.

2.3 Ideals and Quotient Rings

Now assuming that R and S are commutative rings, let's consider a special sort of subset of a commutative ring. Consider the kernel of the ring homomorphism. We can see that if $a, b \in \ker(f)$, then $f(a+b) = f(a) + f(b) = 0 + 0 = 0$, and so $\ker(f)$ is closed under addition. Furthermore, $a \in \ker(f)$ and *any* $b \in R$ gives $f(ab) = f(a)f(b) = 0f(b) = 0$, and so multiplying any element in the kernel by an arbitrary element in the rings keeps it in the kernel. We would like to generalize these properties into an *ideal*.

2.3.1 Ideals

Definition 2.11 (Ideals)

For a commutative ring $(R, +, \times)$, a **two-sided ideal**—or **ideal**—is a subset $I \subset R$ satisfying

1. $a, b \in I \implies a + b \in I.$
2. $a \in I, r \in R \implies ra = ar \in I.$

If R is not necessarily commutative, then we $ra \neq ar$ in general, so we may distinguish between left and right ideals.

Let's try to elaborate more on this interpretation by introducing immediate consequences.

Lemma 2.5 (Ideals are Groups Under $+$)

Given a commutative ring R and ideal $I \subset R$, $(I, +)$ is an abelian group.

Therefore, we can see that it is an abelian group under $+$ and closed under $\times$. However, it is not guaranteed to have a multiplicative identity, which is why we can interpret I as a ring without a multiplicative identity, also known as a *rung*.

Example 2.11 (Multiples of Elements Are an Ideal)

We give 2 ideals:

1. The set of even integers $2\mathbb{Z}$ is an ideal in the ring $\mathbb{Z}$, since the sum of any even integers is even and the product of any even integer with an integer is an even integer. However, the odd integers do not form an ideal.
2. The set of all polynomials with real coefficients which are divisible by the polynomial $x^2 + 1$ is an ideal in the ring of all polynomials.

Given these two examples, we can think of an ideal consisting of all multiples of a specific element a that *generates* the ideal.

Definition 2.12 (Generators of Ideals)

Given a commutative ring R, the **ideal generated by** $a \in R$ is denoted

$$\langle a \rangle \coloneqq \{ra \mid r \in R\} \tag{72}$$

and more generally, we may have multiple generating elements.

$$\langle a_1, \ldots, a_n \rangle \coloneqq \{r_1 a_1 + \ldots r_n a_n \mid r_1, \ldots, r_n \in R\} \tag{73}$$

Therefore, the ideals considered above can be written $\langle 2 \rangle \subset \mathbb{Z}$ and $\langle x - 2 \rangle \subset \mathbb{Q}[x]$. However, it may be the case that two elements generate the same ideal in a non-Euclidean domain, but constructing such an example is a bit challenging.

Example 2.12 (Matrix with Last Row of Zeros)

The set of all $n \times n$ matrices whose last row is zero forms a right ideal in the ring of all $n \times n$ matrices. However, it is not a left ideal.
The set of all $n \times n$ matrices whose last column is zero is a left ideal, but not a right ideal.

Theorem 2.8 (Ideals of Fields)

The only ideals that exist in a field $\mathbb{F}$ is $\{0\}$ and $\mathbb{F}$ itself.

Proof.

Given a nonzero element $x \in \mathbb{F}$, every element of $\mathbb{F}$ can be expressed in the form of ax or xa for some $a \in \mathbb{F}$.

2.3.2 Quotient Rings

What is nice about ideals is that they induce an equivalence relation defined on a ring, which reminds you of working in modulos on the integers.

Theorem 2.9 (Equivalence Relation Induced by an Ideal)

Given a commutative ring R and an ideal $I \subset R$, we say that two elements $a, b \in R$ are equivalent (mod I), written $a \equiv b \pmod{I}$ iff $a - b \in I$. We claim two things:

1. $\equiv$ is indeed an equivalence relation.
2. Given that $a \equiv a' \pmod{I}$ and $b = b' \pmod{I}$,

$$a + b \equiv a' + b' \pmod{I}, \qquad ab \equiv a'b' \pmod{I} \tag{74}$$

Proof.

We first prove that $\equiv$ is indeed an equivalence relation.

1. *Reflexive.* $a \equiv a \pmod{I}$ is trivial since $a - a = 0 \in I$.
2. *Transitive.* If $a \equiv b$.

This quotient space maintains a lot of nice properties of the algebraic operations, and so we can form a new ring structure with this quotient space.

Definition 2.13 (Quotient Rings, Rings of Residue Class)

The quotient space R/I induced by the mapping $a \mapsto [a]$ is indeed a commutative ring, called the **quotient ring**, with addition and multiplication defined

$$[a] + [b] \coloneqq [a + b], \qquad [ab] \coloneqq [a]\,[b] \tag{75}$$

Proof.

Note that the properties of the operation in $\frac{M}{R}$ inherits all the properties of the addition operation on M that are expressed in the form of identities and inverses, along with the existence of the zero identity.

$$\begin{aligned} 0 \in M &\implies [0] \text{ is the additive identity in } \frac{M}{R} \\ a + (-a) = 0 &\implies [a] + [-a] = [0] \\ 1 \in M &\implies [1] \text{ is the multiplicative identity in } \frac{M}{R} \end{aligned}$$

Example 2.13 (Quotient Rings of Integers)

The quotient set $\mathbb{Z}/\langle n \rangle$ by the relation of congruence modulo n is denoted $\mathbb{Z}_n$.

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\} \tag{76}$$

We list some quotient rings of the integers.

1. In $\mathbb{Z}_5 = \mathbb{Z}/\langle 5 \rangle$, the elements $[2]$ and $[3]$ are multiplicative inverses of each other since $[2][3] = [6] = [1]$, and $[4]$ is its own inverse since $[4][4] = [16] = [1]$. The addition and multiplication tables for $\mathbb{Z}_5$ is shown below.
2. Consider the ideal $I = \langle 2 \rangle \subset \mathbb{Z}_6$. We have $0 \equiv 2 \equiv 4 \pmod{I}$ and $1 \equiv 3 \equiv 5 \pmod{I}$, and so the quotient ring $\mathbb{Z}_6/I$ consists of the two equivalence classes $[0]$ and $[1]$.

Example 2.14 (Quotient Rings of Polynomials)

We list some quotient rings of the integers.

1. Consider $\mathbb{Q}[x]/\langle x^2 - 2\rangle$. We can see that any polynomial $f \in \mathbb{Q}[x]$ is equivalent $\pmod{I}$ to a linear polynomial, since $x^2 \equiv 2$. Alternatively we can apply the division algorithm to replace $f(x)$ by its remainder upon division by $x^2 - 2$, and thus in the quotient ring, $[x]$ plays the role of $\sqrt{2}$, which may indicate that $\mathbb{Q}[x]/\langle x^2 - 2\rangle = \mathbb{Q}[\sqrt{2}]$.
2. Consider $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$. As in the previous example, any polynomial in $\mathbb{Z}_2[x]$ is equivalent to a linear polynomial since $x^2 \equiv x + 1 \pmod{I}$. Therefore the elements of the quotient ring are $[0], [1], [x], [x+1]$ with the addition and multiplication tables.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

(a)

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

(b)

Note that just like how quotient topologies do not preserve topological properties, as shown here and here, quotient rings inherit some—but not all—algebraic properties.

Theorem 2.10 (Quotient Inherits Commutativity)

Let R be a commutative ring and $I \subsetneq R$ be an ideal. Then R/I is a commutative ring.

Example 2.15 (Quotient Does Not Inherit Integral Domain Property)

$\mathbb{Z}$ is an integral domain, but $\mathbb{Z}/\langle 6\rangle$ is not since $[2] \times [3] = [0]$.

The ring $\mathbb{Z}_n$ has all the properties of a field except the property of having inverses for all of its nonzero elements. This leads to the following theorem.

Theorem 2.11 (Integer Quotient Rings as Finite Fields)

The ring $\mathbb{Z}_n$ is a field if and only if n is a prime number.

Proof.

$(\rightarrow)$ Assume that n is composite $\implies n = kl$ for $k, n \in \mathbb{N} \implies k, n \neq 0$, but

$$[k]_n [l]_n = [kl]_n = [n]_n = 0 \tag{77}$$

meaning that $\mathbb{Z}_n$ contains 0 divisors and is not a field. The contrapositive of this states $(\rightarrow)$.
$(\leftarrow)$ Given that n is prime, let $[a]_n \neq 0$, i.e. $[a]_n \neq [0]_n, [1]_n$. The set of n elements

$$[0]_n, [a]_n, [2a]_n, ..., [(n-1)a]_n \tag{78}$$

are all distinct. Indeed, if $[ka]_n = [la]_n$, then $[(k-l)a]_n = 0 \implies n = (k-l)a \iff n$ is not prime. Since the elements are distinct, exactly one of them must be $[1]_n$, say $[pa]_n \implies$ the inverse $[p]_n$ exists.

Corollary 2.1 (Invertibility in $\mathbb{Z}_n$)

For any n, $[k]_n$ is invertible in the ring $\mathbb{Z}_n$ if and only if n and k are relatively prime.

Theorem 2.12 (Wilson's Theorem)

Let n be a prime number. Then

$$(n-1)! \equiv -1 \pmod{n} \tag{79}$$

2.4 Principal Ideal Domains

A good intuition to have about ideals is that they are the set of multiples of a certain element. However, this may not be true for ideals in general, but if this intuition is true, then we call this a *principal ideal*.

Definition 2.14 (Principal Ideals)

Given commutative ring R and $I \subset R$, if $I = \langle a \rangle$ for some $a \in R$—i.e. it is generated by a single element—I is called a **principal ideal**.

Definition 2.15 (Principal Ideal Domain)

A **principal ideal domain**, also called a **PID**, is an integral domain in which every ideal is principal.

More generally, a **principal ideal ring** is a nonzero commutative ring in which every ideal is principal (i.e. can be generated by a single element). The distinction is that a principal ideal ring may have zero divisors whereas a principal ideal domain cannot. Principal ideal domains are thus mathematical objects that behave somewhat like the integers. That is,

1. Any element of a PID has a unique decomposition into prime elements.
2. Any two elements of a PID have a greatest common divisor.
3. If x and y are elements of a PID without common divisors, then every element of the PID can be written in the form
$$ax + by \tag{80}$$

We now introduce some examples of PIDs, which are not as trivial and should be introduced as theorems.

Theorem 2.13 (Integers and Polynomials over Fields are PIDs)

The following are all examples of principal ideal domains.
1. Any field $\mathbb{F}$.
2. The ring of integers $\mathbb{Z}$.
3. $\mathbb{F}[x]$, rings of polynomials in one variable with coefficients in a field $\mathbb{F}$.

Proof.

Listed.
1. It is quite easy to see that a field $\mathbb{F}$ is a PID since the only two possible ideals are $\{0\}$ and $\mathbb{F}$, both of which are principal.
2. If $I \subset \mathbb{Z}$ is an ideal, then if $I = \langle 0 \rangle$, then we're done. Otherwise, let $a \in I$ be the smallest positive integer in I. It is clear that $\langle a \rangle \subset I$. Now given an element $b \in I$, by the Euclidean algorithm we have $b = aq + r$ with $r < a$. Since $a, b \in I$, it follows that $r \in I$. But since $0 \leq r < a$ and a is the smallest positive integer, $r = 0$, and so $b = aq \implies b \in \langle a \rangle$.

3. The ring of polynomials $\mathbb{F}[x]$ is a PID since we can imagine a minimal polynomial p in each ideal I. Every element in I must be divisible by p, which means that the entire ideal I can be generated by the minimal polynomial p, making I principal.

Corollary 2.2 (Ideals Generated by Primes)

If $I \subsetneq \mathbb{Z}$ and a prime number $p \in I$, then $I = \langle p \rangle$. If $I \subset F[x]$ is an ideal and irreducible $f(x) \in I$, then $I = \langle f(x) \rangle$.

Proof.

Listed.

1. Since $\mathbb{Z}$ is a PID, $I = \langle a \rangle$ for some nonzero $a \in \mathbb{Z}$. We can assume a is positive, and if $a = 1$, then $I = \mathbb{Z}$, which contradicts the I is a proper subset. So $a \geq 2$. Now because $p \in I$, $p = ra$ for some $r \in \mathbb{Z}$, but since p is prime, $r = 1, a = p$.
2. Since $F[x]$ is a PID and $I = \langle g(x) \rangle$ for some $g(x) \in F[x]$, let us take $f(x) \in I$. Then it must be true that $f(x) = g(x)h(x)$ for some $h(x) \in R$. However, This means that $\deg(g)$ or $\deg(h)$ must be 0 since f is irreducible. But if $g(x)$ was a constant, then $I = R$, so $g(x) = f(x)$.

Corollary 2.3 (Kernel of Evaluation Homomorphism is Generated by Irreducible Factor)

Suppose $f(x) \in F[x]$ is irreducible in $F[x]$, and $K \supset F$ is a field containing a root α of $f(x)$. Then the ideal of all polynomials in $F[x]$ vanishing at α is generated by $f(x)$. That is, given the evaluation homomorphism

$$\text{ev}_\alpha : F[x] \to K \tag{81}$$

we claim $\ker(\text{ev}_\alpha) = \langle f(x) \rangle$.

Proof.

This is an immediate consequence of the previous corollary.

The great thing about PIDs is that they unlock a lot of the familiar properties that we see in the integers. In fact, pretty much everything holds except for the existence of Euclidean algorithm for factorization.

Theorem 2.14 (Greatest Common Divisor)

Given $a, b \in R$ a PID, $\gcd(a, b)$ is unique.

Theorem 2.15 (Unique Factorization Theorem)

Every element $x \in R$ of a PID can be uniquely factored (up to permutations and units) into irreducible elements in R.

Bezout's does not hold in integral domains in general.

Theorem 2.16 (Bezout's Theorem)

Given that one divides (with remainder) polynomial f by $g = x - c$, let the remainder be $r \in F$. That is,

$$f(x) = (x - c)q(x) + r, \; r \in F \tag{82}$$

This implies that the remainder equals the value of f at point c. That is,

$$f(c) = r \tag{83}$$

Note that a corollary of this is the single factorization theorem, but the single factorization holds for commutative rings in general.

2.5 Euclidean Domains

Definition 2.16 (Euclidean Domain)

Let R be an integral domain which is not a field. R is **Euclidean domain** if

1. there exists a *norm* $|\cdot| : R \setminus \mathbb{R}_0^+$, and
2. there exists a well-defined function, called **Euclidean division** $\mathcal{D} : R \times R \rightarrow R \times R$ that is defined
$$\mathcal{D}(a, b) = (q, r) \text{ where } a = bq + r \text{ and } 0 \leq r < |b| \tag{84}$$

The two prime examples are the integers and polynomials.

Example 2.16 (Integers)

$\mathbb{Z}$ is a Euclidean domain with Euclidean division, also called long division, defined

$$\begin{array}{r} 40 \\ 13\,\overline{)\,521} \\ \underline{52} \\ 01 \end{array}$$

Theorem 2.17 (Polynomials are Euclidean Domains)

Let $f(x), g(x) \in F[x]$ and $g(x) \neq 0$. Then, there exists polynomials $q(x), r(x)$ such that

$$f(x) = q(x)g(x) + r(x), \qquad 0 \leq \deg(r) < \deg(g) \tag{85}$$

where deg is the norm.

Example 2.17 (Gaussian Integers)

The subring of $\mathbb{C}$, defined

$$\mathbb{Z}[i] \equiv \{a + bi \mid a, b \in \mathbb{Z}\} \tag{86}$$

is a Euclidean integral domain with respect to the norm

$$N(c) \equiv a^2 + b^2 \tag{87}$$

since $N(cd) = N(c)N(d)$ and the invertible elements of $\mathbb{Z}[i]$ are $\pm 1, \pm i$.

Example 2.18 (Dyadic Rationals)

The ring of rational numbers of the form $2^{-n}m$, $n \in \mathbb{Z}_+, m \in \mathbb{Z}$, is a Euclidean domain. To define the norm, we can first assume that m can be prime factorized into the form

$$m = \pm \prod_i p_i^{k_i}, \; p \text{ prime} \tag{88}$$

and the norm is defined

$$N(\frac{m}{2^n}) \equiv 1 + \sum_i k_i \tag{89}$$

We must further show that division with remainder is possible, but we will not show it here.

Theorem 2.18 (Chinese Remainder Theorem)

2.6 Product Rings

Definition 2.17 (Direct Product of Rings)

2.7 Ring Homomorphisms

So far, we have talked about many properties of rings but have not thoroughly gone over their classification. This is what we will do in this section, just like how we have classified groups. It turns out that classifying rings is significantly harder to do so, so we will talk about some low-order finite rings and provide some examples of isomorphisms between more complex rings. Recall that in point set topology, given a topological space $(X, \mathscr{T})$ and its quotient space, if we can construct a map from X to a cleverly chosen space Z that agrees with the quotient, then this induces a homeomorphism $X \cong Z$.

Definition 2.18 (Ring Homomorphism, Isomorphism)

A **ring homomorphism** $f : R \to S$ is a function that satisfies for all $a, b \in R$

1. $f(a + b) = f(a) + f(b)$
2. $f(ab) = f(a)f(b)$
3. $f(1_R) = 1_S$

for all $a, b \in R$.[a] If f is a bijective ring homomorphism, it is called a **ring isomorphism**.

[a] Note that the first is equivalent to it being a group homomorphism between $(R, +)$ and $(S, +)$. The second property may look like it is a group homomorphism between $(R, \times)$ and $(S, \times)$, but remember that neither are groups and it just states that closure distributes. Combined with the fact that the multiplicative identity matches, f is really a homomorphism of *monoids*.

Definition 2.19 (Kernel)

The **kernel** of a ring homomorphism $f : R \to S$ is the preimage of $0 \in S$.[a]

[a] Note that this is the additive identity, not the multiplicative identity. We must specify which identity, unlike a group which has just one identity.

Lemma 2.6 (Properties of Ring Homomorphisms)

It immediately follows that if $f : R \to S$ is a ring homomorphism, then

1. $f(0) = 0$
2. $\Im(f)$ is a subring of S.

3. A ring homomorphism is injective if and only if $\ker f = \langle 0 \rangle$.

Furthermore, if f is a ring isomorphism, then

1. f^{-1} is a ring isomorphism.

Theorem 2.19 (Compositions of Ring Homomorphisms)

Compositions of ring homomorphisms are ring homomorphisms.

Obviously, we can prove that things like the identity map are homomorphisms. However, the following will be used quite often.

Example 2.19 (Evaluation Homomorphism of Polynomials)

Given fields $F \subset K$, the **evaluation function**

$$\text{ev}_\alpha : F[x] \rightarrow K \tag{90}$$

mapping $f(x) \mapsto f(\alpha)$ is a homomorphism.

