Algebra. Lec 11: Ring. Ring isomorphism theorem.

Rings

def. A ring A is a set w. 2 binary operators $+$, $\times$.

(RI 1) $(A, +)$ abelian group. 0: unit element

(RI 2) $(A, \times)$ multiplication, associative.

$\exists\ 1 \in A$. unit element

(i.e. $1 \cdot a = a = a \cdot 1$. $\forall a \in A$)

(RI 3) $(x+y) \cdot z = xz + yz$

$z(x+y) = zx + zy$) distributive law

Rmk

- may assume $1 \neq 0$, or not
- $0x = 0$. $\forall x \in A$.

  Pf. $0x + x = (0+1)x = x \Rightarrow 0x = 0$
- if $1 = 0$. $\forall x \in A \Rightarrow x = 1x = 0 \cdot x = 0 \Rightarrow$ a ring with single elem.
- $\forall x, y \in A$.

  $(-x)y = -xy$.

  $(-x)(-y) = xy$) ex.

- A : ring.

$U = \{ a \in A \mid a$ has both right and left inverse $\}$.

$\Rightarrow U$: multiplicative group.

pf. $a \in U$, $\left.\begin{array}{l} \exists\, b,\ ab = 1 \\ \exists\, c,\ ca = 1 \end{array}\right\} \Rightarrow c = c \cdot 1 = c \cdot a \cdot b = (c \cdot a) b = b.$

$\Rightarrow U =$ the group of units of A, $A^\times$

def. $(A, +, \times)$ if "$\times$" is commutative

A is called "commutative ring"

def. $(A, +, \times)$ ring. $1 \neq 0$.

if $\forall a \in A$, $a \neq 0$. a has a multi inverse. (ie. $\exists b \in A.\ ab = ba = 1$).

A: division ring

def. A commutative division ring is called a "field"

def. A ring. $B \subseteq A$.

B is called a subring if

① B is an additive subgroup of A.

② $1 \in B$

③ closed under multiplication.

eg. S: set. A: ring

$\underbrace{Map(S, A)}_{\text{is a ring}}$ all map from S to A

$f, g \in Map(S, A)$
$$\begin{cases} (f+g)(x) \triangleq f(x) + g(x) \\ (fg)(x) \triangleq f(x) \cdot g(x) \end{cases}$$

$$\begin{cases} 0 = 0(x) \\ 1 = 1(x). \end{cases}$$

def. A left ideal $\underline{a}$ in a ring A (right ideal)

is a subset of A

s.t. ① $\underline{a}$: additive subgroup of A.

② $A\underline{a} \subseteq \underline{a}$ (actually $A\underline{a} = \underline{a}$ for $1 \in A$.)

two sided ideal

$A\underline{a} \subseteq \underline{a}$. $\underline{a}A \subseteq \underline{a}$) ideal.

Rmk ◦ $a \in A$. $Aa \triangleq \{xa \mid x \in A\}$. left ideal of A

for $\forall y \in A$. $xa \in Aa$, $y(xa) = (yx)a \in Aa$

◦ $(a_1, a_2, \cdots, a_n) \triangleq \{x_1a_1 + \cdots + x_na_n \mid x_i \in A\}$

↪ left ideal of A

◦ A: commutative

A. is called "principle". if every ideal of A is principle

i.e. generated by single elem in A.

i.e. $I \subseteq A$. $\Rightarrow I = (a)$ $a \in A$.

ideal

↓ Some ring operation

◦ A ring $\underline{a}, \underline{b}, \underline{c}$ ideal of A

$\underline{a} \cdot \underline{b} \triangleq \{x_1y_1 + \cdots + x_ny_n \mid x_i \in \underline{a}, y_i \in \underline{b}\}$

verify $\underline{a}\underline{b}$ is an ideal of A

verify $(\underline{a}\underline{b})\underline{c} = \underline{a}(\underline{b}\underline{c})$

e.g. A ring. $\underline{a}$ left ideal.

$$\underline{a}A \triangleq \{a_1x_1 + \cdots + a_nx_n \mid a_i \in \underline{a}, x_i \in A\}$$

$\Rightarrow$ ideal.

Why use finite sum?

