Algebra Lec 12. Chinese Remainder Theorem, Localization

Review

Prop $\underline{a}$: ideal of A, $\underline{a} \neq (0)$. $\underline{a} \neq A$

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

Prop. $\underline{m}$: max ideal of $A \iff A/\underline{m}$: field

pf $\Rightarrow$) $A \to A/\underline{m}$

$x \mapsto x+\underline{m}$ $\ni$ $\begin{cases} 0+\underline{m} \\ 1+\underline{m} \end{cases}$

- nonzero elem in $A/\underline{m}$

$x+\underline{m}$, $x \notin \underline{m}$

we have $\underline{m}+Ax = A$ (for $\underline{m}$ is max)

$\Rightarrow$ $1 = m + yx$ for some $m \in \underline{m}$ $y \in A$.

$(y+\underline{m})(x+\underline{m}) = (xy+\underline{m}) = (1+\underline{m})$

$\Rightarrow$ $(y+\underline{m})$ inverse of $(x+\underline{m})$

Conversely $A/\underline{m}$ field. $\forall x \notin \underline{m}$. $x \in A$

construct the element $x+\underline{m}$

$\exists$ $y+\underline{m}$ s.t. $(x+\underline{m})(y+\underline{m}) = 1+\underline{m}$

$\Rightarrow \ 1+\underline{m} = xy+\underline{m}$

$1 = xy + u$, $u \in \underline{m}$

$\therefore \ \underbrace{\underline{m}}_{\ni 1} + Ax = A \Rightarrow \underline{m}$ .max

多加进一个元素就 $= A$ 了

Prop. $f: A \to A'$ ring hom

p' : prime ideal in A'

$p = f^{-1}(p')$

$\Rightarrow p$: prime in A

Pf.

$$A/p \hookrightarrow A'/p' \quad \text{injective ring hom}$$

A'/p' : domain

A/p : no zero divisor

$\Rightarrow A/p$ domain.

Thm. 2.1 Chinese Remainder

$\underline{a_1}, \dots, \underline{a_n}$ ideals of A

s.t. $\underline{a_i} + \underline{a_j} = A$. $\forall i \neq j$ (comaximal)

Then.
given $x_1, \dots, x_n \in A$

$\exists x \in A$. s.t. $x \equiv x_i \pmod{\underline{a_i}}$ $\forall i = 1, \dots, n$

$(x - x_i \in \underline{a_i}, \forall i)$

Pf $n = 2$. $\underline{a_1} + \underline{a_2} = A$

$\therefore 1 = a_1 + a_2$. $a_1 \in \underline{a_1}$. $a_2 \in \underline{a_2}$

we let $x = x_2 a_1 + x_1 a_2$

$$
\begin{aligned}
x &\equiv x_2 a_1 + x_1 a_2 \pmod{\underline{a_1}} \\
&\equiv x_1 a_2 \pmod{\underline{a_1}} \\
&\equiv x_1 (1 - a_1) \pmod{\underline{a_1}} \\
&\equiv x_1 \pmod{\underline{a_1}}
\end{aligned}
$$

Same $\Rightarrow x \equiv x_2 \pmod{\underline{a_2}}$

$n \geq 3$. for each $i \geq 2$

$a_i \in \underline{a_1}$. $b_i \in \underline{a_i}$

s.t. $a_i + b_i = 1$ $\forall i = 2, \dots, n$

Consider $\prod_{i=2}^{n}(a_i+b_i)=1$

$$\cap$$

$$\underline{a_1}+\prod_{i=2}^{n}\underline{a_i}=A$$

$\exists\, y_1 \in A$. s.t.

$$\begin{cases} y_1 \equiv 1 \pmod{a_1} \\ y_1 \equiv 0 \pmod{\prod_{i=2}^{n}\underline{a_i}} \end{cases} = \begin{cases} y_1 \equiv 0 \pmod{a_2} \\ \vdots \\ y_1 \equiv 0 \pmod{a_n} \end{cases}$$

Let $x = x_1y_1+\cdots+x_ny_n$.

$$f: A \longrightarrow A/\underline{a_1}\times\cdots\times A/\underline{a_n}$$

$$x \longmapsto (x+\underline{a_1},\ldots,x+\underline{a_n})$$

f: ring hom. & we have proved that. f: surjective.

$$\ker(f)=\underline{a_1}\cap\cdots\cap\underline{a_n}$$

$$\Rightarrow A/_{\underline{a_1}\cap\underline{a_2}\cdots\cap\underline{a_n}} \simeq A/\underline{a_1}\times A/\underline{a_2}\times\cdots\times A/\underline{a_n}$$