Theorem 2.20 (Fundamental Ring Homomorphism Theorem)

Let R and S be commutative rings, and suppose $f : R \rightarrow S$ be a surjective ring homomorphism. Then this induces a ring isomorphism

$$R / \ker f \simeq S \tag{91}$$

satisfying $\phi = \bar{\phi} \circ \pi$.

$$\begin{tikzcd}
R \arrow[r, "\phi"] \arrow[d, "\pi"] & S \\
R/\ker(\phi) \arrow[ur, "\bar{\phi}"] &
\end{tikzcd}$$

Figure 9: The theorem states that the following diagram commutes.

Proof.

Overall, we must use this theorem cleverly in order to prove that two rings are isomorphic to each other.

Example 2.20 ()

The evaluation map

$$\phi : \frac{\mathbb{R}[x]}{\langle x^2+1 \rangle} \rightarrow \mathbb{C}, \qquad \phi\big(f(x) \pmod{\langle x^2+1\rangle}\big) = f(i) \tag{92}$$

is an isomorphism.[a] This is because we can think of the evaluation homomorphism $\text{ev}_i : f(x) \in \mathbb{R}[x] \mapsto f(i) \in \mathbb{R}[i]$. We know that $\mathbb{R}$ a field implies $\mathbb{R}[x]$ is a PID. Now take $\ker(\text{ev}_i)$. We can see that it contains the polynomial x^2+1, and since it is irreducible in $\mathbb{R}[x]$, it must be the case that $\ker(\text{ev}_i) = \langle x^2+1 \rangle$. Now it follows by the fundamental ring homomorphism theorem that

$$\frac{\mathbb{R}[x]}{\ker(\text{ev}_i)} = \frac{\mathbb{R}[x]}{\langle x^2+1\rangle} \simeq \mathbb{R}[i] = \mathbb{C} \tag{93}$$

[a] Intuitively, we can see that the quotient ring can only consist up to linear polynomials since $x^2 \equiv -1$. This is a real vector space of dimension 2, and so is $\mathbb{C}$, so it makes sense that they may be isomorphic.

Example 2.21 ()

The evaluation map

$$\text{ev}_{\sqrt{2}} : \mathbb{Q}[x] \mapsto \mathbb{Q}[\sqrt{2}], \qquad \text{ev}_{\sqrt{2}}(f) = f(\sqrt{2}) \tag{94}$$

is a homomorphism. Furthermore, it has a kernel $\langle x^2 - 2 \rangle$ since $(x^2 - 2)$ is an irreducible polynomial in $\mathbb{Q}[x]$ containing the root $\sqrt{2}$. Therefore by the fundamental ring homomorphism theorem we have

$$\frac{\mathbb{Q}[x]}{\langle x^2 - 2 \rangle} \simeq \mathbb{Q}[\sqrt{2}] \tag{95}$$

Theorem 2.21 (Quotient Polynomial Ring Can be Splitting Field)

Let F be a field with $f(x) \in F[x]$.

1. Then $K = F[x]/\langle f(x) \rangle$ is a field iff $f(x)$ is irreducible in $F[x]$.
2. If $f(x)$ is irreducible, then K contains a root α of $f(x)$, and $K \simeq F[\alpha]$.

Corollary 2.4 ()

Any polynomial $f(x) \in F[x]$ has a splitting field.

Corollary 2.5 ()

Let $c \in \mathbb{C}$. Then $\mathbb{Q}[c] \subset \mathbb{C}$ is a field if and only if c is an algebraic number.

2.8 Division Rings

Definition 2.20 (Division Ring)

A **division ring**, also called a **skew field**, is an associative ring where every nonzero element is invertible with respect to ×.[a]

[a] Division rings differ from fields in that multiplication is not required to be commutative.

Let's establish the hierarchy.

Lemma 2.7 (Division Rings are Domains)

Every division ring R is automatically a domain.

Proof.

Every nonzero element is invertible.

Example 2.22 (Invertible Matrices are a Division Ring)

At first, a division ring may not seem different from a field. However, a classic example is the ring of invertible matrices, which is not necessarily commutative, but is a ring in which "division" can be done by right and left multiplication of a matrix inverse.

$$aa^{-1} = a^{-1}a = I \tag{96}$$

This implies that every element in the division ring commutes with the identity, but again commutativity does not necessarily hold for arbitrary elements a, b.

2.9 Exercises

Exercise 2.1 (Shifrin 1.2.1)

For each of the following pairs of numbers a and b, find $d = \gcd(a, b)$ and express d in the form $ma + nb$ for suitable integers m and n.

(a) $14, 35$
(b) $56, 77$
(c) $618, 336$
(d) $2873, 6643$
(e) $512, 360$
(f) $4432, 1080$

Solution 2.1

Listed.

1. $d = 7 = (-2) \cdot 14 + (1) \cdot 35$.
2. $d = 7 = (-4) \cdot 56 + 3 \cdot 77$.
3. $d = 6 = -25 \cdot 618 + 46 \cdot 336$
4. $d = 13 = 37 \cdot 2873 + (-16) \cdot 6643$.
5. $d = 8 = 19 \cdot 512 + (-27) \cdot 360$.
6. $d = 8 = 29 \cdot 4432 + (-119) \cdot 1080$.

Exercise 2.2 (Shifrin 1.2.2)

You have at your disposal arbitrarily many 4-cent stamps and 7-cent stamps. What are the postages you can pay? Show in particular that you can pay all postages greater than 17 cents.

Exercise 2.3 (Shifrin 1.2.3)

Prove that whenever $m \neq 0$, $\gcd(0, m) = |m|$.

Exercise 2.4 (Shifrin 1.2.4)

(a) Prove that if $a|x$ and $b|y$, then $ab|xy$.
(b) Prove that if $d = \gcd(a, b)$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Exercise 2.5 (Shifrin 1.2.5)

Prove or give a counterexample: the integers q and r guaranteed by the division algorithm, Theorem 2.2, are unique.

Exercise 2.6 (Shifrin 1.2.6)

Prove or give a counterexample. Let $a, b \in \mathbb{Z}$. If there are integers m and n so that $d = am + bn$, then $d = \gcd(a, b)$.

Exercise 2.7 (Shifrin 1.2.7)

Generalize Proposition 2.5: if $\gcd(m, c) = 1$ and $m|cz$, then prove $m|z$.

Solution 2.2

Let $\gcd(m, c) = 1$ and $m|cz$. Then there exists $a, b \in \mathbb{Z}$ such that $am + bc = 1$. Multiply both sides of the equation by z to get by the distributive property

$$(am + bc)z = amz + bcz = z \tag{97}$$

$m|amz$ and $m|cz \implies m|bcz$. Therefore, the sum of the two, which is equal to z, must be divisible by m. Therefore $m|z$.

Exercise 2.8 (Shifrin 1.2.8)

Suppose $a, b, n \in \mathbb{N}$, $\gcd(a, n) = 1$, and $\gcd(b, n) = 1$. Prove or give a counterexample: $\gcd(ab, n) = 1$.

Exercise 2.9 (Shifrin 1.2.9)

Prove that if p is prime and $p|(a_1 a_2 \ldots a_n)$, then $p|a_j$ for some j, $1 \leq j \leq n$. (Hint: Use Proposition 2.5 and induction.)

Exercise 2.10 (Shifrin 1.2.10)

Given a positive integer n, find n consecutive composite numbers.

Exercise 2.11 (Shifrin 1.2.11)

Prove that there are no integers m, n so that $(\frac{m}{n})^2 = 2$. (Hint: You may start by assuming m and n are relatively prime. Why? Then use Exercise 1.1.3.)

Exercise 2.12 (Shifrin 1.2.12)

Find all rectangles whose sides have integral lengths and whose area and perimeter are equal.

Exercise 2.13 (Shifrin 1.2.13)

Given two nonzero integers a, b, in analogy with the definition of $\gcd(a, b)$, we define the **least common multiple** $\text{lcm}(a, b)$ to be the positive number μ with the properties:

(i) $a|\mu$ and $b|\mu$, and
(ii) if $s \in \mathbb{Z}$, $a|s$ and $b|s \Rightarrow \mu|s$.

Prove that

(a) if $\gcd(a, b) = 1$, then $\mu = ab$. (Hint: If $\gcd(a, b) = 1$, then there are integers m and n so that $1 = ma + nb$; therefore, $s = mas + nbs$.)
(b) more generally, if $\gcd(a, b) = d$, then $\mu = ab/d$.

Solution 2.3

Listed.

1. We can simply verify the two properties. Since $\mu = ab$, $a|\mu$ and $b|\mu$ trivially by the existence of b and a, respectively. As for the second property, let $s \in \mathbb{Z}$ exist such that $a|s$ and $b|s$. Since $a|s$, $s = xa$ for some $x \in \mathbb{Z}$. But since $b|s$, $b|xa$. Since $\gcd(a, b) = 1$ by assumption, the result in [Shifrin 1.2.7] tells us that $b|x$, i.e. there exists some $k \in \mathbb{Z}$ such that $x = kb$. Therefore $s = xa = kba = kab = k\mu$. By existence of k, $\mu|s$, and we are done.
2. Given a, b with $\gcd(a, b) = d$, there exists some $a', b' \in \mathbb{Z}$ s.t. $a = da', b = db'$. We claim that $\mu = ab/d := da'b'$ is the lcm.[a] It is clear that $a|\mu$ and $b|\mu$ by the existence of integers b' and a', respectively. To prove the second property, let $s \in \mathbb{Z}$ with $a|s$ and $b|s$. Since $a|s \iff da'|s$, there must exist some $x \in \mathbb{Z}$ s.t. $s = da'x$. But since $b|s$, this means that $db'|s \iff db'|da'x \iff b'|a'x$. But $\gcd(a', b') = 1$ which follows from the definition of gcd, and so by [Shifrin 1.2.7] it must be the case that $b'|x$, i.e. there exists some $k \in \mathbb{Z}$ s.t. $x = b'k$. Substituting this back we have $s = da'b'k = \mu k$, and by existence of k it follows that $\mu|s$. Since it satisfies these 2 properties μ is the lcm.

[a] Since division isn't generally closed in the integers, I prefer to define ab/d this way.

Exercise 2.14 (Shifrin 1.2.14)

See Exercise 13 for the definition of $\operatorname{lcm}(a, b)$. Given prime factorizations $a = p_1^{\mu_1} \cdots p_m^{\mu_m}$ and $b = p_1^{\nu_1} \cdots p_m^{\nu_m}$, with $\mu_i, \nu_i \geq 0$, express $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ in terms of $p_1, \ldots, p_m$. Prove that your answers are correct.

Exercise 2.15 (Shifrin 1.3.8)

We see that in mod10,

$$3^{400} \equiv 9^{200} \equiv (-1)^{200} \equiv 1^{100} \equiv 1 \tag{98}$$

so the last digit is 1. To get the last 2 digits, we use the binomial expansion and focus on the last 2 terms.

$$3^{400} = 9^{200} = (10-1)^{200} = \ldots + \binom{200}{199} 10^1 (-1)^{199} + \binom{200}{200} (-1)^{200} \tag{99}$$

since every combination of the form $\binom{n}{k}$ is an integer and all the other terms have a factor of 10^2, the expansion mod100 becomes

$$3^{400} \equiv \binom{200}{199} 10^1 (-1)^{199} + \binom{200}{200} (-1)^{200} = 200 \cdot 10 \cdot (-1)^{199} + 1 \equiv 1 \pmod{100} \tag{100}$$

and so the last two digits is 01. To get the last digit of 7^{99}, we see that in mod10,

$$7^{99} \equiv 7^{96} \cdot 7^3 \equiv (7^4)^{24} \cdot 343 \equiv 2401^{24} \cdot 343 \equiv 1^{24} \cdot 3 \equiv 3 \tag{101}$$

Exercise 2.16 (Shifrin 1.3.10)

We must show that

$$n \equiv 0 \pmod{13} \iff n' = \sum_{i=1}^{k} a_i 10^{i-1} + 4a_0 \equiv 0 \pmod{13} \tag{102}$$

We see that $n \equiv n + 39a_0 \equiv 0 \pmod{13}$, and

$$\begin{aligned} n + 39a_0 &= \sum_{i=0}^{k} 10^i a_i + 39a_0 && (103)\\ &= \sum_{i=1}^{k} 10^i a_i + 40a_0 && (104)\\ &= 10\bigg(\sum_{i=1}^{k} 10^{i-1} a_i + 4a_0\bigg) && (105)\\ &= 10n' && (106)\end{aligned}$$

and so we have $n \equiv 10n' \pmod{13}$, and so $n' \equiv 0 \pmod{13} \implies n \equiv 0 \pmod{13}$. Conversely, if $n \equiv 0 \pmod{13}$, then $4n \equiv 0 \pmod{13}$, but $4n \equiv 40n'$ and so $n' \equiv 40n' \equiv 4n \equiv 0 \pmod{13}$. Therefore both implications are proven.

Exercise 2.17 (Shifrin 1.3.12)

Suppose that p is prime. Prove that if $a^2 \equiv b^2 \pmod{p}$, then $a \equiv b \pmod{p}$ or $a \equiv -b \pmod{p}$.

Solution 2.4

We have

$$\begin{aligned} a^2 \equiv b^2 \pmod{p} &\implies a^2 - b^2 \equiv 0 \pmod{p} && (107)\\ &\implies (a+b)(a-b) \equiv 0 \pmod{p} && (108)\end{aligned}$$

We claim that there are no zero divisors in $\mathbb{Z}_p$. If $mn \equiv 0$ (mod p), then by definition this means $p|mn$, which implies that in the integers this must mean that $p|m$ or $p|n$.[a] But since $m, n \not\equiv 0$, $p \not| n$ and $p \not| m$, arriving at a contradiction. Going back to our main argument, it must be the case that $a + b \equiv 0 \implies a \equiv -b$ or $a - b \equiv 0 \implies a \equiv b$.

[a] Proposition 2.5

Exercise 2.18 (Shifrin 1.3.15)

Let us assume that $n = a^2 + b^2 + c^2$ for some $a, b, c \in \mathbb{Z}$. Let us consider for each integer z, all the possible values of $z^2 \pmod 8$.

$$\begin{aligned}
z \equiv 0 &\implies z^2 \equiv 0 \pmod 8 && (109)\\
z \equiv 1 &\implies z^2 \equiv 1 \pmod 8 && (110)\\
z \equiv 2 &\implies z^2 \equiv 4 \pmod 8 && (111)\\
z \equiv 3 &\implies z^2 \equiv 1 \pmod 8 && (112)\\
z \equiv 4 &\implies z^2 \equiv 0 \pmod 8 && (113)\\
z \equiv 5 &\implies z^2 \equiv 1 \pmod 8 && (114)\\
z \equiv 6 &\implies z^2 \equiv 4 \pmod 8 && (115)\\
z \equiv 7 &\implies z^2 \equiv 1 \pmod 8 && (116)
\end{aligned}$$

Therefore, $a^2 + b^2 + c^2 \pmod 8$ can take any values of the form

$$x + y + z \pmod 8 \text{ for } x, y, z \in \{0, 1, 4\} \tag{117}$$

Since addition is commutative, WLOG let $x \leq y \leq z$. We can just brute force search this.

1. If $z = 0$, then $x = y = z = 0$ and $x + y + z = 0 \not\equiv 7$.
2. If $z = 1$, then we see

$$\begin{aligned}
0 + 0 + 1 &\equiv 1 && (118)\\
0 + 1 + 1 &\equiv 2 && (119)\\
1 + 0 + 1 &\equiv 2 && (120)\\
1 + 1 + 1 &\equiv 3 && (121)
\end{aligned}$$

3. If $z = 4$, then we see that

$$\begin{aligned}
0 + 0 + 4 &\equiv 4 && (122)\\
0 + 1 + 4 &\equiv 5 && (123)\\
0 + 4 + 4 &\equiv 0 && (124)\\
1 + 1 + 4 &\equiv 6 && (125)\\
1 + 4 + 4 &\equiv 1 && (126)\\
4 + 4 + 4 &\equiv 4 && (127)
\end{aligned}$$

And so $a^2 + b^2 + c^2 \not\equiv 7 \pmod 8$ for any $a, b, c \in \mathbb{Z}$.

Exercise 2.19 (Shifrin 1.3.20.a/b/g)

For (a),

$$3x \equiv 2 \pmod 5 \implies 6x \equiv 4 \pmod 5 \implies x \equiv 4 \pmod 5 \tag{128}$$

For (b),

$$\begin{aligned}
6x + 3 \equiv 1 \pmod{10} &\implies 6x \equiv -2 \equiv 8 \pmod{10} && (129)\\
&\implies 10 | (6x - 8) && (130)\\
&\implies 5 | (3x - 4) && (131)\\
&\implies 3x \equiv 4 \pmod 5 && (132)\\
&\implies 3x \equiv 9 \pmod 5 && (133)\\
&\implies x \equiv 3 \pmod 5 && (134)
\end{aligned}$$

For (g),

$$\begin{aligned}
15x \equiv 25 \pmod{35} &\implies 35|(15x-25) && (135)\\
&\implies 7|(3x-5) && (136)\\
&\implies 3x \equiv 5 \pmod 7 && (137)\\
&\implies 3x \equiv 12 \pmod 7 && (138)\\
&\implies x \equiv 4 \pmod 7 && (139)
\end{aligned}$$

Exercise 2.20 (Shifrin 1.3.21.b/c)

For (b), we see that 4 and 13 are coprime with $-3 \cdot 4 + 1 \cdot 13 = 1$. Therefore, by the Chinese remainder theorem

$$x \equiv 1 \cdot 1 \cdot 12 + (-3) \cdot 7 \cdot 4 \pmod{52} \implies x \equiv 33 \pmod{52} \qquad (140)$$

For (c), we solve the first two congruences $x \equiv 3 \pmod 4$ and $x \equiv 4 \pmod 5$. 4 and 5 are coprime with $-1 \cdot 4 + 1 \cdot 5 = 1$. Therefore, by CRT

$$x \equiv -1 \cdot 4 \cdot 4 + 1 \cdot 5 \cdot 3 \pmod{20} \implies x \equiv -1 \pmod{20} \qquad (141)$$

Then we solve $x \equiv -1 \pmod{20}$ with the final congruence $x \equiv 3 \pmod 7$. We see that 20 and 7 are coprime with $-1 \cdot 20 + 3 \cdot 7 = 1$. Therefore by CRT

$$x \equiv -1 \cdot 20 \cdot 3 + 3 \cdot 7 \cdot -1 \pmod{140} \implies x \equiv 59 \pmod{140} \qquad (142)$$

Exercise 2.21 (Shifrin 1.3.25)

We prove bidirectionally.

