LECTURE 1

Author
Tom Jeong

January 6, 2025

Contents

1 Rings

$\mathbb{Z}$, $+$: addition, $\cdot$ multiplication

$$a + (b + c) = (a + b) + c \text{ 0 - aditive identity} \tag{1}$$
$$(ab)c = a(bc) \tag{2}$$
$$a + b = b + a : \text{ multiplication doesn't have to be communtative} \tag{3}$$
$$(a + b)c = ac + bc : \text{ distributinos} \tag{4}$$
$$a + (-a) = 0 : \text{ additive inverse} \tag{5}$$

1_R- Multiplicative idenfity (if exists)
if there exists $1_R \in R$ then R is called unital or ring with unity.
If $ab = ba, \forall a, b \in R$ then R is a commutative ring

$(R, +)$ is an abeligan group
examples: $(\mathbb{Z}, +, \cdot), (2\mathbb{Z}, +, \cdot)$ ring without 1,
$M_n(R)$: $n \times n$ matrices with entreis in a ring R. - Not communatitive ring.

---

2 Integral Domain

Ring D (commutative, unital) is an Integral Domain if it enjoys cancellation property:

$$ab = ac \to b = c \text{ (if } a \neq 0)$$

Definition 2.1 (Equivalent)**.**
$ab = ac \longleftrightarrow ab = ac = 0 \longleftrightarrow a(b - c) = 0$
in other words:

$$ab = 0 \to (a = 0)||(b = 0)$$

Definition 2.2 (zero divisors)**.**

$$ab = 0 \text{ and } a, b \neq 0$$

then a and b are zero divisors

$\mathbb{Z}/6\mathbb{Z}$ (integer mod 6) or $\mathbb{Z}_6$ (same thing diff notation)
proving that this not an I.D. : $2 \cdot 3 = 0$ but $2, 3 \neq 0$

---

3 Fields

A commutative ring where every element has a multiplicative inverse is called a Field.

Definition 3.1 (unit).
An element $a \in R$ is called a unit if it has a multiplicative inverse

(groups of unit) $(ab)^{-1} = b^{-1}a^{-1}$: units in a ring forms a a group. Commutative ring then it is an abelian group.
example $\mathbb{Z}$: units are $\{-1, 1\} \cong \mathbb{Z}_2$
K-field, $K^\star = K \backslash \{0\}$ and $(K^\star, \cdot)$ is an abelian group

example: $R = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$
I claim that $(\sqrt{2}+1)$ is a unit. we show that it has a mult. inverse: $(\sqrt{2}+1)(\sqrt{2}-1) = 1$ and we see that $(\sqrt{2}+1)^k$ are all distinct units for $k \in \mathbb{Z}, k \geq 0$

---

4 Ring Homorphisms

maps between rings: (respect the structure of addition, multiplication) $\phi : R \to S$ is a homomorphism if:

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a)\phi(b)$

property:

1. $\phi(O_R) = O_S$
2. $\phi(-r) = -\phi(r)$
3. $\phi(R) \leq S$ (subring of S)

Definition 4.1 (ker).

$$ker(\phi) = \{r \in R | \phi(r) = 0_S\}$$

Proposition 4.1. $ker\phi$ is a subring of R

Proof.
$\phi(ab) = \phi(a)\phi(b) = 0$
$a, b \in ker\phi$
$\phi(a + b) = \phi(a) + \phi(b) = 0$
$\phi(ra) = 0$ for all $r\ inR$ □

Definition 4.2 (ideal).
$ker\phi$ is an ideal of R.
Ideal: subring closed under multiplcation by any element of R.
ideal I of R if $\forall a, b \in I, r \in R \to a, b \in I$

1. closure under addition and additive inverse $a - b \in I$
2. $ra \in I$

Example: $2\mathbb{Z}$ is an ideal in $\mathbb{Z}$
k-field: $\{0\}, R$ "not interesting ideals contains only zero
Proper Ideal of R is an "interesting" ideal A proper ideal is any ideal that is a strict subset of R (so not R itself). These are considered "interesting" because they:

