

Lecture 4

Sunzi Suanjing Theorem.
(Chinese Remainder Thm) 3rd-5th Century CE.

Let $n_1, \dots, n_k \in \mathbb{Z}$ be pairwise coprime
then the system of congruences:

$$x \equiv a_1 \pmod{n_1}$$

$$\vdots$$

$$x \equiv a_k \pmod{n_k}$$

has a unique solution modulo $N = n_1 \cdot n_k$

$$\mathbb{Z}/(N) \longrightarrow \mathbb{Z}/(n_1) \times \dots \times \mathbb{Z}/(n_k)$$

is a ring isomorphism.

In general, given $R_1, \dots, R_K$ rings

$$\prod_{i=1}^K R_i = R_1 \times \dots \times R_K \\ = \{ (a_1, \dots, a_K) \mid a_i \in R_i \}$$

is the product ring.

addition + multiplication are componentwise

Given ideals $I_1, \dots, I_K$ consider

$$\phi : R \longrightarrow R/I_1 \times \dots \times R/I_K$$

$$r \longmapsto (\phi_1(r), \dots, \phi_K(r))$$

$\phi_i : R \rightarrow R/I_i$ is the quotient

Generalised Sunzi's Theorem.

Assume $I_1, \dots, I_k$ are pairwise coprime $(I_i + I_j = (1) \forall i, j)$

then $\phi: R \rightarrow \prod R/I_i$ is surjective and kernel is

$$I_1 \cdot I_2 \cdot \dots \cdot I_k = I_1 \cap \dots \cap I_k.$$

$$\text{so } R/I_1 \cdot \dots \cdot I_k \cong \prod_{i=1}^k R/I_i.$$

Proof. $k=2$: we know ϕ_1, ϕ_2 are surjective.

show $(1, 0)$ and $(0, 1)$ are in the image:

$$I_1 + I_2 = (1) \Rightarrow a_1 + a_2 = 1 \quad a_i \in I_i$$

$$\begin{aligned}
 \phi(a_1) &= (a_1 + \mathbb{I}_1, a_1 + \mathbb{I}_2) \\
 &= (0, a_1 + a_2 + \mathbb{I}_2) \\
 &= (0, 1 + \mathbb{I}_2).
 \end{aligned}$$

similarly $\phi(a_2) = (1 + \mathbb{I}_2, 0)$.

These two elts are enough to generate the ring. For any $b_1, b_2 \in R$.

$$\begin{aligned}
 \phi(b_1 a_2 + a_1 b_2) &= \phi(b_1 a_2) + \phi(a_1 b_2) \\
 &= \phi(b_1) \phi(a_2) + \phi(a_1) \phi(b_2) \\
 &= (b_1 + \mathbb{I}_1, b_1 + \mathbb{I}_2) \cdot (1 + \mathbb{I}_2, 0) \\
 &\quad + (b_2 + \mathbb{I}_2, b_2 + \mathbb{I}_2) \cdot (0, 1 + \mathbb{I}_2).
 \end{aligned}$$

So it is surjective.

$$\begin{aligned}
 \phi(x) = 0 &\iff x \in \mathbb{I}_1 \cap \mathbb{I}_2 \\
 &= \mathbb{I}_1 \cdot \mathbb{I}_2
 \end{aligned}$$

From $K=2$ to arbitrary K induction

Find $x \in R$ s.t.

$\phi(x) = (1, \dots, 0)$ by taking

$$I_1 + I_i = (1) \Rightarrow$$

$$a_i + b_i = 1 \quad a_i \in I_1$$

$$b_i \in I_i$$

$$x = \pi(1 - a_i)$$

$$\Rightarrow x \in 1 + I_1 \quad \text{and}$$

$$x = \pi b_i \in I_i \quad \forall i \neq 1.$$

Do the same to find $\phi(x_j) = (0, \dots, \underset{\substack{\uparrow \\ j}}{1}, \dots, 0)$
and combine previous ideas $\square$.

Ideal quotients

Def I, J ideals of R the ideal quotient is

$$(I : J) = \{ x \in R \mid xJ \subseteq I \}.$$

Examples 1) $(R : J) = (1)$, in fact

$$(I : J) = (1) \text{ whenever } J \subseteq I$$

$$(J : J) = (1)$$

$$2) (I : (b)) = \{ x \mid xb \in I \}.$$

Def The Annihilator of an ideal

$$\text{is } \text{Ann}(I) := (0 : I)$$

$$= \{ x \in R \mid xa = 0 \ \forall a \in I \}$$

$$\text{Ann}(a) := \text{Ann}((a)).$$

$$= \{ x \in A \mid xa = 0 \}.$$

Examples $\text{Ann}(R) = 0 \quad \text{Ann}(0) = R.$

$$R = \mathbb{Z}/(p_1 p_2) \quad \text{Ann}(p_1) = (p_2).$$

p_i primes

$$0 \neq a \in R \text{ zero divisor} \iff \text{Ann}(a) \neq 0$$

Also $D = \bigcup_{x \neq 0} \text{Ann}(x)$ is the set

of zero divisors

Nilradical + Radicals.

$$N = \{ a \mid a^n = 0 \} \subseteq R$$

$\nwarrow$ nilpotent

is the nilradical ideal of R

Moreover R/N has no $\neq 0$ nilpotents

N ideal: $\therefore$ if $a \in N$ then $xa \in N$

$\forall x \in R$. Show $(N, +)$ group.

