

# §1. Rings and Ideals

回顾环和理想的定义以及基本性质.

近世代数

## §1.1. Rings and ring homomorphisms.

Ring:  $(A, +, \cdot)$  set binary operations such that (s.t.)

- 1).  $(A, +) = \text{abelian group (gp)}$
- 2). associative:  $(xy)z = x(yz) \quad \forall x, y, z$   
distributive:  $x(y+z) = xy+xz$  &  $(y+z)x = yx+zx, \quad \forall x, y, z$
- 3). commutative:  $xy = yx \quad \forall x, y$
- 4). identity element:  $\exists 1 \in A$  s.t.  $x1 = x = 1x \quad \forall x.$

Fact: uniqueness.

此课程中总是要求一个环满足 (3) 和 (4).

例:  $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, \mathbb{Q}, \dots$

zero ring:  $0=1 \Rightarrow A = \{0\}. \quad (x = x \cdot 1 = x \cdot 0 = 0, \forall x)$

ring homomorphism a map  $f: A \rightarrow B$  s.t. 保持  $+, \cdot, 1$

$\swarrow \quad \searrow$   
ring

- i)  $f(x+y) = f(x) + f(y)$
- ii)  $f(xy) = f(x)f(y)$
- iii)  $f(1) = 1.$

Fact:  $A \xrightarrow{f} B \xrightarrow{g} C : \text{ring homos} \Rightarrow g \circ f: A \rightarrow C$  is ring-hom. ①



subring = subset  $S \subset A$

- is closed under  $+$ ,  $\cdot$  and
- contains  $1$ .

Fact:  $S \hookrightarrow A$  ring homo.



## §1.2. ideals, quotient ring.

ideal  $\mathfrak{a} \triangleleft A$  :

- $(\mathfrak{a}, +)$  subgp
- $A\mathfrak{a} \subseteq \mathfrak{a}$

Quotient ring  $A/\mathfrak{a} := \{a + \mathfrak{a} \mid a \in A\}$

$$(a + \mathfrak{a}) + (b + \mathfrak{a}) := (a + b) + \mathfrak{a}$$

$$(a + \mathfrak{a}) \cdot (b + \mathfrak{a}) := ab + \mathfrak{a}$$

Fact:  $\phi: A \rightarrow A/\mathfrak{a}$  surj. ring homo.  
 $a \mapsto a + \mathfrak{a}$

(常用的结论)

$$\text{Prop 1.1} \quad \{ \bar{b} \triangleleft A/\mathfrak{a} \} \xleftrightarrow{1:1} \{ \bar{b} \supseteq \mathfrak{a} \mid \bar{b} \triangleleft A \}$$

$$\bar{b} \longmapsto \phi^{-1}(\bar{b})$$

pf: clear

□

✓ ring hom.

Fact:  $\forall f: A \rightarrow B \Rightarrow A/\ker f \cong \frac{\text{Im}(f)}{\text{subring of } B}$  (as rings)

$\nearrow$   
 $\frac{A}{f^{-1}(0)}$   
 quotient ring of A

$\uparrow$   
 subring of B

Notation:  $x \equiv y \pmod{\mathfrak{a}} \Leftrightarrow x - y \in \mathfrak{a}$ .

③



### §1.3 Zero divisors, Nilpotent elements units

zero divisor  $x \in A$  if " $x|0$ " i.e.  $\exists y \neq 0$  s.t.  $xy=0$ .

integral domain = ring without nontrivial zero divisors.

nilpotent element  $x \in A$ , if  $x^n=0$  for some  $n>0$ .

Fact:  $\{\text{nilpotent elements}\} \stackrel{A \neq 0}{\subseteq} \{\text{zero divisors}\}$

unit  $x \in A$ , if  $x|1$  i.e.  $\exists y$  s.t.  $xy=1$ . ( $x^{-1}=y$ )

Fact:  $A^\times := \{x \in A \mid x \text{ is a unit}\}$  is a mult. abelian gp.

principal ideal  $(x) := Ax := \{ax \mid a \in A\}$

Fact:  $x = \text{unit} \Leftrightarrow (x) = A$

notation:  $0 := (0)$

Field: nonzero ring with every nonzero element being a unit  
i.e.  $1 \neq 0$  &  $A^\times = A \setminus \{0\}$ .



