CHAPTER 2

RING THEORY

2.1 Introduction to Rings

We start by defining rings.

Definition 2.1.1. A *ring* is a collection $(R, +, \cdot)$ where R is a set, and $+$ and $\cdot$ are two binary operations on R such that:

- $(R, +)$ is an abelian group[1];
- for all r_1, r_2, r_3,
$$r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3;$$
- for all r_1, r_2, r_3,
$$(r_1 + r_2) \cdot r_3 = r_1 \cdot r_3 + r_2 \cdot r_3 \qquad \text{and} \qquad r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3.$$

A *unital ring* is a ring with a multiplicative identity, i.e. there exists a $1 \in R \setminus \{0\}$ such that for all $a \in R$, $a \cdot 1 = a = 1 \cdot a$. A ring is called *commutative* if the operation $\cdot$ is commutative.

We have seen many rings, such as $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. For every $n \in \mathbb{Z}_{\geqslant 1}$, the set of cosets $\mathbb{Z}/n\mathbb{Z}$ forms a ring under addition and multiplication modulo n. If R is a commutative ring, then we can form the ring $R[X]$ of polynomials over R in one variable. These are formal finite R-linear combinations of "symbols" x^i for $i \in \mathbb{Z}_{\geqslant 1}$ and multiplication by $x^i \cdot x^j = x^{i+j}$ for $i, j \in \mathbb{Z}_{\geqslant 1}$.[2] If R is a ring, then we can form the ring $M_n(R)$ of $n \times n$ matrices over R under matrix addition and multiplication. Finally, if R is a ring and S is a set, then the set R^S of functions $f : S \to R$ is a ring under pointwise addition and multiplication, i.e. for $f, g \in R^S$ and $s \in S$,

$$(f + g)(s) = f(s) + g(s), \qquad (fg)(s) = f(s) \cdot g(s).$$

For a ring R, $a, b \in R$ and $n \in \mathbb{Z}$, we denote $-a$ for the additive inverse of a,

$$n \cdot a = \underbrace{a + a + \cdots + a}_{n \text{ times}}$$

for $n \in \mathbb{Z}_{>0}$, $0 \cdot a = 0$ and $n \cdot a = -n \cdot -a$ for $n \in \mathbb{Z}_{<0}$. Also, we write $a - b$ for $a + (-b)$. If R is unital, we set $a^0 = 1$ for all $a \in R \setminus \{0\}$ and

$$a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ times}}$$

for $n > 0$. Moreover, if a^{-1} exists, then $a^n = (a^{-1})^{-n}$ for $n \in \mathbb{Z}_{<0}$.

We will now prove some basic ring properties. First, we show that multiplying by zero is always zero.

[1] The additive identity is 0

[2] It turns out that this is enough to define multiplication of polynomials- we can apply ring axioms and use this property.

Proposition 2.1.2. *Let R be a ring, and $a \in R$. Then, $0 \cdot a = 0$ and $a \cdot 0 = 0$.*

Proof. We find that

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a,$$

and

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

Therefore,

$$0 = 0 \cdot a - 0 \cdot a = (0 \cdot a + 0 \cdot a) - 0 \cdot a = 0 \cdot a,$$

and

$$0 = a \cdot 0 - a \cdot 0 = (a \cdot 0 + a \cdot 0) - a \cdot 0 = a \cdot 0.$$

□

Next, we show that the inverse sign can be moved with respect to multiplication.

Proposition 2.1.3. *Let R be a ring, and $a, b \in R$. Then,*

$$a \cdot (-b) = (-a) \cdot b = -(a \cdot b).$$

Proof. We have

$$\begin{aligned} a \cdot (-b) + a \cdot b &= a \cdot (-b + b) \\ &= a \cdot 0 \\ &= 0 \end{aligned} \qquad \begin{aligned} (-a) \cdot b + a \cdot b &= (-a + a) \cdot b \\ &= 0 \cdot b \\ &= 0. \end{aligned}$$

This implies that the additive inverse of $a \cdot b$ is both $a \cdot (-b)$ and $(-a) \cdot b$. In that case,

$$a \cdot (-b) = (-a) \cdot b = -(a \cdot b).$$

□

Now, we show how multiplying inverses work.

Proposition 2.1.4. *Let R be a ring, and $a, b \in R$. Then,*

$$(-a) \cdot (-b) = ab.$$

Proof. We find that

$$\begin{aligned} (-a) \cdot (-b) - (a \cdot b) &= (-a) \cdot (-b) + a \cdot (-b) \\ &= (-a + a) \cdot (-b) \\ &= 0 \cdot (-b) = 0 \end{aligned}$$

This implies that the additive inverse of $-(a \cdot b)$ is $(-a) \cdot (-b)$. In that case,

$$(-a) \cdot (-b) = ab.$$

□

There are a few other propositions as well, but we state it without proof.

Proposition 2.1.5. *Let R be a ring, $a, b \in R$ and $m, n \in \mathbb{Z}$. Then,*

- $(m+n) \cdot a = m \cdot a + n \cdot a$;
- $(mn) \cdot a = m \cdot (n \cdot a)$;
- $m \cdot (a+b) = m \cdot a + m \cdot b$;
- $m \cdot (ab) = (m \cdot a)b = a(m \cdot b)$;
- $(m \cdot a)(n \cdot b) = mn \cdot (ab)$.

We now define the elements in a ring which have a multiplicative inverse.

Definition 2.1.6. Let R be a unital ring. An element u of R is called a *unit* if there exists $u^{-1} \in R$ such that $uu^{-1} = u^{-1}u = 1$. The set of units is denoted by $R^\times$.

By construction, $R^\times$ forms a group under the multiplication operation in R. We would never have $R = R^\times$ since 0 would never have a unit- for all $a \in R$, $a \cdot 0 = 0 \neq 1$. Nonetheless, it is possible for every non-zero element to be invertible.

Definition 2.1.7. A unital ring in which every non-zero element is a unit is called a *division ring*. A commutative division ring is called a *field*.

We know $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. On the other hand, $\mathbb{Z}$ is not a field since 2 does not have an inverse in $\mathbb{Z}$. The ring $\mathbb{Z}/4\mathbb{Z}$ is a unital commutative ring that is not a field- the element $2 + 4\mathbb{Z}$ does not have an inverse. The ring $M_2(\mathbb{R})$ is a unital non-commutative ring that is not a division ring. The quaternions $\mathbb{H}$ is a non-commutative division ring- it is a real vector space with basis $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$, where

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 = \mathbf{ijk}.$$

An element in $\mathbb{H}$ is of the form $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, where $a, b, c, d \in \mathbb{R}$. The inverse of a non-zero element is

$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})^{-1} = \frac{a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}}{a^2 + b^2 + c^2 + d^2}.$$

2.2 Subrings, Ideals and Quotients

In this section, we will try to find a substructure within rings that will allow us to construct quotient rings. We start by defining subrings.

