Lecture 17: Chinese Remainder Thm, prime and maximal ideals

§1. Ideals in a commutative ring:

Fix a commutative ring R. $I \subset R$ is an ideal if it is a subgroup of $(R, +, 0)$ & $R\, I\, R \subset I$

$\mathfrak{a}, \mathfrak{b} \in \mathcal{I}(R)$ (ideals of R)

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

The arithmetic of natural numbers has its analogue in the set of ideals of R.

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

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 $((n)\cdot(m) = (nm))$

With this dictionary in mind,

<u>Def</u>: We say two ideals $\mathfrak{a}, \mathfrak{b} \subset R$ are <u>coprime</u> 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 $\pi(r_1) = \pi(r_2)$.

<u>Chinese Remainder Theorem</u> (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: We will need the following fact (easy to verify):

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

Next, we sketch the proof of CRT:

Main idea: Find $y_1, \ldots, y_n \in R$ such that for all $i = 1, \ldots, n$

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

If we succeed, we set $\boxed{x = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n}$ & conclude $x \equiv x_i \mod \mathfrak{a}_i$ for each i. (arithmetic in $R/\mathfrak{a}_i$)

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

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

[**Check** $y_1 = a_2 \in \mathfrak{a}_2 \Rightarrow y_1 \equiv 0 \mod \mathfrak{a}_2$ ✓

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

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

$1 = a_1^{(j)} + a_j$ for $a_1^{(j)} \in \mathfrak{a}_1$ & $a_j \in \mathfrak{a}_j$

$$\Longrightarrow 1 = \prod_{j=2}^{n} 1 = \prod_{j=2}^{n} (a_1^{(j)} + a_j) = \underbrace{\prod_{j=2}^{n} a_j}_{\in \prod_{j=2}^{n} \mathfrak{a}_j} + \underbrace{\sum_{j=2}^{n} \underbrace{a_1^{(j)}}_{\in \mathfrak{a}_1} \underbrace{\prod_{k \neq j} (a_1^{(k)} + a_k)}_{\in R}}_{\in \mathfrak{a}_1}$$

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

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

$$y_1 \equiv 1 \mod \mathfrak{a}_1 \quad \& \quad y_1 \in \prod_{j=2}^{n} \mathfrak{a}_j \subset \bigcap_{j=2}^{n} \mathfrak{a}_j .$$

That is $y_1 \equiv 1 \mod \mathfrak{a}_1$ & $y_1 \equiv 0 \mod \mathfrak{a}_j \quad \forall j = 2, \ldots n$.

Repeating this argument for each $\mathfrak{a}_i$, we get $y_i \equiv \begin{cases} 1 \mod \mathfrak{a}_i \\ 0 \mod \mathfrak{a}_j \text{ for } j \neq i \end{cases}$

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

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

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

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

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

§2 Prime and Maximal ideals:

Assume R is a commutative ring.

Def: A proper ideal $\mathfrak{p} \subsetneq R$ is a prime ideal if for every a, b in R, we have:

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

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

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

Proposition 1: Maximal ideals exist.

Proof: Write $\mathcal{J}$ = set of all proper ideals of R.

- $\mathcal{J} \neq \emptyset$ since $(0) \in \mathcal{J}$.
- $\mathcal{J}$ is partially ordered by inclusion

Consider a chain (= a totally ordered subset of $\mathcal{J}$)

$(\mathfrak{a}_i)_{i\in I}$ where $\mathfrak{a}_i \subseteq \mathfrak{a}_j$ if $i \leq j$.

Define $\mathfrak{a} = \bigcup_{i\in I} \mathfrak{a}_i \; .= \sup_{i\in I}(\mathfrak{a}_i)$

<u>Claim</u>: $\mathfrak{a} \in \mathcal{J}$.

Pf/. $a, b \in \mathfrak{a}$, then $\exists\, l$ st $a, b \in \mathfrak{a}_l$ ($a\in\mathfrak{a}_i\subset\mathfrak{a}_l$, $b\in\mathfrak{a}_j\subset\mathfrak{a}_l$, $l=\max\{i,j\}$)

$\Rightarrow a \pm b \in \mathfrak{a}_l \subset \mathfrak{a}$.

- $0 \in \mathfrak{a}$
- $a \in \mathfrak{a}$, $r \in R \Rightarrow \exists\, l$ st $a \in \mathfrak{a}_l \Rightarrow ra \in \mathfrak{a}_l \subset \mathfrak{a}$.