Prop 1.2.  $A \neq 0$  ring. The following are equivalent (TFAE)

i)  $A = \text{field}$

ii)  $\mathfrak{a} \triangleleft A \Rightarrow \mathfrak{a} = 0 \text{ or } \mathfrak{a} = A$

iii)  $\forall A \xrightarrow[f]{\neq_0} B \text{ ring hom} \Rightarrow f = \tau \bar{\eta}.$

pf: i)  $\Rightarrow$  ii)  $\Rightarrow$  iii)  $\Rightarrow$  i)

i)  $\Rightarrow$  ii) Assume  $\mathfrak{a} \neq 0, \forall x \in \mathfrak{a} \setminus \{0\} \Rightarrow A = \overset{\text{unit}}{xA} \subseteq \mathfrak{a} \subseteq A \Rightarrow \mathfrak{a} = A$

ii)  $\Rightarrow$  iii)  $1 \notin \ker f \Rightarrow \ker f \neq A \Rightarrow \ker f = 0 \Rightarrow f = \tau \bar{\eta}.$

iii)  $\Rightarrow$  i)  $x \notin A^\times \Rightarrow (x) \neq A \Rightarrow B = A/(x) \neq 0 \Rightarrow (x) = \ker(A \twoheadrightarrow B) = 0$

注: 第1节课



## §1.4. Prime ideals and maximal ideals

Prime ideal  $\mathfrak{p} \triangleleft A$  :  $\mathfrak{p} \neq A$  &  $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \text{ or } y \in \mathfrak{p}$ .

maximal ideal  $\mathfrak{m} \triangleleft A$  :  $\mathfrak{m} \neq A$  &  $\mathfrak{m} \subseteq \mathfrak{a} \triangleleft A \Rightarrow \mathfrak{m} = \mathfrak{a} \text{ or } \mathfrak{a} = A$ .

Fact : •  $\mathfrak{p} \triangleleft A$  prime  $\Leftrightarrow A/\mathfrak{p} = \text{integral domain}$   
 $\Uparrow$

•  $\mathfrak{m} \triangleleft A$  maximal  $\Leftrightarrow A/\mathfrak{m} = \text{field}$

• maximal ideals are prime.

•  $0 \triangleleft A$  prime  $\Leftrightarrow A = \text{int. domain}$ .

•  $f^{-1}(\text{prime}) = \text{prime}$

•  $f^{-1}(\text{maximal}) \not\equiv \text{maximal}$   $\mathbb{Z} \hookrightarrow \mathbb{Q}$ .

Theorem 1.3  $A \neq 0 \Rightarrow \exists \text{ maximal ideal } \mathfrak{m}$ .

pf: (Zorn's lemma) 回顧-7

$$\Sigma := \{ \mathfrak{a} \neq A \mid \mathfrak{a} \triangleleft A \} \neq \emptyset \quad (0 \in \Sigma)$$

order = inclusion

$$\forall \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \dots \quad \text{in } \Sigma$$

$$\mathfrak{a} := \bigcup_{n=1}^{\infty} \mathfrak{a}_n \in \Sigma \quad \text{ie } \begin{cases} \mathfrak{a} \triangleleft A \\ \mathfrak{a} \neq A. \text{ or, } 1 \in \mathfrak{a} \Rightarrow 1 \in \mathfrak{a}_n \end{cases}$$

Zorn's lemma  $\Rightarrow \Sigma$  has maximal element.

⑥



Cor:  $\mathfrak{a} \triangleleft A \left. \begin{array}{l} \mathfrak{a} \neq A \end{array} \right\} \Rightarrow \exists \text{ maximal ideal } \mathfrak{m} \triangleleft A \text{ s.t. } \mathfrak{a} \subseteq \mathfrak{m}.$

Pf:  $\phi: A \rightarrow A/\mathfrak{a} \Rightarrow \exists \bar{\mathfrak{m}} \Rightarrow \exists \mathfrak{m}. \quad \square$

Cor:  $\forall x \in A \setminus A^\times \Rightarrow \exists \text{ maximal ideal } \mathfrak{m} \triangleleft A \text{ s.t. } x \in \mathfrak{m}.$

Pf:  $\mathfrak{a} = (x). \quad \square$

local ring = ring  $A$  with exactly one maximal ideal  $\mathfrak{m}$   
residue field  $k = A/\mathfrak{m}.$