Definition 2.2.1. Let R be a ring. A *subring* of R is an additive subgroup $S \subseteq R$ such that for all $a, b \in S$, $ab \in S$. We denote $S \leqslant R$. If R is unital, then a subring S of R is a *unital subring* if $1 \in S$.[3]

So, S is a subring of R if S forms a ring under the same operation as in R. We will now go through some examples. We have a chain of subrings

$$\mathbb{Z} \leqslant \mathbb{Q} \leqslant \mathbb{R} \leqslant \mathbb{C} \leqslant \mathbb{H}.$$

If R is a commutative ring, then it is a subring of the polynomial ring $R[X]$- the constant polynomials. Is S a subring of a (unital) ring R, then for all $n \in \mathbb{Z}_{\geqslant 1}$, the ring $M_{n\times n}(S)$ is a subring of the (unital) ring $M_{n\times n}(R)$. Now, let R be the ring of all sequences of real numbers- it is a ring under pointwise addition and multiplication, and the sequence of 1's is the multiplicative identity. Then, the set of all sequences that converge to 0 is a subring, but it is not a unital subring since the sequence of 1's does not converge to 0.

We will now consider forming quotient rings. Subrings are not the right structure to quotient- the ring operation will not be well-defined. We would like the ring $\mathbb{Z}/n\mathbb{Z}$ to be the quotient of the rings $\mathbb{Z}$ and $n\mathbb{Z}$. Therefore, cosets in a subring will be of the form $r + I$, for some $r \in R$ and a subset $I \subseteq R$. For addition to be well-defined, we require S to be normal subgroup. However, since R forms an abelian group, I will always be normal subgroup- we just require I to be a subgroup for addition to be well-defined.

Now, we consider how the multiplication can be well-defined. So, let $r \in R$ and $i \in I$. We know that $i + I = I$, and so

$$ri + I = (r + I)(i + I) = (r + I)(0 + I) = 0 + I,$$

and

$$ir + I = (i + I)(r + I) = (0 + I)(i + I) = 0 + I.$$

Therefore, both $ri \in I$ and $ir \in I$. It turns out that this is a sufficient condition to quotient. So, we define this substructure.

Definition 2.2.2. Let R be a ring. A *left ideal* of R is an additive subgroup I of R such that for all $a \in I$ and $r \in R$, we have $ra \in I$, i.e. $rI \subseteq I$. A *right ideal* of R is an additive subgroup I of R such that for all $a \in I$ and $r \in R$, we have $ar \in I$, i.e. $Ir \subseteq I$. A *two-sided ideal* of R is a left ideal I that is also a right ideal. We often write $I \lhd I$. I is called *proper* if $I \neq R$.

Note that not every ideal is a subring- we do not require the multiplicative identity in an ideal, for example.[4] We now define quotient rings.

[3] We will refer to unital subrings of a unital ring just by subrings.

[4] In fact, if an ideal contains the identity element, then it is not proper!

Definition 2.2.3. Let R be a (unital) ring, and let I be a (proper) two-sided ideal in R. The *quotient ring* has, as its underlying set, the set of cosets

$$R/I = \{r + I \mid r \in R\}$$

with the operations of addition

$$(r+I)+(s+I)=(r+s)+I,$$

and multiplication

$$(r+I)(s+I)=rs+I.$$[5]

We will now consider some examples of quotient rings. By construction, $\mathbb{Z}/n\mathbb{Z}$ is a quotient ring for $n \in \mathbb{Z}_{\geqslant 2}$. Next, for a polynomial ring $\mathbb{R}[X]$, the subset

$$I = X^2R = \{a_2X^2 + a_3X^3 + \cdots + a_dX^d \mid d \in \mathbb{Z}_{\geqslant 2}, a_i \in \mathbb{R}\}$$

is an ideal. If we have polynomials $p \in \mathbb{R}[X]$ and $q \in I$, then $\deg(pq) \geq 2$, and so $pq \in I$. In R/I, two polynomials

$$f = a_0 + a_1X + a_2X^2 + \ldots$$

and

$$g = b_0 + b_1X + b_2X^2 + \ldots$$

represent the same coset if and only if $a_0 = b_0$ and $a_1 = b_1$. Therefore, R/I is a 2-dimensional as a vector space over $\mathbb{R}$, spanned by $1+I$ and $X+I$, with the property that $X^2 + I = 0$. This implies that

$$R/I = \{a + bX + I \mid a, b \in \mathbb{R}\}.$$

[5] The multiplication operation is well-defined- if $r, s \in R$, then $(r+I)(s+I) = rs+rI+Is+I = rs+I$.

2.3 Ring Homomorphisms

We now consider ring homomorphisms. Consider the polynomial ring $R = \mathbb{R}[X]$. The subset

$$I = (X^2+1)R = \{(X^2+1)f \mid f \in R\}$$

is an ideal. For $f \in R$, the coset $f + I$ contains a unique polynomial of the form $a_0 + a_1X$. If

$$f = a_0 + a_1X + \cdots + a_dX^d,$$

then we can divide f by X^2+1 so that

$$f = q(X^2+1) + r,$$

where q is the quotient and r is the remainder. The remainder has degree at most 1, so $r = a_0 + a_1X$, meaning that $f + I = a_0 + a_1X + I$. Therefore, R/I is a 2-dimensional vector space over $\mathbb{R}$. Moreover,

$$X^2 + I = (X^2 + 1 - 1) + I = (X^2+1) - 1 + I.$$

We will now define ring homomorphisms.

Definition 2.3.1. Let R and S be rings. A *ring homomorphism* from R to S is a function $\phi : R \to S$ such that for all $a, b \in R$ such that $\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$. Moreover, if R and S are unital, then a ring homomorphism is *unital* if $\phi(1_R) = 1_S$.[6]

Since not every element has a multiplicative inverse, we cannot derive $\phi(1_R) = 1_S$ from the property $\phi(ab) = \phi(a)\phi(b)$. Next, we show that the image of a homomorphism is a subring.

Proposition 2.3.2. *Let R and S be (unital) rings, and let $\phi : R \to S$ be a ring homomorphism. Then, the image $\mathrm{Im}(\phi)$ is a subring of S.*

Proof. We know that the image $\mathrm{Im}(\phi)$ is a subgroup of S. So, let $s_1, s_2 \in \mathrm{Im}(\phi)$. By definition, there exist $r_1, r_2 \in R$ such that $\phi(r_1) = s_1$ and $\phi(r_2) = s_2$. In that case,

$$\phi(r_1r_2) = \phi(r_1)\phi(r_2) = s_1s_2,$$

and so $r_1r_2 \in \mathrm{Im}(\phi)$. This implies that $\mathrm{Im}(\phi)$ is a subring of S. If ϕ is unital, then $\phi(1_R) = 1_S$, and so $1_S \in \mathrm{Im}(\phi)$. So, the image $\mathrm{Im}(\phi)$ is a (unital) subring of S. □

We now define ring isomorphisms.

Definition 2.3.3. Let R and S be rings. A *ring isomorphism* from R to S is a function $\phi : R \to S$ such that ϕ is bijective.

Like in the case of groups, we find that the inverse function of an isomorphism is also an isomorphism.

[6] We will assume homomorphisms from unital rings to be unital.