1. Assume a solution exists for $cx \equiv b \pmod m$. Then $m|(cx-b)$, which means that there exists a $y \in \mathbb{Z}$ s.t. $my = cx - b \iff b = cx - my$. Since $d = \gcd(c, m)$, there exists $c', m' \in \mathbb{Z}$ s.t. $c = dc'$ and $m = dm'$. So

$$b = cx - my = d(c'x - m'y) \implies d|b \qquad (143)$$

2. Assume that $d|b$. Then there exists a $b' \in \mathbb{Z}$ s.t. $b = db'$, and we have

$$\begin{aligned}
cx \equiv b \pmod m &\iff m|(cx-b) && (144)\\
&\iff dm'|d(c'x-b') && (145)\\
&\iff m'|(c'x-b') && (146)\\
&\iff c'x \equiv b' \pmod{m'} && (147)
\end{aligned}$$

Since $\gcd(c', m') = 1^a$, by Shifrin Proposition 3.5 the equation $c'x \equiv b' \pmod{m'}$ is guaranteed to have a solution, and working backwards in the iff statements gives us the solution for $cx \equiv b \pmod m$.

We have proved existence of a solution in $\mathrm{mod}(m/d) = m'$. Now we show uniqueness. Assume that there are two solutions $x \equiv \alpha$, $x \equiv \beta \pmod{m'}$ with $\alpha \not\equiv \beta \pmod{m'}$. Then, x can be written as $x = k_\alpha m' + \alpha$ and $x = k_\beta m' + \beta$. But we see that

$$\begin{aligned}
0 = x - x &= (k_\alpha m' + \alpha) - (k_\beta m' + \beta) && (148)\\
&= m'(k_\alpha - k_\beta) + (\alpha - \beta) && (149)\\
&\equiv \alpha - \beta \pmod{m'} && (150)
\end{aligned}$$

which implies that $\alpha \equiv \beta \pmod{m'}$, contradicting our assumption that they are different in modulo. Therefore the solution must be unique.

[a] Since $\gcd(c, m) = d \implies$ that there exists a $y, z \in \mathbb{Z}$ s.t. $cy + mz = d$, and dividing both sides by d guarantees the existence of y, z satisfying $c'y + m'z = 1$, meaning that $\gcd(c', m') = 1$.

Exercise 2.22 (Shifrin 1.4.1)

For $\mathbb{Z}_7$. There are no zero divisors and the units are all elements.

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(151)

For $\mathbb{Z}_8$. The zero divisors are $2, 4, 6$. The units are $1, 3, 5, 7$.

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(152)

For $\mathbb{Z}_{12}$. The zero divisors are $2, 3, 4, 6, 8, 9, 10$. The units are $1, 5, 7, 11$.

$\times$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

(153)

Exercise 2.23 (Shifrin 1.4.5.a/b/c)

1. Prove that $\gcd(a, m) = 1 \iff \bar{a} \in \mathbb{Z}_m$ is a unit.
2. Prove that if $\bar{a} \in \mathbb{Z}_m$ is a zero-divisor, then $\gcd(a, m) > 1$, and conversely, provided $m \nmid a$.
3. Prove that every nonzero element of $\mathbb{Z}_m$ is either a unit or a zero-divisor.
4. Prove that in any commutative ring R, a zero-divisor cannot be a unit, and a unit cannot be a zero-divisor. Do you think c. holds in general?

Solution 2.5

For (a),

1. ($\rightarrow$). If $\gcd(a,m) = 1$, then there exists $x, y \in \mathbb{Z}$ such that $ax + my = 1$. Taking the modulo on both sides gives $ax \equiv 1 \pmod{m}$, and therefore we have established the existence of $x \in \mathbb{Z}$, which implies the existence of $\bar{x} \in \mathbb{Z}_m$.
2. ($\leftarrow$). If we have $a \in \mathbb{Z}$ and $\bar{a}$ is a unit, then there exists a $\bar{x} \in \mathbb{Z}_m$ s.t. $\bar{a}\bar{x} = \bar{1} \iff ax \equiv 1 \pmod{m}$, which means that $m|(1 - ax)$. So there exists an integer $y \in \mathbb{Z}$ s.t. $my = 1 - ax \iff ax + my = 1$. By Shifrin corollary 2.4 a, m must be coprime.

For (b),

1. ($\rightarrow$) Let $\bar{a} \in \mathbb{Z}_m$ be a zero-divisor. Then there exists $\bar{x} \neq \bar{0}$ in $\mathbb{Z}_m$ such that $\bar{a}\bar{x} = \bar{0}$. This means: $ax \equiv 0 \pmod{m}$, so $m \mid ax$, and $m \nmid x$ (since $\bar{x} \neq \bar{0}$). Since $m \mid ax$ but $m \nmid x$, some prime factor of m must divide a. This prime factor is then a common divisor of a and m greater than 1, so $\gcd(a,m) > 1$.
2. ($\leftarrow$) Let $a \in \mathbb{Z}$, $m \in \mathbb{N}$ where $\gcd(a,m) = d > 1$ and $m \nmid a$. Then $a = a'd$ and $m = m'd$ for some $a', m' \in \mathbb{Z}$. Therefore,

$$\bar{a}\bar{m}' = \overline{am'} = \overline{a'dm'} = \overline{a'm} = \bar{0} \tag{154}$$

Also since $m \nmid a$, we have $\bar{a} \neq \bar{0}$, and since $m = m'd$, we have $m \nmid m'$ (since $m \nmid a \implies d \neq m$), so $\bar{m}' \neq \bar{0}$. Therefore $\bar{a}$ is a zero-divisor in $\mathbb{Z}_m$.

For (c), let $a \in \mathbb{Z}_m$ be a nonzero element. Then it must be the case that $\gcd(a,m) = 1$ or $\gcd(a,m) > 1$. In the former case, a is a unit by (a), and in the latter case, $a \not\equiv 0 \implies m \nmid a$[a], and so by (b) a is a zero divisor.

[a] By contrapositive $m \mid a \implies a \equiv 0 \pmod{m}$ is trivial.

Exercise 2.24 (Shifrin 1.4.6.b/c/d)

Prove that in any ring R:

1. $0 \cdot a = 0$ for all $a \in R$ (cf. Lemma 1.1);
2. $(-1)a = -a$ for all $a \in R$ (cf. Lemma 1.2);
3. $(-a)(-b) = ab$ for all $a, b \in R$;
4. the multiplicative identity $1 \in R$ is unique.

Solution 2.6

For (a), note that $0a = (0 + 0) \cdot a = 0a + 0a$ and by subtracting $0a$ from both sides, we have $0 = 0a$. Similarly, $a0 = a(0 + 0) = a0 + a0 \implies 0 = a0$. For (b),

$$\begin{aligned}
a + (-1) \cdot a &= 1 \cdot a + (-1) \cdot a && \text{(definition of 1)} \\
&= (1 + -1) \cdot a && \text{(left distributivity)} \\
&= 0 \cdot a && \text{(definition of add inverse)} \\
&= 0 && \text{(From (a))}
\end{aligned}$$

For (c), note that by right distributivity,

$$\begin{aligned}
(-1) \cdot a + a &= (-1) \cdot a + 1 \cdot a && \text{(definition of 1)} \\
&= (-1 + 1) \cdot a && \text{(right distributivity)} \\
&= a \cdot 0 && \text{(definition of add inverse)} \\
&= 0 && \text{(From (a))}
\end{aligned}$$

Therefore,

$$\begin{aligned}
(-a)(-b) &= (-1 \cdot a)(-1 \cdot b) && \text{(from (b))} \\
&= -1 \cdot (a \cdot -1) \cdot b && \text{(associativity)} \\
&= -1 \cdot -a \cdot b && \text{(from (b))} \\
&= -1 \cdot -1 \cdot a \cdot b && \text{(from (b))} \\
&= (-1 \cdot -1) \cdot ab && \text{(associativity)} \\
&= 1ab && \text{(shown below)} \\
&= ab && \text{(definition of identity)}
\end{aligned}$$

where $(-1)(-1) = 1$ since by (b), $(-1)(-1) = -(-1)$. We know that $-(-1)$ is an additive inverse for -1 and so is 1. Since the multiplicative identity is unique in a ring, $-(-1) = 1$. We show uniqueness for (d). Let us have $1 \neq 1'$. Then by definition of identity,

$$1 = 11' = 1'1 = 1' \tag{155}$$

which is a contradiction.

Exercise 2.25 (Shifrin 1.4.10)

1. Prove that the multiplicative inverse of a unit a in a ring R is unique. That is, if $ab = ba = 1$ and $ac = ca = 1$, then $b = c$. (You will need to use associativity of multiplication in R.)
2. Indeed, more is true. If $a \in R$ and there exist $b, c \in R$ so that $ab = 1$ and $ca = 1$, prove that $b = c$ and thus that a is a unit.

Solution 2.7

For (a), we see that

$$c = 1c = (ab)c = (ba)c = b(ac) = b(ca) = b1 = b \tag{156}$$

For (b), we have

$$b = 1b = (ca)b = c(ab) = c1 = c \tag{157}$$

Exercise 2.26 (Shifrin 1.4.13)

Let p be a prime number. Use the fact that $\mathbb{Z}_p$ is a field to prove that $(p-1)! \equiv -1 \pmod{p}$. (Hint: Pair elements of $\mathbb{Z}_p$ with their multiplicative inverses; cf. Exercise 1.3.12.).

Solution 2.8

For $p = 2$, the result is trivial. Now let $p > 2$ be a prime. Then since $\mathbb{F}$ is a field, every element $a \in \mathbb{F}$ contains a multiplicative inverse a^{-1}. We claim that the only values for which $a = a^{-1}$ is $1, p-1$. Assume that $a = a^{-1}$. Then

$$a^2 = 1 \implies p|(a^2 - 1) \implies p|(a+1)(a-1) \tag{158}$$

and since p is prime, it must be the case that $p|a+1 \iff a \equiv -1 \pmod{p}$ or $p|a-1 \iff a \equiv 1 \pmod{p}$. Therefore, we are left to consider the $(p-3)$ elements: $2, \ldots, p-2$. Since inverses are unique and the inverses of inverses is the original element, we can partition these $p-2$ elements into $(p-3)/2$ pairs.[a] Let's call the set of pairs $K = \{(a, b)\}$ where $b = a^{-1}$. Therefore, by commutativity and associativity we have

$$(p-1)! \equiv (1)(p-1) \prod_{(a,b)\in K} ab \equiv -1 \cdot \prod_{(a,b)\in K} 1 \equiv -1 \pmod{p}. \tag{159}$$

[a] Since $p \neq 2$, p is odd and therefore $p-3$ is even.

Exercise 2.27 (Shifrin 2.3.2.a/b/c)

Recall that the conjugate of the complex number $z = a + bi$ is defined to be $\bar{z} = a - bi$. Prove the following properties of the conjugate:

1. $\overline{z+w} = \bar{z} + \bar{w}$
2. $\overline{zw} = \bar{z}\bar{w}$
3. $\bar{z} = z \iff z \in \mathbb{R}$ and $\bar{z} = -z \iff iz \in \mathbb{R}$
4. If $z = r(\cos\theta + i\sin\theta)$, then $\bar{z} = r(\cos\theta - i\sin\theta)$

Solution 2.9

Let $z = a + bi, w = c + di$. For (a),

$$\overline{z+w} = \overline{(a+c) + (b+d)i} = (a+c) - (b+d)i = a + c - bi - di = (a-bi) + (c-di) = \overline{z} + \overline{w} \tag{160}$$

For (b),

$$\overline{zw} = \overline{(ac-bd) + (ad+bc)i} = (ac-bd) - (ad+bc)i = ac - bd - adi - bci = (a-bi)(c-di) = \bar{z}\bar{w} \tag{161}$$

For (c), consider

$$\begin{aligned} \overline{z} = z &\iff a + bi = a - bi && (162)\\ &\iff bi = -bi && (163)\\ &\iff 2bi = 0 && (164)\\ &\iff b = 0 && \text{(field has no 0 divisors)} \end{aligned}$$

Therefore, $z = a \in \mathbb{R}$.

$$\begin{aligned} \overline{z} = -z &\iff a - bi = -a - bi && (165)\\ &\iff a = -a && (166)\\ &\iff 2a = 0 && (167)\\ &\iff a = 0 && \text{(field has no 0 divisors.)} \end{aligned}$$

Therefore, $z = bi \implies iz = -b \in \mathbb{R}$.

Exercise 2.28 (Shifrin 2.3.3.a/b/c)

Recall that the modulus of the complex number $z = a + bi$ is defined to be $|z| = \sqrt{a^2 + b^2}$. Prove the following properties of the modulus:

1. $|zw| = |z||w|$
2. $|\bar{z}| = |z|$
3. $|z|^2 = z\bar{z}$
4. $|z + w| \leq |z| + |w|$ (This is called the triangle inequality; why?)

Solution 2.10

Let $z = a + bi$ and $w = c + di$. For (a),

$$\begin{aligned} |zw| &= |(ac - bd) + (ad + bc)i| \\ &= \sqrt{(ac - bd)^2 + (ad + bc)^2} \\ &= \sqrt{a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2} \\ &= \sqrt{(a^2 + b^2)(c^2 + d^2)} \\ &= \sqrt{a^2 + b^2}\sqrt{c^2 + d^2} \\ &= |z||w| \end{aligned}$$

For (b), if $z = a + bi$, then $\bar{z} = a - bi$, so:

$$|\bar{z}| = \sqrt{a^2 + (-b)^2} = \sqrt{a^2 + b^2} = |z| \tag{168}$$

For (c),

$$\begin{aligned} z\bar{z} &= (a + bi)(a - bi) \\ &= a^2 + b^2 \\ &= |z|^2 \end{aligned}$$

3 Fields

Our final structure is field, which are usually pretty tame compared to groups and rings.

Definition 3.1 (Field)

A **field** $(F, +, \times)$ is a commutative, associative ring where every nonzero element is a unit.

Theorem 3.1 ()

Every field is a Euclidean domain.

Proof.

Given $x, y \in \mathbb{F}$, assume $xy = 0$ with $x \neq 0$. Since x is invertible,

$$0 = x^{-1}0 = x^{-1}(xy) = y \tag{169}$$

Now assuming that $y \neq 0$, since y is invertible,

$$0 = 0y^{-1} = (xy)y^{-1} = x \tag{170}$$

Let's give a few examples of fields.

Theorem 3.2 (Wedderburn's little theorem)

Every finite Euclidean domain is a field.

Example 3.1 (Finite Fields)

$\mathbb{Z}_p$ with p prime is a field.

Example 3.2 (Numbers)

The rational, reals, and complex numbers are all fields.[a]

[a] Quaternions are not!

Note the subfield structure $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. However, we will find that there are tons of other fields lurking in between $\mathbb{Q}$ and $\mathbb{C}$ other than $\mathbb{R}$. We can actually say that there are no subfields of $\mathbb{Q}$.

Lemma 3.1 (Rationals are a Minimal Field)

Every subfield of $\mathbb{C}$ contains $\mathbb{Q}$.

Proof.

Must contain 0 and 1. Keep adding 1 and inverting it to get $\mathbb{Z}$. Now $\mathbb{Z}$ must contain units so $1/n$ also contained. Then multiply the elements to get $\mathbb{Q}$.

3.1 Rational Functions

Given a field F, we have constructed the Euclidean domain $F[x]$. However, this is one step away from being a field. We mimick the construction of the rational numbers $\mathbb{Q}$ as a quotient space over $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ by taking $F[x] \times (F[x] \setminus \{0\})$ and putting a quotient on it.

Definition 3.2 (Rational Functions)

The **rational functions** are defined to be the field of quotients (really just 2-tuples) of the form

$$F(x) := \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in F[x], g(x) \neq 0 \right\} \tag{171}$$

where addition and multiplication is defined in the usual sense.

Theorem 3.3 (Partial Fractions Decomposition)

Let $f(x), g(x) \in F[x]$ where $\deg(f(x)) < \deg(g(x))$. If $g(x) = u(x)v(x)$ where u, v are relatively prime, then there are polynomials $a(x), b(x)$ with $\deg(a) < \deg(u), \deg(b) < \deg(v)$ s.t.

$$\frac{f(x)}{g(x)} = \frac{a(x)}{u(x)} + \frac{b(x)}{v(x)} \tag{172}$$

By induction, we can prove this for any finite set of irreducible polynomials.

Proof.

We describe an algorithm to get this decomposition. There are polynomials $s(x), t(x)$ s.t. $1 = s(x)u(x) + t(x)v(x)$. Therefore,

$$\frac{f(x)}{u(x)v(x)} = \frac{f(x)t(x)}{u(x)} + \frac{f(x)s(x)}{v(x)} \tag{173}$$

and we can use the Euclidean algorithm to write

$$\frac{f(x)t(x)}{u(x)} = q(x) + \frac{a(x)}{u(x)}, \qquad \deg(a) < \deg(u) \tag{174}$$

$$\frac{f(x)s(x)}{v(x)} = q(x) + \frac{a(x)}{u(x)}, \qquad \deg(b) < \deg(v) \tag{175}$$

which implies

$$\frac{f(x)}{u(x)v(x)} = \frac{a(x)}{u(x)} + \frac{b(x)}{v(x)} \tag{176}$$

Example 3.3 ()

Consider the rational function $\frac{x+3}{x^3(x-1)^2}$. Applying the Euclidean algorithm, we find that

$$1 = (3x^2 + 2x + 1)(x-1)^2 - (3x-4)x^3 \tag{177}$$

and so

$$\frac{x+3}{x^3(x-1)^2} = \frac{(x+3)(3x^2+2x+1)}{x^3} - \frac{(x+3)(3x-4)}{(x-1)^2} \tag{178}$$

$$= \frac{11x^2 + 7x + 3}{x^3} + \frac{-11x + 15}{(x-1)^2} \tag{179}$$

3.2 Algebraically Closed Fields

Now that we have seen some examples of fields, what properties would we like it to have? Going back to polynomials, recall that if F is a field, then $F[x]$ as a Euclidean domain gave us a lot of nice properties, such as admitting a unique factorization of irreducible polynomials. However, we have only proved that the number of roots is *at most* the degree n, but not that it actually reaches n. In fact, in a more extreme case, a polynomial may not even factor *at all* in $F[x]$, since it could be irreducible. So while we have defined an upper bound for the number of roots for a polynomial, we have not determined whether a polynomial has any roots at all, i.e. a lower bound.

We don't have much *control* over what these irreducible polynomials can look like. We may have to check—either through theorems or manually—that a polynomial or arbitrary degree is irreducible. If we would like to assert that all irreducible polynomials must be of smallest degree—that is, linear—then such a field is called *algebraically closed.* This algebraic closed property asserts also that the lower bound on the number of (non-unique) factors is n.

Definition 3.3 (Algebraically Closed Field)

A field F is **algebraically closed** if every polynomial of positive degree (i.e. non-constant) in $F[x]$ has at least one root in F.

