Abstract Algebra
: Lecture 6

Leo

2024.10.08

usual "x" by default ☆ the set should be closed under "+" "·"

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 ⇒ 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 ($n \geqslant 2$).*

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

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

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 $R/I = \{r + I | r \in R\}$. 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. $\mathbb{F}[x]/(x) \simeq \mathbb{F}$.

$\mathbb{F}[x]/(x^2) = \{a_0 + a_1x + \cdots a_nx^n + \cdots + (x^2) : a_i \in \mathbb{F}\}$
$= \{a_0 + a_1x + (x^2) : a_i \in \mathbb{F}\}$

Example 20. $\mathbb{F}[x]/(x^2) \simeq \mathbb{F}[x]_{\leqslant 1}$.

degree ≤ 1

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

Definition 23. *$\varphi : R_1 \to R_2$ 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 $r_1, r_2 \in R_1$. $\ker \varphi = \{r \in R_1 | \varphi(r) = 0\}$, $\operatorname{Im} \varphi = \{\varphi(r) | r \in R_1\} \subseteq R_2$. It's easy to check that $\ker\varphi$ is an ideal of R_1 and $\operatorname{Im} \varphi$ is a subring of R_2. Moreover, φ is injective if and only if $\ker\varphi = \{0\}$ and surjective if and only if $\operatorname{Im} \varphi = R_2$.*

Theorem 24. *For a ring homomorphism $\varphi : R_1 \to R_2$, $R_1/\ker \varphi \simeq \operatorname{Im} \varphi \leqslant R_2$*

iso Th

Theorem 25. *Let $I \lhd R$ s.t. $\pi : R \to R/I : r \mapsto r + I$, 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 $I \lhd J \lhd R$ then $J/I \lhd R/I$ and $R/J \simeq \frac{R}{I}/\frac{J}{I}$.*

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

1. *$S \cap I \lhd S$ and $I \lhd I + S$;*
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 $R \times S = \{(r, s) | r \in R, s \in S\}$ where addition and multiplication are defined as:*

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1)(r_2, s_2) = (r_1r_2, s_1s_2)$$

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