Prop 1.6 i)  $\mathfrak{m} \triangleleft A$  ( $\mathfrak{m} \neq A$ ).  $A \setminus \mathfrak{m} \subseteq A^\times \Rightarrow (A, \mathfrak{m}) = \text{local}$   
 ii).  $\mathfrak{m} = \text{maximal}$ .  $1 + \mathfrak{m} \subseteq A^\times \Rightarrow (A, \mathfrak{m}) = \text{local}$

Pf: i)  $\forall \mathfrak{a} \triangleleft A$  ( $\mathfrak{a} \neq A$ )  $\Rightarrow \mathfrak{a} \cap A^\times = \emptyset \xRightarrow{A \setminus \mathfrak{m} \subseteq A^\times} \mathfrak{a} \subseteq \mathfrak{m} \Rightarrow (A, \mathfrak{m}) = \text{local}$

ii)  $\forall x \in A \setminus \mathfrak{m} \Rightarrow (x) + \mathfrak{m} = A \ni 1$

$\Rightarrow \exists y \in A, z \in \mathfrak{m} \text{ s.t. } xy + z = 1$

$\Rightarrow xy = 1 - z \in A^\times$

$\Rightarrow x \in A^\times \Rightarrow (A, \mathfrak{m}) = \text{local}.$

Semi-local ring = ring with only finitely many maximal ideal



Principle ideal domain (PID) = domain with every ideal principal.

Fact: In PID, every nonzero prime ideal is maximal.

Example:  $A = \mathbb{Z}$ . prime  $\{0, (2), (3), (5), \dots\}$

max.  $\{(2), (3), (5), \dots\}$



注: 第2节课



## §1.5 nilradical and Jacobson radical

nilradical of  $A := \{ x \in A \mid x^n = 0 \text{ for some } n \geq 1 \}$

Notation:  $r(0)$ ,  $\sqrt{0}$ ,  $\text{Nil}(A)$

Prop 1.7 1)  $\sqrt{0} \triangleleft A$

2)  $A/\sqrt{0}$  has no nonzero nilpotent elements.

Pf: 1)  $\forall a \in A, \forall x, y \in \sqrt{0}$  with  $x^n = 0 = y^m$ .

$$\Rightarrow \begin{cases} (ax)^n = a^n \cdot x^n = 0 \\ (x+y)^{m+n} = \sum_i \binom{m+n}{i} x^m \cdot y^n = 0. \end{cases}$$

$$2). \forall (a + \sqrt{0})^n = 0 \Rightarrow a^n \in \sqrt{0}$$

$$\Rightarrow \exists m \text{ s.t. } (a^n)^m = 0$$

$$\Rightarrow a \in \sqrt{0}$$

Prop 1.8:  $\sqrt{0} = \bigcap_{\mathfrak{P}:\text{prime}} \mathfrak{P}$

Pf: " $\subseteq$ ", clear  $(\forall x \in \sqrt{0} = x^n = 0 \Rightarrow x \in \mathfrak{P} \text{ } \forall \mathfrak{P} \text{ prime})$



" $\geq$ ". 反证: Suppose  $\sqrt{0} \notin \bigcap_{\mathcal{P}:\text{prime}} \mathcal{P}$ .

$$\forall f \in \bigcap_{\mathcal{P}:\text{prime}} \mathcal{P} \mid \sqrt{0}$$

$$\Rightarrow 0 \notin \{1, f, f^2, \dots\} =: S$$

$$\Sigma := \{ \mathcal{U} \triangleleft A \mid S \cap \mathcal{U} = \emptyset \} \neq \emptyset \quad (0 \in \Sigma)$$

Zorn's lemma  
 $\implies \Sigma$  has maximal element.  $\mathcal{P}$ .

$\mathcal{P}$  素理想.  $\downarrow$ .

$$\forall x, y \notin \mathcal{P} \Rightarrow (x) + \mathcal{P}, (y) + \mathcal{P} \notin \Sigma$$

$$\Rightarrow f^m \in (x) + \mathcal{P} \ \& \ f^n \in (y) + \mathcal{P}.$$

$$\Rightarrow f^{m+n} \in (xy) + \mathcal{P}$$

$$\Rightarrow (xy) + \mathcal{P} \notin \Sigma$$

$$\Rightarrow xy \notin \mathcal{P}$$

Thus  $\mathcal{P}$  prime  $\downarrow$ . ( $f \notin \mathcal{P}$ !)