This is equivalent to saying that every polynomial can be expressed as a product of first degree polynomials. To extend our analysis more, we can talk about the multiplicity of these factors, which just tells us more about how many unique and non-unique factors a polynomial has.

Definition 3.4 (Multiplicity)

A root c of polynomial $f(x) \in F[x]$ is called simple if $f(x)$ is not divisible by $(x-c)^2$ and multiple otherwise. The **multiplicity** of a root c is the maximum k such that $(x-c)^k$ divides $f(x)$.

To restate the root-factor theorem for $R[x]$ with arbitrary commutative ring R, the number of roots of a polynomial—counted with multiplicity—does not exceed the degree of this polynomial. Furthermore, these numbers are equal if and only if the polynomial is a product of linear factors.

Example 3.4 (Reals are not Algebraically Closed)

$\mathbb{R}$ is not algebraically closed since we can identify the polynomial $f(x) = x^2 + 1 \in \mathbb{R}[x]$ which does not have any roots in $\mathbb{R}$. Consequently, any subfield of $\mathbb{R}$ (which contains 1) such as $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \ldots$ are not algebraically closed.

It turns out that the complex numbers are algebraically closed, which is presented with the following grand name. Ironically, this theorem cannot be proven with algebra alone. We need complex analysis.[4]

Theorem 3.4 (Fundamental Theorem of Algebra)

Suppose $f \in \mathbb{C}[x]$ is a polynomial of degree $n \geq 1$. Then $f(x)$ has a root in $\mathbb{C}$. It immediately follows from induction that it can be factored as a product of linear polynomials in $\mathbb{C}[x]$.

Proof.

WLOG we can assume that f is monic: $f(z) = z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0$. Since $\mathbb{C}$ is a field, we

[4] Gauss proved this for the first time in 1799.

can set

$$f(z) = z^n \left(1 + \frac{a_{n-1}}{z} + \frac{a_{n-2}}{z^2} + \ldots + \frac{a_0}{z_n}\right) \tag{180}$$

Since

$$\lim_{|z| \to \infty} \left(1 + \frac{a_{n-1}}{z} + \frac{a_{n-2}}{z^2} + \ldots + \frac{a_0}{z_n}\right) = 0 \tag{181}$$

there exists a $R > 0$ s.t.

$$|z| > R \implies \left|1 + \frac{a_{n-1}}{z} + \frac{a_{n-2}}{z^2} + \ldots + \frac{a_0}{z_n}\right| < \frac{1}{2} \tag{182}$$

and hence

$$|z| > R \implies |f(z)| > |z|^n \cdot \left(1 - \frac{1}{2}\right) > \frac{R^n}{2} \tag{183}$$

So z cannot be a root if $|z| > R$. On the other hand, $f(z)$ is continuous (under the Euclidean topology) and so on the compact set $\{z \in \mathbb{C} \mid |z| \leq R\}$, $|f(z)|$ achieves a minimum value say at the point z_0. We claim that $\min_z f(z) = 0$.

For convenience, we let $z_0 = 0$ (we can do a change of basis on the polynomial) and assume that the minimum is some positive number, i.e. $f(0) = a_0 \neq 0$. Let j be the smallest positive integer such that $a_j = 0$. Let

$$g(z) = \frac{a_{j+1}}{a_j} z + \ldots + \frac{a_n}{a_j} z^{n-j} \implies f(z) = a_0 + a_j z^j \big(1 + g(z)\big) \tag{184}$$

We set $\gamma = \sqrt[j]{-a_0/a_j}$ and consider the values of

$$\begin{aligned} f(t\gamma) &= a_0 + a_j (t\gamma)^j \big(1 + g(t\gamma)\big) && (185)\\ &= a_0 - a_0 t^j \big(1 + g(t\gamma)\big) && (186)\\ &= a_0 \big\{1 - t^j \big(1 + g(t\gamma)\big)\big\} && (187) \end{aligned}$$

for $t > 0$. For t sufficiently small, we have

$$|g(t\gamma)| = \left|\frac{a_{j+1}}{a_j}(t\gamma) + \ldots + \frac{a_n}{a_j}(t\gamma)^{n-j}\right| < \frac{1}{2} \tag{188}$$

and for such t, this implies

$$|f(t\gamma)| = |a_0||1 - t^j(1 + g(t\gamma))| \leq |a_0||1 - t^j/2| < |a_0| \tag{189}$$

and so z_0 cannot have been the minimum of $|f(z)|$. Therefore, the minimum value must be 0.

Great, so through this theorem, we can work in any subfield of $\mathbb{C}$ and guarantee that will have all of its roots in $\mathbb{C}$.

Corollary 3.1 ($\mathbb{C}$ is algebraically closed)

$\mathbb{C}$ is algebraically closed, i.e. $\mathbb{C}$ is a splitting field of $\mathbb{C}[x]$.

Put more succinctly, the impossibility of defining division on the ring of integers motivates its extension into the field of rational numbers. Similarly, the inability to take square roots of negative real numbers forces us to extend the field of real numbers to the bigger field of complex numbers.

Theorem 3.5 (Eigenvector Conditions for Algebraic Closedness)

A field F is algebraically closed if and only if for each natural number n, every endomorphism of F^n (that is, ever linear map from F^n to itself) has at least one eigenvector.

Proof.

An endomorphism of F^n has an eigenvector if and only if its characteristic polynomial has some root. $(\rightarrow)$ So, when F is algebraically closed, every characteristic polynomial, which is an element of $F[x]$, must have a root. $(\leftarrow)$ Assume that every characteristic polynomial has some root, and let $p \in F[x]$. Dividing the polynomial by a scalar doesn't change its roots, so we can assume p to have leading coefficient 1. If $p(x) = a_0 + a_1 x + ... + x^n$, then we can identify matrix

$$A = \begin{pmatrix} 0 & 0 & ... & 0 & -a_0 \\ 1 & 0 & ... & 0 & -a_1 \\ 0 & 1 & ... & 0 & -a_2 \\ ... & ... & ... & ... & ... \\ 0 & 0 & ... & 1 & -a_{n-1} \end{pmatrix} \tag{190}$$

such that the characteristic polynomial of A is p.

With this splitting condition, we can get a nice set of formulas often introduced in high-school math competitions.

Theorem 3.6 (Viete's Formulas)

Given that a polynomial f factors into linear terms, that is

$$f(x) = a_0 \prod_{i=1}^{n} (x - c_i), c_i \text{ roots of } f \tag{191}$$

Then the coefficients of f can be presented with the formulas

$$\begin{aligned} \sum_{i=1}^{n} c_i &= -\frac{a_1}{a_0} \\ \sum_{i_1 < i_2} c_{i_1} c_{i_2} &= \frac{a_2}{a_0} \\ \sum_{i_1 < ... < i_k} \prod_{j=1}^{k} c_{i_j} &= (-1)^k \frac{a_k}{a_0} \\ c_1 c_2 c_3 ... c_n &= (-1)^n \frac{a_n}{a_0} \end{aligned}$$

3.3 Extensions and Splitting Fields

Great, so by establishing the fact that $\mathbb{C}$ is algebraically closed, this gives us a "safe space" to work in, in the sense that if we take any subfield $F \subset \mathbb{C}$ and find a polynomial $f(x) \in F[x]$, we are *guaranteed* to find a linear factorization of f in $\mathbb{C}[x]$. Let's define this a bit more generally for arbitrary fields $F \subset K$.

Definition 3.5 (Field Extension)

The pair of fields $F \subset K$ is called a **field extension**.

Therefore, if K is algebraically closed and $F \subset K$ is a field extension, $f(x) \in F[x]$ is guaranteed to *split* completely into linear factors. This is true for *all* $f(x) \in F[x]$, but now if we *fix* $f(x) \in F[x]$, perhaps we don't need the entire field K to split $f(x)$. Maybe we can work in a slightly larger field E—such that $F \subset E \subset K$—where $f(x)$ splits in E. This process of finding such a minimal field is important to understand the behavior of roots of such polynomials.

Definition 3.6 (Splitting Field)

Given a field extension $F \subset K$ and a polynomial $f \in F[x]$,

1. f **splits** in K if f can be written as the product of linear polynomials in $K[x]$.
2. If f splits in K and there exists no field E s.t. $F \subsetneq E \subsetneq K$, then K is called a **splitting field** of f.[a]

[a] i.e. the splitting field is the smallest field that splits f.

Example 3.5 (Don't Need(?) Complex)

Consider the following.

1. Let $f(x) = x^2 - 1$. If $f(x) \in \mathbb{R}[x]$, it does split in $\mathbb{R}$. In fact, even if we consider it as an element of $\mathbb{Z}_2[x]$, it still splits into $(x+1)(x-1)$.
2. Let $f(x) = x^2 - 2$. If $f(x) \in \mathbb{Q}[x]$, it doesn't split in $\mathbb{Q}$ since the roots $\pm\sqrt{2} \notin \mathbb{Q}$, but $\pm\sqrt{2}$ are real numbers, so $f(x)$ does in fact split in $\mathbb{R}$ since it splits into $(x+\sqrt{2})(x-\sqrt{2})$. However, maybe it is not the (smallest) splitting field.
3. Let $f(x) = x^2 + 1$. We can see that if we consider it as an element of $\mathbb{Q}[x]$ or $\mathbb{R}[x]$, neither fields split $f(x)$ since $\pm i$ are its roots and therefore are contained in the coefficients of its linear factors. We know that it definitely splits in $\mathbb{C}$, but can we find a smaller field that splits $f(x)$? Perhaps.

So how does one find a splitting field? Note that in the example above, we have found that there were some roots α of certain polynomials $f(x) \in F[x]$ are not contained in F. Therefore, what we want to do is find the smallest field F containing both F and α (plus any other α's). This smallest such field is called an *adjoining field.*

3.3.1 Ring Extensions

We will introduce this in a slightly different way, but by building up some theorems, we will unify these two soon enough.

Definition 3.7 (Ring of Univariate Polynomial Elements)

Let $F \subset K$ be fields, $F[x]$ a polynomial ring, and a constant $\alpha \in K$,

$$F[\alpha] := \{f(\alpha) \in F \mid f \in F[x]\} \subset K \tag{192}$$

Lemma 3.2 (Ring Extension)

We have the following subring structure.

$$F \subset F[\alpha] \subset K \tag{193}$$

Furthermore, if $\alpha \notin F$, then $F \subsetneq F[\alpha]$.

Proof.

Note that $F \subset F[\alpha]$ since we can just take the constant polynomials, so this is not very interesting. Given two elements $\phi, \gamma \in F[\alpha]$, there exists polynomials $f, g \in F[x]$ s.t. $\phi = f(\alpha), \gamma = g(\alpha)$. Since $F[x]$ is a ring, we see that

$$\phi + \gamma = f(\alpha) + g(\alpha) = (f+g)(\alpha) \tag{194}$$

$$\phi \cdot \gamma = f(\alpha) \cdot g(\alpha) = (fg)(\alpha) \tag{195}$$

Furthermore, it is easy to check that 0 and 1 are the images of α through the 0 and 1 polynomials. What allows us to make this inclusion proper is that the $\alpha \in K$, which does not necessarily have to be in F, *extends* this field a bit further, but since we can only map the one element α, it may not cover all of K.

Let's go through some examples.

Example 3.6 (Radical Extensions of $\sqrt{2}$)

Let $F = \mathbb{Q}$ and $K = \mathbb{C}$. We claim $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

1. $\mathbb{Q}[\sqrt{2}] \subset \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. $\mathbb{Q}[\sqrt{2}]$ are elements of the form

$$f(\sqrt{2}) = a_n(\sqrt{2})^n + a_{n-1}(\sqrt{2})^{n-1} + \ldots + a_2(\sqrt{2})^2 + a_1\sqrt{2} + a_0 \tag{196}$$

   This can be written by collecting terms, of the form $a + b\sqrt{2}$.
2. $\mathbb{Q}[\sqrt{2}] \supset \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Given an element $a + b\sqrt{2}$, this is clearly in $\mathbb{Q}[\sqrt{2}]$ since it is the image of $\sqrt{2}$ under the polynomial $f(x) = a + bx$.

Given this, we may extrapolate this pattern and claim that $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$ consists of all numbers of form $a + (\sqrt{2} + \sqrt{3})b$. However, this is *not* the case.

Example 3.7 ()

Given any element $\beta \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$, it is by definition of the form

$$\beta = \sum_{k=0}^{n} a_k(\sqrt{2} + \sqrt{3})^k \tag{197}$$

Clearly $1, \sqrt{2} + \sqrt{3} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$ by mapping $\sqrt{2} + \sqrt{3}$ through the polynomials $f(x) = 1$ and $f(x) =$. However, we can see that $(\sqrt{2} + \sqrt{3})^2 = 5 + \sqrt{6}$,[a] and so $\sqrt{6} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Furthermore, we have $(\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3}$, and so with the ring properties we can conclude that

$$\frac{1}{2}\big[(11\sqrt{2} + 9\sqrt{3}) - 9(\sqrt{2} + \sqrt{3})\big] = \sqrt{2} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}] \tag{198}$$

$$-\frac{1}{2}\big[(11\sqrt{2} + 9\sqrt{3}) - 11(\sqrt{2} + \sqrt{3})\big] = \sqrt{3} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}] \tag{199}$$

$$\tag{200}$$

If we go a bit further, we can show that

$$\mathbb{Q}[\sqrt{2} + \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\} \tag{201}$$

[a] where we use $\sqrt{6}$ as notation for $\sqrt{2} \cdot \sqrt{3}$

This method in which we have taken higher powers of α to reveal elements in $\mathbb{Q}$ reveals a deeper structure of a finite-dimensional vector space, which will be useful for analyzing certain fields in the examples below.

Lemma 3.3 (Vector Space Structure)

$F[\alpha]$ is a finite-dimensional vector space over F. If $f(x) = a_n x^n + \ldots a_0$, then $S = \{1, \alpha, \ldots, \alpha^{n-1}\}$ spans $F[\alpha]$.[a]

[a] Note that this does not mean that it is a basis.

Proof.

An element of $F[\alpha]$ is of the form

$$f(\alpha) = \sum_{k=0}^{n} a_k \alpha^k \tag{202}$$

for some $f \in F[x]$, and so it is immediate that $\{\alpha^k\}_{k \in \mathbb{N}_0}$ spans $F[\alpha]$. We claim that α^{n-1+i} is in S for all $i > 0$. By induction, if $i = 1$, then

$$\alpha^n = -\frac{1}{a_n}\big(a_{n-1}\alpha^{n-1} + \ldots + a_0\big) \tag{203}$$

which proves the claim. Now assume that $\alpha^n, \alpha^{n+1}, \ldots, \alpha^{n-1+i} \in \operatorname{span}\{1, \ldots, \alpha^{n-1}\}$. Then

$$\alpha^i f(\alpha) = 0 \implies a_n \alpha^{n+i} + \alpha_{n-1}\alpha^{n+i-1} + \ldots + a_0 \alpha^i = 0 \tag{204}$$

and so

$$\alpha^{n+i} = -\frac{1}{a_n}\big(a_{n-1}\alpha^{n+i-1} + \ldots + a_0 \alpha^i\big) \tag{205}$$

which means that $\alpha^{n+i} \in \operatorname{span}\{1, \ldots, \alpha^{n-1}\}$, completing the proof.

3.3.2 Field Extensions

Great, so we automatically have the ring and vector space structures on $F[\alpha]$. However, what we would really like is a field structure since that was our original goal. Remember that $F[\alpha]$ is a ring that contains both F and α. With one more assumption, we can claim that it is a field.

Theorem 3.7 (Adjoining Fields)

Given fields $F \subset K$, if there exists a $f \in F[x]$ s.t. $\alpha \in K$ is a root of f, then $F[\alpha] \subset K$ is a field. To emphasize that it is a field, we usually denote it as $F(\alpha)$ and refer it as the field obtained by **adjoining** α to F.

Proof.

It is clear that $F[\alpha]$ is a commutative ring since F is a field. So it remains to show that every nonzero element of $\beta \in F[\alpha]$ is a unit. By definition $\beta = p(\alpha)$ for some polynomial $p \in F[x]$. Factor $f \in F[x]$ as the product of irreducible polynomials. Then α must be a root of one of those irreducible factors, say $g(x)$. Note that $g(x) \nmid p(x)$ since $p(\alpha) \neq 0$. Since g is irreducible, we know that $\gcd(g, p) = 1$ and so $\exists s, t \in F[x]$ s.t.

$$1 = sp + tg \implies 1 = s(\alpha)p(\alpha) + t(\alpha)g(\alpha) = s(\alpha)p(\alpha) \tag{206}$$

Therefore we have found a multiplicative inverse $s = p^{-1} \in F[\alpha]$.

Proof.

We can prove it using the vector space structure. Treating $F[\alpha]$as a finite-dimensional vector space over F, let us define the F-linear function[a]

$$m_b : F[\alpha] \to F[\alpha], \qquad m_b(\beta) = b\beta \tag{207}$$

Since $F[\alpha] \subset K$, $F[\alpha]$ is an integral domain. Thus $\nexists \beta \in F[\alpha] \setminus \{0\}$ s.t. $b\beta = 0$. This means that the kernel of m_b is 0, and so m_b is injective. By the rank-nullity theorem, it is bijective, and so there exists a $\beta \in F[\alpha]$ s.t. $b\beta = 1 \implies b$ is a unit.

[a] linearity is easy to check

Corollary 3.2 (Adjoining Field is Minimal)

$F[\alpha]$ is the smallest field containing F and α.

Example 3.8 ($\mathbb{Q}[\sqrt{3}i]$ is a Field)

$\mathbb{Q}[\sqrt{3}i]$ is a field, hence denoted $\mathbb{Q}(\sqrt{3}i)$ since $\sqrt{3}i$ is a root of the polynomial $f(x) = x^2 + 3$.

Example 3.9 ($\mathbb{Q}[\pi]$ not a Field)

However, $\mathbb{Q}[\pi]$ is not a field.

Example 3.10 (Finding Multiplicative Inverses of elements in $\mathbb{Q}[\alpha]$)

Given $\beta = p(\alpha) = \alpha^2 + \alpha - 1 \in \mathbb{Q}[\alpha]$, where α is a root of $f(\alpha) = \alpha^3 + \alpha + 1$, we first know that β must have a multiplicative inverse since $\mathbb{Q}[\alpha]$ is a field. Applying the Euclidean algorithm, we have

$$1 = \frac{1}{3}\big\{(x+1)f(x) - (x^2+2)p(x)\big\} = -\frac{1}{3}(\alpha^2+2)p(\alpha) \tag{208}$$

and so $\beta^{-1} = (\alpha^2 + \alpha - 1)^{-1} = -\frac{1}{3}(\alpha^2 + 2)$. We can check that

$$\begin{aligned} -\frac{1}{3}(\alpha^2+2)(\alpha^2+\alpha-1) &= -\frac{1}{3}(\alpha^4+\alpha^3+\alpha^2+2\alpha-2) && (209)\\ &= -\frac{1}{3}(\alpha^3+\alpha-2) && (210)\\ &= -\frac{1}{3}(-3) = 1 && (211) \end{aligned}$$

Intuitively, the extra $\alpha \in K$ allows us to "expand" our field F into a bigger field of K. We can also define this for multivariate polynomials.