Proposition 2.3.4. *Let R and S be rings, and let $\phi : R \to S$ be a ring isomorphism. Then, $\phi^{-1} : S \to R$ is a ring isomorphism.*

Proof. Let $s_1, s_2 \in S$. Since ϕ is surjective, there exist $r_1, r_2 \in R$ such that $\phi(r_1) = s_1$ and $\phi(r_2) = s_2$. In that case,

$$\begin{aligned}\phi^{-1}(s_1 s_2) &= \phi^{-1}(\phi(r_1)\phi(r_2)) \\ &= \phi^{-1}(\phi(r_1 r_2)) \\ &= r_1 r_2 \\ &= \phi^{-1}(s_1)\phi^{-1}(s_2).\end{aligned}$$

Since ϕ^{-1} is a group homomorphism and satisfies this property, the function ϕ^{-1} is a ring homomorphism. Since it is also bijective, it is a ring isomorphism. □

We will now look at some examples of ring homomorphisms and isomorphisms. Let R be a (unital) ring and let I be a (proper) two-sided ideal. Then, the quotient map $R \to R/I$ given by $r \mapsto r + I$ is a ring homomorphism. Now, let R be a commutative ring, and $r \in R$. Then, the evaluation map $R[X] \to R$ given by $f \mapsto f(r)$ is a ring homomorphism.[7] Finally, there is a ring isomorphism $\mathbb{R}[X]/(X^2+1)\mathbb{R}[X] \to \mathbb{C}$. In the isomorphism map, the element $X + (X^2+1)\mathbb{R}[X]$ gets mapped to $i \in \mathbb{C}$, since

$$(X)^2 + (X^2+1)\mathbb{R}[X] = -1 + (X^2+1)\mathbb{R}[X].$$

The isomorphism is given by $f + (X^2+1) \mapsto f(i)$.

We now define the kernel of a ring homomorphism.

Definition 2.3.5. Let R and S be rings, and let $\phi : R \to S$ be a ring homomorphism. The *kernel* of the map is

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

As a group, we know that the kernel is a normal subgroup. It turns out that the kernel is an ideal.

Proposition 2.3.6. *Let R and S be (unital) rings, and let $\phi : R \to S$ be a ring homomorphism. Then, the kernel is a (proper) ideal of R.*

Proof. We know that the kernel $\ker(\phi)$ is a subgroup of R. Now, for $r \in R$ and $i \in \ker(\phi)$,

$$\phi(ri) = \phi(r)\phi(i) = \phi(r) \cdot 0 = 0,$$

and

$$\phi(ir) = \phi(i)\phi(r) = 0 \cdot \phi(r) = 0,$$

So, $ri, ir \in \ker(\phi)$. This implies that the kernel is an ideal of R. If the homomorphism is unital, then we know that $\phi(1) \neq 0$, so $1 \notin \ker(\phi)$. Therefore, $\ker(\phi)$ is not a proper ring homomorphism. □

Now, we look at the First Isomorphism Theorem for rings.

Theorem 2.3.7 (First Isomorphism Theorem)**.** *Let R and S be rings, and let $\phi : R \to S$ be a ring homomorphism. Then,*

$$R/(\ker\phi) \cong \mathrm{Im}(\phi).$$

[7] This follows from the definition of polynomial ring addition and multiplication!

Proof. Let $\psi : R/\ker(\phi) \to \text{Im}(\phi)$ be the map $\psi(r + \ker(\phi)) = \phi(r)$. From the First Isomorphism Theorem for groups, we know that ψ is a group isomorphism. Now, for $r_1, r_2 \in R$,

$$\psi(r_1 r_2) = r_1 r_2 + \ker(\phi) = (r_1 + \ker(\phi))(r_2 + \ker(\phi)) = \psi(r_1)\psi(r_2).$$

So, ψ is a ring isomorphism. Therefore, $R/(\ker(\phi)) \cong \text{Im}(\phi)$. □

Now, consider the ring homomorphism $\phi : \mathbb{R}[X] \to \mathbb{C}$ given by $f \mapsto f(i)$. This is a ring homomorphism. The map is surjective- for a complex number $a + bi \in \mathbb{C}$, $a + bX \mapsto a + bi$. We know that $X^2 + 1 \mapsto 0$, so any multiple of $X^2 + 1$ also maps to 0. It turns out that

$$\ker(\phi) = (X^2 + 1)\mathbb{R}[X] = \{(X^2 + 1)f \mid f \in \mathbb{R}[X]\}.$$

So, the First Isomorphism Theorem tells us that $R/(X^2 + 1) \cong \mathbb{C}$. Let $C^0(\mathbb{R})$ be the set of continuous functions $\mathbb{R} \to \mathbb{R}$. It is a ring under pointwise addition and multiplication. Consider the evaluation homomorphism $C^0(\mathbb{R}) \to \mathbb{R}$ given by $f \mapsto f(0)$. Its image is $\mathbb{R}$, and the kernel is

$$I = \{f \in C^0(\mathbb{R}) \mid f(0) = 0\}.$$

Therefore, $C^0(\mathbb{R})/I \cong \mathbb{R}$ by the First Isomorphism Theorem.

We finish by showing that (unital) ring homomorphisms from fields must be injective.

Proposition 2.3.8. *Let K be a field and let R be a unital ring, and let $\phi : K \to R$ be a ring homomorphism. Then, ϕ is injective.*

Proof. Assume that ϕ is not injective. In that case, $\ker(\phi) \neq \{0\}$. That is, there exists an $x \in \ker(\phi)$ such that $x \neq 0$. Since K is a field, x has a multiplicative inverse x^{-1}. Moreover, we know that $\ker(\phi)$ is an ideal, so

$$1 = x^{-1}x \in \ker(\phi).$$

Therefore, $\phi(1) = 0$- ϕ is not a unital. This is a contradiction, so ϕ must be injective. □

This proof also works for division rings- commutativity is not required.

2.4 Integral Domains

Introduction to Integral Domains

We will now look at a substructure of rings. In this case, we are looking at some properties that the integers satisfy, starting with zero divisors.

Definition 2.4.1. Let R be a ring. An element $a \in R$ is a *left zero divisor* in R if $a \neq 0$ and there exists $b \in R \setminus \{0\}$ such that $ab = 0$. An element $a \in R$ is a *right zero divisor* in R if $a \neq 0$ and there exists $b \in R \setminus \{0\}$ such that $ba = 0$. An element $a \in R$ is a *zero divisor* if a is a left zero divisor or a right zero divisor.

For example, in $\mathbb{Z}/8\mathbb{Z}$, $2 + 8\mathbb{Z}$ is a zero divisor since

$$(2 + 8\mathbb{Z})(4 + 8\mathbb{Z}) = 0 + 8\mathbb{Z}.$$

Also, in $R = \mathbb{R}[X] + X^2\mathbb{R}[X]$, the element $X + X^2\mathbb{R}[X]$ is a zero divisor since

$$(X + X^2\mathbb{R}[X])(X + X^2\mathbb{R}[X]) = X^2 + X^2\mathbb{R}[X] = 0 + X^2\mathbb{R}[X].$$

Finally, The ring $\mathbb{Z}$ has no zero divisors, although not every element in $\mathbb{Z}$ is invertible in $\mathbb{Z}$. Next, we show that left and right divisors are equivalent to each other and the multiplication cancellation rules.

