8. The theory of ideals

8.1 Ring homomorphisms and ideals

From now on, we will only consider **commutative rings**.

Ideals in ring theory play a similar role as normal subgroups in group theory and are used to construct **quotient rings**.

We have seen that $\ker(\varphi)$ of a group homomorphism $\varphi : G_1 \to G_2$ is a **normal** subgroup of G_1. That's why we start by studying ring homomorphisms and their kernels.

Definition 8.1.1: Ring homomorphism

Let $(R, +_R, \cdot_R)$ and $(S, +_S, \cdot_S)$ be two rings. A function

$$\varphi : R \to S$$

is a **ring homomorphism** if it satisfies

1. $\boxed{\varphi \text{ is a group homomorphism}}$ between the groups $(R, +_R)$ and $(S, +_S)$.
   - $\varphi(0_R) = 0_S$
   - $\varphi(r +_R s) = \varphi(r) +_S \varphi(s)$ for all $r, s \in R$
2. $\boxed{\varphi(1_R) = 1_S}$
3. $\boxed{\varphi(r \cdot_R s) = \varphi(r) \cdot_S \varphi(s)}$ for all $r, s \in R$

Example: $\psi : \begin{cases} \mathbb{Z} \to \mathbb{Z}_n \\ a \mapsto a \bmod n \end{cases}$ is a ring homomorphism from $(\mathbb{Z}, +, \cdot)$ to $(\mathbb{Z}_n, +_n, \cdot_n)$.

It says that you can perform the addition and multiplication operations before or after taking the modulus, and the result is the same. We already saw this in Corollary 1.3.8:

$$\forall a, b \in \mathbb{Z} : a +_n b = (a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$$

Which is equivalent to

$$\psi(a + b) = \psi(a) +_n \psi(b).$$

Similarly for multiplication:

$$\forall a, b \in \mathbb{Z} : a \cdot_n b = (a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$$

Which is equivalent to

$$\psi(a \cdot b) = \psi(a) \cdot_n \psi(b).$$

Ring Isomorphism

A **ring isomorphism** is a **bijective** ring homomorphism $\varphi : R \to S$.

A rich source of ring homomorphisms comes from the evaluation of polynomials of subrings $R \subseteq S$ in points of the larger rings S.

Definition: Subring

Let $(S, +, \cdot)$ be a ring. Then R is a **subring** of S if

- $R \subseteq S$
- $0_R = 0_S$
- $1_R = 1_S$
- we restrict the operations $+$ and $\cdot$ of S to R, making $(R, +, \cdot)$ a ring.

In such a setting, a polynomial $p(X) \in R[X]$ is also a polynomial in $S[X]$. Thus, we can define the evaluation of $p(X)$ at a point $a \in S$.

Example: $\mathbb{Z}$ is a subring of $(\mathbb{R}, +, \cdot)$. Because a polynomial $p(X) \in \mathbb{Z}[X]$ is also a polynomial in $\mathbb{R}[X]$, we can define the evaluation of $p(X)$ at a point $a \in \mathbb{R}$.

Proposition 8.1.2

Let R be a subring of S. Then for any $a \in S$, the **evaluation map**

$$\psi : \begin{cases} R[X] \to S \\ p(X) \mapsto p(a) \end{cases}$$

is a **ring homomorphism**.

Example: $R = \mathbb{Z}$ is a subring of $(S, +, \cdot) = (\mathbb{C}, +, \cdot)$. Choosing $a = 2 \in \mathbb{C}$, we get the ring homomorphism

$$\psi : \begin{cases} \mathbb{Z}[X] \to \mathbb{C} \\ p(X) \mapsto p(2) \end{cases}$$

which is not a ring isomorphism since it is not injective ($\psi(2) = 2 = \psi(X^2)$).

Definition 8.1.4: Kernel of a ring homomorphism

Let $\varphi : R \to S$ be a ring homomorphism. The **kernel** of φ is the set

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

By Theorem 6.1.9, $\ker(\varphi)$ is a **normal** subgroup of the group $(R, +_R)$. However, by the definition of a ring (Definition 7.1.1), $(R, +_R)$ is an **abelian** group, so

$$\boxed{\textbf{every subgroup of } (R, +_R) \textbf{ is automatically normal}}$$

Thus, we conclude that $\ker(\varphi)$ is a subgroup of $(R, +_R)$.