Definition 3.8 (Ring of Multivariate Polynomial Elements)

Given a polynomial ring $F[x,y]$ over a field F and constants $\alpha, \beta \in F$, the following definitions are equivalent.

$$\begin{aligned} F[\alpha,\beta] &\coloneqq \{f(\alpha,\beta) \in F \mid f \in F[x,y]\} && (212)\\ &= (F[\alpha])[\beta] && (213)\\ &= (F[\beta])[\alpha] && (214) \end{aligned}$$

Proof.

Example 3.11 (Extensions of $\sqrt{2}$ and i)

We claim that

$$\mathbb{Q}[\sqrt{2}, i] = \{a + b\sqrt{2} + ci + d(\sqrt{2}i) \mid a, b, c, d \in \mathbb{Q}\} \tag{215}$$

From the previous example, we know that $\mathbb{Q}[\sqrt{2}]$ are all numbers of the form $a + b\sqrt{2}$. Now we take $i \in \mathbb{C}$ and map it through all polynomials with coefficients in $\mathbb{Z}[\sqrt{2}]$, which will be of form

$$f(i) = (a_n + b_n\sqrt{2})i^n + (a_{n-1} + b_{n-1}\sqrt{2})i^{n-1} + \ldots + (a_2 + b_2\sqrt{2})i^2 + (a_1 + b_1\sqrt{2})i + (a_0 + b_0\sqrt{2}) \tag{216}$$

However, we can see that since $i^2 = -1$, we only need to consider up to degree 1 polynomials of form

$$(a + b\sqrt{2}) + (c + d\sqrt{2})i \tag{217}$$

which is clearly of the desired form. For the other way around, this is trivial since we can construct a linear polynomial as before.

Example 3.12 ()

We claim $\mathbb{Q}[\sqrt{3} + i] = \mathbb{Q}[\sqrt{3}, i]$.

1. $\mathbb{Q}[\sqrt{3} + i] \subset \mathbb{Q}[\sqrt{3}, i]$
2. $\mathbb{Q}[\sqrt{3} + i] \supset \mathbb{Q}[\sqrt{3}, i]$. Note that

$$(\sqrt{3} + i)^3 = 8i \implies i \in \mathbb{Q}[\sqrt{3} + i] \tag{218}$$

$$\implies (\sqrt{3} + i) - i = \sqrt{3} \in \mathbb{Q}[\sqrt{3} + i] \tag{219}$$

Therefore, $\mathbb{Q}[\sqrt{3} + i]$ contains the elements $1, \sqrt{3}, i$, which form the basis of $\mathbb{Q}[\sqrt{3}, i]$.

Example 3.13 (Extensions of $\sqrt{3}i$ and $\sqrt{3}, i$)

We claim that $\mathbb{Q}[\sqrt{3}i] \subsetneq \mathbb{Q}[\sqrt{3}, i]$.

1. We can see that $\{1, \sqrt{3}i\}$ span $\mathbb{Q}[\sqrt{3}i]$ as a $\mathbb{Q}$-vector space. Therefore,

$$\sqrt{3}, i \in \mathbb{Q}[\sqrt{3}, i] \implies \sqrt{3}i \in \mathbb{Q}[\sqrt{3}, i] \tag{220}$$

implies that $\mathbb{Q}[\sqrt{3}i] \subset \mathbb{Q}[\sqrt{3}, i]$.

2. To prove proper inclusion, we claim that $i \notin \mathbb{Q}[\sqrt{3}i]$. Assuming that it can, we represent it in the basis $i = b_0 + b_1\sqrt{3}i$, and so

$$-1 = (b_0 + b_1\sqrt{3}i)^2 = (b_0^2 - 3b_1^2) + 2b_0b_1\sqrt{3}i \tag{221}$$

Therefore we must have $2b_0b_1\sqrt{3} = 0 \implies b_0$ or b_1 should be 0. If $b_0 = 0$, then $b_0^2 - 3b_1^2 = -3b_1^2 \implies b_1^2 = 1/3$, which is not possible since $b_1^2 \in \mathbb{Q}$. If $b_1 = 0$, then $b_0 - 3b_1^2 = b_0^2 > 0$, and so it cannot be -1.

3.3.3 Splitting Fields

Now we return to the problem of taking a polynomial $f \in \mathbb{Q}[x]$ and finding the *smallest* possible field $K \subset \mathbb{C}$ s.t. f can be factored as a product of linear polynomials in $K[x]$.

Example 3.14 (Simple Splitting Fields)

We provide some simple examples to gain intuition.

1. Let $f(x) = x^2 + 2x + 2 \in \mathbb{Q}[x]$. Then the roots of $f(x)$ are $-1 \pm i$, so
$$f(x) = (x - (-1 + i))(x - (-1 - i)) \tag{222}$$
and we can show that $\mathbb{Q}[-1 - i, -1 + i] = \mathbb{Q}[i]$ is the splitting field of f.
2. Let $f(x) = x^2 - 2x - 1 \in \mathbb{Q}[x]$. The roots are $1 \pm \sqrt{2}$, and so
$$f(x) = (x - (1 + \sqrt{2}))(x - (1 - \sqrt{2})) \tag{223}$$
and so $\mathbb{Q}[\sqrt{2}]$ is the splitting field of f.
3. Let $f(x) = x^6 - 1 \in \mathbb{Q}[x]$. We can factor
$$f(x) = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1) \tag{224}$$
and the non-rational roots are $\frac{\pm 1 \pm \sqrt{3}i}{2}$. Thus the splitting field of f is $\mathbb{Q}[\sqrt{3}i]$.

Example 3.15 ()

Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. It follows that the roots are

$$\{\sqrt[4]{2}, \sqrt[4]{2}, -\sqrt[4]{2}, -\sqrt[4]{2}i\} = \Big\{\sqrt[4]{2}, \sqrt[4]{2}e^{\frac{2\pi i}{4}}, \sqrt[4]{2}e^{\frac{4\pi i}{4}}, \sqrt[4]{2}e^{\frac{6\pi i}{4}}\Big\} \tag{225}$$

thus the splitting field of f is

$$\mathbb{Q}\big(\sqrt[4]{2}, \sqrt[4]{2}e^{\frac{2\pi i}{4}}, \sqrt[4]{2}e^{\frac{4\pi i}{4}}, \sqrt[4]{2}e^{\frac{6\pi i}{4}}\big) \subset \mathbb{Q}(\sqrt[4]{2}, e^{\frac{2\pi i}{4}}) \tag{226}$$

since $\sqrt[4]{2}e^{\frac{m\pi i}{4}} \in \mathbb{Q}(\sqrt[4]{2}, e^{\frac{2\pi i}{4}})$. In fact, the two are equal, and to prove this we can see that since we are working in a field,

$$e^{2\pi i/4} = \frac{\sqrt[4]{2}e^{2\pi i/4}}{\sqrt[4]{2}} \in \mathbb{Q}\big(\sqrt[4]{2}, \sqrt[4]{2}e^{\frac{2\pi i}{4}}, \sqrt[4]{2}e^{\frac{4\pi i}{4}}, \sqrt[4]{2}e^{\frac{6\pi i}{4}}\big) \tag{227}$$

which implies that $\sqrt[4]{2} \in \mathbb{Q}\big(\sqrt[4]{2}, \sqrt[4]{2}e^{\frac{2\pi i}{4}}, \sqrt[4]{2}e^{\frac{4\pi i}{4}}, \sqrt[4]{2}e^{\frac{6\pi i}{4}}\big)$. Therefore we can conclude that the splitting field is

$$\mathbb{Q}\big(\sqrt[4]{2}, \sqrt[4]{2}e^{\frac{2\pi i}{4}}, \sqrt[4]{2}e^{\frac{4\pi i}{4}}, \sqrt[4]{2}e^{\frac{6\pi i}{4}}\big) = \mathbb{Q}(\sqrt[4]{2}, e^{\frac{2\pi i}{4}}) \tag{228}$$

3.4 Reducibility of Real Polynomials

Theorem 3.8 ()

If c is a complex root of polynomial $f \in \mathbb{R}[x]$, then $\bar{c}$ is also a root of the polynomial. Moreover, $\bar{c}$ has the same multiplicity as c.

Corollary 3.3 ()

Every nonzero polynomial in $\mathbb{R}[x]$ factors into a product of linear terms and quadratic terms with negative discriminants.

Example 3.16 ()

$$\begin{aligned} x^5 - 1 &= (x-1)\bigg(x - \Big(\cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}\Big)\bigg)\bigg(x - \Big(\cos\frac{2\pi}{5} - i\sin\frac{2\pi}{5}\Big)\bigg) \\ &\times \bigg(x - \Big(\cos\frac{4\pi}{5} + i\sin\frac{4\pi}{5}\Big)\bigg)\bigg(x - \Big(\cos\frac{4\pi}{5} - i\sin\frac{4\pi}{5}\Big)\bigg) \\ &= (x-1)\bigg(x^2 - \frac{\sqrt{5}-1}{2}x + 1\bigg)\bigg(x^2 + \frac{\sqrt{5}+1}{2}x + 1\bigg) \end{aligned}$$

Corollary 3.4 ()

Every polynomial $f \in \mathbb{R}[x]$ of odd degree has at least one real root.

Proof.

This is a direct result of Theorem **. Alternatively, without loss of generality we can assume that the leading coefficient of f is positive. Then

$$\lim_{x\to+\infty} f(x) = +\infty, \quad \lim_{x\to-\infty} f(x) = -\infty \tag{229}$$

By the intermediate value theorem, there must be some point where f equals 0.

Theorem 3.9 (Descartes' Rule of Signs)

Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$. Let C_+ be the number of times the coefficients of $f(x)$ change signs (here we ignore the zero coefficients); let Z_+ be the number of positive roots of $f(x)$, counting multiplicities. Then $Z_+ \leq C_+$ and $Z_+ \equiv C_+ \pmod 2$. Moreover, if we set $g(x) = f(-x)$, let C_- be the number of times the coefficients of $g(x)$ change signs, and Z_- the number of negative roots of $f(x)$. Then $Z_- \leq C_-$ and $Z_- \equiv C_- \pmod 2$.

Theorem 3.10 ()

The number of positive roots of $f(x)$ is the same as the number of negative roots of $f(-x)$.

Example 3.17 (Easy Way to Find Number of Positive Roots)

Given $f(x) = x^5 + x^4 - x^2 - 1$,

1. We have $C_+ = 1$. By Descartes' rule of signs, it must be the case that $Z_+ \leq 1$ and $Z_+ \equiv 1 \pmod 2 \implies Z_+ = 1$.
2. Since $f(-x) = -x^5 + x^4 - x^2 - 1$, we have $C_- = 2$, so $Z_- = 0$ or 2. This is the best that we can do, though it turns out that it actually has 0 negative roots.[a]

[a] On the other hand, $x^5 + 3x^3 - x^2 - 1$ has 2 negative roots.

Note that if a polynomial has a multiple root but its coefficients are known only approximately (but with any degree of precision), then it is impossible to prove that the multiple roots exists because under any perturbation of the coefficients, however small, it may separate into simple roots or simply cease to exist. This fact leads to the "instability" of the Jordan Normal form because under any perturbation of the elements of a matrix A, the change may drastically affect the characteristic polynomial, hence affecting the geometric multiplicities of its eigenvectors.

3.5 Reducibility of Integer Polynomials

Even though we have covered a more general theory of polynomials with rational coefficients, it is worthwhile to visit integer polynomials for two reasons. First, there are a few specialized theorems that allow us to easily determine reducibility in $\mathbb{Z}[x]$. Second, Gauss's lemma allows us to check for reducibility in $\mathbb{Q}[x]$ by checking for reducibility in $\mathbb{Z}[x]$, at which point we can abuse the specialized theorems we have developed.

Theorem 3.11 (Rational Root Theorem)

Let $a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$. If $r/s \in \mathbb{Q}$ with $\gcd(r,s) = 1$, then $r \mid a_0$ and $s \mid a_n$.

Proof.

Given that r/s is a root, we have

$$a_n (r/s)^n + \ldots + a_0 = 0 \tag{230}$$

Multiplying by s^n, we get

$$a_n r^n + a_{n-1} r^{n-1} s + \ldots + a_1 s^{n-1} r + a_0 s^n = 0 \tag{231}$$

and putting this equation on mod r and mod s implies that $r | a_0 s^n$ and $s | a_n r^n$, respectively. But since we assumed that $\gcd(r,s) = 1$, $r | a_0$ and $s | a_n$.

The next is quite a remarkable result, since it says that decompositions in $\mathbb{Q}[x]$ imply decompositions in $\mathbb{Z}[x]$! Therefore, to check irreducibility in $\mathbb{Q}[x]$, it suffices to check irreducibility in $\mathbb{Z}[x]$.

Lemma 3.4 (Gauss's Lemma)

Let $f \in \mathbb{Z}[x]$. If $\exists g, h \in \mathbb{Q}[x]$ s.t. $f(x) = g(x)h(x)$, then $\exists \bar{g}, \bar{h} \in \mathbb{Z}[x]$ s.t. $f(x) = \bar{g}(x)\bar{h}(x)$.

Proof.

We can find $k, l \in \mathbb{Z}$ s.t. $g_1(x) = kg(x)$ and $h_1(x) = lh(x)$ have integer coefficients, i.e. $g_1, h_1 \in \mathbb{Z}[x]$. Then, $klf(x) = g_1(x)h_1(x) \in \mathbb{Z}[x]$. Let p be a prime factor of kl. We have

$$0 \equiv \bar{k}\bar{l}\bar{f}(x) \equiv \bar{g}_1(x)\bar{h}_1(x) \text{ in } \mathbb{Z}_p[x] \tag{232}$$

Since $\mathbb{Z}_p$ is an integral domain, $\mathbb{Z}_p[x]$ is an integral domain, and so $\bar{g}_1$ or $\bar{h}_1$ must be 0. WLOG let it be $\bar{g}_1$. Then every coefficient of $g_1(x)$ is divisible by p, and we can write it in the form $g_2(x) = pg_1(x)$. Therefore,

$$p(x) \cdot \frac{kl}{p} = \underbrace{\frac{g_1(x)}{p}}_{g_2(x)} \cdot \underbrace{h_1(x)}_{h_2(x)} \iff f(x)\frac{kl}{p} = g_2(x)h_2(x) \tag{233}$$

Since there are only finitely many prime divisors, we do this for all prime factors of kl, and we have

$$f(x) = g_n(x)h_n(x), \qquad g_n, h_n \in \mathbb{Z}[x] \tag{234}$$

Example 3.18 (Reducibility of Integer Polynomials)

Let $f(x) = x^4 - x^3 + 2$. The rational roots are in the set $S = \{\pm 1, \pm 2\}$, but none of them work since $f(\pm 1), f(\pm 2) \neq 0$. By degree considerations and Gauss's lemma, if $f(x)$ is reducible, then

$$f(x) = (x^2 + ax + b)(x^2 + cx + d), \qquad a, b, c, d \in \mathbb{Z} \tag{235}$$

We know that $bd \in S$, with $a + c = -1$, $d + b + ac = 0$, and so on for each coefficients. We can brute force this finite set of possibilities.

A great way to check irreducibility is to check in mod p.

Theorem 3.12 ()

Let $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$. If $p \nmid a_n$ and $f \in \mathbb{Z}_p[x]$ is irreducible, then f is irreducible in $\mathbb{Q}[x]$.[a]

[a] May need to verify this again.

Proof.

Suppose that $f(x) = g(x)h(x) \in \mathbb{Z}[x]$ with $\deg(g), \deg(h) > 0$. Then

$$f(x) \equiv g(x)h(x) \text{ in } \mathbb{Z}_p[x] \tag{236}$$

Since $f(x)$ is irreducible in $\mathbb{Z}_p[x]$, we must have that one of $g(x)$ or $h(x)$ has degree 0 in $\mathbb{Z}_p[x]$. WLOG let it be $g(x)$, but this means that the leading coefficient of $g(x)$ must be divisible by $p \implies$ leading coefficient of $f(x)$ is divisible by $p \iff p \mid a_n$.

Example 3.19 ()

x^4+x+1 is irreducible in $\mathbb{Z}_2[x]$. So we can extend this to $\mathbb{Z}[x]$ to see that *all* fourth degree polynomials of form $ax^4 + bx^3 + cx^2 + dx + e$, which a, d, e odd and b, c even is irreducible in $\mathbb{Q}[x]$.

This is a powerful theorem to quickly find a large class of polynomials that are irreducible. However, being reducible in $\mathbb{Z}_p[x]$ does not imply reducibility in $\mathbb{Q}$. In fact, there are polynomials $f(x) \in \mathbb{Z}[x]$ which are irreducible but reducible in $\mathbb{Z}_p$ for *every* prime p.

Theorem 3.13 (Eisenstein's Criterion)

Let $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$ and $p \in \mathbb{Z}$ a prime s.t. $p \nmid a_n$, $p \mid a_i$ for $i = 0, \ldots, a_{n-1}$, and $p^2 \nmid a_0$. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof.

Suppose that $f(x) = g(x)h(x) \in \mathbb{Q}[x]$ with $\deg(g), \deg(h) > 0$. Then, by Gauss's lemma, $g, h \in \mathbb{Z}[x]$. Reducing the equations mod p,

$$f(x) = g(x)h(x) \text{ in } \mathbb{Z}_p[x] \tag{237}$$

But $f(x) = a_n x^n$. By unique factorization theorem in $\mathbb{Z}_p[x]$, $g, h \in \mathbb{Z}_p[x]$ must be products of units and prime factors of $a_n x^n$, which are $\{x\}$. Therefore, let

$$g(x) = b_m x^m, h(x) = \frac{a_n}{b_m} x^{n-m} \in \mathbb{Z}_p[x] \tag{238}$$

with $\deg(g) = m > 0$ and $\deg(h) = n - m > 0$ in $\mathbb{Z}[x]$. This implies that the constant coefficients of $g(x), h(x)$ are divisible by p, which implies that the constant coefficients of $f(x) = g(x)h(x)$ are divisible by p^2, a contradiction.

Example 3.20 (Easy Checks for Irreducibility with Eisenstein)

Listed.