Proposition 2.4.2. *Let R be a ring. Then, the following are equivalent:*

(1) R has no left zero divisors;

(2) R has no right zero divisors;

(3) for all $a, b, c \in R$, if $ab = ac$, then either $a = 0$ or $b = c$;

(4) for all $a, b, c \in R$, if $ba = ca$, then either $a = 0$ or $b = c$.

Proof. We know that R has a left zero divisor if and only if there exist $a, b \in R$ with $a, b \neq 0$ such that $ab = 0$. Moreover, there exist $a, b \in R$ with $a, b \neq 0$ such that $ab = 0$ if and only if R has a right zero divisor. Therefore, (1) if and only if (2).
Now, assume that R has no left zero divisors, and suppose that $ab = ac$ with $a \neq 0$. In that case,

$$a(b - c) = ab - ac = 0.$$

Since $a \neq 0$ and a is not a left zero divisor, we must have $b - c = 0$. So, $b = c$. So, (1) implies (3).
Now, assume that R has no right zero divisors, and suppose that $ba = ca$ with $a \neq 0$. In that case,

$$(b - c)a = ba - ca = 0.$$

Since $a \neq 0$ and a is not a right zero divisor, we must have $b - c = 0$. So, $b = c$. So, (2) implies (4).
Now, we know that there exist $a, b, c \in R$ such that although $ab = ac$, we have $a \neq 0$ and $b \neq c$. Moreover, $ab = ac$ if and only if $a(b - c) = ab - ac = 0 = 0(b - c)$, with $a \neq 0$ and $b - c \neq 0$. Then, $a(b - c) = 0(b - c)$, with $a \neq 0$ and $b - c \neq 0$. Therefore, there exist $a, b, c \in R$ such that although $ab = ac$, we

have $a \neq 0$ and $b \neq c$ if and only if there exist $a, b, c \in R$ such that although $a(b-c) = 0(b-c)$, we have $a \neq 0$ and $b - c \neq 0$. So, (3) if and only if (4). Therefore, the 4 statements are equivalent. □

Also, a unit cannot be a zero divisor.

Proposition 2.4.3. *Let R be a unital ring, and let $u \in R$ be a unit. Then, u is not a zero divisor.*

Proof. Let $v \in R$ such that $uv = 0$. Since u is a unit, we find that

$$v = u^{-1}uv = u^{-1} \cdot 0 = 0.$$

Let $w \in R$ such that $wu = 0$. Since u is a unit, we find that

$$w = wuu^{-1} = 0 \cdot u^{-1} = 0.$$

So, u is not a zero divisor. □

However, it is possible for a non-zero divisor to not be a unit. For example, $2 \in \mathbb{Z}$ is not a unit, but it is a not zero divisor.

We now define integral domains.

Definition 2.4.4. Let R be a commutative unital ring. If R has no zero divisors, then it is called an *integral domain*.

We now look at some examples of integral domains. Since every non-zero element in a field is a unit, a field is automatically an integral domain. Moreover, the ring $\mathbb{Z}$ is an integral domain, but it is not a field. It turns out that a finite integral domain is a field.

Proposition 2.4.5. *Let R be a finite integral domain. Then, R is a field.*

Proof. Let $r \in R$ with $r \neq 0$. We want to show that r is a unit. Define the set

$$S = \{r^n \mid n \in \mathbb{Z}_{\geqslant 0}\}.$$

Since R is finite, the Piegenhole principle tells us that there exist $n, m \in \mathbb{Z}$ with $n > m$ such that $r^n = r^m$. In that case,

$$r \cdot r^{m-1}(1 - r^{n-m}) = r^n - r^m = 0 = r \cdot 0.$$

Since $r \neq 0$, this implies that $r^{m-1}(1 - r^{n-m}) = 0$. We can iteratively cancel an r until we find that

$$r^0(1 - r^{n-m}) = 1 - r^{n-m} = 0.$$

This implies that $r^{n-m} = 1$, and so $r^{-1} = r^{n-m-1}$. Therefore, r is a unit- R is a field. □

We can use this result to show that $\mathbb{Z}/p\mathbb{Z}$ is a field for a prime p.

Proposition 2.4.6. *Let p be a prime. Then, $\mathbb{Z}/p\mathbb{Z}$ is a field.*

Proof. We know that $\mathbb{Z}/p\mathbb{Z}$ is a finite commutative unital ring. So, we show that $\mathbb{Z}/p\mathbb{Z}$ has no zero divisors. Let $a+p\mathbb{Z}, b+p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$ such that

$$ab + p\mathbb{Z} = (a+p\mathbb{Z})(b+p\mathbb{Z}) = 0 + p\mathbb{Z}.$$

Therefore, $ab \in p\mathbb{Z}$, meaning that $p \mid ab$. Since p is a prime, then either $p \mid a$ or $p \mid b$. So, either $a+p\mathbb{Z} = 0+p\mathbb{Z}$ or $b+p\mathbb{Z} = 0+p\mathbb{Z}$. This implies that $\mathbb{Z}/p\mathbb{Z}$ has no zero divisors, and is therefore an integral domain. So, $\mathbb{Z}/p\mathbb{Z}$ must be a field. □

Prime, Maximal and Principal Ideals

Now, we look at prime and maximal ideals. We start with the definitions.

Definition 2.4.7. Let R be a ring. An ideal I of R is *maximal* if I is a proper ideal, and for an ideal $I \subseteq J \subseteq R$, then either $J = I$ or $J = R$.

Definition 2.4.8. Let R be a commutative ring. An ideal I of R is *prime* if I is a proper ideal, and for $a, b \in R$ with $ab \in I$, either $a \in I$ or $b \in I$.

The definition for prime ideals generalises prime numbers in $\mathbb{Z}$- for $a, b \in \mathbb{Z}$, if $n \mid ab$, then either $n \mid a$ or $n \mid b$. Next, we define ideals generated by element(s).

Definition 2.4.9. Let R be a ring, and let $r \in R$. The left ideal

$$Rr = \{xr \mid x \in R\}$$

is called the *left ideal generated by* r. Similarly, the right ideal

$$rR = \{rx \mid x \in R\}$$

is called the *right ideal generated by* r. The *two-sided ideal generated by* r is

$$RrR = \{\text{finite sums } \sum_i x_i r y_i \mid x_i, y_i \in R\}.$$

We denote it by $RrR = (r)$. An ideal of this form is called a *principal ideal*. Moreover, for $S \subseteq R$, the ideal generated by S is the set

$$(S) = \{\text{finite sums } \sum_{s \in S} x_s s y_s \mid x_s, y_s \in R\}.$$

The ideals defined above are the smallest ideals containing the element r. The definition for left and right ideals can be written like for two-sided ideals, e.g.

$$Rr = \{\text{finite sums } \sum_i x_i r \mid x_i \in R\},$$

but using distributivity, we can write this element as ar, for some $a \in R$. This is not possible in the last case. Nonetheless, if R is commutative, then the left/right ideal of $a \in R$ is the same as the principal ideal (a).

