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 $(R, +, 0)$
- $R \cdot I \cdot R \subset I$

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

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

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

Divisibility $\longleftrightarrow$

Greatest common divisor $\longleftrightarrow$

Least common multiple $\longleftrightarrow$

Multiplication $\longleftrightarrow$

Chinese Remainder Theorem

<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

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

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

Corollary 1: $$\frac{R}{\bigcap_{i=1}^{n} \mathfrak{a}_i} \xrightarrow{\sim} \prod_{i=1}^{n} R/\mathfrak{a}_i$$

if $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are pairwise coprime ideals of R (commutative)

Prime & Maximal ideals

R commutative ring

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

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

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.

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

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

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

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

Corollary 3: Every maximal ideal is prime.

Examples: $R = \mathbb{Z}$

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

⚠ The statement fails for maximal ideals!

Prime Avoidance

R commutative ring

Theorem: 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 j with $\mathfrak{a} \subset \mathfrak{p}_j$.

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 $\mathfrak{a}_l \subseteq \mathfrak{p}$.

$(=)$ $(=)$