$\Rightarrow$ to generate a structure of subgroup

e.g. A: comm ring

$\underline{a}$, $\underline{b}$: ideal

$\Rightarrow \underline{a}\underline{b} \subset \underline{a} \cap \underline{b}$

---

if $\underline{a} + \underline{b} = A$. then. $\underline{a}\underline{b} = \underline{a} \cap \underline{b}$

Pf. $\exists x \in \underline{a}$ $y \in \underline{b}$ s.t. $x + y = 1$.

let $z \in \underline{a} \cap \underline{b}$ $\qquad \underset{z}{\underset{\|}{z \cdot 1}} = z(x+y) \in \underline{a}\underline{b}$

Example.

$\mathbb{Z}$. comm ring

$3\mathbb{Z}$, $5\mathbb{Z}$. ideal

$6\mathbb{Z}$.

$(3\mathbb{Z})(6\mathbb{Z}) \subset 6\mathbb{Z}$

$(3\mathbb{Z})(5\mathbb{Z}) = 15\mathbb{Z}$

Ring homomorphism $A \cdot B$ ring

$f: A \to B$. if $\begin{cases} f(a+a') = f(a) + f(a') \Rightarrow f(0)=0 \\ f(a \cdot a') = f(a) \cdot f(a') \quad \forall a, a' \in A \\ f(1) = 1 \end{cases}$

$\ker(f) = \{a \in A \mid f(a) = 0\}$

· verify. $\underset{x}{\ker f} \in$: ideal of $\underset{a}{A}$

$f(ax) = f(a)f(x) = f(a) \cdot 0 = 0$.

$\Rightarrow ax \in \ker f)$

$f(xa) = f(x)f(a) = 0 \cdot f(a) = 0$

$\Rightarrow xa \in \ker f)$.

Conversely let $\underline{a}$ be an ideal of A

$A/\underline{a}$ the quotient group.

$\left.\begin{cases} (x+\underline{a})(y+\underline{a}) \triangleq xy + \underline{a} \\ (x+\underline{a}) + (y+\underline{a}) \triangleq x+y+\underline{a} \end{cases}\right) \Rightarrow$ ring structure on $A/\underline{a}$

$\Rightarrow A/\underline{a}$ is a ring

$f: A \longrightarrow A/\underline{a}$

$x \longmapsto x + \underline{a}$

$\left.\begin{array}{l} f(x+y) = x+y+\underline{a} = (x+\underline{a}) + (y+\underline{a}) = f(x) + f(y) \\ f(xy) = xy + \underline{a} = (x+\underline{a})(y+\underline{a}) = f(x) f(y) \end{array}\right) \Rightarrow$ hom.

$f(1) = 1 + \underline{a}$

---

universal property.

$$\begin{tikzcd} A \arrow[r, "g"] \arrow[d, "f"'] & A' \\ A/\underline{a} \arrow[ur, "\exists ! g_*"'] \end{tikzcd}$$

ring hom.

$\underline{a}$: ideal of A

$\underline{a} \subseteq \ker(g)$

$\Rightarrow \exists ! \ g_* : A/\underline{a} \longrightarrow A'$ ring hom.

s.t. $g = g_* \cdot f$

pf. Regarding f, g are group hom.

$\exists ! \ g_*$. $g = g_* \cdot f$

$\forall x \in A$. $\quad g(x) = g_* f(x)$

$\forall x, y \in A \quad g_*(f(x) f(y)) = g_* f(xy) = g(xy) = g(x) g(y)$

$= g_* f(x) \ g_* f(y)$

f is surjective $\Rightarrow$ all elem in $A/\underline{a}$ is checked.

$g_*(1+\underline{a}) = g_* f(1) = g(1) = 1 \in A'$

$\Rightarrow$ g_* is ring hom.

HW.

- Lang chap II. ex 2.3.4.8
- Prove that a finite subgroup of the multiplicative group of a field is cyclic. (Apply FTFGAB)

  (i.e. F: field. $G \le (F-\{0\}, \cdot)$. $|G| < \infty$. $\Rightarrow$ G cyclic)

Isomorphism. Theorem for rings

① $g: A \to B$ ring hom.