. So $\mathfrak{a}$ is an ideal

. $\mathfrak{a}$ is proper since $1 \notin \mathfrak{a}_i \; \forall i$ so $1 \notin \bigcup_{i\in I} \mathfrak{a}_i$.

<u>In conclusion</u>: every chain in $\mathcal{J}$ has a supremum in $\mathcal{J}$.

By Zorn's Lemma, there are maximal elements in $\mathcal{J}$

<u>Corollary 2</u>: Let $\mathfrak{a} \subsetneq R$ be a proper ideal. Then, there exists a maximal ideal $\mathfrak{m}$ of R containing $\mathfrak{a}$.

<u>Proof</u> 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:

<u>Proposition 2</u>: $\mathfrak{p} \subsetneq R$ ideal is prime $\Leftrightarrow$ $R/\mathfrak{p}$ is an integral domain

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

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

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

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

Lemma: A commutative ring R is a field if & only if (0) & R are the only ideals in R

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

($\Leftarrow$) 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 $\Leftrightarrow$ $R/\mathfrak{m}$ is a field

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

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

We conclude:

$R/\mathfrak{m}$ is a field $\Leftrightarrow$ the only ideals of R containing $\mathfrak{m}$ are $\mathfrak{m}$ and R $\Leftrightarrow$ $\mathfrak{m} \subsetneq R$ is a maximal ideal. $\square$

Corollary 3: Every maximal ideal is prime.

Pf/ Fields are integral domains.

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

- (0) is prime but <u>not</u> maximal
- (p) is maximal for every $p \geq 2$ prime.

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

⚠ The statement fails for maximal ideals!

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

<u>Proof</u>: 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 $b \in \mathfrak{p}$.

§3 Prime avoidance:

Fix R commutative ring

<u>**Theorem**</u>: Fix $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ 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 some $j = 1, \ldots, n$ with $\mathfrak{a} \subset \mathfrak{p}_j$.

<u>Proof</u> We will prove the contrapositive:

$$\mathfrak{a} \not\subset \mathfrak{p}_j \;\; \forall j = 1, \ldots, n \Longrightarrow \mathfrak{a} \not\subset \bigcup_{i=1}^{n} \mathfrak{p}_i. \qquad \text{(prime avoidance)}$$

We argue by induction on n

- The assertion is true for $n=1$.
- Assume $n>1$ & that the assertion has been verified for $n-1$.

Thus for $i \in \{1, \dots, n\}$ we have:

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

That is, we can find $a_i \in \mathfrak{a}$ with $a_i \notin \mathfrak{p}_j \quad \forall j \neq i$.

- Now, if $a_i \notin \mathfrak{p}_i$ for some i, we are done since $\underset{\mathfrak{a}}{a_i} \notin \bigcup_{j=1}^{n} \mathfrak{p}_j$.
- On the contrary, if $a_i \in \mathfrak{p}_i \quad \forall i=1, \dots n$, we consider the element $\boxed{a = \sum_{l=1}^{n} a_1 \cdots a_{l-1} a_{l+1} \cdots a_n \in \mathfrak{a}}$

For each $i=1, \dots, n$ every summand of $\mathfrak{a}$, except $a_1 \cdots a_{i-1} a_{i+1} \cdots a_n$ lies in $\mathfrak{p}_i$ (as $a_i \in \mathfrak{p}_i$)

Since $a_1 \cdots a_{i-1} a_{i+1} \cdots a_n \notin \mathfrak{p}_i$ as none of its factors are in $\mathfrak{p}_i$, then we conclude $a \notin \mathfrak{p}_i \quad \forall i=1 \dots n$. which is a contradiction.

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

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

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

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

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

$$\left.\begin{array}{l} \cdot\ a \in \mathfrak{a}_l \quad \forall l \\ \cdot\ a \notin \mathfrak{p} \quad (\mathfrak{p} \text{ is prime}) \end{array}\right\} \Rightarrow \bigcap_{l=1}^{n} \mathfrak{a}_l \not\subseteq \mathfrak{p}.$$

To prove the statement for the equations, we argue as follows

If $\bigcap_{j=1}^{n} \mathfrak{A}_j = \mathfrak{P}$, we know $\mathfrak{A}_\ell \subseteq \mathfrak{P}$ for some ℓ.

Conversely, $\mathfrak{P} = \bigcap_{j=1}^{n} \mathfrak{A}_j \subseteq \mathfrak{A}_\ell$, so $\mathfrak{P} = \mathfrak{A}_\ell$. $\square$