Chapter 7

Week6

7.1. Ring

Definition 7.1 [Ring] A **ring** $R = (R, +, *)$ is a set equipped with **two** binary operations:

$$+, * : R \times R \to R,$$

1. $(R, +)$ is an **abelian** group with an **additive identity** 0
2. The multiplication $*$ is **associative**, i.e.,

$$(a * b) * c = a * (b * c), \quad \forall a, b, c \in R$$

3. R satisfies the **distributive laws**: for $\forall a, b, c \in R$, we have

   (a) $a * (b + c) = a * b + a * c$

   (b) $(a + b) * c = a * c + b * c$

Moreover, if R has a **multiplicative identity** $1 \in R$ such that

$$1 * a = a * 1 = a, \forall a \in R,$$

then R is called a **unital ring**. ■

Question for ring: Does the ring contain the additive inverse?

■ **Example 7.1** 1. $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ are unital rings; $2\mathbb{Z}$ is a ring but not unital: since $1 \notin 2\mathbb{Z}$

2. The set of polynomials $\mathbb{Z}[x],\mathbb{Q}[x],\mathbb{R}[x],\mathbb{C}[x]$ are **unital rings**
3. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ is a unital ring
4. $\boldsymbol{M}_2(\mathbb{Z})$ is a unital ring; $\{\begin{bmatrix} a & a \\ a & a \end{bmatrix} \mid a \in \mathbb{Z}\}$ is also a unital ring (Question?)
5. $\mathcal{C}[a,b]$ is a unital ring
6. $(\mathbb{N},+,*)$ is **not** a ring. (Question? Is the set $\mathbb{N}$ not containing 0?)

■

R

1. We write ab for $a * b$
2. The additive identity 0 for R is **unique**
3. The additive inverse for any $r \in R$ is **unique** (we pre-assume its existence)
4. **Commutativity** is required for addition but not necessarily for multiplication
5. Each element in R has an additive inverse, but not necessarily a multiplicative inverse, i.e., $\exists a \in R$ such that $ab \neq 1$ for $\forall b \in R$.

Proposition 7.1 Each **unital** ring R contains a unique additive identity and a unique multiplicative identity

Proof. It suffices to show the uniqueness of multiplicative identity. Suppose r_1, r_2 are two multiplicative identity of R, then $r_1 = r_1 r_2 = r_2$. ■

Proposition 7.2 If $r \in R$ has a multiplicative inverse r^{-1}, then r^{-1} is unique.

Proof. Suppose r_1^{-1}, r_2^{-1} are two multiplicative inverse of r, then $rr_1^{-1} = rr_2^{-1} = 1$, which follows that

$$r_1^{-1} = r_1^{-1}(rr_2^{-1}) = (r_1^{-1}r)r_2^{-1} = r_2^{-1}$$

■

Proposition 7.3 For each $r \in R$, we have $0r = r0 = 0$.

Proof. By distributive laws,

$$0r = (0+0)r = 0r + 0r,$$

which follows that

$$0 = (0r + 0r) + (-0r) = 0r + (0r + (-0r)) = 0r + 0 = 0r.$$

Question: Why not left-adding the term $0r$?

Similarly, we have $r0 = 0$. ■

Proposition 7.4 For each $r \in R$, we have $(-1)(-r) = (-r)(-1) = r$.

Proof. Consider the equation

$$0 = 0(-r) = (1 + (-1))(-r) = -r + (-1)(-r),$$

which follows that $(-1)(-r) = r$.

Similarly, $(-r)(-1) = r$. ■

Proposition 7.5 For each $r \in R$, we have $(-1)r = r(-1) = -r$.

Proof. Consider the equation

$$0 = 0r = (1 + (-1))r = r + (-1)r$$

which follows that $-r = (-1)r$ ■

Proposition 7.6 If a ring R contains only a single element, then $R = \{0\}$. We call such R a **zero** ring.

Proposition 7.7 Let R be a set with binary operations $+$ and $*$ such that $(R, +)$ is a group; $(R, *)$ is a monoid (i.e., associative and identity); $(R, +, *)$ satisfies the distributive laws. Then $+$ is commutative.

Proof. Note that

$$\begin{aligned}(1+1)(x+y) &= (x+y)+(x+y) = x+y+x+y \\ &= (1+1)x+(1+1)y = x+x+y+y\end{aligned}$$

■

Definition 7.2 [Commutative] A ring R is **commutative** if its multiplication is **commutative**:

$$ab = ba, \forall ab \in R$$

■ **Example 7.2**

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are commutative rings, and so are $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$.
2. The ring $\boldsymbol{M}_n(\mathbb{Z})$ is not commutative for $n > 2$ (Question: is $n = 2$ ok?)

