

bb def: field: commutative ring, with unity, in which  $\forall$  nonzero element is a unit

def: ring with unity; commutative ring; division ring; subring

zero factors; integral domain; ideal; quotient ring 在这书里不好

def:  $M \subset R$ ,  $R$  is a ring with unity, 由  $M$  生成的 ideal 记为  $\langle M \rangle$

$\langle M \rangle = \sum_{i \in \mathbb{Z}} I_i = RMR$ ,  $I_i$  为全体含  $M$  的 ideal

$\bullet$   $R$  中无 unity,  $\langle M \rangle = RMR + RM + MR + \sum M$

例:  $a \in R$ ,  $R$  is ring,  $\langle a \rangle = \{ \sum_{i \in \mathbb{Z}} r_i a^i + p a q + n a = r s, p, q \in R, n \in \mathbb{Z} \}$  记为  $I$

CAAP239: finite integral domain is a field

设  $D$  为有限积分域, unity = 1,  $x, y \in D$   $xy = yx$

let  $a \in D$ ; WTS:  $a$  is a unit (有逆元)

consider  $a, a^2, a^3, \dots$   $\exists i > j$  s.t.  $a^i = a^j$ ,  $a^{i-j} = a^{-j} \Rightarrow$  unit

Th:  $\forall$  prime  $p$ :  $\mathbb{Z}_p$ : the ring of integers mod  $p$  is a field

$\mathbb{Z}_p$  finite, integral  $\Leftrightarrow$  commutative + 无 zero factors

$x \neq 0, y \neq 0 \Rightarrow xy \bmod p \neq 0$   $p$  is prime

例:  $\mathbb{Z}/n\mathbb{Z}$  is field  $\Leftrightarrow n$  is prime

$\mathbb{Z}/n\mathbb{Z} = \{x + n\mathbb{Z} : x \in \mathbb{Z}, n\mathbb{Z} = \{0, n, 2n, \dots\}\}$

"+" Abel, "x" distributive & associative  $\Rightarrow$  ring

存在乘法 unity = 1, 且 "x" commutative; 只要  $\forall$  non zero element 有逆

$\Rightarrow \forall x \in \mathbb{Z} \setminus n\mathbb{Z}, (x + n\mathbb{Z})(y + n\mathbb{Z}) = xy + n\mathbb{Z} = 1 + n\mathbb{Z}$

Bezout  $\rightarrow$  then  $xy = 1 + n\mathbb{Z}$  for some  $z$

1) 若  $\gcd(x, n) = 1$ ,  $\exists s, t$  s.t.  $sx + tn = 1$ , 证毕.

$\gcd(x, n) \neq 1$  then  $n \mid x$ ,  $\gcd(x + n, 1) = 1$  同样可证

2) 若  $n$  不为素数  $\gcd(x, n) \neq 1$  记为  $m$ ,  $x + m$  和  $n + m$  互质  $\exists s, t$  s.t.  $s(x + m) + t(n + m) = 1$

在  $\mathbb{Z}_p$  下,  $p, q$  没有 inverse for multiplicity

$s$  和  $t$  不是  $m$  的倍数

若有: need  $px = (pq)k + 1$  for some  $x, k$

$p \nmid qs, p \nmid qs$

# Abstract Algebra

## : Lecture 6

Leo

2024.10.08

usual "x" by default

\* the set should be closed under "+" and "·"

✓ **Definition 1.** A Ring  $(R, +, \cdot)$  is a set  $R$  with two binary operations  $+$  and  $\cdot$  such that:

$(R, +)$  is an abelian group;

$(R, \cdot)$  is a semigroup; Associative  $\Rightarrow$  semi-group

$a \cdot (b + c) = a \cdot b + a \cdot c$  for all  $a, b, c \in R$ ;

$(a + b) \cdot c = a \cdot c + b \cdot c$  for all  $a, b, c \in R$ .

A ring  $R$  which has a multiplicative identity  $1$  is called a ring with unity.

✓ **Definition 2.** Let  $R$  be a ring with unity. Given  $a \in R$ , if  $ba = 1$ ,  $b$  is a left inverse of  $a$ , and if  $ab = 1$ ,  $b$  is a right inverse of  $a$ . Further, if  $ab = 1$  and  $ba = 1$ ,  $b$  is the two-sided inverse of  $a$ .  $a$  is called invertible if it has a two-sided inverse.

✓ **Definition 3.** If for  $a, b \in R$ ,  $a \neq 0$  and  $b \neq 0$ ,  $ab = 0$ . Then  $a, b$  are called zero factors.

✓ **Definition 4.** If  $ab = ba$  for all  $a, b \in R$ , then  $R$  is called a commutative ring.

✓ **Definition 5.** If each element of  $R$  has a multiplicative inverse, then  $R$  is called a division ring.

✓ **Definition 6.** If  $R$  is commutative and has no zero factors, then  $R$  is called an integral domain.

**Example 7.**  $(\mathbb{Z}, +, \cdot)$  is an integral domain.

**Example 8.**  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$  is a commutative ring. If  $n$  is a prime number, then  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$  is a field.