Jacobson radical:

$$\text{Rad}(A) := \bigcap_{\mathfrak{m}:\text{max}} \mathfrak{m}$$

Prop:  $x \in \text{Rad}(A) \Leftrightarrow 1 - xy \in A^\times$

Pf:  $\Rightarrow$ ) Suppose  $1 - xy \notin A^\times$ .

$\Rightarrow 1 - xy \in \mathfrak{m}$  for some  $\mathfrak{m}$  maximal ideal

$\Rightarrow 1 \in xy + \mathfrak{m} = \mathfrak{m} \quad \downarrow$

$\Leftarrow$ ). Suppose  $x \notin \mathfrak{m}$ .

$\Rightarrow (x) + \mathfrak{m} = A$

$\Rightarrow xy + u = 1$  for some  $y \in A, u \in \mathfrak{m}$

$\Rightarrow u = 1 - xy \in A^\times \quad \downarrow$ .



## §1.6 operations on ideals

$$\mathfrak{a}, \mathfrak{b} \text{ coprime} \stackrel{\text{def}}{\iff} \mathfrak{a} + \mathfrak{b} = A.$$

$$\text{Fact: } \mathfrak{a}, \mathfrak{b} \text{ coprime} \Rightarrow \mathfrak{a} \cap \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b}$$

$$\text{Pf: } x + y = 1 \Rightarrow \forall z \in \mathfrak{a} \cap \mathfrak{b}, z = z \cdot 1 = zy + xz \in \mathfrak{a} \cdot \mathfrak{b}.$$

$$\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n \triangleleft A$$

$$\begin{aligned} \Rightarrow \phi : A &\longrightarrow A/\mathfrak{a}_1 \times A/\mathfrak{a}_2 \times \dots \times A/\mathfrak{a}_n \\ x &\longmapsto (x + \mathfrak{a}_1, x + \mathfrak{a}_2, \dots, x + \mathfrak{a}_n) \\ &\text{ring homo.} \end{aligned}$$

$$\text{Prop 1.10} \quad \text{i). } \mathfrak{a}_i, \mathfrak{a}_j \text{ coprime } \forall i \neq j \Rightarrow \prod_i \mathfrak{a}_i = \bigcap_i \mathfrak{a}_i$$

$$\text{ii). } \phi = \text{surj} \iff \mathfrak{a}_i, \mathfrak{a}_j \text{ coprime } \forall i \neq j$$

$$\text{iii). } \phi = \text{inj} \iff \bigcap \mathfrak{a}_i = 0$$

Pf: i) " $\leq$ " clear

注: 第3节课

$$" \geq " \text{ By induction, } \prod_{i=1}^{n-1} \mathfrak{a}_i = \bigcap_{i=1}^{n-1} \mathfrak{a}_i =: \mathfrak{a}. \quad (\mathfrak{b} := \mathfrak{a}_n)$$

$$\mathfrak{a} + \mathfrak{b} \supseteq (\mathfrak{a}_1 + \mathfrak{b}) \cdot (\mathfrak{a}_2 + \mathfrak{b}) \cdots (\mathfrak{a}_{n-1} + \mathfrak{b}) = A$$

$$\Rightarrow \prod_{i=1}^n \mathfrak{a}_i = \mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} \cap \mathfrak{b} = \left( \bigcap_{i=1}^{n-1} \mathfrak{a}_i \right) \cap \mathfrak{a}_n = \bigcap_{i=1}^n \mathfrak{a}_i$$



ii).  $\Rightarrow$

$$\phi = \text{surj} \Rightarrow \exists x \quad \phi(x) = (1, 0, \dots, 0)$$

$$\Rightarrow \begin{cases} x \equiv 1 \pmod{\mathfrak{A}_1} \\ x \equiv 0 \pmod{\mathfrak{A}_2} \end{cases}$$

$$\Rightarrow 1 = (1-x) + x \in \mathfrak{A}_1 + \mathfrak{A}_2$$

$$\Rightarrow \mathfrak{A}_1, \mathfrak{A}_2 \text{ coprime (similar for } i \neq j)$$

$\Leftarrow$ ) only need to show (DNTS):

$$(1, 0, \dots, 0) \in \text{im}(\phi).$$

i.e.  $\exists x$  s.t.