7.1.1. Modular Arithmetic

Definition 7.3 [Congruent modulo] Let $m \in \mathbb{Z}^+$. Then for $\forall a, b \in \mathbb{Z}$, we say they are **congruent modulo** m if $m \mid (a-b)$, i.e., $a \equiv b \pmod m$.

This modular congruent defines an equivalence relation on $\mathbb{Z}$.

R

1. Consider the set $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$. For each $n \in \mathbb{Z}$, let $\bar{n}$ denote the remainder of n divided by m, and therefore $\bar{n} \in \mathbb{Z}_m$. Here $\mathbb{Z}_m$ can be viewed as a collection of equivalence class representatives, i.e., for $\forall a \in \mathbb{Z}$, it congruent modulo m to unique one element in $\mathbb{Z}_m$

2. Define the operations

$$\bar{a} + \bar{b} = \overline{a+b}$$

$$\bar{a} * \bar{b} = \overline{a*b}$$

We can verify these operations are well-defined. Note that $(\mathbb{Z}_m, +)$ is a group; but $(\mathbb{Z}_m, *)$ is not necessarily a group, since the inverse of some element does not exist.

3. Unless otherwise mentioned,
   - $(\mathbb{Z}_m, +)$ denotes a group
   - $(\mathbb{Z}_m, +, *)$ denotes a ring.

4. The modular congruence classes corresponds to the **cosets** of $m\mathbb{Z}$ of $\mathbb{Z}$, and therefore $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$.

Proposition 7.8 $(\mathbb{Z}_m, +, *)$ is a unital commutative ring.

Proof. We have shown $(\mathbb{Z}_m, +)$ is a group. It suffices to show $(\mathbb{Z}_m, *)$ is a commutative monoid, and the distributive laws:

1. The associativity of multiplication is clear; the multiplication is commutative is easy to verify; the multiplicative identity is 1
2.
$$\bar{a} * (\bar{b} + \bar{c}) = \bar{a} * \overline{b+c} = \overline{a*(b+c)} = \bar{ab} + \bar{ac} = \bar{a} * \bar{b} + \bar{a} * \bar{c}$$

   The commutativity gives another distributive law.

■

Proposition 7.9 Let $m \in \mathbb{Z}^+$, suppose $a \equiv c (\bmod m)$ and $b \equiv d (\bmod m)$, then

$$a + b \equiv c + d (\bmod m), \quad ab \equiv cd (\mod m)$$

Proof. Since $x \equiv x' (\bmod m)$ iff $\bar{x} = \bar{x'}$; immediately we have

$$\overline{a+b} = \bar{a} + \bar{b} = \bar{c} + \bar{d} = \overline{c+d};$$

the other equality follows similarly. ■

7.1.2. Rings of Polynomials

Definition 7.4 [polynomial over rings] Let R be a **commutative** ring. A **polynomial** (in a variable x) over R is a formal sum

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

with $a_i \in R$ and $n = 0$ or the leading coefficient $a_n \neq 0$.

1. Here the degree of $f(x)$ is $\deg(f) = n$
2. $R[x]$ denotes the set of all polynomials over R.
3. The addition and multiplication for any two elements $f := \sum_{i=0}^{m} a_i x^i, g := \sum_{i=1}^{n} b_i x^i$ in R is given by:

$$f + g := \sum_{i=0}^{\max\{m,n\}} (a_i + b_i) x^i$$
$$fg := \sum_{i=0}^{m+n} \Big(\sum_{j+k=i} a_j b_k \Big) x^i$$

.

Proposition 7.10 With R defined above, $(R[x], +, *)$ is a commutative ring.

Proof. Note that $(R[x], +)$ forms an abelian group.

1. The multiplication is associative
2. $(R[x], *)$ has an identity element $f := 1$
3. The multiplication is commutative
4. The distributive laws are satisfied

■

(R) A polynomial f defines a function $f : R \to R$ by $a \mapsto f(a)$, but f may not be determined by $f : R \to R$, e.g.,

$$f(x) = 1 + x + x^2, g(x) = 1,$$

with the argument defined on $\mathbb{Z}_2$.

Proposition 7.11 Find a nonzero function $f(x) \in \mathbb{Z}_6[x]$ such that $f(x) \equiv 0$, i.e., $f(x) = 0$ for all $x \in \mathbb{Z}_6$.

Proof.

$$f(x) = x(x-1)(x-2)(x-3)(x-4)(x-5)$$

■

Question: abuse of notation for $\mathbb{Z}_6[x]$.

7.1.3. Integral Domains and Fields

Definition 7.5 [Integral Domain] Let D be a ring. A **nonzero** $r \in D$ is called a **zero divisor** if there exists a non-zero $s \in D$ such that $rs = 0$ or $sr = 0$. If D has no zero divisors, then D is called a **domain**. A **domain** that is a **commutative ring** is an **integral domain**.