**Example 9.**  $(M_n(\mathbb{F}), +, \times)$  is a ring. It is not commutative or division ( $n \geq 2$ ).

**Example 10.**  $(\mathbb{F}[x], +, \times)$  is a integral domain.

**Definition 11.** A subset  $S$  of a ring  $R$  is called a subring of  $R$  if  $S$  is a ring under the operations of  $R$ .

⇓  
CAA P230. "+"和"·"封闭

**Example 12.**  $(2\mathbb{Z}, +, \cdot)$  is a subring of  $(\mathbb{Z}, +, \cdot)$ .

**Example 13.** Diagonal matrices form a subring of  $M_n(\mathbb{F})$ .

**Example 14.**  $\{f(x) \mid f(x) \in \mathbb{F}[x]\}$  is a subring of  $(\mathbb{F}[x], +, \cdot)$ .

$f_1(x) \pm f_2(x) = (f_1 \pm f_2)(x) \in S$

**Definition 15.** A subring  $I$  of a ring  $R$  is called an ideal if  $rI, Ir \subseteq I$  for all  $r \in R$ .

**Definition 16.** For a ring  $R$  and an ideal  $I$  of  $R$ , the quotient ring  $R/I$  is defined as  $R/I = \{r + I \mid r \in R\}$ . And  $+$  and  $\cdot$  are defined as  $(r + I) + (s + I) = (r + s) + I$  and  $(r + I) \cdot (s + I) = rs + I$ .

**Example 17.**  $\mathbb{Z}/2\mathbb{Z}$  is a field.  $= \{x+n\mathbb{Z} : x \in \mathbb{Z}\}$   $(x_1+n\mathbb{Z})(x_2+n\mathbb{Z}) = x_1x_2+n\mathbb{Z}$  乘法 Abelian

**Example 18.**  $\mathbb{Z}/n\mathbb{Z}$  is a field if and only if  $n$  is a prime number.

**Example 19.**  $\mathbb{F}[x]/(x) \simeq \mathbb{F}$ .  $\mathbb{F}[x]/(x) = \{a_0 + a_1x + \dots + a_nx^n + \dots + (x) : a_i \in \mathbb{F}\}$

**Example 20.**  $\mathbb{F}[x]/(x^2) \simeq \mathbb{F}[x]_{\leq 1}$ .  $= \{a_0 + a_1x + (x^2) : a_i \in \mathbb{F}\}$

**Definition 21.** Let  $M \subset R$  where  $R$  is a ring with unity. The (double sided-)ideal generated by  $M$  is defined as  $(M) = \bigcap_{j \in J} I_j = RMR$ , where  $I_j$ 's are all ideals of  $R$  containing  $M$ . If  $R$  has no unity then  $(M) = RMR + RM + MR + \mathbb{Z}M$

**Example 22.**  $a \in R$ ,  $R$  is a ring.  $(a) = \{ \sum_{finite} ra + as + paq + na \mid r, s, p, q \in R, n \in \mathbb{Z} \}$ .

**Definition 23.**  $\varphi : R_1 \rightarrow R_2$  is a ring homomorphism if  $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$  and  $\varphi(r_1r_2) = \varphi(r_1)\varphi(r_2)$  for all  $r_1, r_2 \in R_1$ .  $\ker \varphi = \{r \in R_1 \mid \varphi(r) = 0\}$ ,  $\text{Im } \varphi = \{\varphi(r) \mid r \in R_1\} \subseteq R_2$ . It's easy to check that  $\ker \varphi$  is an ideal of  $R_1$  and  $\text{Im } \varphi$  is a subring of  $R_2$ . Moreover,  $\varphi$  is injective if and only if  $\ker \varphi = \{0\}$  and surjective if and only if  $\text{Im } \varphi = R_2$ .

**Theorem 24.** For a ring homomorphism  $\varphi : R_1 \rightarrow R_2$ ,  $R_1/\ker \varphi \simeq \text{Im } \varphi \leq R_2$

**Theorem 25.** Let  $I \triangleleft R$  s.t.  $\pi : R \rightarrow R/I : r \mapsto r + I$ , natural homomorphism. Then:

1. The ideal(subring) of  $R$  containing  $I$  and ideal(subring) of  $R/I$  are in one-to-one correspondence;
2. If  $I \triangleleft J \triangleleft R$  then  $J/I \triangleleft R/I$  and  $R/J \simeq \frac{R/I}{J/I}$ .

**Theorem 26.** Let  $I \triangleleft R$ ,  $S \leq R$ . Then  $I + S$  is a subring of  $R$ , and:

1.  $S \cap I \triangleleft S$  and  $I \triangleleft I + S$ ;
2.  $(I + S)/I \simeq S/S \cap I$ .

**Exercise 27.** Prove those 3 theorems. HW

**Definition 28.** Given two rings  $(R, +, \times)$  and  $(S, +, \times)$ , define  $R \times S = \{(r, s) \mid r \in R, s \in S\}$  where addition and multiplication are defined as:

$$\begin{aligned}(r_1, s_1) + (r_2, s_2) &= (r_1 + r_2, s_1 + s_2) \\ (r_1, s_1)(r_2, s_2) &= (r_1r_2, s_1s_2)\end{aligned}$$

It's easy to check  $R \times S$  is a ring.  $R \times S$  is called the direct product of  $R$  and  $S$ .