Chinese Remainder Theorem, Maximal and prime ideals, PIDs

Chinese Remainder Theorem

If $n_1, \dots, n_r$ are pair-wise coprime integers, then

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \text{ is surjective}$$

$$\text{and the kernel is } n_1\mathbb{Z} \cap \cdots \cap n_r\mathbb{Z} = n_1 \cdots n_r\mathbb{Z}$$

<u>Definition</u> We say two ideals I and J of a commutative ring R are <u>comaximal</u> if $I+J=R$

i.e. $1 \in R$ can be written as $1 = a+b$ with $a \in I$, $b \in J$

(E.g. $R = \mathbb{Z}$, $I = (m)$, $J = (n)$ s.t. $\gcd(m,n) = 1$.

This says $(m)+(n) = (m,n) = (1)$, i.e. $1 = mx+ny$ for $x,y \in \mathbb{Z}$.)

<u>Theorem</u> Let $I_1, \cdots, I_k$ be ideals of a commutative ring R

Then the natural map $\varphi : R \longrightarrow R/I_1 \times \cdots \times R/I_k$ is a ring homomorphism

$$x \longmapsto (x \bmod I_1, \cdots, x \bmod I_k)$$

with $\ker \varphi = I_1 \cap \cdots \cap I_k$

- If $I_1, \cdots, I_k$ are pairwise comaximal, then

  (1) φ is surjective

  (2) $I_1 \cap \cdots \cap I_k = I_1 \cdots I_k$

$$\Rightarrow \varphi : R/I_1 \cdots I_k = R/I_1 \cap \cdots \cap I_k \xrightarrow{\sim} R/I_1 \times \cdots \times R/I_k$$

Proof: First assume $k=2$.

- $I_1 I_2 \subseteq I_1 \cap I_2$ ✓
- $I_1 \cap I_2 \overset{?}{\subseteq} I_1 I_2$: Since $R = I_1 + I_2 \Rightarrow 1 = a_1 + a_2$ for $a_1 \in I_1, a_2 \in I_2$

  So for $b \in I_1 \cap I_2$, $b = a_1 b + a_2 b \in I_1 I_2$. ✓

Now, consider $\varphi(a_1) = (a_1 \bmod I_1,\ \overset{1-a_2}{\overset{\shortparallel}{a_1}} \bmod I_2) = (0,1) \in A/I_1 \times A/I_2$

$\varphi(a_2) = (\overset{1-a_1}{\overset{\shortparallel}{a_2}} \bmod I_1,\ a_2 \bmod I_2) = (1,0) \in A/I_1 \times A/I_2$

So any $(x_1 \bmod I_1,\ x_2 \bmod I_2) = \varphi(x_1 a_2 + x_2 a_1)$.

In general, we use induction

$$\varphi : R \twoheadrightarrow R/I_1 \times R/I_2 \cdots I_k \twoheadrightarrow R/I_1 \times \cdots \times R/I_k$$

<u>check</u>: $I_1 + I_2 \cdots I_k \overset{?}{=} R$

Write $1 = b_i + a_i$ for $b_i \in I_1$, $a_i \in I_i$ $\forall i = 2, \dots, k$

$\Rightarrow 1 = (b_2 + a_2) \cdots (b_k + a_k)$

$= \underbrace{b_2 \cdots b_k + \text{something with } b_i}_{\text{in } I_1} + \underbrace{a_2 \cdots a_k}_{\text{in } I_2 \cdots I_k}$ ✓

□

<u>Some logics</u>:

<u>Definition</u> A <u>partial order</u> (偏序) on a nonempty set A is a relation $\preccurlyeq$ on A satisfying

for all $x, y, z \in A$,
(1) $x \preccurlyeq x$ (reflexive)
(2) if $x \preccurlyeq y$ and $y \preccurlyeq x$, then $x = y$ (antisymmetric)
(3) if $x \preccurlyeq y$ and $y \preccurlyeq z$, then $x \preccurlyeq z$ (transitive)

- A <u>chain</u> is a subset $B \subseteq A$ where $\forall x, y \in B$, either $x \preccurlyeq y$ or $y \preccurlyeq x$.