$$\begin{cases} x \equiv 1 \pmod{\mathfrak{A}_1} \\ x \equiv 0 \pmod{\mathfrak{A}_2} \\ \vdots \\ x \equiv 0 \pmod{\mathfrak{A}_n} \end{cases}$$

$$\mathfrak{A}_1 + \mathfrak{A}_2 \mathfrak{A}_3 \dots \mathfrak{A}_n \supseteq (\mathfrak{A}_1 + \mathfrak{A}_2)(\mathfrak{A}_1 + \mathfrak{A}_3) \dots (\mathfrak{A}_1 + \mathfrak{A}_n) = A$$

$$\Rightarrow \exists y \in \mathfrak{A}_1, x \in \mathfrak{A}_2 \mathfrak{A}_3 \dots \mathfrak{A}_n \text{ s.t.}$$

$$1 = y + x$$

$$\text{iii). } \phi = \text{inj} \Leftrightarrow \ker \phi = 0 \Leftrightarrow \bigcap_{i=1}^n \mathfrak{A}_i = 0.$$



Prop 1.11 i)  $\mathfrak{P}_1, \dots, \mathfrak{P}_n$  prime.  $\mathfrak{A} \triangleleft A$ .

$$\mathfrak{A} \subseteq \bigcup_{i=1}^n \mathfrak{P}_i \Rightarrow \exists i \text{ s.t. } \mathfrak{A} \subseteq \mathfrak{P}_i$$

ii).  $\mathfrak{A}_1, \dots, \mathfrak{A}_n$  ideal,  $\mathfrak{P}$  prime

$$\bigcap_i \mathfrak{A}_i \subseteq \mathfrak{P} \Rightarrow \exists i \text{ s.t. } \mathfrak{A}_i \subseteq \mathfrak{P}$$

In particular  $\bigcap_i \mathfrak{A}_i = \mathfrak{P} \Rightarrow \exists i \text{ s.t. } \mathfrak{A}_i = \mathfrak{P}.$   
 $(\mathfrak{P} \subseteq \mathfrak{A}_i \subseteq \mathfrak{P})$

pf: i) induction on  $n$

Suppose  $\mathfrak{A} \not\subseteq \mathfrak{P}_1 \cup \dots \cup \mathfrak{P}_{i-1} \cup \mathfrak{P}_{i+1} \cup \dots \cup \mathfrak{P}_n \quad \forall i$

$$\Rightarrow \exists x_i \in \mathfrak{A} \text{ s.t. } x_i \notin \mathfrak{P}_j \quad \forall j \neq i. (\Rightarrow x_i \in \mathfrak{P}_i)$$

$$y := \sum x_1 \dots x_{i-1} x_{i+1} \dots x_n$$

$$\Rightarrow y \in \mathfrak{A} \text{ \& } y \notin \mathfrak{P}_i \quad \forall i \quad \downarrow$$

ii) Suppose  $\mathfrak{A}_i \not\subseteq \mathfrak{P} \quad \forall i \Rightarrow \exists x_i \in \mathfrak{A}_i \setminus \mathfrak{P} \quad \forall i$

$$\Rightarrow \prod_{i=1}^n x_i \in \bigcap \mathfrak{A}_i \setminus \mathfrak{P} = \emptyset \quad \downarrow$$



ideal quotient of  $\mathfrak{a}, \mathfrak{b} \triangleleft A$

$$(\mathfrak{a} : \mathfrak{b}) := \{x \in A \mid x\mathfrak{b} \subseteq \mathfrak{a}\}$$

annihilator of  $\mathfrak{b}$

$$\text{Ann}(\mathfrak{b}) := (0 : \mathfrak{b})$$

Notion:  $(\mathfrak{a} : x) := (\mathfrak{a} : (x))$ ,  $\text{Ann}(x) := \text{Ann}((x))$ .

Fact:  $\{\text{zero divisors}\} = \bigcup_{x \neq 0} \text{Ann}(x)$ .