1. $x^{13} + 2x^{10} + 4x + 6$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein for $p = 2$.
2. $x^3 + 9x^2 + 12x + 3$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein for $p = 3$.
3. Let $f(x) = x^4 + x^3 + x^2 + x + 1$. Then, we know that $f(x) = \frac{x^5-1}{x-1}$ and so

$$\begin{aligned} f(x+1) &= \frac{(x+1)^5 - 1}{(x+1) - 1} && (239) \\ &= \frac{1}{x}\left(x^5 + \binom{5}{1}x^4 + \binom{5}{2}x^3 + \binom{5}{3}x^2 + \binom{5}{4}x + \binom{5}{5} - 1\right) && (240) \\ &= x^4 + 5x^3 + 10x^2 + 10x + 5 && (241) \end{aligned}$$

So all nonleading coefficients are divisible by 5 exactly once, which by Eisenstein implies that $f(x+1)$ is irreducible which implies that $f(x)$ is irreducible.

We have prod that for $\alpha \in \mathbb{C}$, subfield $F \subset \mathbb{C}$, and $f(x) \in F[x]$, with $f(\alpha) = 0$, then $B = \{1, \alpha, \ldots, \alpha^{\deg(f)-1}\}$ spans $F[\alpha]$ as a F-vector space. If $f(x)$ is irreducible then B is a basis.

4 Polynomial Rings

One of the most widely studied rings are the ring of polynomials. Let's reintroduce them.

Definition 4.1 (Univariate Polynomials)

For a ring R, the **univariate polynomial ring over** R, denoted $R[x]$ consists of elements called **polynomials** which are formal expressions of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \text{ where } a_i \in R \tag{242}$$

with coefficients $a_i \in R$ and x is called a **variable**, or **indeterminant**.[a] Two polynomials are equal if and only if the sequences of their corresponding coefficients are equal. We can also see a polynomial as a function $f : R \to R$ as well.
Furthermore, $R[x]$ is a ring, with addition and multiplication defined

$$a_i x^i + b_i x^i = (a_i + b_i) x^i, \qquad x^i x^j = x^{i+j} \tag{243}$$

along with 0 as the additive identity and 1 as the multiplicative identity.

[a] Note that x is just a formal symbol, whose powers x^i are just placeholders for the corresponding coefficients a_i so that the given formal expression is a way to encode the finitary sequence. $(a_0, a_1, a_2, ..., a_n)$.

While we will mainly deal with univariate polynomials, we can also define multivariate polynomials similarly.

Definition 4.2 (Multivariate Polynomials)

For a ring R, the **multivariate polynomial ring over** R, denoted $R[x_1, \dots, x_n]$ consists of elements called **polynomials** which are formal expressions of the form

$$f(x_1, \dots, x_n) = \sum_{0 \leq k_i \leq n} a_{k_1 \dots k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n} \tag{244}$$

with coefficients $a \in R$ and x_i's the **variables**. We can treat an element $f \in R[x_1, \dots, x_n]$ as a function $f : R^n \to R$.
Furthermore, $R[x_1, \dots, x_n]$ is a ring, with addition and multiplication defined

$$a_{k_1 \dots k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n} + b_{k_1 \dots k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n} = (a_{k_1 \dots k_n} + b_{k_1 \dots k_n}) x_1^{k_1} x_2^{k_2} \dots x_n^{k_n} \tag{245}$$

$$x^{k_1 \dots k_n} x^{l_1 \dots l_n} = x^{k_1 + l_1, k_2 + l_2, \dots, k_n + l_n} \tag{246}$$

Usually, the properties of the base ring R determines the properties on R.

Lemma 4.1 (Commutativity Extends to Polynomials)

We have the following.

1. R is a commutative ring iff $R[x]$ is a commutative ring.
2. R is an integral domain iff $R[x]$ is an integral domain.
3. F is a field iff $F[x]$ is a Euclidean domain.

Proof.

TBD.

With this theorem we unlock all the properties that we have studied in general for the subclasses of rings. Almost always we will assume that R is at least commutative, so let's get that out of the way. Before we move on, let's get some terms out of the way.

Definition 4.3 (Some Terms for Polynomials)

Given a univariate polynomial $f(x)$.

1. The **leading coefficient** is the last nonzero coefficient
2. The **degree** of f—denoted $\deg f$—is the index of the leading coefficient.
3. A **monomial** is a polynomial of a single term $a_j x^j$.
4. A **linear** polynomial is a polynomial of degree 1.
5. A **quadratic** polynomial is a polynomial of degree 2.
6. A **cubic** polynomial is a polynomial of degree 3.

4.1 Basic Properties of Polynomials

We need to be very careful about the properties that hold for polynomials, as they may not be intuitive. For example, for certain finite fields (which are rings), some formally different polynomials may be indistinguishable in terms of mappings.[5] Second, a polynomial may have more roots than its degree. Therefore, we will work in different rings R and provide conditions where our intuition is true in $R[x]$. It is clear that if you have two polynomials of degree n and m, their sum may be degree $k < n, m$. This is not always true for multiplication.

Example 4.1 (Product of Two Linear Polynomials is 0)

Given $f, g \in \mathbb{Z}_6[x]$ with $f(x) = 2x + 4$ and $g(x) = 3x + 3$, we have

$$f(x) \cdot g(x) = (2x+4)(3x+3) = 6x^2 + 18x + 12 = 0 \tag{247}$$

There is a simple condition in which the degree is additive, however.

Theorem 4.1 (Bounds on Degrees From Operations)

Given that R is a ring and $f, g \in R[x]$,

$$\deg(f+g) \leq \max\{\deg f, \deg g\} \tag{248}$$

If R is a domain, then

$$\deg(fg) = \deg f + \deg g \tag{249}$$

Note that this automatically implies that $R[x]$ is a domain. Combined with the lemma above, we have: R is an integral domain $\implies$ $R[x]$ is an integral domain.

Proof.

The second may not be true if R has zero divisors.

Just working in domains do not make things all better. Sometimes, we may have two different polynomials but they may define the same function from R to R!

Example 4.2 (Polynomials as Same Function)

Given $f, g \in \mathbb{Z}_2[x]$,

$$f(x) = x \sim g(x) = x^2 \tag{250}$$

As shown in the example above, it is not so simple as to restrict which underlying set you are working on. Some rings R may or may not assert uniqueness of functions in $F[x]$, and vice versa. Therefore, here are

[5] x and x^2 are equivalent in the polynomial algebra defined on the domain $\mathbb{Z}_2$.

some special theorems.

Theorem 4.2 (Uniqueness of Polynomials over Field)

If the field $\mathbb{F}$ is infinite, then different polynomials in $\mathbb{F}[x]$ determine different functions.

4.1.1 Euclidean Division

Just like how we can do Euclidean division with integers, there is an analogous result for polynomials. However, we require to work with a *field* F rather than an arbitrary ring R.

Theorem 4.3 (Polynomials as Euclidean Domain)

Given a field F, $F[x]$ is a Euclidean domain. That is, given polynomials $f(x), g(x) \in F[x]$, there are unique polyomials $q(x), r(x) \in F[x]$ s.t.

$$f(x) = q(x)g(x) + r(x), \qquad \deg(r(x)) < \deg(g(x)) \tag{251}$$

Proof.

We first prove existence. If $\deg(f(x)) < \deg(g(x))$, then we can trivially set $q(x) = 0, r(x) = f(x)$. Therefore we can assume that $\deg(f(x)) \geq \deg(g(x))$. We can prove this by strong induction on $k = \deg(f(x))$. Assume that $\deg(f(x)) = 1$. Then if $\deg(g(x)) > 1$ it is trivial as before, so we show for $\deg(g(x)) = 1$. So let

$$f(x) = a_1 x + a_0, \qquad g(x) = b_1 x + b_0 \tag{252}$$

and we can find the solutions

$$f(x) = \frac{a_1}{b_1} g(x) + \bigg(a_0 - \frac{a_1 b_0}{b_1} \bigg) \tag{253}$$

Now suppose that the results is known for whenver $\deg(f(x)) \leq k$ and we have a polynomial $F(x) = a_{k+1}x^{k+1} + \ldots a_0$ of degree $k+1$. Then we must check that there exists a quotient and remainder for $0 \leq \deg(g(x)) = m \leq k+1$. Note that the coefficients of x^{k+1} in $F(x)$ and in the polynomial $\frac{a_{k+1}}{b_m} x^{k+1-m} g(x)$ are the same, so the polynomial

$$f(x) = F(x) - \frac{a_{k+1}}{b_m} x^{k+1-m} g(x) \tag{254}$$

has degree at most k. Thus by our induction hypothesis we can write $f(x) = q(x)g(x) + r(x)$, and so

$$\begin{aligned} F(x) &= f(x) + \frac{a_{k+1}}{b_m} x^{k+1-m} g(x) && (255) \\ &= q(x)g(x) + r(x) + \frac{a_{k+1}}{b_m} x^{k+1-m} g(x) && (256) \\ &= \bigg(q(x) + \frac{a_{k+1}}{b_m} x^{k+1-m} \bigg) g(x) + r(x) && (257) \end{aligned}$$

which is indeed a decomposition. Now to prove uniqueness, suppose we had two different decompositions

$$f(x) = q(x)g(x) + r(x) = q'(x)g(x) + r'(x) \implies \big(q(x) - q'(x)\big)g(x) = r(x) - r'(x) \tag{258}$$

IF $q(x) \neq q'(x)$, then the degree of the LHS is at least $\deg(g(x))$, while the degree of the RHS must be strictly less, a contradiction.

Example 4.3 (Polynomials over Fields)

The algorithimc way to get such $q(x), r(x)$ is through *polynomial long division.*

$$
\begin{array}{rrrrr}
 & & x^2 & +6x & +11 \\ \cline{2-5}
x-2\big) & x^3 & +4x^2 & -x & +7 \\
 & -x^3 & +2x^2 & & \\ \cline{2-3}
 & & 6x^2 & -x & \\
 & & -6x^2 & +12x & \\ \cline{3-4}
 & & & 11x & +7 \\
 & & & -11x & +22 \\ \cline{4-5}
 & & & & 29
\end{array}
$$

Given field $\mathbb{Z}_5$, $\mathbb{Z}_5[x]$ is a Euclidean domain, with Euclidean division.

In fact, it turns out that you don't necessarily require a polynomial to always come from a field in order to do long division. You can do polynomial long division over *any* commutative rings, as long as the leading coefficient of the divisor is a unit (and since all elements of a field are units, we can do so). This is because at each step, you only need to divide the leading coefficient of the divisor into the leading coefficient of the polynomial you have left. An immediate consequence of this theorem is the following.

Corollary 4.1 (Remainder Theorem)

Let $c \in F$ and $f(x) \in F[x]$. When we divide $f(x)$ by $g(x) = x - c$, the remainder is $f(c)$.

Proof.

By the Euclidean algorithm,

$$f(x) = (x-c)q(x) + r(x) \implies f(c) = (c-c)q(c) + r(c) = r(c) \tag{259}$$

4.1.2 Roots and Factorization

Next, we can define the all too familiar factors and roots of a polynomial.

Definition 4.4 (Factor)

Given a ring R and a polynomial $f(x) \in R[x]$, if there exists $g(x), h(x)$ of degree at least 1 such that

$$f(x) = g(x)h(x) \tag{260}$$

then g, h are said to be **factors**, or **divisors**, of f. If there are no such factors of f, then $f(x)$ is said to be **irreducible**.

Irreducible polynomials are analogous to prime numbers in $\mathbb{Z}$.

Definition 4.5 (Polynomial Root)

An element $r \in R$ is a **root** of polynomial $f \in R[x]$ if and only if

$$f(r) = 0 \tag{261}$$

Note that both factors and roots are intimately tied to Euclidean division, so the two are closely related.

Theorem 4.4 (Root-Factor Theorem)

Given a commutative ring R (usually R is a field) and $f(x) \in R[x]$, $(x-c)$ is a factor of $f(x)$, i.e. can be factored into

$$f(x) = (x-c)q(x) \tag{262}$$

for some $q(x) \in R[x]$ of degree $\deg(f) - 1$ if and only if $f(c) = 0$.[a]

[a] Note that this is not true for an arbitrary ring. R must be commutative at least.

Proof.

We prove for when R is a field F, but it turns out that the theorem also holds for commutative rings R.

1. $(\rightarrow)$. Given that $(x-c)$ is a factor of $f(x)$, this means that by the Euclidean algorithm $f(x) = (x-c)q(x)$ for some $q(x)$, and so $f(c) = (c-c)q(c) = 0$.
2. $(\leftarrow)$. Given that $f(c) = 0$. By the remainder theorem this means that when we divide $f(x)$ by $(x-c)$, the remainder is $f(c) = 0$, and so $f(x) = (x-c)q(x) + 0 = (x-c)q(x) \implies (x-c)$ is a factor of $f(x)$.

Notice how these polynomials mimick integers, and to drive this point even further, let's introduce the greatest common divisor.

Theorem 4.5 (GCD of Two Polynomials Exist)

Given nonzero polynomials $f(x), g(x) \in F[x]$, let

$$S = \{h(x) \in F[x] \mid h(x) = a(x)f(x) + b(x)g(x) \text{ for some } a(x), b(x) \in F[x]\} \tag{263}$$

Then there exists some polynomial $d(x) \in S$ of smallest degree, and every $h(x) \in S$ is divisible by $d(x)$.

Proof.

The existence is trivial since by the well-ordering principle on the degrees of polynomials in S, such a minimal degree must exist. Now we prove the second claim by proving $d(x) \mid f(x)$. We apply the division algorithm to write

$$f(x) = q(x)d(x) + r(x) \tag{264}$$

If $r(x) = 0$, then by root factor theorem we are done. If $r(x) \neq 0$, we then write

$$\begin{aligned} r(x) &= f(x) - q(x)d(x) && (265)\\ &= f(x) - \big(s(x)f(x) + t(x)g(x)\big)q(x) && (266)\\ &= \big(1 - s(x)q(x)\big)f(x) - \big(t(x)q(x)\big)g(x) \in S && (267) \end{aligned}$$

Since $r(x) \in S$ due to its form, the fact that $\deg(r(x)) < \deg(d(x))$ contradicts the way that $d(x)$ was chosen. Therefore $r(x) = 0$. It turns out that $d(x)$ is unique up to a constant factor.

Definition 4.6 (GCD)

$d(x)$ as above is called the **greatest common divisor** of $f(x), g(x)$, denoted $d(x) = \gcd(f(x), g(x))$ satisfying

1. $d(x) \mid f(x)$, $d(x) \mid g(x)$, and
2. $\forall e(x) \in F[x]$, if $e(x) \mid f(x)$ and $e(x) \mid g(x)$, then $e(x) \mid d(x)$.

$f(x), g(x)$ are said to be **relatively prime** if $\gcd(f(x), g(x)) = 1$.

The algorithmic way for computing the GCD is done the same way by performing Euclidean algorithm on two polynomials: dividing on by the other, taking the remainder, and dividing the lesser degree by the remainder again, until the remainder is 0.

Lemma 4.2 ()

Suppose $f(x)$ is irreducible and $f(x) \mid g(x)h(x)$. Then $f(x) \mid g(x)$ or $f(x) \mid h(x)$.

Now, we show an extremely important theorem. This should be intuitive since F a field implies $F[x]$ a Euclidean domain, which is a PID, which has the unique factorization theorem.

Theorem 4.6 (Unique Factorization of Polynomials over Fields)

Given field F and nonconstant polynomial $f(x) \in F[x]$ of degree n, we can always write $f(x)$ as a unique[a] product of at most n irreducible polynomials in $F[x]$.

[a] up to constant factors and rearrangement

Proof.

To prove the bound, the general idea is that by the root factor theorem, each root gives rise to a linear factor, and so inductively we cannot have more than n linear factors. Strong induction on degree of $f(x)$ by starting with linear.

Note that this is *not* true in arbitrary rings.

Example 4.4 (Linear Polynomial with 3 Roots)

Consider $f(x) = x^2 - 1 \in \mathbb{Z}_8[x]$, a commutative ring. Then $1, 3, 5, 7$ are all roots of $f(x)$, which is greater than its degree. Furthermore, it has two different factorizations

$$x^2 - 1 = (x+1)(x-1) = (x+3)(x-3) \tag{268}$$

Theorem 4.7 (Interpolation)

For any collection of given field values $y_1, y_2, ..., y_n \in F$ at given distinct points $x_1, x_2, ..., x_n \in F$, there exists a unique polynomial $f \in F[x]$ with $\deg f < n$ such that

$$f(x_i) = y_i, \quad i = 1, 2, ..., n \tag{269}$$

This is commonly known as the **interpolation problem**, and when $n = 2$, this is called **linear interpolation**.

4.2 Exercises

Exercise 4.1 (Shifrin 3.1.2.c/d)

Find the greatest common divisors $d(x)$ of the following polynomials $f(x), g(x) \in F[x]$, and express $d(x)$ as $s(x)f(x) + t(x)g(x)$ for appropriate $s(x), t(x) \in F[x]$:

1. $f(x) = x^3 - 1$, $g(x) = x^4 + x^3 - x^2 - 2x - 2$, $F = \mathbb{Q}$

2. $f(x) = x^2 + (1-\sqrt{2})x - \sqrt{2}$, $g(x) = x^2 - 2$, $F = \mathbb{R}$
3. $f(x) = x^2 + 1$, $g(x) = x^2 - i + 2$, $F = \mathbb{C}$
4. $f(x) = x^2 + 2x + 2$, $g(x) = x^2 + 1$, $F = \mathbb{Q}$
5. $f(x) = x^2 + 2x + 2$, $g(x) = x^2 + 1$, $F = \mathbb{C}$

Solution 4.1

For (c), the gcd is 1, with

$$-\frac{1}{1-i}(x^2+1) + \frac{1}{1-i}(x^2 - i + 2) = \frac{1}{1-i}(x^2 - i + 2 - x^2 - 1) = \frac{1}{1-i}(1-i) = 1 \tag{270}$$

where $1/(1-i) = (1+i)/2$. For (d), the gcd is 1, with

$$\frac{1}{5}(2x+3)(x^2+1) + \frac{1}{5}(1-2x)(x^2+2x+2) \tag{271}$$

$$= \frac{1}{5}(2x^3 + 3x^2 + 2x + 3) + \frac{1}{5}(-2x^3 - 3x^2 - 2x + 2) = 1 \tag{272}$$

Exercise 4.2 (Shifrin 3.1.6)

Prove that if F is a field, $f(x) \in F[x]$, and $\deg(f(x)) = n$, then $f(x)$ has at most n roots in F.

Solution 4.2

We start when $n = 1$. Then $f(x) = mx + b$ and we claim that the only root is $x = -b/m$ since we can solve for $0 = mx + b$ with the field operations, which leads to a unique solution. This implies by corr 1.5 that $(x + b/m)$ is the only factor of f. Now suppose this holds true for some degree $n-1$ and let us have a degree n polynomial f. Assume that some c is a root of f (if there exists no c, then we are trivially done), which means $(x - c)$ is a factor of f, and we can write

$$f(x) = (x-c)\,g(x) \tag{273}$$

for some polynomial $g(x)$ of degree $n-1$. By our inductive hypothesis, $g(x)$ must have at most $n-1$ roots, and so f has at most n roots.