<u>Zorn's Lemma</u> (This is an axiom!)

If A is a partially ordered set in which every chain B has an upper bound
(i.e. $\exists$ an element $m \in A$ s.t. $m \succcurlyeq b$ for every $b \in B$.)
then A has a maximal element x (i.e. an element s.t. no $y \succ x$)

Maximal ideals

<u>Definition</u> If R is a ring, a (two-sided) ideal $\mathfrak{m} \subseteq R$ is called <u>maximal</u> (极大理想) if $\mathfrak{m} \neq R$ and the only (two-sided) ideals containing $\mathfrak{m}$ are $\mathfrak{m}$ and R.

<u>Proposition</u> Every proper ideal $I \subseteq R$ is contained in a maximal ideal of R

Proof: Let $\mathcal{S} := \{$proper ideals of R containing $I\}$, partially ordered by inclusion

Check the increasing chain condition: $\cdots J_i \subseteq \cdots$ has an upper bound:

$J := \bigcup_{i \in S} I_i$ is an ideal yet $1 \notin J \Rightarrow J$ is a proper ideal containing I.

So $\mathcal{S}$ admits a maximal element: the maximal ideal we need. $\square$

<u>Proposition</u> Suppose that R is commutative. Then an ideal $\mathfrak{m} \subseteq R$ is maximal $\Leftrightarrow R/\mathfrak{m}$ is a field

Proof: By 4^{th} Isom. Theorem,

$$\mathfrak{m} \subseteq R \text{ is maximal } \Leftrightarrow R/\mathfrak{m} =: \bar{R} \text{ has only two ideals } (0)\ (1) \overset{?}{\Leftrightarrow} \bar{R} \text{ is a field}$$

$\Leftarrow$ obvious

$\Rightarrow$ $\forall a \in \bar{R}, a \neq 0$, then $(a) \neq (0) \Rightarrow (a) = (1)$ i.e. $\exists a' \in \bar{R}$ s.t. $aa' = 1$

$\Rightarrow a \in \bar{R}^\times$. So $\bar{R}$ is a field. $\square$

<u>Remark</u>: If R is non-commutative, $R/\mathfrak{m}$ is a skew field $\Rightarrow \mathfrak{m}$ is a maximal ideal.

The converse is not true, e.g. $R = \mathrm{Mat}_{n \times n}(\mathbb{C})$ has no nontrivial two-sided ideal.

<u>Example</u>: ① $R = \mathbb{Z}$, p a prime number, $(p) = p\mathbb{Z}$ is a maximal ideal.

② $R = \mathbb{Z}[x]$, $(p) = p\mathbb{Z}[x]$ is not maximal

But $\underset{\cap\!\!\!|}{}(p, x)$, or $(p, x+1)$, $(p, f(x))$ is maximal (any poly irred mod p.)

③ G finite group. $R = \mathbb{C}[G] \supseteq I_R = \langle g - 1 ; g \in G \rangle$ is max'l (two-sided) ideal

$R/I_R \simeq \mathbb{C}$

Prime ideals / prime elements Now, assume that R is commutative

Definition A proper ideal $\mathfrak{p} \subseteq R$ is called a prime ideal (素理想) if

for any $a, b \in R$, $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$

E.g. p prime, $p\mathbb{Z}$ is a prime ideal.

$p\mathbb{Z}[x] \subseteq \mathbb{Z}[x]$ is also a prime ideal.