Theorem 8.1.6: Properties of the kernel of a ring homomorphism

Let $\varphi : R \to S$ be a ring homomorphism. Then its kernel $\ker(\varphi)$ has the following properties:

1. $\ker(\varphi) \subseteq R$ is a (normal) **subgroup** of the **additive group** $(R, +_R)$ of the ring R.
2. $\forall r \in R, \forall x \in \ker(\varphi) :$ $\boxed{r \cdot_R x \in \ker(\varphi)}$.

Definition 8.1.7: Ideal

Let $(R, +_R, \cdot_R)$ be a *commutative ring*. A subset $I \subseteq R$ is an **ideal** of R if

1. $I \subseteq R$ is a **subgroup** of the **additive group** $(R, +_R)$ (and thus **normal**).
2. $\boxed{\forall r \in R, \forall x \in I: \quad r \cdot_R x \in I}$.

Examples:

1. Trivial ideals:

$$\{0_R\} \text{ and } R$$

2. In the ring $(\mathbb{Z}, +, \cdot)$:

$$\boxed{I = n\mathbb{Z} = \{n \cdot k \mid k \in \mathbb{Z}\} \text{ is an ideal for any integer } n}$$

- I is a subgroup of $(\mathbb{Z}, +)$, because $I = n\mathbb{Z} = \langle n \rangle$ (the subgroup generated by n)
- We show that $\forall x \in I, \forall r \in \mathbb{Z}: \boxed{r \cdot x \in I}$. Take any $x \in n\mathbb{Z}$. Then there exists $k \in \mathbb{Z}$ such that $x = n \cdot k$. Thus, for any $r \in \mathbb{Z}$, we have that

$$r \cdot x = r \cdot (n \cdot k) = n \cdot (r \cdot k) \in n\mathbb{Z} = I$$

because $\mathbb{Z}$ is **commutative**.

Every ideal contains 0_R

Let I be an ideal of a commutative ring $(R, +_R, \cdot_R)$. Then

$$\boxed{0_R \in I}$$

This is because I is a subgroup of the group $(R, +_R)$, and thus contains the identity element 0_R of this group.

Exam

$$\boxed{x \in I \implies \langle x \rangle \subseteq I}$$

Proof: $\langle x \rangle \overset{\Delta}{=} \{x \cdot_R r \mid r \in R\} = \{r \cdot_R x \mid r \in R\}$. By the definition of an ideal, $\forall r \in R: r \cdot_R x \in I$. Thus, $\langle x \rangle \subseteq I$.

Exercise 8.10: Intersection of Ideals

The **intersection** $I \cap$ of two ideals $I,$ of a commutative ring $(R, +_R, \cdot_R)$ is again an **ideal** of R.

However, the union I of two ideals $I,$ of a commutative ring $(R, +_R, \cdot_R)$ is in general **not** an ideal of R.
Consider, for example, $I = 2\mathbb{Z} = \langle 2 \rangle$ and $= 3\mathbb{Z} = \langle 3 \rangle$, which are both ideals of the ring $(\mathbb{Z}, +, \cdot)$. Now, it holds that $2 \in I$ and $3 \in$, but $2 + 3 = 5 \notin I$. Thus, I is not closed under addition and therefore not an ideal of $(\mathbb{Z}, +, \cdot)$ (it is not even a subgroup of $(\mathbb{Z}, +)$).

The kernel of a ring homomorphism is an ideal

Let $\varphi: R \to S$ be a ring homomorphism. Then its **kernel** $\ker(\varphi)$ **is an ideal** of the ring R.

Trivial ideals of the commutative ring $(R, +, \cdot)$ are $\{0_R\}$ and R itself.
In fact, these trivial ideals are **principal ideals**, since $\{0_R\} = \langle 0_R \rangle$ and $R = \langle 1_R \rangle$:

Exercise 8.6

If an ideal $I \subseteq R$ contains a **unit** $u \in R^*$, then $I = R$.

$$\exists u \in R^* : \boxed{u \in I \implies I = R}$$

For example, if $1_R \in I$, then for any $r \in R$, we have that $r = r \cdot_R 1_R \in I$ by the definition of an ideal. Thus, $I = R$.

