Lecture 20: Prime ideals, prime avoidance, local rings

Last Time: CRT & existence of maximal ideals in a commutative ring R

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

Proof: Maximal ideals in $R' = R/\mathfrak{a}$ $\longleftrightarrow$ maximal ideals $\mathfrak{m}$ of R containing $\mathfrak{a}$.

§1 Prime ideals: R = commutative ring

Def $\mathfrak{p} \subset R$ ideal is prime if $a\cdot b \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Obs: We still don't know we have prime ideals!

- An equivalent characterization is:

Proposition: $\mathfrak{p} \subsetneq R$ 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. (no zero-divisors) $\square$

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

Pf/ $\Rightarrow$) Fix $I \neq (0)$ an ideal of R. If $x \in I \smallsetminus \{0\}$ then $\exists y$ st (R is a field) $xy = 1$ so x is a unit and $1 \in I$, i.e. $I = R$.

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

Proposition 2: $\mathfrak{m} \subsetneq R$ ideal is maximal $\Leftrightarrow$ $R/\mathfrak{m}$ is a field

Pf/ $R/\mathfrak{m}$ is a field $\overset{\text{Lemma}}{\Leftrightarrow}$ (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 2: 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 3: Let $f: A \longrightarrow B$ be a ring homomorphism, where A, B are 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!

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

Proof: We know that $f^{-1}(\mathfrak{q})$ is an ideal of A (Lecture 17)

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

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

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

§2. Prime avoidance:

Fix R commutative ring

Theorem: Fix $\wp_1, \dots, \wp_n$ prime ideals of R & let $\mathfrak{a} \subset R$ be an ideal with $\mathfrak{a} \subset \bigcup_{i=1}^n \wp_i$. Then, there exists some $j = 1, \dots, n$ with $\mathfrak{a} \subset \wp_j$.

Proof We will prove the contrapositive:

$$\mathfrak{a} \not\subset \wp_j \quad \forall j = 1, \dots, n \implies \mathfrak{a} \not\subset \bigcup_{i=1}^n \wp_i. \qquad \text{(prime avoidance)}$$

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:

$$\mathfrak{a} \not\subset \wp_j \quad \text{for } j \in \{1, \dots, n\} \setminus \{i\} \implies \mathfrak{a} \not\subset \bigcup_{j \neq i} \wp_j.$$

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

We analyze 2 cases:

(1) Now, if $a_i \notin \wp_i$ for some i, we are done since $\underset{\mathfrak{a}}{a_i} \notin \bigcup_{j=1}^n \wp_j$.

(2) On the contrary, if $a_i \in \wp_i \quad \forall i = 1, \dots n$, 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 $\wp_i$ (as $a_i \in \wp_i$)

Since $a_1 \cdots a_{i-1} a_{i+1} \cdots a_n \notin \wp_i$ as none of its factors are in $\wp_i$, then we conclude $a \notin \wp_i \quad \forall i = 1, \dots n$, so $\mathfrak{a} \not\subset \bigcup_{i=1}^n \wp_i$.

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

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 can find $a_l \in \mathfrak{a}_l \setminus \mathfrak{p} \quad \forall l$.

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 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 $\mathfrak{p} = \mathfrak{a}_l$. $\square$

§3. Local rings:

Fix R to be a commutative ring

Def: R is a local ring if it has only one maximal ideal

Notation: $(R, \mathfrak{m})$ where $\mathfrak{m}$ is its unique maximal ideal.

Examples: ① Every field is a local ring ($\mathfrak{m} = (0)$)

② $R = \mathbb{K}[x]/(x^3)$ is local when $\mathbb{K}$ is any field

Mxl ideals of $R \longleftrightarrow$ mxl ideals of $\mathbb{K}[x]$ containing (x^3),

But $\mathbb{K}[x]$ is PID, so any $\mathfrak{m} \subset \mathbb{K}[x]$ maximal equals (f) for some $f \in \mathbb{K}[x]$ irreducible

But $f \mid x^3$, so $(f) = (x)$. This is maximal in $\mathbb{K}[x]$!

$\Rightarrow \tilde{\mathfrak{m}} = (x)/(x^3)$ is the unique mxl ideal of R

③ $R = \mathbb{K}[\![x]\!]$ = power series in one variable over $\mathbb{K}$.

<u>Claim</u>: R is a ring.

<u>Operations</u>: • Componentwise addition (degree-by-degree)

$$\Big(\sum_{k\geq 0} a_k x^k\Big) + \Big(\sum_{k\geq 0} b_k x^k\Big) = \sum_{k\geq 0} (a_k+b_k) x^k.$$

• Multiplication: $\Big(\sum_{k\geq 0} a_k x^k\Big)\Big(\sum_{\ell\geq 0} b_\ell x^\ell\Big) = \sum_{n\geq 0} \Big(\sum_{k=0}^{n} a_k b_{n-k}\Big) x^n.$

<u>Q</u>: Why is R local?

<u>Claim</u>: Any $f \in R$ with constant term $\neq 0$ is invertible!

So any $g \in R$ is $g = x^n u$ with $u \in R^\times$ & $n \geq 0$.

<u>Conclusion</u>: $\mathfrak{m} = (x)$ is the unique maximal ideal of R.

<u>Proof of claim</u>: Write $f = \sum_{n\geq 0} a_n x^n$ with $a_0 \neq 0$.

We build f^{-1} term-by-term. Write $g = \sum_{n\geq 0} b_n x^n$ with $fg = 1$

This gives
$$a_0 b_0 = 1 \rightsquigarrow b_0 = 1$$
$$a_1 b_0 + a_0 b_1 = 0 \rightsquigarrow b_1 = \frac{-a_1 b_0}{a_0} = -a_1$$
$$a_2 b_0 + a_1 b_1 + a_0 b_2 = 0 \rightsquigarrow b_2 = \frac{-a_2 b_0 - a_1 b_1}{a_0}$$

In general, assuming $b_0, \ldots, b_{n-1}$ have been determined, we have:
$$a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 = 0 \rightsquigarrow b_n = \frac{-a_1 b_{n-1} - \cdots - a_n b_0}{a_0}$$

We've computed b_n. $\square$

<u>Obs</u>: In our definition of $+$ & $\cdot$ on $\mathbb{K}[x]$ only <u>finitely many operations</u> in $\mathbb{K}$ were performed to get the coefficient of x^n once n is fixed.

Eg $\sum_{k=0}^{n} a_k b_{n-k}$ & $a_n + b_n$ gave the x^n-coeff of $\cdot$ & $+$.

The same idea will give us a ring structure on $\mathbb{K}(\!(x)\!)$ = ring of Laurent series $= \Big\{ \sum_{j=-N}^{\infty} a_j x^j \quad a_j \in \mathbb{K} \ \forall j \geq -N,\ N \in \mathbb{Z}_{\geq 0} \Big\}$

<u>Fun exercise</u>: This definition of $\cdot$ will not work for the abelian gp $K[\![x^{-1}, x]\!] = \left\{ \sum_{j=-\infty}^{\infty} a_j x^j : a_j \in K \ \forall j \in \mathbb{Z} \right\}$

(Because if it did: $\cdots + x^{-2} + x^{-1} + 1 + x + x^2 + \cdots = \frac{-x^{-1}}{1-x^{-1}} + \frac{1}{1-x} = 0$)

Compare coeff of x^k to get $1 = 0$!

$\square$