Proposition An ideal $\mathfrak{p} \subseteq R$ is prime if and only if $R/\mathfrak{p}$ is an integral domain

Proof: $\pi : R \longrightarrow R/\mathfrak{p}$

$a \longmapsto \bar{a}$ ← denote the image

"$\Leftarrow$" If $a, b \in R$ with $ab \in \mathfrak{p} \Rightarrow \overline{ab} = 0 \Rightarrow$ either $\bar{a} = 0$ or $\bar{b} = 0$

$\Rightarrow$ either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. So $\mathfrak{p}$ is prime

"$\Rightarrow$" Suppose that $R/\mathfrak{p}$ is not an integral domain,

then $\exists\, \bar{a}^{\neq 0}, \bar{b}^{\neq 0} \in R/\mathfrak{p}$ s.t. $\bar{a} \cdot \bar{b} = 0$

$\Rightarrow \exists\, a, b \in R \setminus \mathfrak{p}$ s.t. $ab \in \mathfrak{p}$.

Thus $\mathfrak{p}$ cannot be a prime ideal. $\square$

Corollary: A maximal ideal is always a prime ideal

An interesting property of prime ideals

Proposition (1) Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be prime ideals and let $\mathfrak{a}$ be an ideal contained in $\bigcup_{i=1}^n \mathfrak{p}_i$.

Then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i

(2) Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals and let $\mathfrak{p}$ be a prime ideal containing $\bigcap_{i=1}^n \mathfrak{a}_i$. Then $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some i.

If $\mathfrak{p} = \cap\, \mathfrak{a}_i$, then $\mathfrak{p} = \mathfrak{a}_i$ for some i.

Proof: (2) Suppose not. $\exists\, x_i \in \mathfrak{a}_i \setminus \mathfrak{p}$.

Then $x_1 \cdots x_n \in \mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \bigcap_{i=1}^{n} \mathfrak{a}_i \subseteq \mathfrak{p}$. Contradiction!

If $\mathfrak{p} = \cap \mathfrak{a}_i$, then $\mathfrak{p} = \cap \mathfrak{a}_i \subseteq \mathfrak{a}_i \Rightarrow \mathfrak{p} = \mathfrak{a}_i$.

(1) We prove by induction on n that

$$\mathfrak{a} \not\subseteq \mathfrak{p}_i \text{ for } i=1,\dots,n \Longrightarrow \mathfrak{a} \not\subseteq \mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_n$$

$n=1$ ✓ suppose proved for $n-1$.

$\forall i$, $\exists\, x_i \in \mathfrak{a}$ but $x_i \notin \mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_{i-1} \cup \mathfrak{p}_{i+1} \cup \dots \cup \mathfrak{p}_n$

If some $x_i \notin \mathfrak{p}_i$, we are done. So assume that $x_i \in \mathfrak{p}_i$ $\forall i$

Consider $y = \sum_{i=1}^{n} x_1 \cdots x_{i-1} x_{i+1} \cdots x_n$.

$y \in \mathfrak{a}$, and $y \notin \mathfrak{p}_i$ for any i. ✓ □

* $f: R \longrightarrow S$ ring homomorphism of commutative rings
  - $\mathfrak{b} \subseteq S$ an ideal $\Rightarrow f^{-1}(\mathfrak{b})$ is an ideal "contraction of an ideal"
  - $\mathfrak{a} \subseteq R$ an ideal $\rightsquigarrow f(\mathfrak{a})S$ is an ideal of S "extension of an ideal"

Key result: If $\mathfrak{b} \subseteq S$ is a prime ideal, then $f^{-1}(\mathfrak{b})$ is a prime ideal of R

Proof: $\dfrac{R}{f^{-1}(\mathfrak{b})} \hookrightarrow \dfrac{S}{\mathfrak{b}}$ integral domain because $\mathfrak{b}$ is a prime ideal

So $f(R)/\mathfrak{b}$ is also an integral domain

$\cong R/f^{-1}(\mathfrak{b}) \Rightarrow f^{-1}(\mathfrak{b}) \subseteq R$ prime ideal. □

- Initial study of rings is modeled on properties of $\mathbb{Z}$ and some possible extensions: $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$

Definition A Principal ideal domain (PID) (主理想整环) is an integral domain in which every ideal is principal

Example: $\mathbb{Z}$, all ideals are of the form $n\mathbb{Z}$ for some n.