$0 \in N$, if $a, b \in N$ $a^n = 0 = b^m$
for some n, m

$$(a+b)^k = \sum \binom{k}{i} a^{k-i} b^i$$

if $k-i < n$, then $m < i$ so $b^i = 0$.

otherwise $a^{k-i} = 0 \Rightarrow$ closed under $+$.

$$(-a)^k = (-1)^k a^k \Rightarrow -a \in N. \quad \square$$

$$N = \bigcap_{I \text{ prime}} I$$

Suppose $a^n = 0$ $0 \in I \forall I \text{ ideals}$
 If I is prime $a(a^{n-1}) \in I \Rightarrow$
 a or $a^{n-1} \in I$ continue by reducing
 exponent $\Rightarrow$

$$N \subseteq \bigcap_{I \text{ prime}} I$$

If $a^n \neq 0$ for some n , consider the
set of ideals $\Sigma = \{I \mid a^n \notin I \text{ for all } n > 0\}$

$0 \in \Sigma \neq \emptyset$ apply Zorn's lemma again

(check chain condition). $\Rightarrow \Sigma$ has a max
 element $\overline{I}$

Claim $\mathcal{J}$ is prime take $x, y \in R$

Suppose $x, y \notin \mathcal{J}$. show $xy \notin \mathcal{J}$

$\mathcal{J} + (x)$ and $\mathcal{J} + (y) \not\supseteq \mathcal{J}$ so

$\mathcal{J} + (x), \mathcal{J} + (y) \not\subseteq \Sigma. \Rightarrow$

$a^n \in \mathcal{J} + (x), a^m \in \mathcal{J} + (y) \exists n, m$

$$\begin{aligned} \Rightarrow a^{n+m} &\in ((x) + \mathcal{J})((y) + \mathcal{J}) \\ &= (xy) + \mathcal{J}. \Rightarrow \end{aligned}$$

$(xy) + \mathcal{J} \not\subseteq \Sigma \Rightarrow xy \notin \mathcal{J}.$

$\Rightarrow \mathcal{J}$ is prime, $\Rightarrow \exists$ a prime ideal $\mathcal{J}$ s.t. $a \notin \mathcal{J}$. $\square$.

Examples $\mathbb{Z}/(p^k) = R$.

$\mathcal{N} = (p + p^k) =$ unique prime ideal of $\mathbb{Z}/(p^k)$.

$$K[x]/(x^k) = (x + (x^k))$$

Def The radical of an ideal I is
 $\sqrt{I} = \{ x \mid x^n \in I \text{ for some } n \}$.
($r(a)$ in [AM]) $\subseteq I$.

Example: $\sqrt{(0)} = \mathcal{N}$ Nilradical of R .

Proposition. $\sqrt{I}$ is an ideal moreover

$$\sqrt{I} = \bigcap_{\substack{P \text{ prime} \\ I \subseteq P}} P.$$

P prime
 $I \subseteq P$.

Proof Consider $\phi: R \rightarrow R/I$.

$$\sqrt{R/I} = \sqrt{I/I} \quad \text{and}$$

$$\phi^{-1}(\sqrt{I/I}) = \sqrt{I}.$$

$$\left(x \in \sqrt{I} \iff x^n \in I \iff \right.$$

$$\phi(x)^n = \phi(x^n) = 0$$

This proves that $\sqrt{I}$ is an ideal.

Recall we have a correspondence:

$$\left\{ \begin{array}{c} \text{ideals containing} \\ I \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{ideals in} \\ R/I \end{array} \right\}.$$

$\phi^{-1}(P)$ is prime for P prime.

For quotient map $\phi(P)R/I$ is also prime for $P \subseteq R$ prime.

 This is not true in general.

Lemma

If $f: R \rightarrow S$ is surjective and $\mathcal{P} \subseteq R$ prime ideal such that $\text{Ker } f \subseteq \mathcal{P}$ then $f(\mathcal{P})$ is prime in S .

Proof We know $f(\mathcal{P})$ is an ideal
Suppose $s_1, s_2 \in f(\mathcal{P})$
 $\parallel$
 $f(r_1) f(r_2) \in f(\mathcal{P})$ by surjectivity

$$\Rightarrow f(r_1 r_2) \in f(\mathcal{P})$$

$$\Rightarrow r_1 r_2 + K \in \mathcal{P} \quad \text{for some } K \in \text{Ker } f \subseteq \mathcal{P}$$

$$\Rightarrow r_1 r_2 \in \mathcal{P} \Rightarrow r_1 \text{ or } r_2 \in \mathcal{P}$$

Since $\mathcal{P}$ is prime. Hence $f(\mathcal{P})$ is prime □

Errata + Notation

$f: R \rightarrow S$ a homomorphism

recall I ideal of R

$f(I)$ is not necessarily an ideal of S .

(True $\nleftrightarrow f$ is surjective)

The pushout/extension of I under f is ideal generated by $f(I)$. Denoted $f(I) \cdot S$ or I^e

BOTH NOTATIONS ARE LACKING ^{oo}

one suggests multiplication by S .
the other doesn't involve f !

The contraction/pullback is
simply $f^{-1}(J)$ J ideal of S .