Example:  $((m) : (n)) = \left( \frac{m}{\gcd(m, n)} \right) \triangleleft \mathbb{Z}$ .

$$\text{pf: } an \in (m) \Leftrightarrow m \mid an \Leftrightarrow \frac{m}{\gcd(m, n)} \mid a \cdot \frac{n}{\gcd(m, n)} \Leftrightarrow \frac{m}{\gcd(m, n)} \mid a$$

$$a \in ((m) : (n)) \Leftrightarrow a \in \left( \frac{m}{\gcd(m, n)} \right) \quad \square$$

lemma: i)  $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b}) \subseteq A$

ii)  $(\mathfrak{a} : \mathfrak{b}) \cdot \mathfrak{b} \subseteq \mathfrak{a}$

iii)  $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$

iv)  $(\bigcap_i \mathfrak{a}_i : \mathfrak{b}) = \bigcap_i (\mathfrak{a}_i : \mathfrak{b})$

v)  $(\mathfrak{a} : \sum_i \mathfrak{b}_i) = \bigcap_i (\mathfrak{a} : \mathfrak{b}_i)$

注: 第4节课 (15)



## Radical of $\mathfrak{A} \triangleleft A$

$$\sqrt{\mathfrak{A}} := \{ x \in A \mid x^n \in \mathfrak{A} \text{ for some } n > 0 \}$$

$$\text{Fact: } \phi: A \twoheadrightarrow A/\mathfrak{A} \Rightarrow \sqrt{\mathfrak{A}} = \phi^{-1}(\sqrt{0}) \Rightarrow \sqrt{\mathfrak{A}} \triangleleft A.$$

Lemma: i)  $\mathfrak{A} \subseteq \sqrt{\mathfrak{A}}$

$$\text{ii) } \sqrt{\sqrt{\mathfrak{A}}} = \sqrt{\mathfrak{A}}$$

$$\text{iii) } \sqrt{\mathfrak{A} \mathfrak{B}} = \sqrt{\mathfrak{A} \cap \mathfrak{B}} = \sqrt{\mathfrak{A}} \cap \sqrt{\mathfrak{B}}$$

$$\text{iv) } \sqrt{\mathfrak{A}} = A \Leftrightarrow \mathfrak{A} = A$$

$$\text{v) } \sqrt{\mathfrak{A} + \mathfrak{B}} = \sqrt{\sqrt{\mathfrak{A}} + \sqrt{\mathfrak{B}}}$$

$$\text{vi) } \mathfrak{P} = \text{prime} \Rightarrow \sqrt{\mathfrak{P}^n} = \mathfrak{P} \quad \forall n > 0.$$

pf: i)  $\checkmark$

$$\text{ii) } x \in \sqrt{\mathfrak{A}} \Rightarrow (x^n)^m \in \mathfrak{A} \Rightarrow x \in \sqrt{\mathfrak{A}}$$

$$\text{iii) } \sqrt{\mathfrak{A} \mathfrak{B}} \subseteq \sqrt{\mathfrak{A} \cap \mathfrak{B}} \subseteq \sqrt{\mathfrak{A}} \cap \sqrt{\mathfrak{B}}$$

$$\forall x \in \sqrt{\mathfrak{A}} \cap \sqrt{\mathfrak{B}} \Rightarrow x^n \in \mathfrak{A} \text{ \& } x^m \in \mathfrak{B}$$

$$\Rightarrow x^{n+m} \in \mathfrak{A} \cdot \mathfrak{B} \Rightarrow x \in \sqrt{\mathfrak{A} \mathfrak{B}}$$

$$\text{iv) } \sqrt{\mathfrak{A}} = A \Leftrightarrow 1^n \in \mathfrak{A} \Leftrightarrow 1 \in \mathfrak{A} \Leftrightarrow \mathfrak{A} = A$$

$$\text{v) "}\leq\text{" \& "}\geq\text{" } \forall x \in \sqrt{\mathfrak{A} + \mathfrak{B}} \quad x^m = a + b, \quad a^s \in \mathfrak{A} \quad b^t \in \mathfrak{B}$$

$$\Rightarrow x^{m(s+t)} = \sum_i \binom{s+t}{i} a^i b^{s+t-i} \in \mathfrak{A} + \mathfrak{B}$$

$$\Rightarrow x \in \sqrt{\mathfrak{A} + \mathfrak{B}}$$

$$\text{vi) } \mathfrak{P} \subseteq \sqrt{\mathfrak{P}^n} \text{ (v)}. \quad x^m \in \mathfrak{P}^n \subseteq \mathfrak{P} \Rightarrow x \in \mathfrak{P} \Rightarrow \sqrt{\mathfrak{P}^n} \subseteq \mathfrak{P}$$



Prop 1.14  $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \supseteq \mathfrak{a}: \text{prime}} \mathfrak{p}$