So, if we want to **find non-trivial ideals**, we have to look for ideals that **do not contain any units**.

The proof of the more general case for any unit $u \in R^*$ is as follows: assume that $u \in I$ then:

$$\begin{aligned} \forall r \in R : r \cdot u^{-1} \in R \quad &\implies r \cdot u^{-1} \cdot u \in I \qquad (\text{by definition of ideal, since } u \in I) \\ &\implies r \in I \qquad (\text{since } u^{-1} \cdot u = 1_R) \end{aligned}$$

Definition 8.1.10: Principal ideal

Let $(R, +_R, \cdot_R)$ be a commutative ring and $x \in R$. Define
A **principal ideal** is an ideal $I \subseteq R$ such that $I = \langle x \rangle$ with

$$\boxed{I = \langle x \rangle := \{x \cdot r \mid r \in R\}}$$

We call x a **generator** of the ideal $I = \boxed{\langle x \rangle \overset{\text{not}}{=} xR} \subseteq R$.

It turns out that any ideal in the ring $(\mathbb{Z}_6, +_6, \cdot_6)$ is a principal ideal. **Lagrange's theorem** says that the subgroup $I \subseteq (\mathbb{Z}_6, +_6)$ has order $|I|$ dividing 6. Thus, $|I| \in \{1, 2, 3, 6\}$. The subgroups of these orders are $\{0\}$, $\{0, 3\}$, $\{0, 2, 4\}$ and $\mathbb{Z}_6$ itself. One can check that these are also ideals of the ring $(\mathbb{Z}_6, +_6, \cdot_6)$:

- $\{0\} = \langle 0 \rangle$
- $\{0, 3\} = \langle 3 \rangle$
- $\{0, 2, 4\} = \langle 2 \rangle$
- $\mathbb{Z}_6 = \langle 1 \rangle$

Finding ideals I

By Langrange's Theorem,

$$\boxed{|I| \text{ divides } |R|}$$

for any ideal I of a finite commutative ring $(R, +_R, \cdot_R)$.
Furthermore, because of exercise 8.6, $I = R$ if I contains a unit of R. So to find non-trivial ideals, we look for ideals that satisfy

$$\boxed{I \cap R^* = \emptyset}, \qquad |I| \text{ divides } |R|, \qquad I \neq 0_R, R.$$

Lemma 8.1.13 (p165)

Let $(R, +_R, \cdot_R)$ be a commutative ring and $x_1, \ldots, x_n \in R$. Then the set

$$\boxed{\langle x_1, x_2, \ldots, x_n \rangle := \{r_1 \cdot_R x_1 +_R \ldots +_R r_n \cdot_R x_n \mid r_1, r_2, \ldots, r_n \in R\}}$$

is an **ideal** of R, called the **ideal generated by** $x_1, x_2, \ldots, x_n$.
The elements $x_1, x_2, \ldots, x_n$ are called **generators** of the ideal $\langle x_1, x_2, \ldots, x_n \rangle$.

Definition: Finitely generated ideal (p165)

An **ideal** I of a commutative ring $(R, +_R, \cdot_R)$ is called **finitely generated** if there exist $x_1, x_2, \ldots, x_n \in R$ such that

$$I = \langle x_1, x_2, \ldots, x_n \rangle.$$

These ideals are also called **Noetherian ideals**.

Noetherian ring

A **Noetherian ring** is a commutative ring in which **every ideal is finitely generated**.

Principal ideal ring (p165)

A **principal ideal ring** is a commutative ring in which **every ideal is a principal ideal**.

- An example of a principal ideal ring is $(\mathbb{Z}_6, +_6, \cdot_6)$
- Consider the ring $(\mathbb{Z}, +, \cdot)$. Then the congruence class $n\mathbb{Z}$ is a principal ideal of $(\mathbb{Z}, +, \cdot)$ generated by n:

$$\langle n \rangle = n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}.$$

Even if a finitely generated ring doesn't look like a principal ideal ring, it might still be one. For example, consider the ideal $\langle 5, 7 \rangle \subseteq \mathbb{Z}$ generated by 5 and 7. It turns out that this ideal is actually equal to the principal ideal $\langle 1 \rangle = \mathbb{Z}$, because 5 and 7 are relatively prime.

