Lecture 17: Chinese Remainder Thm, prime and maximal ideals

TODAY: Fix a commutative ring R.

Recall $I \subset R$ is an ideal if
- I is a subgroup of $(R, +, 0)$
- $R \cdot I \cdot R \subset I$

$\mathfrak{a}, \mathfrak{b} \in \mathcal{J}(R) = \{\text{ideals of } R\}$

$$\Rightarrow \begin{cases} \mathfrak{a} + \mathfrak{b} = (a+b : a \in \mathfrak{a}, b \in \mathfrak{b}) \in \mathcal{J}(R) \\ \mathfrak{a} \cdot \mathfrak{b} = \{\sum_{i=1}^{N} a_i b_i \quad a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, N \in \mathbb{Z}_{\geq 1}\} \in \mathcal{J}(R) \end{cases}$$

Analogies: $\mathbb{N}$ vs $\mathcal{J}(R)$

Divisibility $\longleftrightarrow$ Inclusion (for $\mathbb{Z}$: $n \mid m \Leftrightarrow (m) \subseteq (n)$)

Greatest common divisor $\longleftrightarrow$ Sum ($(n) + (m) = (\gcd(n, m))$)

Least common multiple $\longleftrightarrow$ Intersection ($(n) \cap (m) = (\operatorname{lcm}(n, m))$)

Multiplication $\longleftrightarrow$ Product ($(n) \cdot (m) = (nm)$)

Chinese Remainder Theorem

Def. We say two ideals $\mathfrak{a}, \mathfrak{b} \subset R$ are *coprime* if $\mathfrak{a} + \mathfrak{b} = R$.

- Similarly, we write $\boxed{r_1 \equiv r_2 \pmod{\mathfrak{a}}}$ if $r_1 - r_2 \in \mathfrak{a}$, that is $\pi : R \longrightarrow R/\mathfrak{a}$ gives $\pi(r_1) = \pi(r_2)$.

Chinese Remainder Theorem (Sun Tzu)

Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals of R, pairwise coprime ($\mathfrak{a}_i + \mathfrak{a}_j = R \ \forall i \neq j$).
Then, for any $x_1, \ldots, x_n \in R$, $\exists \, x \in R$ such that

$$x \equiv x_i \pmod{\mathfrak{a}_i} \quad \text{for } 1 \leq i \leq n.$$

Proof sketch: Find $y_1, \ldots, y_n \in R$ such that

$$y_i \equiv 1 \mod \mathfrak{a}_i \quad \& \quad y_i \equiv 0 \mod \mathfrak{a}_j \quad \forall j \neq i$$

If we succeed, we set $\boxed{x = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n}$

$\boxed{\text{Need } y_1, \dots, y_n \in R \text{ with } y_i \equiv 1 \bmod \mathfrak{a}_i \ \& \ y_i \equiv 0 \bmod \mathfrak{a}_j \ \forall j \neq i}$

We will need the following fact (easy to verify):

<u>Claim 1</u>: $\mathfrak{b}_1, \dots, \mathfrak{b}_r \subset R$ ideals $\Longrightarrow \prod_{i=1}^{r} \mathfrak{b}_i \subset \bigcap_{i=1}^{r} \mathfrak{b}_i$.

<u>Case $n=2$</u>: $R = \mathfrak{a}_1 + \mathfrak{a}_2 \Longrightarrow 1 = a_1 + a_2$ for some $a_i \in \mathfrak{a}_i$

Take $y_1 = a_2$ & $y_2 = a_1$.

[<u>Check</u> $y_1 = a_2 \in \mathfrak{a}_2 \Longrightarrow y_1 \equiv 0 \bmod \mathfrak{a}_2$ ✓

$y_1 = 1 - a_1 \Longrightarrow 1 - y_1 \in \mathfrak{a}_1$, ie $y_1 \equiv 1 \bmod \mathfrak{a}_1$ ✓]

<u>General case</u>: Since $R = \mathfrak{a}_1 + \mathfrak{a}_j$, $2 \leq j \leq n$, then

$1 = a_1^{(j)} + a_j$ for $a_1^{(j)} \in \mathfrak{a}_1$ & $a_j \in \mathfrak{a}_j$. We build y_1 from this

$$\Longrightarrow 1 = \prod_{j=2}^{n} 1 = \prod_{j=2}^{n} \left(a_1^{(j)} + a_j\right)$$

$$= \underbrace{\prod_{j=2}^{n} a_j}_{\in \prod_{j=2}^{n} \mathfrak{a}_j} + \underbrace{\sum_{j=2}^{n} \underbrace{a_1^{(j)}}_{\in \mathfrak{a}_1} \underbrace{\prod_{k \neq j} \left(a_1^{(k)} + a_k\right)}_{\in R}}_{\in \mathfrak{a}_1}$$

So $\mathfrak{a}_1$ & $\mathfrak{b} = \prod_{j=2}^{n} \mathfrak{a}_j$ are coprime

By the $n=2$ case, we can find $y_1 \in R$ s.t.