(we have if $\underline{a_1}+\underline{a_2}=A$. $\underline{a_1}\cap\underline{a_2}=\underline{a_1}\underline{a_2}$

$$A/_{\underline{a_1}\cdots\underline{a_n}} \simeq A/_{\underline{a_1}}\times\cdots\times A/\underline{a_n}$$

Polynomial ring

A : comm ring

$A[x]$: $\{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in A\}$. $(+, \times)$

comm ring

<u>Rmk</u> $A \hookrightarrow A[x]$ ring hom

$a \longmapsto ax^0$ injective

- $A \subseteq B$ A, B comm. ring

$b \in B$

$ev_b : A[x] \longrightarrow B$

$f \longmapsto f(b)$

evaluation at b

$$\left\{\begin{aligned} & ev_b(f_1+f_2) = ev_b(f_1) + ev_b(f_2) \\ & ev_b(f_1f_2) = ev_b(f_1)\, ev_b(f_2) \\ & ev_b(1) = 1 \end{aligned}\right. \Rightarrow \text{ring hom}$$

<u>def</u> $A \subseteq B$ $x \in B$

$ev_x : A[x] \longrightarrow B$

$f \longmapsto f(x)$

if ev_x gives an iso $A[x] \xrightarrow{\sim} im(ev_x) \subseteq B$ subring

then $x \in B$ is said to be <u>transcendental</u> over A

Rmk $\varphi: A \to B$ ring hom

$A[x] \longmapsto B[x]$ associative ring hom.

$f(x) = \sum a_i x^i \longrightarrow \sum \varphi(a_i) x^i = (\varphi f)[x]$

Rmk A: comm ring

$\mathfrak{p} \subseteq A$ prime ideal

$\varphi: A \to A/\mathfrak{p}$ can. quot

$A[x] \longrightarrow (A/\mathfrak{p})[x]$ ring hom

$f(x) \longmapsto (\varphi f)[x]$ reduction of f module $\mathfrak{p}$

- $\varphi: A \to B$

$x \in B$. $\exists!$ $\overbrace{\text{ring hom}}^{A[X] \to B}$ extending φ

s.t. $X \to x$

$A[x] \longrightarrow B$

$\sum a_i X^i \longmapsto \sum \varphi(a_i) x^i$

---

or we can see as

$A[x] \to B[x] \xrightarrow{ev_x} B$

$\sum a_i x^i \to \sum \varphi(a_i) X^i \to \sum \varphi(a_i) x^i$

group ring (Lang p104~107)

A: comm ring

G: monoid

$A[G] = \{ \sum a_i g_i \mid a_i \in A,\ g_i \in G \}$ "+" "×" $\Rightarrow$ a ring

finite sum.

not always comm

- unit elem. $\underset{\in A}{1} \cdot \underset{\in G}{e}$

- $\varphi_0 : G \to A[G]$

  $g \mapsto 1 \cdot g$ monoid hom. , & injective

  $\varphi_0(g_1 g_2) = \varphi_0(g_1)\varphi_0(g_2)$

- $f_0 : A \to A[G]$

  $a \mapsto ae.$ ring hom.

verify

Lacalization. A. comm. $\left(\underline{\mathbb{Z} \to \mathbb{Q}\ ?}\right)$

<u>multiplicative subset of A</u> : S

a subset of A, containing 1, closed under multiplication.

<u>goal</u>. construct <u>the quotient ring of A by S.</u>

<u>the ring of fractions of A by S</u>

Consider the pair (a, s) $a \in A$. $s \in S$

define the relation. $(a.s) \sim (a', s')$

iff $\exists s_1 \in S$ st. $s_1(s'a - sa') = 0$

verify: <u>equivalent relation</u>

then we denote the equivalence class, containing (a, s), by a/s

$S^{-1}A = \{a/s\}$: the set of equivalence classes

(if $0 \in S$. $S^{-1}A = \{0/1\}$. for $(0,1) \sim (a.s)$
$0(1.a - 0.s) = 0.$)

<u>multiplication</u> $(a/s) \cdot (a'/s') \triangleq aa'/ss'$

unit elem. $(1/1)$

<u>addition</u>. $a/s + a'/s' \triangleq \dfrac{as'+a's}{ss'}$

"$\times$" is well-defined. "$+$"

- — - .

$\left.\begin{array}{l} a/s = b/t \\ a'/s' = b'/t' \end{array}\right)$ i.e. $\begin{array}{l} \bar{s}(at-bs)=0 \\ \bar{\bar{s}}(a't'-b's')=0 \end{array}$ (Ex).

want to show $aa'/ss' = bb'/tt'$ (Ex)

<u>Rmk</u>. $a/s = s'a/s's$

$(S^{-1}A, +, \times)$. Commutative ring

still need to verify distributive law.

