Lecture 19: 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 $(R,+,0)$ & $RIR \subset I$

$\mathfrak{a}, \mathfrak{b} \in \mathcal{I}(R)$ (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 $\mathbb{Z}$: $n \mid m \iff (m) \subseteq (n)$)

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,

Def: 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: $\mathfrak{b}_1, \dots, \mathfrak{b}_r \subset R$ ideals $\Rightarrow \prod_{i=1}^{r} \mathfrak{b}_i \subset \bigcap_{i=1}^{r} \mathfrak{b}_i$.

Next, we sketch the proof of CRT:

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

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

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

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

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

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

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

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

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

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

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

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 1st 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:

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

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

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

Proposition 1: Maximal ideals exist.

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

- $\mathcal{I} \neq \emptyset$ since $(0) \in \mathcal{I}$.
- $\mathcal{I}$ 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 $\mathfrak{a} = \bigcup_{i\in I} \mathfrak{a}_i \mathrel{.=} \sup_{i\in I}(\mathfrak{a}_i)$

Claim: $\mathfrak{a} \in \mathcal{J}$.

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 $1 \notin \bigcup_{i\in I} \mathfrak{a}_i$.

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

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

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 2nd Isomorphism Theorem.