Lecture 18: Local rings, nilpotent elements & rings of fractions

Recall: An ideal $\mathfrak{m} \subsetneq R$ is maximal if the only ideals of R containing $\mathfrak{m}$ are $\mathfrak{m}$ & R.

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

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

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

Claim: R is a ring.

Operations: • Componentwise addition (degree-by-degree)

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

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

Q: Why is R local?

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

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

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

Proof of claim: WLOG, assume $f = \sum_{n\geq 0} a_n x^n$ with $a_0 = 1$.

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. $\square$

Obs: In our definition of $+$ & $\cdot$ on $\mathbb{K}[x]$ only finitely many operations 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 $= \{ \sum_{j=-N}^{\infty} a_j x^j \quad a_j \in \mathbb{K} \ \forall j \geq -N, \ N \in \mathbb{Z}_{\geq 0} \}$

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

(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 $1 = 0$! $\square$

- Local rings can be characterized by their group of units:

Proposition: R is local if & only if the set of all non-units of R is an ideal of R.

Pf/ ($\Rightarrow$) Set $I = R \setminus R^\times$. Assume R is local with unique maximal ideal $\mathfrak{m}$. Since $\mathfrak{m} \subsetneq R$, we have $\mathfrak{m} \subseteq I$.

Conversely if $x \in R \setminus R^\times$, then (x) is a proper ideal & we can find a maxl ideal of R containing x. Since R is local, $x \in \mathfrak{m}$. Thus $R \setminus R^\times \subseteq \mathfrak{m} \subseteq R \setminus R^\times$ gives $\mathfrak{m} = R \setminus R^\times$, so $R \setminus R^\times$ is an ideal of $\mathfrak{m}$.

($\Leftarrow$) If $\mathfrak{m} = R \setminus R^\times$ is an ideal, then $\mathfrak{m}$ is maximal

Any $x \notin \mathfrak{m}$ will be a unit so if $\mathfrak{a} \supsetneq \mathfrak{m}$ is an ideal with $x \in \mathfrak{a} \setminus \mathfrak{m}$, we conclude $\mathfrak{a} = (1) = R$.

Now, if $\mathfrak{b}$ is any proper ideal of R, then $\mathfrak{b} \subseteq R \setminus R^\times$, so $\mathfrak{b} \subseteq \mathfrak{m}$. Thus, $\mathfrak{m}$ is the unique maximal ideal of R.

<u>Example</u>: $R = \mathbb{K}[x]/(x^3) = \{ \underbrace{a_0 + a_1\bar{x} + a_2\bar{x}^2}_{=: f(x)} \quad a_0, a_1, a_2 \in \mathbb{K} \}$

<u>Claim</u>: f is a unit $\Leftrightarrow a_0 \in \mathbb{K} \setminus \{0\}$

Pf/ $(a_0 + a_1\bar{x} + a_2\bar{x}^2)(b_0 + b_1\bar{x} + b_2\bar{x}^2) = 1$

$$\Leftrightarrow \begin{cases} \boxed{a_0 b_0 = 1} \\ a_0 b_1 + a_1 b_0 = 0 \\ a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 \end{cases} \quad \text{ie} \quad \begin{array}{ll} b_0 = a_0^{-1} & (\text{so } a_0 \neq 0) \\ b_1 = -a_1 a_0^{-2} & \\ b_2 = a_0^{-1}(-a_0^{-1}a_2 + a_0^{-2}a_1^2) & \end{array}$$

<u>Conclude</u>: $R \setminus R^\times = (x)$, so it's an ideal. Proposition $\Rightarrow$ R is local.