$\varphi_s : A \longrightarrow S^{-1}A$

$a \longmapsto a/1$

$$\begin{cases} \varphi_s(a_1+a_2) = (a_1+a_2)/1 = a_1/1 + a_2/1 = \varphi_s(a_1)+\varphi_s(a_2) \\ \varphi_s(a_1a_2) = a_1a_2/1 = a_1/1 \cdot a_2/1 = \varphi_s(a_1)\cdot\varphi_s(a_2) \Longrightarrow \text{ring hom.} \\ \varphi_s(1) = 1/1 \end{cases}$$

$s \in S$. $\varphi_S(s) = s/1 \to$ invertible in $S^{-1}A$

inverse is $1/s$

Universal property of $S^{-1}A$

$f: A \to B$. ring hom of comm rings.

s.t. $\forall s \in S$. $f(s)$: invertible in B

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\varphi_S"'] & B \\ S^{-1}A \arrow[ur, "\exists! h"'] & \end{tikzcd}$$

$\exists! h : S^{-1}A \to B$ ring hom.

def. $h(a/s) = f(a) \cdot f(s)^{-1}$

⓪ h. well-defined ?

① $h\varphi_S(a) = h \cdot (\frac{a}{1}) = f(a)$. $\forall a \in A$.

② h: hom. $h(\frac{a_1}{s_1} + \frac{a_2}{s_2}) = h\left(\frac{a_1 s_2 + a_2 s_1}{s_1 s_2}\right) = \left(f(a_1 s_2) + f(a_2 s_1)\right) f(s_1)^{-1} f(s_2)^{-1}$

$= f(a_1) f(s_1)^{-1} + f(a_2) f(s_2)^{-1}$

$= h(\frac{a_1}{s_1}) + h(\frac{a_2}{s_2})$

$h(\frac{a_1}{s_1} \frac{a_2}{s_2}) = \text{---}$

$$h(1/1) = f(1) f^{-1}(1) = f(1) = 1 \in B$$

③ h unique. If $f = h \cdot \varphi_S = h' \varphi_S$

$$f(a) = h(a/1) = h'(a/1)$$

$$f(s) = h(s/1) = h'(s/1) \quad s \in S$$

$$B \ni 1 = f(1) = h(1/1) = h(s/1 \; 1/s)$$

$$= h(s/1) \, h(1/s)$$

$$\Rightarrow h(1/s) = h(s/1)^{-1}$$

$$\shortparallel$$

$$h'(1/s) = h'(s/1)^{-1}$$

$$\Rightarrow h(a/s) = h(a/1 \; 1/s) = h(a/1) \, h(1/s)$$

$$\shortparallel$$

$$h'(a/s) = h'(a/1 \; 1/s) = h'(a/1) \, h'(1/s)$$

Examples. A. domain (entire ring)

- $S \subseteq A$. multi subsets, not containg 0.

$$\varphi_S : A \to S^{-1}A \quad \Rightarrow \text{ injective}$$
$$a \mapsto a/1$$

Compute kernal: $\varphi_S(a) = a/1 = 0/1 \Rightarrow \exists\, s \in S.$ s.t. $(a1 - 01)s = 0$

$as = 0$

$s \neq 0 \Rightarrow a = 0.$

- we let $S = A - \{0\}$

$\Rightarrow S^{-1}A$: field (quotient field of A.

field of fractions)

(eg. $\mathbb{Q} \cong (\mathbb{Z} - \{0\})^{-1}\mathbb{Z}$.

A ring A is called a local ring.

if it's comm. and has a unique max ideal

- $(A, \underline{m})$ local ring

$x \in A - \underline{m}$

$\Rightarrow x$: unit

eg. $p \subseteq A$ p. prime ideal

let $S = A - p. \Rightarrow$ multi subset

containing 1.

$A_p \triangleq S^{-1}A = (A-p)^{-1}A$

Pf. If x is not a unit

$\Rightarrow$ Ax . proper ideal

then $Ax \subseteq \underline{m} \Rightarrow x \in \underline{m}$ $\times$

$(A_p, S^{-1}p)$ local ring

A : comm ring. $J(A)$ = the set of all ideals of A

$$\psi_S : J(A) \longrightarrow J(S^{-1}A)$$

$$\underline{a} \longmapsto S^{-1}\underline{a} = \{ a/s \mid a \in \underline{a},\ s \in S \}$$

varify $S^{-1}\underline{a}$ is an ideal in $S^{-1}A$

ex.

$$\begin{cases} S^{-1}(\underline{a}+\underline{b}) = S^{-1}\underline{a} + S^{-1}\underline{b} \\ S^{-1}\underline{a}\underline{b} = (S^{-1}\underline{a})(S^{-1}\underline{b}) \\ S^{-1}(\underline{a} \cap \underline{b}) = S^{-1}\underline{a} \cap S^{-1}(\underline{b}) \end{cases}$$