$\Rightarrow$ $\ker(g)$: ideal of A. $\mathrm{im}(g)$ is subring of B

$$A/\ker(g) \simeq \mathrm{im}(g)$$

②. R: ring, A subring, B ideal

$$A+B/B \simeq A/A\cap B$$

③. R ring I, J ideal of R

$I \subseteq J$

$$(R/I)/(J/I) \simeq R/J.$$

Rmk. $f: A \to A'$ ring hom. $\underline{a}'$ ideal of A'

$$\underline{a} \triangleq f^{-1}(\underline{a}')$$

$\Rightarrow$ $\underline{a}$ ideal of A.

$A/\underline{a} \hookrightarrow A'/\underline{a}'$ (i.e. $\exists$ injective ring hom)

pf

- $x \cdot y \in \underline{a}$

$f(x-y) = f(x) - f(y) \in \underline{a}'$ $\quad x - y \in \underline{a}$ $\overset{\text{subgroup criterion.}}{\Rightarrow}$ additive subgroup

- $x \in \underline{a}$ $\quad y \in A$

$$\left\{ \begin{array}{l} f(xy) = f(x) f(y) \in \underline{a}' A' \subseteq \underline{a}' \Rightarrow xy \in \underline{a} \\ f(yx) = f(y) f(x) \in A' \underline{a}' \subseteq \underline{a}' \Rightarrow yx \in \underline{a} \end{array} \right.$$

$\Rightarrow$ $\underline{a}$ is ideal.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "\varphi"'] & A' \arrow[r, "\text{can. proj}"] & A'/\underline{a}' \end{tikzcd}$$

$\ker(\varphi) = \underline{a}$

$A/\ker(\varphi) = A/\underline{a} \simeq \operatorname{im}(\varphi) \subseteq A'/\underline{a}'$

/

def. A ring $x, y \in A$. $xy = 0$, $x \neq 0$, $y \neq 0$

$x \cdot y$ are called zero-divisors.

0-divisors.

def. A is called "domain" "integral domain" "entire ring"

if A comm. has and has no 0-divisor

Rmk A. entire ring. $a \neq 0$, $b \neq 0 \in A$ $\mathbb{Z}$ is a good example

$(a) = (b) \iff \exists\, u$ unit in A

s.t. $b = au$

pf. $\Leftarrow$) $b = au$. $Ab = Aua = Aa$

$\Rightarrow$). $Aa = Ab$.

$$\begin{cases} a = bc \\ b = ad \end{cases} \text{ for some } c, d \in A$$

$a = bc = adc \Rightarrow a(1 - cd) = 0$

$\Rightarrow 1 - cd = 0 \Rightarrow cd = 1$

Commutative ring

A: comm. ring

def. A prime ideal in A is an ideal $\mathfrak{p} \neq A$.

s.t. $A/\mathfrak{p}$ is entire.

equi def. $\mathfrak{p}$ an ideal of A.

st. $xy \in \mathfrak{p}$ for $x, y \in A \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$

eg. $p\mathbb{Z}$ is prime ideal.

def. $\mathfrak{m}$: max ideal of A

if $\mathfrak{m} \neq A$ and no other proper ideal of A containing $\mathfrak{m}$

$\neq A$

Prop. max ideal is prime.

Pf. $\mathfrak{m}$: max.

$x \cdot y \in A$. st. $xy \in \mathfrak{m}$

say $x \notin \mathfrak{m}$ $\quad \mathfrak{m} + Ax$ is ideal and $\supsetneq \mathfrak{m}$. $\Rightarrow \mathfrak{m} + Ax = A$

two ideal add.

$$\Rightarrow 1 = \underset{\mathfrak{m}}{\underset{\cap}{u}} + \underset{A}{\underset{\cap}{ax}} \Rightarrow y = yu + axy \in \mathfrak{m}.$$

Prop. $\mathfrak{a}$ ideal of A $\mathfrak{a} \neq A$.

$\Rightarrow$ $\mathfrak{a}$ is contained in some max ideal

Zorn's lemma: Suppose a partially ordered set P. has the property that every chain in P has an upper bound in P

$\Rightarrow$ Set P contains at least one max elem

pf. $P = \{$ proper ideals in A containing $\mathfrak{a}$ $\}$

$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \cdots$ (chain)

Let $\mathfrak{b} = \bigcup_i \mathfrak{a}_i$. $\Rightarrow 1 \notin \mathfrak{b} \Rightarrow \mathfrak{b} \in P$ $\Rightarrow \mathfrak{b}$ is the bound of

$\Rightarrow$ P has at least one maximal elem.