Pf:  $A \twoheadrightarrow A/\mathfrak{a} \quad \{\mathfrak{p} \supseteq \mathfrak{a}: \text{prime}\} \xleftrightarrow{|\cdot|} \{\bar{\mathfrak{p}}: \text{prime in } A/\mathfrak{a}\}$

$$\Rightarrow \sqrt{\mathfrak{a}} = \phi^{-1}(\sqrt{0}) = \phi^{-1}\left(\bigcap_{\bar{\mathfrak{p}}: \text{prime}} \bar{\mathfrak{p}}\right) = \bigcap_{\bar{\mathfrak{p}}: \text{prime}} \phi^{-1}(\bar{\mathfrak{p}}) = \bigcap_{\substack{\mathfrak{p}: \text{prime} \\ \mathfrak{p} \supseteq \mathfrak{a}}} \mathfrak{p}$$

$E \subseteq A$  subset

$$\sqrt{E} := \{x \in A \mid \exists n > 0 \text{ s.t. } x^n \in E\} \quad (\text{not ideal})$$

$$\text{Fact: } \sqrt{\bigcup_{\alpha} E_{\alpha}} = \bigcup_{\alpha} \sqrt{E_{\alpha}}$$

Prop 1.15  $\{\text{zero-divisors}\} = \bigcup_{x \neq 0} \text{Ann}(x) = \bigcup_{x \neq 0} \sqrt{\text{Ann}(x)}.$

Prop 1.16:  $\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}} = A \Rightarrow \mathfrak{a} + \mathfrak{b} = A$

Pf:  $\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}} = \sqrt{A} = A \Rightarrow \mathfrak{a} + \mathfrak{b} = A.$

□



# §1.7 Extension and contraction

$f: A \rightarrow B$  ring hom.  $\mathfrak{a} \triangleleft A, \mathfrak{b} \triangleleft B$

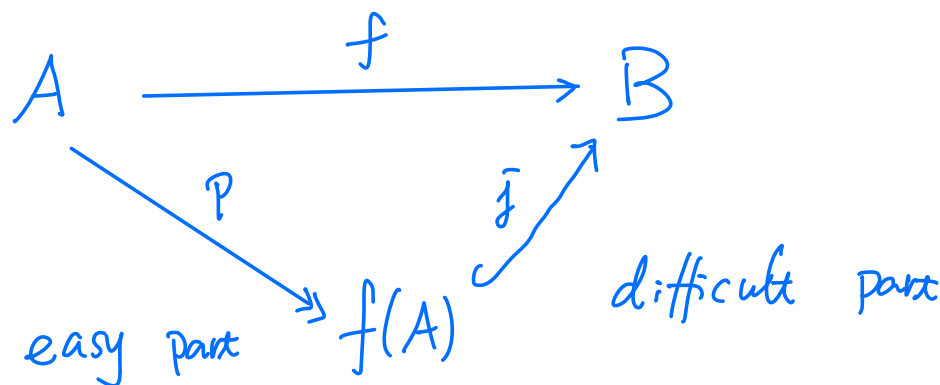
$f(\mathfrak{a}) \triangleleft B$  ?  $\times$   $f^{-1}(\mathfrak{b}) \triangleleft A$  ?  $\checkmark$

extension of  $\mathfrak{a}$   $\mathfrak{a}^e := f(\mathfrak{a}) \cdot B \triangleleft B$  由  $f(\mathfrak{a})$  生成的理想.

contraction of  $\mathfrak{b}$   $\mathfrak{b}^c := f^{-1}(\mathfrak{b})$

Fact:  $\mathfrak{b} = \text{prime} \Rightarrow \mathfrak{b}^c = \text{prime}$

Question:  $\mathfrak{a} = \text{prime} \stackrel{?}{\Rightarrow} \mathfrak{a}^e = \text{prime}$



$$\{\mathfrak{a} \triangleleft A \mid \mathfrak{a} \supseteq \ker f\} \xleftrightarrow{f} \{\bar{\mathfrak{a}} \triangleleft f(A)\} \rightleftharpoons \{\mathfrak{b} \triangleleft B\}$$

↑  
complicated.

Example:  $\mathbb{Z} \hookrightarrow \mathbb{Z}[i], i^2 = -1$ .

$$2^e = (1+i)^2, \quad p^e = \begin{cases} p_1 \cdot p_2 & p \equiv 1 \pmod{4} \\ (p) & p \equiv 3 \pmod{4} \end{cases}$$



one central problem of algebraic number theory:

the behavior of prime ideals under extensions.