$y_1 \equiv 1 \bmod \mathfrak{a}_1$

$y_1 \in \prod_{j=2}^{n} \mathfrak{a}_j \subset \bigcap_{j=2}^{n} \mathfrak{a}_j \Rightarrow y_1 \equiv 0 \bmod \mathfrak{a}_j \ \forall j \neq 2.$

Corollary 1: $\dfrac{R}{\bigcap_{i=1}^{n} \mathfrak{a}_i} \xrightarrow{\sim} \prod_{i=1}^{n} R/\mathfrak{a}_i$ if $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are pairwise coprime ideals of R (commutative)

Pf/ Let $R \xrightarrow{f} R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n$. for $\pi_i : R \to R/\mathfrak{a}_i$

$x \longmapsto (\pi_1(x), \ldots, \pi_n(x))$

- f is a ring homomorphism.
- f is surjective by CRT ($x_1, \ldots, x_n$ with given $\pi_1(x_1), \ldots, \pi_n(x_n)$)
- $\operatorname{Ker} f = \bigcap_{i=1}^{n} \mathfrak{a}_i$

So by the 1st Iso Theorem, we are done. $\square$

Prime & Maximal ideals

R commutative ring

<u>Def</u>: A proper ideal $\mathfrak{p} \subsetneq R$ is a <u>prime ideal</u> if $\forall a, b \in R$:

$$ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}.$$

<u>Def</u>: A proper ideal $\mathfrak{m} \subsetneq R$ is a <u>maximal ideal</u> if

$$\mathfrak{m} \subsetneq \mathfrak{a} \subseteq R, \ \mathfrak{a} \text{ ideal} \implies \mathfrak{a} = R$$

<u>Proposition 1</u>: Maximal ideals exist.

Pf/ Zorn's Lemma. Set $\mathcal{I} = \{\text{proper ideals of } R\}$

- $\mathcal{I} \neq \emptyset$ $\quad ((0) \in \mathcal{I})$
- Order $\mathcal{I}$ by inclusion
- Every chain is bounded:

$$(\mathfrak{a}_i)_j \quad \mathfrak{a}_i < \mathfrak{a}_j \ \ i<j \implies \mathfrak{a} := \bigcup_{i \in I} \mathfrak{a}_i \ \in \mathcal{I}$$

Corollary 2: Let $\mathfrak{a} \subsetneq R$ be a proper ideal. Then, there exists a maximal ideal $\mathfrak{M}$ of R containing $\mathfrak{a}$.

Proof Use the Proposition 1 for $R' = R/\mathfrak{a}$ & check that maximal ideals of R' correspond to maximal ideals of R containing $\mathfrak{a}$. This is true by the 2^{nd} Isomorphism Theorem.

. Next we characterize prime ideals:

Proposition 2: $\mathfrak{p} \subsetneq R$ ideal is prime $\iff$ $R/\mathfrak{p}$ is an integral domain

Proof: $\mathfrak{p}$ is prime $\iff$ $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

$\iff$ $\pi(a)\,\pi(b) = 0$ in $R/\mathfrak{p}$ implies $\pi(a) = 0$ or $\pi(b) = 0$

(Here $\pi : R \longrightarrow R/\mathfrak{p}$).

$\iff$ $R/\mathfrak{p}$ is an integral domain. $\square$

Lemma: A commutative ring R is a field if & only if $\mathcal{I}(R) = \{0\}, R\}$

Pf/ $(\Rightarrow)$ $I \in \mathcal{I}(R)$ $\quad I \neq (0)$, Pick $x \in I \setminus \{0\}$ then $\exists y$ st $xy = 1$
$\Rightarrow I = R$.

$(\Leftarrow)$ Pick $x \in R \setminus \{0\}$ & consider $I = (x)$ ideal. Then $I = R \ni 1$, meaning $\exists y \in R$ with $1 = yx$ so $x \in R^*$. $\square$

Proposition 3: $\mathfrak{m} \subsetneq R$ ideal is maximal $\Longleftrightarrow$ $R/\mathfrak{m}$ is a field

Pf/ $R/\mathfrak{m}$ is a field $\underset{\text{Lemma}}{\Longleftrightarrow}$ (0) & $R/\mathfrak{m}$ are the only ideals in $R/\mathfrak{m}$

But $\{$ ideals in $R/\mathfrak{a}$ $\}$ $\xleftrightarrow{\text{1-to-1}}$ $\{$ ideals in R containing $\mathfrak{a}$ $\}$

So: $R/\mathfrak{m}$ is a field $\Longleftrightarrow$ the only ideals of R containing $\mathfrak{m}$ are $\mathfrak{m}$ & R
$\Longleftrightarrow$ $\mathfrak{m} \subsetneq R$ is a maximal ideal. $\square$

Corollary 3: Every maximal ideal is prime.