■ **Example 7.3**

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all integral domains, and so are $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$. R is an integral domain iff $R[x]$ is an integral domain.
2. $\mathbb{Z}_6$ is **not** an integral domain since $2 * 3 \equiv 0 \pmod 6$. Thus $\mathbb{Z}_m$ is an integral domain iff m is a prime.
3. Let $R = C[-1,1]$, then R is not a integral domain. Consider piecewise function.

Proposition 7.12 Let D be a commutative ring, then the followings are equivalent:

1. D is an integral domain
2. For $\forall$ nonzero $a, b \in D$, we have $ab \neq 0$

3. D satisfies the **cancellation law**:

$$ca = cb, c \neq 0 \implies a = b$$

Proof. It is clear that (1) is equivalent to (2);

For (1) implies (3): If $ca = cb$, then by distributive laws:

$$c[a + (-b)] = ca + c(-b) = cb + c(-b) = c[b + (-b)] = 0,$$

which implies $c = 0$ or $a + (-b) = 0$ by applying the definition of integral domain, which implies $a = b$.

For (3) implies (1): suppose there exists nonzero $a, b \in D$ such that $ab = 0$. Note that $0 = a0$, which implies

$$ab = a0 \implies b = 0,$$

which is a contradiction. ■

R The proposition above can be generalized into non-commutative rings. Question.

Definition 7.6 Let R be a ring, then an element $a \in R$ is called a **unit** if it has a **multiplicative inverse** $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Question: Does such a ring **unital**?

■ **Example 7.4**

1. The only units of $\mathbb{Z}$ are ± 1
2. Let $R := \mathcal{F}(\mathbb{R})$, then a function $f \in R$ is a unit iff

$$f(x) \neq 0, \forall x \in \mathbb{R}$$

3. Let $R := \mathcal{C}(\mathbb{R})$, then $f \in R$ is a unit iff it is either **strictly positive** or **strictly negative**.

Proposition 7.13 The only units of $\mathbb{Q}[x]$ are **nonzero constants**.

Proof. Take $f \in \mathbb{Q}[x]$ with $\deg(f) \geq 1$, aruge that f cannot be unit. Then argue $f = 0$ can not. For nonzero constant f, construct $g = 1/f$ to be the inverse. ■

Definition 7.7 [Division Ring] A **division ring** R is a ring that all its nonzero elements are units; furthermore, if R is also commutative, then R is a field.

■ **Example 7.5**
1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, but $\mathbb{Z}$ is not
2. $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ are not division rings.
3. The **quaternions**

$$\mathbb{H} := \{a + bi + cj + dk \mid a,b,c,d \in \mathbb{R}, i^2 = j^2 = k^2 = ijk = -1\}$$

is a division ring with the usual addition and multiplication, but not a field.

Proposition 7.14 A field is an integral domain.

Proof. Assume not, then $rs = 0$ implies $r^{-1}rss^{-1} = 0$, which is a contradiction. ■

Proposition 7.15 Let $m \in \mathbb{Z}^+, k \in \mathbb{Z}_m^\# := \mathbb{Z}_m \setminus \{0\}$. Let $d = \gcd(k,m)$

1. If $d = 1$, then k is a unit.
2. If $d > 1$, then k is a zero divisor.

Proof. 1. If $d = 1$, there exists $a, b \in \mathbb{Z}$ such that

$$ak + bm = 1 \implies \bar{a} \cdot k = 1 \implies k \text{ is a unit}$$

If $d > 1$, then $k = hd$ for some $h \in \mathbb{Z}_m$, which implies

$$k \cdot (m/d) = hm = 0,$$

where $m/d \in \mathbb{Z}_m$

■

The results are summarized as follows:

$$\{\text{zero divisors in } \mathbb{Z}_m\} = \{k \in \mathbb{Z}_m^\# \mid \gcd(k,m) > 1\}$$
$$\{\text{units in } \mathbb{Z}_m\} := \mathbb{Z}_m^* = \{k \in \mathbb{Z}_m^\# \mid \gcd(k,m) = 1\}$$

Proposition 7.16 $(\mathbb{Z}_m^*, \cdot)$ forms a group, called the group of units in $\mathbb{Z}_m$.

Corollary 7.1 $\mathbb{Z}_m$ is a field iff m is prime.

For each prime p, the field $\mathbb{Z}_p$ can be written as $\mathbb{F}_q$

Definition 7.8 [Euler's phi function] $\phi(n) := |\mathbb{Z}_n^*|$ is called the Euler's phi function, which denotes the number of units in the ring $\mathbb{Z}_m$. ■

Theorem 7.1 — Euler's Theorem. Let $n \in \mathbb{Z}^+, a \in \mathbb{Z}_n^*$ be such that $\gcd(a,n) = 1$. Then $a^{\phi(n)} \equiv 1 (\bmod n)$.