$k[x]$ for k field

$\mathbb{Z}[i]$ to be proved later

Non-example $\mathbb{Z}[\sqrt{-5}]$ $\quad (3, 1+2\sqrt{-5})$ is not a principal ideal (see later)

Proposition. Every non-zero prime ideal in a PID is a maximal ideal.

Proof: Let (p) be a prime ideal in a PID R

If $M=(m) \supseteq (p)$ is a maximal ideal containing (p)

$\Rightarrow p = mn$ for some $n \in R$

$\Rightarrow$ either m or n belongs to (p) $\begin{cases} \text{if } m \in (p) \Rightarrow (m) \subseteq (p) \Rightarrow (m)=(p) \\ \text{if } n \in (p) \Rightarrow n = ps \Rightarrow \cancel{p} = m\cancel{p}s \Rightarrow m \text{ is a unit} \end{cases}$

$\Rightarrow M = (1)$. $\square$

Quadratic integer rings

D = square-free integers (positive or negative) $D \neq 1$

$$\begin{array}{ccc} \mathcal{O}_? & — & \mathbb{Q}(\sqrt{D}) = \{x+y\sqrt{D} \mid x,y \in \mathbb{Q}\} \\ | & & | \\ \mathbb{Z} & — & \mathbb{Q} \end{array}$$

a "quadratic field extension" of $\mathbb{Q}$

$$\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{if } D \equiv 2,3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{if } D \equiv 1 \pmod 4 \end{cases}$$

Let $f(z) = z^2 - D$ or $z^2 - z + \frac{1-D}{4} \in \mathbb{Z}[z]$. Then $\mathcal{O} = \mathbb{Z}[z]/(f(z))$

In the quotient, z is a proxy of $\sqrt{D}$ or $\frac{1+\sqrt{D}}{2}$

Conjugate: $\overline{x+y\sqrt{D}} := x - y\sqrt{D}$ (no matter $D>0$ or $D<0$)

$$\overline{zw} = \bar{z}\cdot\bar{w}.$$

↑This is the benefit of working algebraically over working with $\mathbb{C}$.

Norm map: $N : \mathbb{Q}(\sqrt{D}) \longrightarrow \mathbb{Q}$

$$N(x+y\sqrt{D}) := (x+y\sqrt{D})(x-y\sqrt{D}) = x^2 - Dy^2$$

Exercise: ① if $x+y\sqrt{D} \in \mathcal{O} \Rightarrow N(x+y\sqrt{D}) \in \mathbb{Z}$

② N is multiplicative, $N(ab) = N(a)\cdot N(b)$.

③ $N(a) = a\cdot\bar{a}$

Lemma For an element $u \in \mathcal{O}$, $u \in \mathcal{O}^\times \Leftrightarrow N(u) = \pm 1$

Proof: "$\Leftarrow$" $N(u) = u\bar{u} = \pm 1$ so $u \in \mathcal{O}^\times$

"$\Rightarrow$" Say $uv = 1$ for some $v \in \mathcal{O}$, then $N(u)N(v) = N(uv) = 1$

$\Rightarrow N(u) = \pm 1$. □

Pell's equation When $D \equiv 2,3 \pmod 4$,

$$x \pm y\sqrt{D} \in \mathcal{O}^\times \Leftrightarrow N(x \pm y\sqrt{D}) = \pm 1 \Longleftrightarrow x^2 - Dy^2 = \pm 1$$

So, solutions of Pell's equation form the group $\mathcal{O}^\times$.

Fact: $D > 0 \Rightarrow \mathcal{O}^\times = \pm(x_0 + Dy_0)^{\mathbb{Z}}$ for a "fundamental" element $x_0 + Dy_0 \in \mathcal{O}^\times$

$D < 0 \Rightarrow \mathcal{O}^\times = \{\pm 1\}$ unless $D = -1$ $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

$D = -3$, $\mathbb{Z}[\zeta_3]^\times = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$