It turns out that every ideal in $\mathbb{Z}$ is principal.

Proposition 2.4.10. *Let I be an ideal in $\mathbb{Z}$. Then, there exists an $n \in \mathbb{Z}_{\geqslant 1}$ such that $I = (n)$.*

Proof. If $I = \{0\}$, then $I = (0)$. If $I \neq \{0\}$, then there exists an $x \in I$ such that $x \neq 0$. In that case, $|x| \in I$. Therefore, we can find an $n > 0$ such that n is the smallest positive element in I. Since I is an ideal, we find that $(n) \subseteq I$. Now, let $a \in I$. By the division algorithm for integers, there exist $q, r \in \mathbb{Z}$ with $0 \leqslant r < n$ such that $a = qn + r$. Since $n \in I$,

$$r = (qn + r) - qn \in I.$$

Since $0 \leqslant r < n$ and n is the smallest positive integer in I, we must have $r = 0$. Therefore, $a = qn \in (n)$, and so $I \subseteq (n)$. Therefore, $I = (n)$. □

We can also characterise the prime and maximal ideals in $\mathbb{Z}$.

Proposition 2.4.11. *Let $n \in \mathbb{Z}$, and let $I = (n)$. Then, the ideal I is prime if and only if $n = 0$ or $|n|$ is prime.*

Proof. We consider the 4 possibilities of n:

- If $n = 0$, then the ideal $(0) = \{0\}$ is prime. This is because, for $r \in R$, $r \cdot 0 = 0$.
- If $|n| = 1$, then the ideal $I = (1) = \mathbb{Z}$. So, I cannot be prime.
- Assume that n is a prime. Let $a, b \in \mathbb{Z}$ such that $ab \in I$. In that case, $n \mid ab$. Since n is a prime, this implies that either $n \mid a$ or $n \mid b$. So, either $a \in I$ or $b \in I$. Therefore, I is prime.
- Assume that n is not $-1, 0, 1$ or a prime. In that case, n is composite. So, let $a, b \in \mathbb{Z}$ with $a, b \neq \pm 1$ such that $n = ab$. We have $a, b \notin I$, so $ab \in I$. Therefore, I is not prime.

□

Proposition 2.4.12. *Let $n \in \mathbb{Z}$, and let $I = (n)$. Then, the ideal I is maximal if and only if $|n|$ is prime.*

Proof. We consider the 4 possibilities of n:

- If $n = 0$, then the ideal $I = (0) = \{0\}$. We have $I \subseteq (2) \subseteq \mathbb{Z}$, so I is not maximal.
- If $|n| = 1$, then the ideal $I = (1) = \mathbb{Z}$. So, I cannot maximal.
- Assume that n is a prime. Let J be an ideal of $\mathbb{Z}$ such that $I \subsetneq J \subseteq \mathbb{Z}$. In that case, there exists an $a \in J$ such that $a \notin I$. Since n is a prime, we know that $\gcd(a, n) = 1$. So, Euclid's Theorem tells us that there exist $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Since $a, n \in J$, we find that $1 = ax + ny \in J$. Since $1 \in \mathbb{Z}$ is a unit, we find that $J = \mathbb{Z}$. Therefore, I is maximal.
- Assume that n is not $-1, 0, 1$ or a prime. In that case, n is composite. So, let $a, b \in \mathbb{Z}$ with $a, b \neq \pm 1$ such that $n = ab$. We have $(n) \subsetneq (a) \subsetneq \mathbb{Z}$. So, I cannot be maximal.

□

Now, we show how to form a bigger ideal by adding two ideals.

Proposition 2.4.13. *Let R be a ring, and let I, J be ideals of R. Then,*

$$I + J = \{i + j \mid i \in I, j \in J\}$$

is an ideal of R.

Proof. Let $a, b \in I + J$. In that case, there exist $i_1, r_2 \in I$ and $j_1, j_2 \in J$ such that $a = i_1 + j_1$ and $b = i_2 + j_2$. Therefore,

$$a + b = (i_1 + j_1) + (i_2 + j_2) = (i_1 + i_2) + (j_1 + j_2) \in I + J.$$

So, $I + J$ is closed under addition. Moreover, since $0 \in I$ and $0 \in J$, we have $0 \in I + J$. Next, let $c \in I + J$. In that case, there exist $i \in I$ and $j \in J$ such that $c = i + j$. In that case, $-i \in I$ and $-j \in J$. Therefore, $-c = -i - j \in I + J$. Finally, for $a \in I + J$ and $r \in R$,

$$ra = r(i + j) = ri + rj \in I + J,$$

and

$$ar = (i + j)r = ir + jr \in I + J$$

since I and J are ideals. Therefore, $I + J$ is an ideal. □

Moreover, the ideal $I + J$ is the smallest containing I and J. That is, for an ideal K such that $I \subseteq K$ and $J \subseteq K$, then $I + J \subseteq K$. This is because if the ideal contains both I and J, it must contain sums of elements in I and J since it is closed under addition.

We now show two big results concerning prime and maximal ideals. It turns out that an ideal is prime if and only if the corresponding quotient is an integral domain.

Proposition 2.4.14. *Let R be a commutative unital ring, and let I be a proper ideal. Then, I is prime if and only if R/I is an integral domain.*

Proof.

- Assume that I is prime. Let $a + I, b + I \in R/I$ such that $(a + I)(b + I) = 0 + I$. In that case, $ab + I = 0 + I$, and so $ab \in I$. Since I is prime, we find that either $a \in I$ or $b \in I$. This implies that either $a + I = 0$ or $b + I = 0$. So, R/I is an integral domain.
- Assume that R/I is an integral domain. Let $a, b \in R$ such that $ab \in I$. In that case,
$$ab + I = (a + I)(b + I) = 0 + I.$$
Since R/I is an integral domain, either either $a+I = 0+I$ or $b+I = 0+I$. Therefore, either $a \in I$ or $b \in I$. So, I is prime.

Therefore, I is prime if and only if R/I is an integral domain. □

For example, $\mathbb{Z}[X]$ is a commutative unital ring, and $I = (X)$ is an ideal. Here, $\mathbb{Z}[X]/I \cong \mathbb{Z}$,[8] so I must be a prime ideal. Next, we show that an ideal is maximal if and only if the corresponding quotient is a field.

[8] We can consider the (surjective) evaluation map $\mathbb{Z}[X] \to \mathbb{Z}$ given by $f \mapsto f(0)$. Then, the kernel is (X), so the result follows from the First Isomorphism Theorem.

Proposition 2.4.15. *Let R be a commutative unital ring, and let I be a proper ideal. Then, I is maximal if and only if R/I is a field.*

Proof.