- Reveal the ring's algebraic structure
- Help classify rings
- Are used to construct quotient rings
- Can determine properties like primality and maximality

For example, in $\mathbb{Z}$ (integers), $(4) = \{\dots, -8, -4, 0, 4, 8, \dots\}$ is an interesting proper ideal, while $\{0\}$ and $\mathbb{Z}$ are uninteresting.
:: I- ideal.

$$I \subsetneq R \leftrightarrows 1_R \notin I \leftrightarrows I \text{ contains no units}$$

Proof. Let $I \subset K$ be a proper ideal. If $a \neq 0$ and $a \in I$, then $a \cdot a^{-1} \in I$ since I is an ideal. But $a \cdot a^{-1} = 1$ (multiplicative identity), therefore $1 \in I$. Since I is an ideal, for any $k \in K$, $k \cdot 1 = k \in I$. Thus $I = K$, contradicting that I is proper. ☐

---

5 Quotient Rings

R/I: cosets of I :

$$a + I \forall a \in R$$
$$(a + I) \cdot (b + I) = ab + I$$
$$(a + I) + (b + I) = a + b + I$$
$$0_{R/I} = 0 + I = I$$

Definition 5.1 (canonical projection)**.**

$$\pi : R \to R/I$$
$$a \mapsto a + I$$
$$ker\pi = I$$
$$\phi : R \to S$$
$$im\phi \cong R/\ker\phi$$

All ring homomorphisms are canonical projections (because kernel is always the ideal.)

---

6 Fields of Fraction (tbc)

$\mathbb{Z} \to \mathbb{Q}$,
D integral Domain

Definition 6.1 (rational)**.**
$(a, b) : \frac{a}{b}, a, b \in \mathbb{Z}$
but we have a problem: (1,2) = (2,4) = (3,6) = ... So tequivalence classes of pairs of integersL

$$(a, b) \sim (a', b') \leftrightarrows ab' = a'b$$

actions on rational numbers

1. multiplication: $(a, b) \cdot (a', b') = (aa', bb')$ ID is needed.
2. addition: $(a, b) + (a', b') = \frac{a}{b} + \frac{a'}{b'} = \frac{ab'+a'b}{bb'} = (ab' + a'b, bb')$

Why ID is needed:

Proof. The identity element (1,1) is required because:

1. In a ring, multiplication must have an identity element
2. For component-wise multiplication $(a, b) \cdot (1, 1) = (a \cdot 1, b \cdot 1) = (a, b)$ must hold
3. Without $(1, 1)$, the structure would not satisfy ring axioms:
   - Existence of multiplicative identity
   - Distributive property over addition
   - Closure under multiplication

This ensures the direct product maintains ring properties from its component rings. □

equivalence relation?

1. $(a, b) \sim (a, b)$
2. $(a, b) \sim (a', b') \leftrightarrow (a', b') \sim (a, b)$
3. $(a, b) \sim (a', b')$ and $(a', b') \sim (a'', b'') \to (a, b) \sim (a'', b'')$

If $(a, b) \sim (a', b')$ then $\exists k_1 \in \mathbb{Q} : a - a' = k_1$ and $b - b' = k_1$
If $(a', b') \sim (a'', b'')$ then $\exists k_2 \in \mathbb{Q} : a' - a'' = k_2$ and $b' - b'' = k_2$
Adding equations: $(a - a') + (a' - a'') = k_1 + k_2$ and $(b - b') + (b' - b'') = k_1 + k_2$
Therefore $a - a'' = k_1 + k_2$ and $b - b'' = k_1 + k_2$ where $k_1 + k_2 \in \mathbb{Q}$
Thus $(a, b) \sim (a'', b'')$ (there is an easier way i just pasted the above from claude)

this construction adds a multiplicative inverse to every non-zero element, making it into a field. $Q(D)$