注: 第5节课

Prop 1.17 i)  $\mathfrak{A} \subseteq \mathfrak{A}^{ec}$ ,  $\mathfrak{B}^{ce} \subseteq \mathfrak{B}$ ;

ii)  $\mathfrak{A}^e = \mathfrak{A}^{ece}$ ,  $\mathfrak{B}^c = \mathfrak{B}^{cec}$ , in particular

$$\mathfrak{A}^{ec} = \mathfrak{A} \Leftrightarrow \exists \mathfrak{B} \text{ s.t. } \mathfrak{A} = \mathfrak{B}^c$$

$$\mathfrak{B}^{ce} = \mathfrak{B} \Leftrightarrow \exists \mathfrak{A} \text{ s.t. } \mathfrak{B} = \mathfrak{A}^e$$

$$\text{iii) } \left\{ \mathfrak{A} \mid \mathfrak{A}^{ec} = \mathfrak{A} \right\} \xleftrightarrow{1:1} \left\{ \mathfrak{B} \triangleleft B \mid \mathfrak{B}^{ce} = \mathfrak{B} \right\}$$

C !!

$$\begin{array}{ccc} \mathfrak{A} & \xrightarrow{\quad} & \mathfrak{A}^e \\ \mathfrak{B}^c & \xleftarrow{\quad} & \mathfrak{B} \end{array}$$

E !!

Lemma:  $\mathfrak{A}_1, \mathfrak{A}_2 \triangleleft A$ ,  $\mathfrak{B}_1, \mathfrak{B}_2 \triangleleft B$ . Then

$$(\mathfrak{A}_1 + \mathfrak{A}_2)^e = \mathfrak{A}_1^e + \mathfrak{A}_2^e$$

$$(\mathfrak{B}_1 + \mathfrak{B}_2)^c \supseteq \mathfrak{B}_1^c + \mathfrak{B}_2^c$$

$$(\mathfrak{A}_1 \cap \mathfrak{A}_2)^e \subseteq \mathfrak{A}_1^e \cap \mathfrak{A}_2^e$$

$$(\mathfrak{B}_1 \cap \mathfrak{B}_2)^c = \mathfrak{B}_1^c \cap \mathfrak{B}_2^c$$

$$(\mathfrak{A}_1 \mathfrak{A}_2)^e = \mathfrak{A}_1^e \mathfrak{A}_2^e$$

$$(\mathfrak{B}_1 \mathfrak{B}_2)^c \supseteq \mathfrak{B}_1^c \mathfrak{B}_2^c$$

$$(\mathfrak{A}_1 : \mathfrak{A}_2)^e \subseteq (\mathfrak{A}_1^e : \mathfrak{A}_2^e)$$

$$(\mathfrak{B}_1 : \mathfrak{B}_2)^c \subseteq (\mathfrak{B}_1^c : \mathfrak{B}_2^c)$$

$$\sqrt{\mathfrak{A}}^e \subseteq \sqrt{\mathfrak{A}^e}$$

$$\sqrt{\mathfrak{B}}^c = \sqrt{\mathfrak{B}^c}$$



- $C$  closed under  $\cap, \cup, \sqrt{\phantom{x}}$
- $E$  closed under  $+$ ,  $\cdot$

$(\delta_1 : \delta_2)^c \subseteq (\delta_1^c : \delta_2^c)$  等号不成立的反例

$$A = \mathbb{Z} \hookrightarrow B = \mathbb{Z}[\sqrt{-1}]$$

$$\delta_1 = (2), \quad \delta_2 = (1 + \sqrt{-1})$$

$$\Rightarrow (\delta_1 : \delta_2) = (1 + \sqrt{-1}) = \delta_2$$

$$\delta_1^c = (2), \quad \delta_2^c = (2)$$

$$\Rightarrow (\delta_1^c : \delta_2^c) = A$$

$C$  is closed under ":"

$$(\delta_1^c : \delta_2^c)^{ec} \subseteq (\delta_1^{ce} : \delta_2^{ce})^c$$

$$\subseteq (\delta_1^{cec} : \delta_2^{cec})$$

$$= (\delta_1^c : \delta_2^c)$$

$$\Rightarrow (\delta_1^c : \delta_2^c) \in C \quad \square$$