Lemma 8.1.15 (p166)

Let $n, m \in \mathbb{Z}$ be two integers and let $\langle n, m \rangle \subseteq \mathbb{Z}$ be the **ideal** of the ring of integers $(\mathbb{Z}, +, \cdot)$ generated by n and m. Then

$$\boxed{\langle n, m \rangle = \langle \gcd(n, m) \rangle}$$

The proof makes use of **Bézout's identity** from the *Extended* Euclidean algorithm:

Bézout's identity and the Extended Euclidean algorithm

$$\exists s, r \in \mathbb{Z} : \boxed{\gcd(n, m) = d = s \cdot n + r \cdot m}$$

In fact, in the next section, we will see that **any ideal** $I \subseteq \mathbb{Z}$ is a **principal** ideal, i.e.

$$\exists n \in \mathbb{Z} : I = \langle n \rangle$$

Given a concrete ideal, how to find its generator x? Page 167 gives the answer. We summarize it here:

Finding the generator of an ideal generated by finitely many elements (p167)

Let I be the ideal of the ring $(\mathbb{Z}, +, \cdot)$ that is generated by ℓ elements:
Then, by recursively applying Lemma 8.1.15, we get that

$$\boxed{I = \langle d_1, \ldots, d_\ell \rangle = \langle \gcd(d_1, \ldots, d_\ell) \rangle}.$$

8.2 Principal ideal domains

Definition: Principal ideal domain

A **principal ideal domain** (PID) is a commutative ring $(R, +_R, \cdot_R)$ that is both

- an **integral domain** (no zero divisors)
- a **principal ideal ring** ($\forall$ ideals $I \subseteq R : \exists x \in R : \boxed{I = \langle x \rangle}$)

Proposition 8.2.1 (p166)

The ring of integers is a **principal ideal domain** (PID):

$$\boxed{(\mathbb{Z}, +, \cdot) \text{ is a D}}$$

So **every ideal** $I \subseteq \mathbb{Z}$ is a **principal** ideal, i.e.

$$\forall I \subseteq \mathbb{Z} : \exists n \in \mathbb{Z} : \boxed{I = \langle n \rangle = n\mathbb{Z}}$$

So any ideal in $(\mathbb{Z}, +, \cdot)$ is of the form $n\mathbb{Z}$ for some integer n.
If $a + n\mathbb{Z}$ is a coset of such ideal, we may assume that $a \in \mathbb{Z}_n$, since because of Theorem 1.3.7, $a + n\mathbb{Z} = (a \bmod n) + n\mathbb{Z}$. If $a \in \mathbb{Z}_n$, we say that a is the **standard representative** of the coset $a + n\mathbb{Z}$ and that $a + n\mathbb{Z}$ is in **standard form**.

Now, we want to replicate this result for ideals in polynomial rings over a field $\mathbb{F}$.

Proposition 8.2.3 (p167)

Let $(\mathbb{F}, +, \cdot)$ be a field. Then the polynomial ring with coefficients in $\mathbb{F}$ is a PID:

$$\boxed{(\mathbb{F}[X], +, \cdot) \text{ is a principal ideal domain (D)}}$$

A divisor of polynomials in $(\mathbb{F}[X], +, \cdot)$

A polynomial $d(X) \in \mathbb{F}[X]$ is called a **divisor** of a polynomial $f(X) \in \mathbb{F}[X]$ if there exists a polynomial $q(X) \in \mathbb{F}[X]$ such that

$$f(X) = d(X) \cdot q(X).$$

Greatest common divisor (gcd) of polynomials in $(\mathbb{F}[X], +, \cdot)$

Let $f_1(X), f_2(X) \in \mathbb{F}[X]$ be two polynomials. We define **a greatest common divisor** (gcd) of $f_1(X)$ and $f_2(X)$ as a polynomial $d(X) \in \mathbb{F}[X]$ such that it has the **highest degree** among all common divisors of $f_1(X)$ and $f_2(X)$.

