Contents

Chapter 1

Unique Factorization

For us, ring means commutative ring with identity.

Definition 1.0.1 A *ring* is a set with two binary operations $(+, \cdot)$ satisfying

1. $(R, +)$ is an *abelian group*, which means
   - $+$ is commutative and associative.
   - $\exists\ 0_R, a + 0_R = 0_R + a$ for all $a \in R$.
   - Given $a \in R$, $\exists a' \in R$ such that $a + a' = 0_R$.
2. $\cdot$ is commutative and associative.
   $\exists\ 1_R$ such that $a \cdot 1_R = 1_R \cdot a = a$ for all $a \in R$.
3. $\cdot$ is distributive over addition, which means
   - $a \cdot (b + c) = a \cdot b + a \cdot c$
   - $(a + b) \cdot c = a \cdot c + b \cdot c$

Exercise 1.0.1

1. Show that $a + b = a + c \Rightarrow b = c$.(Cancellation)

   Proof.

   $$\begin{aligned} a + b = a + c &\Leftrightarrow a' + (a + b) = a' + (a + c) \\ &\Leftrightarrow (a' + a) + b = (a' + a) + c \\ &\Leftrightarrow 0_R + b = 0_R + c \\ &\Leftrightarrow b = c \end{aligned}$$

   ■

2. Show a' is unique. We denote this a' by $-a$.

   Proof. if the statement doesn't hold, then there exist a', a'' such that $a + a' = 0_R = a + a''$. We then apply cancellation and get $a' = a''$. ■

3. Show 0_R is unique.

   Proof. Say there are two zero element 0_R and $0'_R$, then we have

   $$0_R = 0_R + 0'_R = 0'_R$$

   ■

4. Show 1_R is unique.

Proof. Say there are two unit element 1_R and $1'_R$, then we have

$$1_R = 1_R \cdot 1'_R = 1'_R$$

■

5. Show $a \cdot 0_R = 0_R \cdot a = 0_R$

   Proof. We know that $a \cdot 0_R + a = a \cdot (0_R + 1_R) = a \cdot 1_R = a = 0_R + a$, apply cancellation then we are done. ■

6. Show that $(-1_R) \cdot a = -a$.

   Proof. Since $a \cdot 0_R = 0_R$, we have $a \cdot (1_R + (-1_R)) = 0_R$ or $a + (-1_R) \cdot a = 0_R$. Then $-a = (-1_R) \cdot a$, for a' is unique. ■

7. The zero ring is the ring with 1 element. Show R is zero ring $\Leftrightarrow 1_R = 0_R$.

   Proof.
   " $\Rightarrow$ " : Trivial.
   " $\Leftarrow$ " : Since we have $a \cdot 1_R = 1_R \cdot a = a$ for all $a \in R$ and $1_R = 0_R$, we have $0_R = a \cdot 0_R = a$ for all $a \in R$. ■

8. Does cancellation hold for $\cdot$?
   Sol. No. Consider $a \cdot b = a \cdot c$ and $a \neq 0_R$, then $a \cdot (b - c) = 0_R$. So if R is an *integral domain*, then we can apply cancellation of non-zero element.

Definition 1.0.2 R is said to be an *integral domain* if

$$a \cdot b = 0 \iff a = 0 \text{ or } b = 0.$$

Definition 1.0.3 R is said to be a field if every non-zero element in R has a multiplication inverse.

Exercise 1.0.2

1. If R is an integral domain, then we can apply cancellation of non-zero element.
2. Show that every field is an integral domain.

   Proof. If $a \cdot b = 0$ and $a \neq 0_R$, let a' be the multiplication inverse of a, then $b = 1_R \cdot b = a' \cdot a \cdot b = a' \cdot 0_R = 0$. ■

3. Check that a^{-1} is unique.

   Proof. If a^{-1} and a' are both multiplication inverse of a, then $a \cdot a^{-1} = a \cdot a' = 1_R$. Apply cancellation of non-zero element, we have $a' = a^{-1}$. ■

Remark 1.0.1 Though every field is an integral domain, not every integral domain is a field. For example, $\mathbb{Z}$ is an integral domain but not a field.

Ways to make new rings:

Let R be an integral domain, how to construct a new ring?
Let $K = \{(a, b), a, b \in R, b \neq 0\}$. We also define an equivalent relation $(a, b) \sim (c, d)$ if $ad = bc$.

- Check this is an equivalent class.
  - $(a, b) = (a, b)$
  - if $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, then $(a, b) \sim (e, f)$
- We define

  - $(a,b)+(c,d)=(ad+bc.bd)$
  - $(a,b)\cdot(c,d)=(ac,bd)$

  Check these two operation pass to equivalent class.
- $0_K=[(0,1_R)]$, $1_K=[(1_R,1_R)]$

Definition 1.0.4 If R,S are two rings, a homomorphism $\phi: R\to S$ is a map such that
1. $\phi(1_R)=1_S$.
2. $\phi(a+b)=\phi(a)+\phi(b)$.
3. $\phi(ab)=\phi(a)\phi(b)$.

An isomorphism is a homomorphism that is both injective and surjective.

$\phi: R\to S$, $a\mapsto[(a,1_R)]$ is an injective homomophism. For example, we have $\mathbb{Z}\subset\mathbb{Q}$.

Remark 1.0.2 If R is a field, then the homomorphism is isomorphism, i.e., ϕ is also surjective. Because for any $[(a,b)]\in K$, we have $\phi(ab^{-1})=[(ab^{-1},1)]=[(a,b)]$.

Ways to kill elements:

Definition 1.0.5 An ideal I in R is a non-empty subset such that
1. I is closed under addition.
2. I is closed under multiplication by arbitrary elt in R.

Note that $(I,+)\subset(R,+)$ is an abelian subgroup.

Example 1
- (0) is an ideal.
- R itself is an ideal.
- if $a\in R$, the $R\cdot a$ is an ideal, denoted by $(a)_R$.
- $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$.

Quotient Ring: Let $I\subset R$ be an ideal. $R/I=$ coset of I in $R=\{a+I, a\in R\}$, we define
1. $(a+I)\oplus(b+I)=(a+b)+I$.
2. $(a+I)\odot(b+I)=ab+I$.

with zero elt $(0+I)$ and identity elt $(1+I)$.