- Assume that I is maximal, and let $a + I \in R/I$ with $a + I \neq 0 + I$. In that case, $a \notin I$. So, define the ideal

$$S = (a) + I = \{ra + i \mid r \in R, i \in I\}.$$

  We know that $I \subsetneq S$. Since I is maximal, so we must have $S = R$. In that case, there exists an $r \in R$ and an $i \in I$ such that $ra + i = 1$. Moreover,

$$(r + I)(a + I) = ra + I = (ra + i) + I = 1 + I.$$

  So, $r + I$ is a unit. Therefore, every non-zero element in R/I is a unit- it is a field.

- Assume that R/I is a field, and let J be an ideal of R such that $I \subsetneq J$. So, there exists a $j \in J$ such that $j \notin I$. Since R/I is a field, this implies that $j + I$ is a unit. Therefore, let $k + I$ be the inverse of $j + I$. In that case,

$$(j + I)(k + I) = jk + I = 1 + I.$$

  In that case, there exists an $i \in I$ such that $jk + i = 1$. Since $j, i \in J$, we find that $1 \in J$. Therefore, $J = R$. So, I is maximal.

□

Since every field is an integral domain, for a commutative unital ring R, we can use the results above to find that a maximal ideal is prime. The converse is false, however. For example, in the polynomial ring $\mathbb{Z}[X]$, the ideal (X) is prime since the quotient $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ is an integral domain. But, the ideal (X) is not maximal since $\mathbb{Z}$ is not a field. We find that (X) is strictly contained within $(X, 2)$, so (X) cannot be maximal. Note that

$$(X, 2) = \{f = a_0 + a_1X + \cdots + a_dX^d \in \mathbb{Z}[X] \mid 2 \mid a_0\},$$

meaning that a polynomial in $(X, 2)$ has an even constant term. However, $(X, 2)$ is maximal.[9]

[9] In fact, $\mathbb{Z}[X]/(X, 2) = \mathbb{Z}/2\mathbb{Z}$, which is a field.

2.5 Polynomial Rings

Division in Polynomial Rings

In this section, we will look at division in polynomial rings. To establish that the remainder polynomial is 'smaller', we need to define the degree of a polynomial.

Definition 2.5.1. Let K be a field, and let $f(X) = a_0 + a_1X + \cdots + a_dX^d \in K[X]$ be a polynomial, with $a_d \neq 0$. Then, the *degree* $\deg f$ of f is defined to be d.

We haven't defined the degree for the zero polynomial.

Now, we are ready to consider the division algorithm in polynomial rings over a field.

Proposition 2.5.2 (Division Algorithm)**.** *Let K be a field, and let $f(X)$, $g(X) \in K[X]$ with $g(X) \neq 0$. Then, there exist unique $q(X), r(X) \in K[X]$ such that*

$$f(X) = g(X)q(X) + r(X),$$

with $\deg r < \deg g$ or $r(X) = 0$.

Proof.

- We first show existence. If $\deg g > \deg f$, then we can take $q(X) = 0$ and $r = f$. Now, suppose that $\deg g \geqslant \deg g$. Denote

  $$f = a_nX^n + \cdots + a_0, \qquad g = b_mX^m + \cdots + b_0,$$

  with $n \geqslant m$. Moreover, suppose that claim is true for all f_0 with $\deg f_0 < \deg f$. Let $q_0(X) = a_nb_m^{-1}X^{n-m}$. Then, $f_0(X) = f(X) - g(X) \cdot q_0(X)$ has degree $< n = \deg f$.[10] So, the assumption tells us that $f_0(X)$ can be written as $q_1(X)g(X) + r(X)$ $q_1(X) \in K[X]$ and $r(X)$ with either $r = 0$ or $\deg r < \deg f_0$. Then,

  $$f(X) = q_0(X) \cdot g(X) + f_0(X) = (q_0(X) + q_1(X)) \cdot g(X) + r(X).$$

  We have either $r = 0$ or $\deg r < \deg f_0 < \deg f$, so the statement is true by induction.

- Now, we show uniqueness. So, assume that there exist polynomials $q_0(X), r_0(X), q_1(X), r_1(X) \in K[X]$ with either $r_1(X) = 0$ or $\deg r_1 < \deg g$, and either $r_2(X) = 0$ or $\deg r_2 < \deg g$ such that

  $$f(X) = g(X)q_1(X) + r_1(X) = g(X)q_2(X) + r_2(X).$$

  In that case,

  $$g(X)[q_1(X) - q_2(X)] = r_2(X) - r_1(X).$$

  We know that either $r_2(X) - r_1(X) = 0$ or $\deg(r_2 - r_1) < \deg g$. Moreover, we know that either $g(X)[q_1(X) - q_2(X)] = 0$ or $\deg(g(q_1 - q_2)) \geqslant g$. So, we must have both $r_2(X) - r_1(X) = 0$ and $g(X)[q_1(X) - q_2(X)] = 0$. So, both $r_2(X) = r_1(X)$ and $q_1(X) = q_2(X)$ (since $g(X) \neq 0$ and $K[X]$ is an integral domain). Therefore, the polynomials $q_1(X)$ and $r_1(X)$ are unique.

[10] The degree need not be $n-1$, since we could have cancelled further terms as well!

□

We illustrate this with an example. Let $f(X) = 4X^4 - 2X^2 - X$ and $g(X) = X^2 - 15X$. First, we multiply g by $q_0 = 4X^2$ so that $f - gq_0$ has degree 3- we lower the degree iteratively until it is less than $\deg g = 2$. We have

$$f - g \cdot q_0 = 60X^3 - 2X^2 - X.$$

Next, we multiply g by $q_1 = 4X^2 + 60X$ so that $f - g \cdot q_1$ now has degree 2. We have

$$f - g \cdot q_1 = 898X^2 - X.$$

So, now we multiply g by $q_2 = 4X^2 + 60X + 898$ so that $f - g \cdot q_2$ has degree 1. This degree is less than 2, so we are done- the remainder is

$$f - g \cdot q_2 = 13469X.$$

We can use this result to show that $f(a) = 0$ if and only if $X - a \mid f$.

Corollary 2.5.3. *Let K be a field, let $f(X) \in K[X]$, and let $a \in K$. Then, $f(a) = 0$ if and only if there exists $g(X) \in K[X]$ such that $f(X) = (X - a) \cdot g(X)$.*

Proof.

- First, assume that $f(X) = (X - a) \cdot g(X)$. In that case,

$$f(a) = (a - a) \cdot g(a) = 0 \cdot g(a) = 0.$$

- Now, assume that $f(a) = 0$. The division algorithm for polynomial rings tells us that there exist $g, r \in K[X]$ such that $r(X) = c$, for some $c \in R$, with

$$f(a) = (X - a)g(X) + c.$$

We have

$$0 = f(0) = (a - a)g(0) + c = c.$$

Therefore, $f(a) = (X - a) \cdot g(X)$.

So, $f(a) = 0$ if and only if there exists $g(X) \in K[X]$ such that $f(X) = (X - a) \cdot g(X)$. □

Using this result, we can show that in a field K, a non-zero polynomial $f \in K[X]$ hast at most $\deg f$ zeroes- we can keep factorising f, and there can be at most $\deg f$ distinct factors.