We wrote **a** common divisor because the gcd is **only unique up to multiplication by a non-zero constant** in $\mathbb{F}$. If $d(X)$ is a gcd of $f_1(X)$ and $f_2(X)$, then so is $a \cdot d(X)$ for any $a \in \mathbb{F}^* = \mathbb{F} \setminus \{0\}$. We can get around this by defining the gcd to be **monic** (leading coefficient equal to 1). This convention makes the **gcd unique**.

Exam

The GCD is **unique** if it is **monic**

$$\boxed{\gcd(f_1(X), f_2(X)) \textbf{ is uniue if it is monic}}$$

Lemma 8.2.4 (p168)

Let $f(X), g(X) \in \mathbb{F}[X]$ be two polynomials with coefficients in a field $\mathbb{F}$. Then

$$\boxed{\langle f(X), g(X)\rangle = \langle \gcd(f(X), g(X))\rangle}$$

Lemma 8.2.6 (p168)

Let $(\mathbb{F}, +, \cdot)$ be a field and let $f(X) \in \mathbb{F}[X]$ be a polynomial of degree at least 1.
Then **any coset**

$$\boxed{g(X) + \langle f(X)\rangle} = \{g(X) + q(X) \cdot f(X) \mid q(X) \in \mathbb{F}[X]\}$$

of the ideal $I := \langle f(X)\rangle$ can be **uniquely** described in the **standard form**

$$\boxed{r(X) + I} \quad \text{with } \boxed{\deg(r(X)) < \deg(f(X))}.$$

Where the **unique standard representative** $r(X)$ is the **remainder** of the polynomial division of $g(X)$ by $f(X)$.

Proof: we have either

- $\boxed{deg(g(X)) < \deg(f(X))}$: The coset is already in standard form; just choose $r(X) := g(X)$.
- $\boxed{deg(g(X)) \geq \deg(f(X))}$: then perform **polynomial division** of $g(X)$ by $f(X)$ to get

  $$\boxed{g(X) = q(X) \cdot f(X) + r(X)}$$

  Because $q(X) \cdot f(X) \in \mathbb{F}[X]$, and because for any subgroup $H \subseteq G : fH = H \Leftrightarrow f \in H$:

  $$\begin{aligned} g(X) + I &= [q(X) \cdot f(X) + r(X)] + I \\ &= [(q(X) \cdot f(X)) + \langle f(X)\rangle] + [r(X) + \langle f(X)\rangle] \\ &= [0 + \langle f(X)\rangle] + [r(X) + I] \\ &= r(X) + I \end{aligned}$$

8.3 Quotient rings

In group theory, we considered **normal** subgroups in order to construct **quotient groups**. In ring theory, we will consider **ideals** in order to construct **quotient rings**.

Cosets of an ideal

Since an ideal I of the ring $(R, +, \cdot)$ is by definition a *subgroup* of the *additive group* $(R, +)$, we can define cosets of I in R by r as:

$$r + I = \{r + x \mid x \in I\}$$

Recall that any $r_1 \in r + I$ is called a **representative** of that coset.
Also recall that two cosets fH and gH are equal $\Leftrightarrow f^{-1}g \in H$ (Theorem 4.3.4). In the case of ideals, this means that two cosets $r + I$ and $s + I$ are equal if...

Equality of cosets of an ideal

Let I be an ideal of the commutative ring $(R, +, \cdot)$. Then

$$\boxed{r + I = s + I \iff s - r \in I} \qquad \text{(Theorem 4.3.4)}$$

Because $I \subseteq R$ is a subgroup of the additive group $(R, +)$ and the additive inverse of any element $r \in R$ is $-r$.