Exercise 4.3 (Shifrin 3.1.8)

Let F be a field. Prove that if $f(x) \in F[x]$ is a polynomial of degree 2 or 3, then $f(x)$ is irreducible in $F[x]$ if and only if $f(x)$ has no root in F.

Solution 4.3

We prove bidirectionally.

1. ($\rightarrow$). Let f be irreducible. Then it cannot be factored into polynomials $p(x)q(x)$ where $\deg(p) + \deg(q) = n$. Note that two positive integers adding up to 2 or 3 means that at least one of the integers must be 1, by the pigeonhole principle. This means that f irreducible is equivalent to saying that f does not have linear factors of form $(x - c)$, which by corollary 1.5 implies that there exists no root c for $f(x)$.
2. ($\leftarrow$). Let f have no root in F. Then by corollary 1.5 there exists no linear factors $(x - c)$. By the same pigeonhole principle argument, we know that having a linear factor for degree 2 or 3 polynomials is equivalent to having (general) factors, and so f has no factors. Therefore f is

irreducible.

Exercise 4.4 (Shifrin 3.1.13)

List all the irreducible polynomials in $\mathbb{Z}_2[x]$ of degree ≤ 4. Factor $f(x) = x^7 + 1$ as a product of irreducible polynomials in $\mathbb{Z}_2[x]$.

Solution 4.4

Listed by degree.

1. 1: $x, x+1$.
2. 2: $x^2 + x + 1$.
3. 3: $x^3 + x^2 + 1, x^3 + x + 1$.
4. 4: $x^4 + x + 1, x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1$.

We have

$$\begin{aligned} x^7 + 1 &= (x+1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) && (274) \\ &= (x+1)(x^3 + x + 1)(x^3 + x^2 + 1) && (275) \end{aligned}$$

Exercise 4.5 (Shifrin 3.2.2.b/c)

Prove that

1. $\mathbb{Q}[\sqrt{2}, i] = \mathbb{Q}[\sqrt{2} + i]$, but $\mathbb{Q}[\sqrt{2}i] \subsetneq \mathbb{Q}[\sqrt{2}, i]$
2. $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$, but $\mathbb{Q}[\sqrt{6}] \subsetneq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$
3. $\mathbb{Q}[\sqrt[3]{2} + i] = \mathbb{Q}[\sqrt[3]{2}, i]$; what about $\mathbb{Q}[\sqrt[3]{2}i] \subset \mathbb{Q}[\sqrt[3]{2}, i]$?

Solution 4.5

From Shifrin, I use the fact that $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, and the same proof immediately shows that $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ along with that for $\mathbb{Q}[\sqrt{6}]$. As for $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$, I also follow the same logic to show

$$\begin{aligned} \mathbb{Q}[\sqrt{2}, \sqrt{3}] &= \mathbb{Q}[\sqrt{2}][\sqrt{3}] && (276) \\ &= \{\alpha + \beta\sqrt{3} \mid a, b \in \mathbb{Q}[\sqrt{2}]\} && (277) \\ &= \{(a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3} \mid a, b, c, d \in \mathbb{Q}\} && (278) \\ &= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\} && (279) \end{aligned}$$

Where $\sqrt{2} \times \sqrt{3} = \sqrt{2 \times 3} = \sqrt{6}$ follows from the definition of nth roots plus associativity on the reals. For (b), we prove bidirectionally.

1. $\mathbb{Q}[\sqrt{2} + \sqrt{3}] \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Consider $y \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Then there exists $p \in \mathbb{Q}[x]$ s.t.

$$y = p(\sqrt{2} + \sqrt{3}) = a_n(\sqrt{2} + \sqrt{3})^n + \ldots + a_1(\sqrt{2} + \sqrt{3}) + a_0 \qquad (280)$$

   where the terms can be expanded an rearranged to the form $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.
2. $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \subset \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Consider $\sqrt{2} + \sqrt{3} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Since it is a field and $\sqrt{2} + \sqrt{3}$ is a unit, by rationalizing the denominator, we can get

$$(\sqrt{2} + \sqrt{3})^{-1} = \frac{\sqrt{2} - \sqrt{3}}{2 - 3} = \sqrt{3} - \sqrt{2} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}] \qquad (281)$$

   Therefore by adding and subtracting the two elements, we have $\sqrt{2}, \sqrt{3} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}] \implies \sqrt{6} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Since $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2} + \sqrt{3}]$, from the ring properties all elements of the form $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$.

For the second part, I claim that $\sqrt{2} \notin \mathbb{Q}[\sqrt{6}]$. Assuming it is, we have $\sqrt{2} = a + b\sqrt{6} \implies 2 = a^2 + 6b^2 + 2ab\sqrt{6}$. So $a = 0$ or $b = 0$. If $a = 0$, then $b^2 = 1/3 \implies b = 1/\sqrt{3}$ which contradicts that b is rational. If $b = 0$, then $a^2 = 2 \implies a = \sqrt{2}$ which contradicts that a is rational.

Solution 4.6

Note that $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4}\}$, and so

$$\begin{aligned}
\mathbb{Q}[\sqrt[3]{2}, i] &= \mathbb{Q}[\sqrt[3]{2}][i] && (282)\\
&= \{\alpha + \beta i \mid \alpha, \beta \in \mathbb{Q}[\sqrt[3]{2}]\} && (283)\\
&= \{(a + b\sqrt[3]{2} + c\sqrt[3]{4}) + (d + e\sqrt[3]{2} + f\sqrt[3]{4})i \mid a, b, c, d, e, f \in \mathbb{Q}\} && (284)\\
&= \{a + b\sqrt[3]{2} + c\sqrt[3]{4} + di + e\sqrt[3]{2}i + f\sqrt[3]{4}i \mid a, b, c, d, e, f \in \mathbb{Q}\} && (285)
\end{aligned}$$

We prove bidirectionally.

1. $\mathbb{Q}[\sqrt[3]{2} + i] \subset \mathbb{Q}[\sqrt[3]{2}, i]$. Consider $y \in \mathbb{Q}[\sqrt[3]{2} + i]$. Then there exists a $p \in \mathbb{Q}[x]$ s.t.

$$y = p(\sqrt[3]{2} + i) = a_n(\sqrt[3]{2} + i)^n + \ldots + a_1(\sqrt[3]{2} + i) + a_0 \qquad (286)$$

   Then we can expand and rearrange the terms to be of the form

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} + di + ei\sqrt[3]{2} + fi\sqrt[3]{4} \in \mathbb{Q}[\sqrt[3]{2}, i] \qquad (287)$$

2. $\mathbb{Q}[\sqrt[3]{2}, i] \subset \mathbb{Q}[\sqrt[3]{2} + i]$. Consider $\alpha = \sqrt[3]{2} + i \in \mathbb{Q}[\sqrt[3]{2} + i]$. Then $(\alpha - i)^3 = 2$. Therefore

$$\begin{aligned}
\alpha^3 - 3\alpha^2 i - 3\alpha + i = 2 &\implies i(1 - 3\alpha^2) = 2 + 3\alpha - \alpha^3 && (288)\\
&\implies i = \frac{2 + 3\alpha - \alpha^3}{1 - 3\alpha^2} \in \mathbb{Q}[\sqrt[3]{2} + i] && (289)
\end{aligned}$$

   Therefore $\sqrt[3]{2} = \alpha - i \in \mathbb{Q}[\sqrt[3]{2} + i]$, which allows us add all combinations $\{1, \sqrt[3]{2}, \sqrt[3]{4}, i, \sqrt[3]{2}i, \sqrt[3]{4}i\}$ into our basis.

Exercise 4.6 (Shifrin 3.2.6.b/c/d/g)

Suppose $\alpha \in \mathbb{C}$ is a root of the given irreducible polynomial $f(x) \in \mathbb{Q}[x]$. Find the multiplicative inverse of $\beta \in \mathbb{Q}[\alpha]$.

1. $f(x) = x^2 + 3x - 3$, $\beta = \alpha - 1$
2. $f(x) = x^3 + x^2 - 2x - 1$, $\beta = \alpha + 1$
3. $f(x) = x^3 + x^2 + 2x + 1$, $\beta = \alpha^2 + 1$
4. $f(x) = x^3 - 2$, $\beta = \alpha + 1$
5. $f(x) = x^3 + x^2 - x + 1$, $\beta = \alpha + 2$
6. $f(x) = x^3 - 2$, $\beta = r + s\alpha + t\alpha^2$
7. $f(x) = x^4 + x^2 - 1$, $\beta = \alpha^3 + \alpha - 1$

Solution 4.7

For (b), using the Euclidean algorithm gives

$$(1)(x^3 + x^2 - 2x - 1) + (-x^2 + 2)(x + 1) = 1 \qquad (290)$$

and substituting the root α gives $(-\alpha^2 + 2)(\alpha + 1) = 1$. So we have $\beta^{-1} = -\alpha^2 + 2$. For (c), doing the same thing gives

$$(-x)(x^3 + x^2 + 2x + 1) + (x^2 + x + 1)(x^2 + 1) = 1 \qquad (291)$$

and substituting α gives $(\alpha^2+\alpha+1)(\alpha^2+1)=1$, so $\beta^{-1}=\alpha^2+\alpha+1$. For (d), we have

$$(-\frac{1}{3})(x^3-2)+(\frac{1}{3}x^2-\frac{1}{3}x+\frac{1}{3})(x+1)=1 \tag{292}$$

and so substituting α gives $(\frac{1}{3}\alpha^2-\frac{1}{3}\alpha+\frac{1}{3})(\alpha+1)=1$, so $\beta^{-1}=\frac{1}{3}\alpha^2-\frac{1}{3}\alpha+\frac{1}{3}$. For (g), we have

$$(-x^2-x-2)(x^4+x^2-1)+(x^3+x^2+2x+1)(x^3+x-1)=1 \tag{293}$$

and so substituting α gives $(\alpha^3+\alpha^2+2\alpha+1)(\alpha^3+\alpha-1)=1$, and so $\beta^{-1}=\alpha^3+\alpha^2+2\alpha+1$.

Exercise 4.7 (Shifrin 3.2.7)

Let $f(x)\in\mathbb{R}[x]$.

1. Prove that the complex roots of $f(x)$ come in "conjugate pairs"; i.e., $\alpha\in\mathbb{C}$ is a root of $f(x)$ if and only if $\overline{\alpha}$ is also a root.
2. Prove that the only irreducible polynomials in $\mathbb{R}[x]$ are linear polynomials and quadratic polynomials ax^2+bx+c with $b^2-4ac<0$.

Solution 4.8

Listed.

1. If $\alpha\in\mathbb{C}$ is a root of f, then

$$0=f(\alpha)=a_n\alpha^n+\ldots+a_1\alpha+a_0 \tag{294}$$

for $a_i\in\mathbb{R}$. Since

$$\begin{aligned}0=\overline{0}&=\overline{f(\alpha)} && (295)\\ &=\overline{a_n\alpha^n+\ldots+a_1\alpha+a_0} && (296)\\ &=\overline{a_n}\overline{\alpha}^n+\ldots+\overline{a_1}\overline{\alpha}+\overline{a_0} && (297)\\ &=a_n\overline{\alpha}^n+\ldots+a_1\overline{\alpha}+a_0 && (298)\\ &=p(\overline{\alpha}) && (299)\end{aligned}$$

we can see that $\overline{\alpha}\in\mathbb{C}$ is immediately a root as well. Since $\overline{\overline{\alpha}}=\alpha$, the converse is immediately proven.

2. Linear polynomials in $F[x]$ for a given field are trivially irreducible (since multiplying polynomials increases the degree of the product as there are no zero divisors in a field). Perhaps without Theorem 4.1, we can assume that a real quadratic polynomial $p(x)=ax^2+bx+c$ is reducible, which is equivalent to

$$p(x)=(dx+e)(fx+g)=dfx^2+(dg+ef)x+eg \tag{300}$$

For $d,e,f,g\in\mathbb{R}$, and evaluating $b^2-4ac=(dg+ef)^2-4dfeg=(dg-ef)^2\geq 0$ since this is a squared term of a real number. So we have proved that if it is quadratic and reducible, then the discriminant ≥ 0. To prove the other way, we assume that it is not reducible, i.e. there exists some complex root α from the fundamental theorem of algebra. Then from (1), we know that $\overline{\alpha}$ must also be a complex conjugate. Then this is reducible in $\mathbb{C}$ as

$$p(x)=a(x-\alpha)(x-\overline{\alpha}) \tag{301}$$

for some constant factor a. Letting $\alpha=d+ei$ for $d,e\in\mathbb{R}$, expanding it gives us

$$\begin{aligned}p(x)&=a\big(x^2-(\alpha+\overline{\alpha})x+\alpha\overline{\alpha}\big) && (302)\\ &=ax^2+-2adx+a(d^2+e^2) && (303)\end{aligned}$$

and evaluating the discriminant gives

$$4a^2d^2 - 4a^2(d^2+e^2) = -4a^2e^2 < 0 \tag{304}$$

and we are done. For higher degree polynomials, we can proceed by taking a complex root (which is guaranteed to exist by fundamental theorem of algebra). If it contains an imaginary term, then its conjugate is also a root, and we factor out the quadratic. If it is real, then we can factor out the linear term. We can keep going this until we hit our base cases of a quadratic or linear term.

Exercise 4.8 (Shifrin 3.2.13)

Let K be a field extension of F, and suppose $\alpha, \beta \in K$. Show that $(F[\alpha])[\beta] = (F[\beta])[\alpha]$, so that $F[\alpha, \beta]$ makes good sense.
(Remark: One way to do this is to think about the ring of polynomials in two variables. The other way is just to show directly that every element of one ring belongs to the other.)

Solution 4.9

Let $y \in (F[\alpha])[\beta]$. Then there exists a polynomial $p \in (F[\alpha])[x]$ s.t.

$$y = p(\beta) = b_n\beta^n + \ldots + b_1\beta + b_0 = \sum_{i=0}^{n} b_i\beta^i \tag{305}$$

for $b_i \in F[\alpha]$. But since $b_i \in F[\alpha]$, there exists a polynomial $q_i \in F[x]$ s.t. (omitting the subscript i for clarity)

$$b_i = q_i(\alpha) = a_{n_i}\alpha^n + \ldots + a_1\alpha + a_0 = \sum_{j=0}^{n_i} a_j\alpha^j \tag{306}$$

for $a_j \in F$. Substituting each b_i in gives

$$y = \sum_{i=0}^{n}\left(\sum_{j=0}^{n_i} a_j\alpha^j\right)\beta^i = \sum_{i=0}^{n}\sum_{j=0}^{n_i} a_j\alpha^j\beta^i \tag{307}$$

With the same logic, every element of $(F[\beta])[\alpha]$ can be written as

$$y = \sum_{i=0}^{n}\left(\sum_{j=0}^{n_i} a_j\beta^j\right)\alpha^i = \sum_{i=0}^{n}\sum_{j=0}^{n_i} a_j\alpha^i\beta^j \tag{308}$$

Note that since $F[\alpha]$ is a vector space spanned by $\{1, \ldots, \alpha^{n-1}\}$, and $F[\beta]$ is a also a vector space spanned by $\{1, \ldots, \beta^{m-1}\}$ for some m, the two spaces above are spanned by all products $\{\alpha^i\beta^j\}_{i<n, j<m}$, and they are the same set.

Exercise 4.9 (Shifrin 3.3.2.a/d/e/g)

Decide which of the following polynomials are irreducible in $\mathbb{Q}[x]$.

a $f(x) = x^3 + 4x^2 - 3x + 5$
1. $f(x) = 4x^4 - 6x^2 + 6x - 12$
2. $f(x) = x^3 + x^2 + x + 1$

d $f(x) = x^4 - 180$
e $f(x) = x^4 + x^2 - 6$

3. $f(x) = x^4 - 2x^3 + x^2 + 1$
g $f(x) = x^3 + 17x + 36$
4. $f(x) = x^4 + x + 1$
5. $f(x) = x^5 + x^3 + x^2 + 1$
6. $f(x) = x^5 + x^3 + x + 1$

Solution 4.10

For (a), by the rational root theorem the rational roots, if any, must be in the set $\{\pm 1, \pm 5\}$. Calculating them gives $f(x) = 7, 11, 215, -5$. Since this is third degree, no linear factors means that it is irreducible, so f is irreducible.
For (d), by the Eisenstein's criterion with $p = 5$ this polynomial is irreducible.
For (e), the rational root theorem states that the rational roots must be in $\{\pm 1, \pm 2, \pm 3, \pm 6\}$. This polynomial is clearly even, so it suffices to check the positive candidates. This gives $-4, 14, 84, 1326$. Therefore if it is reducible, by Gauss's lemma it must be of the form

$$(ax^2 + bx + c)(dx^2 + ex + f) \tag{309}$$

for integer coefficients. $a = d = 1$ is trivial ($-1, -1$ is also possible but constant factors don't matter). Expanding this gives

$$x^4 + (b + e)x^3 + (c + f + be)x^2 + (bf + ce)x + cf = x^4 + x^2 - 6 \tag{310}$$

The coefficients of x^3 tell us that $e = -b$, which means that for the coefficents of x, $bf + ce = bf - bc = 0 \implies f = c$. So $c^2 = -6$, which has no solution. Therefore f is irreducible.
For (g), we must check rational roots of $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 9, \pm 12, \pm 18, \pm 36\}$. Since this polynomial is monotonically increasing, with $f(-2) = -6$ and $f(0) = 36$. It only suffices to check $x = -1$, which gives $f(-1) = 18$. Therefore there are no linear factors. Since this is third degree, no linear factors means that it is irreducible, so f is irreducible.

Exercise 4.10 (Shifrin 3.3.4)

Show that each of the following polynomials has no rational root:
1. $x^{200} - x^{41} + 4x + 1$
2. $x^8 - 54$
3. $x^{2k} + 3x^{k+1} - 12$, $k \geq 1$

Solution 4.11

Listed.
1. By the rational root theorem, the only possible rational roots are ± 1. Solving for both of these values gives
$$f(1) = 1 - 1 + 4 + 1 = 5 \tag{311}$$
$$f(-1) = 1 + 1 - 4 + 1 = -1 \tag{312}$$
Therefore there are no rational roots.
2. The only possible rational roots are $\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18, \pm 27, \pm 54$. But this polynomial is even, so it suffices to check the positive roots. $f(1) = -53$, $f(2) = 256 - 54 = 202$, and any greater inputs will increase the output since f is monotonic in $\mathbb{Z}^+$. Therefore f has no rational roots.
3. By Eisenstein's criterion with $p = 3$, this polynomial is irreducible and therefore has no rational roots.