Irreducible Polynomials

Now, we look at irreducible polynomials.

Definition 2.5.4. Let K be a field, and let $f \in K[X]$ have $\deg f > 0$. Then, f is called *irreducible over K* if whenever $g, h \in K[X]$ are such that $f = gh$, then either $\deg g = 0$ or $\deg h = 0$. If f is not irreducible, then it is called *reducible*.

So, the polynomial $f(X) = X - 1 \in \mathbb{R}[X]$ is irreducible, although we can write it as $f(X) = \frac{1}{2}(2X - 2)$. Also, the polynomial $f(X) = X^2 + 1$ is irreducible in $\mathbb{R}[X]$. However, the polynomial $f(X) = X^2 + 1$ is reducible in $\mathbb{C}[X]$- we can write $f(X) = (X + i)(X - i)$. So, irreducibility depends on the field we are looking at.

Now, we show that every ideal in a polynomial ring over a field is principal.

Proposition 2.5.5. *Let K be a field, and let $I \subseteq K[X]$ is an ideal. Then, there exists $f \in K[X]$ such that $I = (f)$.*

Proof. If $I = \{0\}$, then $I = (0)$. Now, assume that $I \neq \{0\}$. In that case, there exists a $g \in I$ such that $g(X) \neq 0$. So, fix $f \in I$ such that the degree of f is minimal. Since $f \in I$, we find that $(f) \subseteq I$. Now, let $g \in I$. By the division algorithm for rings, we can find $q, r \in K[X]$ such that

$$g = f \cdot q + r,$$

where $r(X) = 0$ or $\deg r < \deg f$. Since $f, g \in I$, we find that

$$r = g - f \cdot q \in I.$$

Since $\deg f$ is minimal and $r \in I$, we must have $r(X) = 0$. Therefore, $g = f \cdot q \in (f)$. This implies that $(f) = I$. □

Note that we require K to be a field[11]- for example, in $\mathbb{Z}$, the ideal $(X, 2)$ is not principal. Now, let I be the ideal of $\mathbb{Q}[X]$ generated by $X^2 + X$ and $X^4 + X^3 + X$, i.e.

$$I = (X^2 + X, X^4 + X^3 + X) = \{f \cdot (X^2 + X) + g \cdot (X^4 + X^3 + X) \mid f, g \in \mathbb{Q}[X]\}.$$

By the result above, we know that I is principal. Like in the proof, we will try to find a polynomial $h \in I$ such that $I = (h)$ by finding the minimum possible degree. First, we try $h(X) = X^2 + X$. Dividing $X^4 + X^3 + X$ gives us

$$X^4 + X^3 + X = (X^2) \cdot (X^2 + X) + X.$$

So, the polynomial $X^2 + X$ is not of minimal degree; we have found a polynomial with degree 1- the polynomial X is in the ideal I. So, we now try $h(X) = X$. Since $h \in I$, we find that $(h) \subseteq I$. Moreover, the generators $X^2 + X$ and $X^4 + X^2 + X$ are multiples of h. Therefore, $I = (h)$.

We will now show that the maximal/prime ideals are generator by irreducible polynomials.

Proposition 2.5.6. *Let K be a field, and let $f \in K[X]$ be non-zero. Then, the following are equivalent:*

(1) the ideal $(f) = \{fg \mid g \in K[X]\}$ is maximal;

(2) the ideal (f) is prime;

(3) the polynomial f is irreducible in $K[X]$.

[11] In fact, K is a field if and only if every ideal I of $K[X]$ is principal!

Proof. We know that every maximal ideal is prime in a commutative unital ring, so (1) implies (2).
Assume that the ideal (f) is prime. If $\deg f = 0$, then $f(X) = x$, for some $x \in K$. Since $f \neq 0$, we know that $x \neq 0$. Therefore, x is a unit. This implies that $(f) = K[X]$, so (f) is not proper. So, we must have $\deg f \geqslant 1$. Now, let $f = gh$, for some $g, h \in K[X]$. Since $g, h \in K[X]$ such that $gh \in I$, and I is a prime ideal, we find that either $g \in I$ or $h \in I$. Without loss of generality, assume that $g \in I$. In that case, $g = fj$, for some $j \in K[X]$. Since $f = gh$, we find that $\deg g \leqslant \deg f$, and since $g = fj$, $\deg g \geqslant \deg f$. Therefore, $\deg g = \deg f$. In that case, $\deg h = \deg f - \deg g = 0$. This implies that f is irreducible. So, (2) implies (3).
Assume that f is irreducible. Therefore, $\deg f > 0$. So, (f) has no units, i.e. (f) is proper. Now, let J be an ideal of $K[X]$ such that $I \subseteq J \subseteq K[X]$. We know that $J = (g)$, for some polynomial $g \in K[X]$. We have $f \in J$, so $g = fh$, for some polynomial $h \in K[X]$. Since f is irreducible, we find that either $\deg g = 0$ or $\deg h = 0$. If $\deg g = 0$, then $g(X) = x$, for some $x \in K$ with $x \neq 0$. Since x is a unit, we find that $J = (g) = K[X]$. Instead, if $\deg h = 0$, then $h(X) = x$, for some $x \in K$ with $x \neq 0$. Since x is a unit, we find that $(f) = (xg) = J$.[12] This implies that (f) is maximal. So, (3) implies (1).
Therefore, the three statements are equivalent. □

So, if K is a field, and $f \in K[X]$ is an irreducible polynomial, then the quotient $K[X]/(f)$ is another field.

We will now focus on showing irreducibility. One simple proposition is- a polynomial of degree 2 or 3 is reducible if it has a root over the field.

Proposition 2.5.7. *Let K be a field, and let $f \in K[X]$ have degree 2 or 3. Then, f is reducible if and only if it has a root in K, i.e. there exists an $a \in K$ such that $f(a) = 0$.*

Proof.

- If there exists an $a \in K$ such that $f(a) = 0$, then we know that $f(X) = (X - a)g(X)$. In that case, f is reducible.
- Now, assume that f is reducible. By definition, there exist $g, h \in K[X]$ such that $f = gh$ with $\deg g < \deg f$ and $\deg f < \deg f$ and $\deg g + \deg h = \deg f$. Since $\deg f = 2$ or $\deg f = 3$, we find that either $\deg g = 1$ or $\deg h = 1$. Without loss of generality, assume that $\deg h = 1$. In that case, $f(X) = (a_0 + a_1 X)g(X)$. Therefore,

$$f(-a_0 a_1^{-1}) = (a_0 - a_1 a_1^{-1} a_0)g(X) = 0.$$

□

For instance, consider the field $K = \mathbb{Z}/3\mathbb{Z}$. The polynomial $f(X) = X^2 + 1 \in K[X]$ is irreducible. Since $\deg f = 2$, we know it is reducible if and only if it has a zero. But, $f(0 + 3\mathbb{Z}) = 1 + 3\mathbb{Z}$, $f(1 + 3\mathbb{Z}) = f(2 + 3\mathbb{Z}) = 2 + 3\mathbb{Z}$, so f must be irreducible using the result above. Therefore, the quotient $K[X]/(f)$ is a field. It is spanned by $1 + (f)$ and $X + (f)$, such that $X^2 + (f) = 2 + (f)$.