Furthermore, since $(R, +)$ is an **abelian** group, the left coset $r + I$ is equal to the right coset $I + r$ for any $r \in R$. This implies that I is a **normal subgroup of** R and therefore we can define the **quotient group** $(R/I, +)$ with addition defined by

$$\boxed{(r + I) + (s + I) := (r + s) + I}.$$

Lemma 8.3.1 (p169)

Let $I \subseteq R$ be an ideal of the commutative ring $(R, +, \cdot)$. Then the following operation on cosets is well defined:

$$\boxed{(r + I) \cdot (s + I) := (r \cdot s) + I}$$

Now we give the set R/I of all cosets of the ideal I in R the structure of a ring by defining addition and multiplication of cosets:

Theorem 8.3.2: quotient ring (p170)

Let $I \subseteq R$ be an ideal of the commutative ring $(R, +, \cdot)$. Then

$$\boxed{(R/I, +, \cdot)} \quad \text{with } R/I := \{r + I \mid r \in R\}$$

equipped with the addition and multiplication of cosets defined by

$$\begin{aligned}(r + I) + (s + I) &:= (r + s) + I \\ (r + I) \cdot (s + I) &:= (r \cdot s) + I\end{aligned}$$

is a commutative ring with

- **zero element** $\boxed{0_R + I = I = i + I} \quad \forall i \in I$
- **unit element** $\boxed{1_R + I} = \{1_R + x \mid x \in I\}$.

This ring is called the **quotient ring** of R by the ideal I.

We call the pronounce R/I as R **modulo** I.

Exam

$$\forall i \in I : \boxed{i + I = I} = 0_{R/I} = 0_R + I$$

Why is $I = i + I$ for any $i \in I$? Because I is a subgroup of the additive (abelian) group $(R, +_R)$, so for any $i \in I$, we have that

$$\boxed{I = i + I_R} \iff 0_R +_R I = i +_R I \iff 0_R \sim_I i \iff -0_R +_R i = \boxed{i \in I}$$

Theorem 8.3.5: Isomorphism Theorem of Rings (p171)

Let $\psi : R \to S$ be a ring homomorphism between rings $(R, +_R, \cdot_R)$ and $(S, +_S, \cdot_S)$.
Then the map

$$\boxed{\overline{\psi} : \begin{cases} R/\ker(\psi) \to \operatorname{im}(\psi) \\ r + \ker(\psi) \mapsto \psi(r) \end{cases}}$$

is **ring isomorphism**, and thus

$$\boxed{R/\ker(\psi) \simeq \operatorname{im}(\psi)}.$$

8.4 Extended Euclidean algorithm for polynomials

For polynomials $f(X), g(X) \in (\mathbb{Z}_p[X], +_p, \cdot_p) = (\mathbb{F}_p[X], +_p, \cdot_p)$ over a finite field $\mathbb{F}_p$ (with p prime), we can compute their gcd using the **Extended Euclidean algorithm**: we find $r(X), s(X) \in \mathbb{F}_p[X]$ such that

Extended Euclidean algorithm for polynomials

For $f(X), g(X) \in \mathbb{F}_p[X]$, we can compute their gcd $m(X) = \gcd(f(X), g(X))$ together with polynomials $r(X), s(X) \in \mathbb{F}_p[X]$ such that

$$\boxed{\gcd(f(X), g(X)) \quad = \quad m(X) \quad = \quad r(X) \cdot f(X) + s(X) \cdot g(X)}$$

Where $m(X)$ is **unique** if it is **monic**.

To do so, we construct a matrix with two rows R_1 and R_2 initialized as

$$\left[\begin{array}{c|cc} f(X) & 1 & 0 \\ g(X) & 0 & 1 \end{array}\right]$$

Where each row represents the equation

$$R_i : \quad \text{position } 1 = (\text{position } 2) \cdot f(X) + (\text{position } 3) \cdot g(X)$$

We iteratively update this matrix with

$$\begin{cases} R_1 \;\; R_1 +_p v(X) \cdot R_2 & \text{if } \deg(R_1) \geq \deg(R_2) \\ R_1 \;\; R_2 & \text{if } \deg(R_2) > \deg(R_1) \end{cases}$$

where $v(X) \in \mathbb{F}_p[X]$ is the polynomial that makes the degree of R_1 strictly smaller after the update.

We stop when R_1 position 1 becomes **constant** (degree 0). Then, we have two possibilities:

- If R_1 position 1 is equal to 0, we ignore R_1 and look at the identity in R_2.
- If R_1 position 1 is equal to a non-zero constant $c \in \mathbb{F}_p^*$, we multiply the entire row R_1 by $c^{-1} \in \mathbb{F}_p^*$ to make the GCD **MONIC** (leading coefficient equal to 1).