Proof. It's clear that $\bar{a} \in \mathbb{Z}_n^*$. Suppose $\mathbb{Z}_n^* = \{u_1, \dots, u_{\phi(n)}\}$, and therefore

$$u_1\bar{a} \cdots u_{\phi(n)}\bar{a} \equiv u_1 \cdots u_{\phi(n)} (\bmod n),$$

which implies $a^{\phi(n)} \equiv (u_1 \cdots u_{\phi(n)})^2 \equiv 1 (\bmod n)$ ■

Proposition 7.17 Let $F = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, then F is a field.

Question: A field F can be equivalent to:

1. closed addition and multiplication
2. Identity and inverse for addition and multiplication
3. Associativity of $*$
4. Distributive law

Proof. For the multiplicative inverse,

$$(a+b\sqrt{2}) = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$$

■

Proposition 7.18 Every finite integral domain D with 1_D is a field

Proof. Consider $aa_i = aa_j$ iff $i = j$ by applying the distributive law ■

Proposition 7.19 Every finite integral domain D contains a multiplicative identity 1_D

Proof.

$$xa^n = xa^m \implies xa^{n-m} = x$$

■

Definition 7.9 [Characteristic] Let R be a ring. For each $n \in \mathbb{N}, a \in R$, define

$$n \circ a = \underbrace{a + \cdots + a}_{n \text{ terms}}, \quad 0 \circ a = 0_R$$

then n is called the **characteristic** of the ring R; if such n does not exist, then R is of characteristic 0. The characteristic of R is denoted as $\text{char}(R)$. If $R = F$ is a field, then $\text{char}(F)$ is the **characteristic** of the field F.

■ **Example 7.6**

$$\text{char}(\mathbb{Z}_n) = n$$

$$\text{char}(\mathbb{Z}) = \text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = \text{char}(\mathbb{C}) = 0$$

Proposition 7.20 The characteristic of an integral domain is either 0 or a prime,

Proof. Consider

$$(m \circ a) * (n \circ a) = (m * n) \circ a = 0$$

which implies $k \circ a = 0$ or $l \circ a = 0$. ■

Question: multiplication?

Theorem 7.2 Let R be a **unital** ring. If there exists a smallest $n \in \mathbb{Z}^+$ such that $n \circ 1 = 0$, then $\text{char}(R) = 0$, otherwise $\text{char}(R) = 0$

Proof. Suppose there exists, then $\text{char}(R) \geq n$.

$$n \circ a = a(1 + \cdots + 1) = a * (n \circ 1) = 0$$

thus $\text{char}(R) \leq n$. ■

7.1.4. Field of fractions

To make up a integral domain to be a field, we need to add some extra elements.

Equivalence relation. Let R be an integral domain and $S := \{(a,b) \mid a,b \in R, b \neq 0\}$

$$(a,b) \sim (c,d) \text{ iff } ad = bc$$

Define

$$(a,b) + (c,d) = (ad + bc, bd); (a,b) * (c,d) = (ac, bd)$$

Proposition 7.21 Suppose $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$, then

$$(a,b) + (c,d) \sim (a',b') + (c',d'), \qquad (a,b) * (c,d) \sim (a',b') * (c',d')$$

Definition 7.10 [Quotient set] Equipped with $(S, \sim)$, we define **quotient** set $S/\sim$ to be the set of all equivalence classes of S w.r.t. $\sim$ ■

■ **Example 7.7** For $\sim$ on $\mathbb{Z}$ s.t. $a \sim b$ iff $a \equiv b (\bmod 2)$, we have

$$\mathbb{Z}/\sim = \{2\mathbb{Z}, 2\mathbb{Z}+1\}$$

■

Definition 7.11 [Fraction field] Equipped with $(S, \sim)$, where $S = \{(a,b) \mid a,b \in R, b \neq 0\}$, we define **fraction field** of R to be the set $\text{Frac}(R) := S/\sim$, with the operation

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

■

Proposition 7.22 Let R be an integral domain, then $\text{Frac}(R)$ forms a field with additive identity $0 = [(0,1)]$ and the multiplicative identity $1 = [(1,1)]$. The multiplicative inverse of a non-zero element $[(a,b)] \in \text{Frac}(R)$ is $[(b,a)]$

R When $R = \mathbb{Z}$, we find $[(a,b)] \in \text{Frac}(\mathbb{Z})$ since $a/b \in \mathbb{Q}$, and therefore $\text{Frac}(\mathbb{Z}) \cong \mathbb{Q}$