Exercise 4.11 (Shifrin 3.3.6)

Listed.

1. Prove that $f(x) \in \mathbb{Z}_2[x]$ has $x+1$ as a factor if and only if it has an even number of nonzero coefficients.
2. List the irreducible polynomials in $\mathbb{Z}_2[x]$ of degrees $2, 3, 4$, and 5.

Solution 4.12

Listed. Since $f(x)$ has $x+1$ as a factor iff

$$f(1) = a_n 1^n + \ldots + a_1 1^1 + a_0 = a_n + \ldots + a_1 + a_0 = 0 \tag{313}$$

where each $a_i \in \{0, 1\}$. Therefore, this is equivalent to saying that there are an even number of 1's (nonzero coefficients), which sum to 0 mod 2. Therefore, the irreducible polynomials should at least have a constant coefficient of 1 (so we can't factor x) and should have odd number of terms (so that we can't factor $x+1$). This will guarantee that $f(0) = f(1) = 1$.

1. Degree 2: $x^2 + x + 1$ is the only candidate and indeed is an irreducible polynomial.
2. Degree 3: $x^3 + x^2 + 1$, $x^3 + x + 1$ and indeed $f(0) = f(1) = 1$. Since it's only degree 3 we don't need to check irreducibility into 2 terms of both degree at least 2.
3. Degree 4: $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$, $x^4 + x^2 + 1$, $x^4 + x + 1$ are candidates. However we need to check that they cannot be factored into two irreducible quadratic polynomials. The only possible such factorization is

$$(x^2 + x + 1)(x^2 + x + 1) = x^4 + x^2 + 1 \tag{314}$$

and so the irreducible polynomials are $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$, $x^4 + x + 1$.

4. Degree 5: $x^5 + x^4 + 1$, $x^5 + x^3 + 1$, $x^5 + x^2 + 1$, $x^5 + x + 1$, $x^5 + x^4 + x^3 + x^2 + 1$, $x^5 + x^4 + x^3 + x + 1$, $x^5 + x^4 + x^2 + x + 1$, $x^5 + x^3 + x^2 + x + 1$ are the possible candidates. But we need to check that it is not factorable into an irreducible quadratic and cubic. The three candidates are

$$(x^2 + x + 1)(x^3 + x^2 + 1) = x^5 + x + 1 \tag{315}$$

$$(x^2 + x + 1)(x^3 + x + 1) = x^5 + x^4 + 1 \tag{316}$$

and so the irreducible polynomials are $x^5 + x^3 + 1$, $x^5 + x^2 + 1$, $x^5 + x^4 + x^3 + x^2 + 1$, $x^5 + x^4 + x^3 + x + 1$, $x^5 + x^4 + x^2 + x + 1$, $x^5 + x^3 + x^2 + x + 1$.

Exercise 4.12 (Shifrin 3.3.7)

Prove that for any prime number p, $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible in $\mathbb{Q}[x]$.

Solution 4.13

We can use the identity

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1} \tag{317}$$

Therefore,

$$\begin{aligned} f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} &= \frac{1}{x}\bigg\{ \bigg(\sum_{k=0}^{p} \binom{p}{k} x^k \bigg) - 1 \bigg\} && (318) \\ &= \frac{1}{x} \sum_{k=1}^{p} \binom{p}{k} x^k = \sum_{k=1}^{p} \binom{p}{k} x^{k-1} && (319) \end{aligned}$$

Focusing on the coefficients, the leading coefficient is $\binom{p}{p} = 1$, and the rest of the coefficients are divisible by p. The constant coefficient is $\binom{p}{1} = p$, which is not divisible by p^2. By Eisenstein's criterion, $f(x+1)$ is irreducible $\implies f(x)$ is irreducible. To justify the final step, assume that $f(x)$ is reducible. Then $f(x) = g(x)h(x)$ for positive degree polynomials g, h. Then by substituting $x+1$, we have that $f(x+1) = g(x+1)h(x+1)$, which means that $f(x+1)$ is irreducible.

Exercise 4.13 (Shifrin 4.1.3)

(a) Prove that if $I \subset R$ is an ideal and $1 \in I$, then $I = R$.
(b) Prove that $a \in R$ is a unit if and only if $\langle a \rangle = R$.
(c) Prove that the only ideals in a (commutative) ring R are $\langle 0 \rangle$ and R if and only if R is a field.

Solution 4.14

Listed.

(a) If $1 \in I$, then for every $r \in R$, we must have $r1 = r \in I$. Therefore $I = R$.
(b) If $a \in R$ is a unit, then $a^{-1} \in R$, and so for every $r \in R$, $ra^{-1} \in R$. Therefore, $\langle a \rangle$ must contain all elements of form $ra^{-1}a = r$, which is precisely R. Now assume that a is not a unit, and so there exists no $a^{-1} \in R$. Therefore, $\langle a \rangle$, which consists of all ra for $r \in R$, cannot contain 1 since $r \neq a^{-1}$, and so $\langle a \rangle \neq R$.
(c) For the forwards implication, assume that R is not a field. Then there exists some $a \neq 0$ that is not a unit, and taking $\langle a \rangle$ gives us an ideal that—from (b)—is not R. For the backward implication we know that $\langle 0 \rangle$ is an ideal. Now assume that there exists another ideal I containing $a \neq 0$. Since R is a field, a is a unit, and so by (b) $R = \langle a \rangle \subset I \subset R \implies I = R$.

Exercise 4.14 (Shifrin 4.1.4.a/b/c)

Find all the ideals in the following rings:

(a) $\mathbb{Z}$
(b) $\mathbb{Z}_7$
(c) $\mathbb{Z}_6$
(d) $\mathbb{Z}_{12}$
(e) $\mathbb{Z}_{36}$
(f) $\mathbb{Q}$
(g) $\mathbb{Z}[i]$ (see Exercise 2.3.18)

Solution 4.15

Listed.

(a) All sets of form $\{kz \in \mathbb{Z} \mid z \in \mathbb{Z}\}$ for all $k \in \mathbb{Z}$.
(b) Only $\{0\}$ and $\mathbb{Z}_7$ is an ideal.
(c) We have $\{0\}, \{0, 2, 4\}, \{0, 3\}, \mathbb{Z}_6$.

Exercise 4.15 (Shifrin 4.1.5)

(a) Let $I = \langle f(x) \rangle$, $J = \langle g(x) \rangle$ be ideals in $F[x]$. Prove that $I \subset J \Leftrightarrow g(x) | f(x)$.
(b) List all the ideals of $\mathbb{Q}[x]$ containing the element $f(x) = (x^2 + x - 1)^3 (x-3)^2$.

Solution 4.16

For (a), we prove bidirectionally.

1. $(\rightarrow)$. Since $f(x) \in \langle f(x) \rangle \implies f(x) \in \langle g(x) \rangle$, this means that $f(x) = r(x)g(x)$ for some $r(x) \in F[x$. Therefore $g(x) \mid f(x)$.
2. $(\leftarrow)$. Given that $g(x) \mid f(x)$, let us take some $f_1(x) \in I$. Then it is of the form $f_1(x) = r(x)f(x)$ for some $r(x) \in F[x]$. But since $g(x) \mid f(x)$, $f(x) = h(x)g(x)$ for some $h(x) \in F[x]$. Therefore $f_1(x) = r(x)h(x)g(x) = (rh)(x)g(x)$, where $(rh)(x) \in F[x]$, and so $f_1(x) \in J$.

For (b), we can use the logic from (a) to find all the factors of $f(x)$, which generate all sup-ideals of $\langle f(x) \rangle$, which is the minimal ideal containing $f(x)$.

1. $g(x) = 1 \implies \langle 1 \rangle = F[x]$
2. $g(x) = x^2 + x - 1 \implies \langle x^2 + x - 1 \rangle$
3. $g(x) = (x^2 + x - 1)^2 \implies \langle (x^2 + x - 1)^2 \rangle$
4. $g(x) = (x^2 + x - 1)^3 \implies \langle (x^2 + x - 1)^3 \rangle$
5. $g(x) = x - 3 \implies \langle x - 3 \rangle$
6. $g(x) = (x^2 + x - 1)(x - 3) \implies \langle (x^2 + x - 1)(x - 3) \rangle$
7. $g(x) = (x^2 + x - 1)^2(x - 3) \implies \langle (x^2 + x - 1)^2(x - 3) \rangle$
8. $g(x) = (x^2 + x - 1)^3(x - 3) \implies \langle (x^2 + x - 1)^3(x - 3) \rangle$
9. $g(x) = (x - 3)^2 \implies \langle (x - 3)^2 \rangle$
10. $g(x) = (x^2 + x - 1)(x - 3)^2 \implies \langle (x^2 + x - 1)(x - 3)^2 \rangle$
11. $g(x) = (x^2 + x - 1)^2(x - 3)^2 \implies \langle (x^2 + x - 1)^2(x - 3)^2 \rangle$
12. $g(x) = (x^2 + x - 1)^3(x - 3)^2 \implies \langle (x^2 + x - 1)^3(x - 3)^2 \rangle$

Exercise 4.16 (Shifrin 4.1.14.a/b)

Mimicking Example 5(c), give the addition and multiplication tables of

(a) $\mathbb{Z}_2[x]/\langle x^2 + x \rangle$
(b) $\mathbb{Z}_3[x]/\langle x^2 + x - 1 \rangle$
(c) $\mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$

In each case, is the quotient ring an integral domain? a field?

Solution 4.17

For (a), note that the quotient allows us to state that $x^2 \equiv x \pmod{I}$, and therefore every polynomial in $\mathbb{Z}_2[x]/\langle x^2 + x \rangle$ is equivalent to a linear polynomial. Therefore, the elements in this quotient are $0, 1, x, x+1$. As you can see, this is not an integral domain (and hence not a field) since $x, x+1$ are zero divisors.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	x	0
$x+1$	0	$x+1$	0	$x+1$

Figure 10: Addition and multiplication tables for $\mathbb{Z}_2[x]/\langle x^2 + x \rangle$.

For (b), note that the quotient allows us to state that $x^2 \equiv 2x + 1 \pmod{I}$, and therefore every polynomial in $\mathbb{Z}_3[x]/\langle x^2 + x - 1 \rangle$ is equivalent to a linear polynomial. Therefore, the elements in this quotient are $0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2$. This is indeed an integral domain since there are no zero divisors, and it is a field since every nonzero element is a unit (all rows/columns are filled with all elements of the set).

$+$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

Figure 11: Addition table for $\mathbb{Z}_3[x]/\langle x^2+x-1\rangle$.

$\times$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	$2x+1$	1	$x+1$	$x+2$	$2x+2$	2
$x+1$	0	$x+1$	$2x+2$	1	$x+2$	$2x$	2	x	$2x+1$
$x+2$	0	$x+2$	$2x+1$	$x+1$	$2x$	2	$2x+2$	1	x
$2x$	0	$2x$	x	$x+2$	2	$2x+2$	$2x+1$	$x+1$	1
$2x+1$	0	$2x+1$	$x+2$	$2x+2$	x	1	$x+1$	2	$2x$
$2x+2$	0	$2x+2$	$x+1$	2	$2x+1$	x	1	$2x$	$x+2$

Figure 12: Multiplication table for $\mathbb{Z}_3[x]/\langle x^2+x-1\rangle$.

Exercise 4.17 (Shifrin 4.1.17)

Let R be a commutative ring and let $I, J \subset R$ be ideals. Define

$$I \cap J = \{a \in R : a \in I \text{ and } a \in J\}$$
$$I + J = \{a + b \in R : a \in I, b \in J\}.$$

(a) Prove that $I \cap J$ and $I + J$ are ideals.
(b) Suppose $R = \mathbb{Z}$ or $F[x]$, $I = \langle a\rangle$, and $J = \langle b\rangle$. Identify $I \cap J$ and $I + J$.
(c) Let $a_1, \ldots, a_n \in R$. Prove that $\langle a_1, \ldots, a_n\rangle = \langle a_1\rangle + \cdots + \langle a_n\rangle$.

Solution 4.18

For (a), we have the following.

1. $I \cap J$ is an ideal. Given $a, b \in I \cap J$, then $a, b \in I \implies a + b \in I$, and $a, b \in J \implies a + b \in J$. So $a + b \in I \cap J$. Furthermore, for every $r \in R$, $a \in I \implies ra \in I$ and $a \in J \implies ra \in J$, so $a \in I \cap J \implies ra \in I \cap J$.
2. $I + J$ is an ideal. Given $x, y \in I + J$, then $x = a_x + b_x$ and $y = a_y + b_y$ for $a_x, a_y \in I, b_x, b_y \in J$. So
$$x + y = (a_x + b_x) + (a_y + b_y) = (a_x + a_y) + (b_x + b_y) \tag{320}$$
where $a_x + a_y \in I, b_x + b_y \in J$ by definition of an ideal, and so $x + y \in I + J$. Noe let $x = a_x + b_x \in I + J$. Then given $r \in R$,
$$rx = r(a_x + b_x) = ra_x + rb_x \tag{321}$$
where $ra_x \in I$ and $rb_x \in J$ since I, J are ideals. Therefore $rx \in I + J$.

For (b), the argument is equivalent for $\mathbb{Z}$ and $F[x]$. $I \cap J$ consists of all elements that are divisible by both a and b, so $I \cap J = \langle \text{lcm}(a,b) \rangle$. $I + J$ consists of all elements that are of form $ra + sb$, but this are all multiples of $\gcd(a,b)$ and so $I + J = \langle \gcd(a,b) \rangle$.
For (c), it suffices to prove $\langle a, b \rangle = \langle a \rangle + \langle b \rangle$.

1. $\langle a, b \rangle \subset \langle a \rangle + \langle b \rangle$. $x \in \langle a, b \rangle \implies x = r_a a + r_b b$ for $r_a, r_b \in R$. But $a \in \langle a \rangle, b \in \langle b \rangle \implies r_a a \in \langle a \rangle, r_b b \in \langle b \rangle$, and so $x \in \langle a \rangle + \langle b \rangle$.
2. $\langle a, b \rangle \supset \langle a \rangle + \langle b \rangle$. $x \in \langle a \rangle + \langle b \rangle \implies x = a_x + b_x$ for $a_x \in \langle a \rangle, b_x \in \langle b \rangle$. But $a_x \in \langle a \rangle \implies a_x = r_a a$ for some $r_a \in R$, and $b_x \in \langle b \rangle \implies b_x = r_b b$ for some $r_b \in R$. So $x = r_a a + r_b b \iff x \in \langle a, b \rangle$.

We know that for $\langle a_1 \rangle = \langle a_1 \rangle$, and so by making this argument $n-1$ times we can build up by induction that $\langle a_1, \ldots a_{n-1}, a_n \rangle = \langle a_1, \ldots, a_{n-1} \rangle + \langle a_n \rangle$.

Exercise 4.18 (Shifrin 4.2.1)

(a) Prove that the function $\phi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]$ defined by $\phi(a+b\sqrt{2}) = a - b\sqrt{2}$ is an isomorphism.
(b) Define $\phi : \mathbb{Q}[\sqrt{3}] \to \mathbb{Q}[\sqrt{7}]$ by $\phi(a + b\sqrt{3}) = a + b\sqrt{7}$. Is ϕ an isomorphism? Is there any isomorphism?

Solution 4.19

For (a), we first prove that it is a homomorphism.

$$\begin{aligned}
\phi((a+b\sqrt{2}) + (c+d\sqrt{2})) &= \phi((a+c) + (b+d)\sqrt{2}) && (322)\\
&= (a+c) - (b+d)\sqrt{2} && (323)\\
&= (a - b\sqrt{2}) + (c - d\sqrt{2}) && (324)\\
&= \phi(a+b\sqrt{2}) + \phi(c+d\sqrt{2}) && (325)\\
\phi((a+b\sqrt{2})(c+d\sqrt{2})) &= \phi((ac+2bd) + (ad+bc)\sqrt{2}) && (326)\\
&= (ac+2bd) - (ad+bc)\sqrt{2} && (327)\\
&= (a-b\sqrt{2})(c-d\sqrt{2}) && (328)\\
&= \phi(a+b\sqrt{2}) \times \phi(c+d\sqrt{2}) && (329)\\
\phi(1) &= 1 && (330)
\end{aligned}$$

This is injective since given that $a + b\sqrt{2} \neq c + d\sqrt{2}$, then at least $a \neq b$ or $c \neq d$, in which case $a - b\sqrt{2} \neq c - d\sqrt{2}$. Alternatively, we can see that the kernel is 0, so it must be injective. It is onto since given any $c + d\sqrt{2}$, the preimage is $c - d\sqrt{2}$. Therefore ϕ is an isomorphism.
For (b), no it is not an isomorphism since

$$\begin{aligned}
\phi((a+b\sqrt{3})(c+d\sqrt{3})) &= \phi((ac+3bd) + (ad+bc)\sqrt{3}) && (331)\\
&= (ac+3bd) + (ad+bc)\sqrt{7} && (332)\\
&\neq (ac+7bd) + (ad+bc)\sqrt{7} && (333)\\
&= (a+b\sqrt{7})(c+d\sqrt{7}) && (334)\\
&= \phi(a+b\sqrt{3})\phi(c+d\sqrt{3}) && (335)
\end{aligned}$$

We claim that there is no isomorphism. Assume that such ϕ exists. Then $\phi(1) = 1$, and so $\phi(3) = \phi(1+1+1) = \phi(1) + \phi(1) + \phi(1) = 1 + 1 + 1 = 3$. Now given $\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$, we follows that

$$\phi(\sqrt{3})^2 = \phi(3) = 3 \qquad (336)$$

and so $\phi(\sqrt{3})$ must map to the square root of 3 which must live in $\mathbb{Q}[\sqrt{7}]$. Assume such a number is $a + b\sqrt{7} \implies (a^2 + 7b^2) + (2ab)\sqrt{7} = \sqrt{3}$. This implies that $2ab = 0$, leaving the rational term, but we know that $\sqrt{3}$ does not exist in the rationals, and so $\sqrt{3}$ does not exist.

Exercise 4.19 (Shifrin 4.2.12)

Let R be a commutative ring, $I \subset R$ an ideal. Suppose $a \in R$, $a \notin I$, and $I + \langle a \rangle = R$ (see Exercise 4.1.17 for the notion of the sum of two ideals). Prove that $\bar{a} \in R/I$ is a unit.

Solution 4.20

Since $R = I + \langle a \rangle$, $1 \in R = I + \langle a \rangle$. So there exists $i \in I, ra \in \langle a \rangle$ s.t. $1 = i + ra \implies ra = 1 - i$. Therefore, in the quotient ring, $\bar{i} = 0$ and we have

$$\bar{r}\bar{a} = \bar{1} - \bar{0} = \bar{1} \tag{337}$$

and so $\bar{r}$ is a multiplicative inverse of $\bar{a}$. So $\bar{a}$ is a unit.