Pf/ Fields are integral domains.

Examples: $R = \mathbb{Z}$ $\{(0), (p) : p \in \mathbb{Z}_{\geq 2} \text{ prime}\}$ are all the prime ideals.

- (0) is prime but **not** maximal
- (p) is maximal for every $p \geq 2$ prime.

Proposition 4: Let $f : A \longrightarrow B$ be a ring hom, with A, B commutative rings. Let $q \subsetneq B$ be a prime ideal. Then $\mathfrak{p} = f^{-1}(q) \subsetneq A$ is a prime ideal.

Proof: We know that $f^{-1}(q)$ is an ideal of A (Lecture 15).

Given $a, b \in A$ with $ab \in \mathfrak{p}$, we want to show $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

But $f(ab) = f(a) f(b) \in q \underset{q \text{ prime}}{\Longrightarrow} f(a) \in q$ or $f(b) \in q$.

Hence, $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

⚠ The statement fails for maximal ideals!

Ex: $\mathbb{Z} \overset{f}{\hookrightarrow} \mathbb{Q}$, $q = (0)$ is the only maximal ideal but $f^{-1}(0) = (0)$ is not maximal in $\mathbb{Z}$.

Prime Avoidance

R commutative ring

Theorem: Fix $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ prime ideals of R & let $\mathfrak{a} \subset R$ be an ideal with $\mathfrak{a} \subset \bigcup_{i=1}^{n} \mathfrak{p}_i$. Then, there exists j with $\mathfrak{a} \subset \mathfrak{p}_j$.

Proof We'll prove "$\mathfrak{a} \not\subset \mathfrak{p}_j \ \forall j \Rightarrow \mathfrak{a} \not\subset \bigcup_{i=1}^{n} \mathfrak{p}_i$." (prime avoidance)

Induct on n

- Base case $n=1$ is clear
- Inductive Step: By IH: for $i \in \{1, \dots, n\}$ we have:

$$\mathfrak{a} \not\subset \mathfrak{p}_j \text{ for } j \in \{1, \dots, n\} \setminus \{i\} \Rightarrow \mathfrak{a} \not\subset \bigcup_{j \neq i} \mathfrak{p}_j.$$

$\Rightarrow \exists\, a_i \in \mathfrak{a}_i \setminus \bigcup_{j \neq i} \mathfrak{p}_j$

- If $a_i \notin \mathfrak{p}_i$ for some i, we are done
- Otherwise: set $\boxed{a = \sum_{\ell=1}^{n} a_1 \cdots a_{\ell-1} a_{\ell+1} \cdots a_n \in \mathfrak{a}}$

All summands except $a_1 \cdots a_{i-1} a_{i+1} \cdots a_n \in \mathfrak{p}_i$. Since $a_1 \cdots a_{i-1} a_{i+1} \cdots a_n \notin \mathfrak{p}_i$ (because $a_j \notin \mathfrak{p}_i \ \forall j \neq i$), we conclude $a \notin \mathfrak{p}_i \ \forall i \Rightarrow a \in \mathfrak{a} \setminus \bigcup_i \mathfrak{p}_i$ $\square$

Theorem 2: Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals of R (commutative) and $\mathfrak{p} \subsetneq R$ be a prime ideal.

If $\bigcap_{j=1}^{n} \mathfrak{a}_j \subseteq \mathfrak{p}$ $(=)$, then there exists $l = 1, \ldots, n$ with $\mathfrak{a}_l \subseteq \mathfrak{p}$ $(=)$.

Proof: We will show: $\mathfrak{a}_l \not\subseteq \mathfrak{p}$ $\forall l \Rightarrow \bigcap_{l=1}^{n} \mathfrak{a}_l \not\subseteq \mathfrak{p}$

By hypothesis, we have $a_l \in \mathfrak{a}_l \setminus \mathfrak{p}$ $\forall l$.

Take $\boxed{a = a_1 \cdots a_n}$.

- $a \in \mathfrak{a}_l$ $\forall l$
- $a \notin \mathfrak{p}$ ($\mathfrak{p}$ is prime)

$\Big\} \Rightarrow \bigcap_{l=1}^{n} \mathfrak{a}_l \not\subseteq \mathfrak{p}$.

To prove the statement for the equalities, we argue as follows:

If $\bigcap_{j=1}^{n} \mathfrak{a}_j = \mathfrak{p}$, we know $\mathfrak{a}_l \subseteq \mathfrak{p}$ for some l.

Conversely, $\mathfrak{p} = \bigcap_{j=1}^{n} \mathfrak{a}_j \subseteq \mathfrak{a}_l$, so $\mathfrak{p} = \mathfrak{a}_l$. $\square$