[12] Since $f = xg$, $g = x^{-1}f$. So, $f \in (g)$ and $g \in (f)$, and so the two ideals are equal.

Since the quotient is a vector space over $K = \mathbb{Z}/3\mathbb{Z}$ with dimension 2, we find that the quotient $K[X]/f$ has $3^2 = 9$ elements. In particular,

$$K[X]/(f) = \{a_0 + a_1X + (f) \mid a_0, a_1 \in \mathbb{Z}/3\mathbb{Z}\}.$$

The ring $\mathbb{Z}/9\mathbb{Z}$ is not a field, since $3 + 9\mathbb{Z}$ is a zero divisor. Similarly, the ring $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is not a field, since

$$(0 + 3\mathbb{Z}, 1 + 3\mathbb{Z})(1 + 3\mathbb{Z}, 0 + 3\mathbb{Z}) = (0 + 3\mathbb{Z}, 0 + 3\mathbb{Z}),$$

meaning that $(0 + 3\mathbb{Z}, 1 + 3\mathbb{Z})$ is a zero divisor. So, the field we have above is a group that is not isomorphic to either of these two rings. Nonetheless, as a group, the field is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ since the coefficents live in $\mathbb{Z}/3\mathbb{Z}$. Now, let $d \in \mathbb{Z}$ be a non-square. We know that the polynomial $X^2 - d \in \mathbb{Q}[X]$ is irreducible. So, the quotient $\mathbb{Q}[X]/(X^2 - d)$ is a field. It is spanned by $1 + (X^2 - d)$ and $X + (X^2 - d)$, with $X^2 + (X^2 - d) = d + (X^2 - d)$. Therefore,

$$\mathbb{Q}[X]/(X^2 - d) \cong \mathbb{Q}(\sqrt{d}) = \{a_0 + a_1\sqrt{d} \mid a_0, a_1 \in \mathbb{Q}\},$$

where the isomorphism map is $a + bX + (X^2 - d) \mapsto a + b\sqrt{d}$. Moreover, for a non-zero element $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, the inverse is

$$\frac{a - b\sqrt{d}}{a^2 - b^2 d}.$$

We will now look at showing polynomials are irreducible for higher degrees. We start by defining primitive polynomials.

Definition 2.5.8. A polynomial $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ is called *primitive* if $\gcd(a_n, \ldots, a_0) = 1$, i.e. there exists no prime p that divides all a_j.

It turns out that if we can factor a primitive polynomial, then there is some way to factor it with integer coefficients.

Proposition 2.5.9. *Let $f \in \mathbb{Z}[X]$ be primitive. Then, f is reducible in $\mathbb{Q}[X]$ into polynomials of degree $r, s \in \{1, \ldots, n-1\}$ if and only if it factorises as a product of degree r and s polynomials in $\mathbb{Z}[X]$.*

Using this fact, we can show that $X^4 + 2$ is irreducible in $\mathbb{Q}[X]$. If it was reducible, then let $X^4 + 2 = f \cdot g$. We can have $\{\deg f, \deg g\} = \{1, 3\}$, meaning that $X^4 + 2$ has a root in $\mathbb{Q}$. However, this is not true, so we must have $\deg f = \deg g = 2$. By Gauss's Lemma, assume that $f, g \in \mathbb{Z}[X]$ without loss of generality. Denote

$$f(X) = a_2X^2 + a_1X + a_0, \qquad g(X) = b_2X^2 + b_1X + b_0.$$

The coefficient of X^4 in fg is $a_2 \cdot b_2 = 1$, so either $a_2 = b_2 = 1$ or $a_2 = b_2 = -1$. Without loss of generality, assume that $a_2 = b_2 = 1$. Now,

$$\begin{aligned} f(X)g(X) &= (X^2 + a_1X + a_0)(X^2 + b_1X + b_0) \\ &= X^4 + (a_1 + b_1)X^3 + (a_0 + a_1b_1 + b_0)X + a_0b_0 \\ &= X^4 + 2. \end{aligned}$$

Comparing terms, we find that $a_1 = -b_1$. Since $a_0 b_0 = 2$, we have $a_0, b_0 \in \{1, -1, 2, -2\}$. Without loss of generality, assume that $a_0 \in \{1, -1\}$ and $b_0 \in \{2, -2\}$. Moreover,

$$a_0 + a_1 b_1 + b_0 = a_0 + b_0 - a_1^2 = 0$$

We can either have $a_0 + b_0 = 3$ or $a_0 + b_0 = -3$. However, there are no integers such that $a_1^2 = \pm 3$. Therefore, we cannot reduce $X^4 + 2$ over $\mathbb{Z}$, and therefore we cannot reduce $X^4 + 2$ over $\mathbb{Q}$.

We now look at another criterion for irreducibility- Eisenstein's criterion.

Proposition 2.5.10 (Eisenstein's Criterion)**.** *Let p be a prime number, and let*

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$$

be such that $p \nmid a_n$ and $p \mid a_i$ for all $i < n$, and $p^2 \nmid a_0$. Then, f is irreducible in $\mathbb{Q}[X]$.

We can easily show that the polynomial $X^4 + 2$ is irreducible over $\mathbb{Q}$ using Eisenstein's criterion with $p = 2$. We will use the criterion to show that the polynomial $X^{p-1} + X^{p-2} + \cdots + X + 1$ is not reducible over $\mathbb{Q}$ for a prime p.

Proposition 2.5.11. *Let p be a prime. Then, the polynomial*

$$f(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$$

is irreducible in $\mathbb{Q}[X]$.

Proof. We have

$$\begin{aligned} f(X+1) &= (X+1)^{p-1} + (X+1)^{p-2} + \cdots + (X+1) + 1 \\ &= X^{p-1} + (p-1)X^{p-2} + \frac{(p-1)(p-2)}{2} X^{p-3} + \cdots + (p-1)X + 1 \\ &\quad + X^{p-2} + (p-2)X^{p-3} + \cdots + (p-2)X + 1 + \cdots + X + 1 + 1. \end{aligned}$$

So, the X^{p-1} term is 1, so not divisible by p. However, all the other terms are divisible by p, and the constant term is p, and so not divisible by p^2. Therefore, Eisenstein's Criterion tells us that $f(X+1)$ is irreducible. Therefore, $f(X)$ too is irreducible. □

The polynomial $X^p - 1 = (X+1)(X^{p-1} + X^{p-2} + \cdots + X + 1)$, so

$$\begin{aligned} f(X+1) &= \frac{(X+1)^p - 1}{X + 1 - 1} \\ &= \frac{X^p + pX^{p-1} + \cdots + pX + 1 - 1}{X} \\ &= X^{p-1} + pX^{p-2} + \cdots + p. \end{aligned}$$

This allows us to expand $f(X+1)$ in a different way- since p is a prime, all the coefficients will be multiples of p except for X^{p-1}.