<u>Example 2</u>: Fix $p \in \mathbb{Z}_{\geq 2}$ prime & set

$$R = \left\{ \tfrac{a}{b} \in \mathbb{Q} \;\middle|\; p \nmid b \;\&\; \gcd(a,b) = 1 \right\} \quad (\text{usual name } \mathbb{Z}_{(p)})$$

<u>Claim 1</u>: R is a ring (subring of $\mathbb{Q}$)

- $\frac{0}{1}, \frac{1}{1} \in R$ ✓
- $\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$

$p \nmid b_1,\ p \nmid b_2 \Rightarrow p \nmid b_1 b_2$

$\Rightarrow p \nmid \frac{b_1 b_2}{\gcd(c, b_1 b_2)} \qquad c = a_1 b_2 + a_2 b_1$

$\Rightarrow \frac{a_1}{b_1} + \frac{a_2}{b_2} \in R$ ✓

- $\frac{a}{b} \in R \implies \frac{-a}{b} \in R$ ✓

- $\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$ $\quad p \nmid b_1,\ p \nmid b_2 \implies p \nmid b_1 b_2$

  $\implies p \nmid \frac{b_1 b_2}{\gcd(c, b_1 b_2)}$ $\quad c = a_1 a_2$

  $\implies \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} \in R$

Moreover $R^\times = \{ \frac{a}{b} : a, b \in \mathbb{Z}_{\neq 0}\ \gcd(a,b) = 1\ p \nmid a, p \nmid b \}$

$\implies R^\times \setminus R = (p) = pR$ is an ideal. $\implies R$ is local.

§2 Nilpotent elements:

Fix any commutative ring R.

Def: An element $x \in R$ is called nilpotent if $\exists\ n \geq 1$ such that $x^n = 0$.

Let $\mathcal{N}$ = set of all nilpotent elements of R.

Lemma: $\mathcal{N}$ is an ideal of R (called nilradical)

Proof: Pick $a, b \in \mathcal{N}$. Then $\exists\ k, l \geq 1$ s.t. $a^k = b^l = 0$

$$\implies (a \pm b)^{k+l} = \sum_{j=0}^{k+l} \binom{k+l}{j} a^j b^{k+l-j} (\pm 1)^{k+l-j}$$

$$= \sum_{j=0}^{k} (\pm 1)^{k+l-j} \binom{k+l}{j} a^j \underbrace{b^{l + \overbrace{(k-j)}^{\geq 0}}}_{=0} + \sum_{j=k+1}^{k+l} \binom{k+l}{j} \underbrace{a^j}_{\substack{=0 \\ (j>k)}} (-b)^{k+l-j} = 0$$

So $a \pm b \in \mathcal{N}$

- $0 \in \mathcal{N}$
- $a \in \mathcal{N}$ $(a^k = 0)$ $\quad r \in R \implies (ra)^k = r a^k = r \cdot 0 = 0$

So $\mathcal{N}$ is an ideal. $\square$

⚠ This fails if R is noncommutative.

Eg: $E = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ & $F = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$. Then $E^2 = F^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

but $EF = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is not nilpotent $(EF)^n = EF \ \forall n \geq 1$.

So $\mathcal{N}$ is neither left nor a right ideal of $M_{2\times 2}(\mathbb{C})$.

§3. Ring of fractions:

Motivation 1: Geometric viewpoint towards commutative rings.

Commutative ring R = [type] functions on [type] space X with values in $\mathbb{C}$ or other field.

Eg: continuous — topological

polynomial — vector

⋮ ⋮

Ideals = subsets of functions which vanish on a given subset $Y \subset X$ (in the Top context, Y must be closed)

In this context, open sets will be given by non-vanishing of functions.

Eg: $GL_2(\mathbb{R}) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times 2}(\mathbb{R}) \mid \underbrace{ad - bc}_{\text{determinant}} \neq 0 \}$

open in $M_{2\times 2}(\mathbb{R})$

The non-vanishing functions will have the structure of a multiplicatively closed set.

Localization: Study the behaviour of a space near a point.

Motivation 2: Number Theory - Diophantine Equations

$P_1(x_1, \dots, x_m), \dots, P_n(x_1, \dots x_m) \in \mathbb{Z}[x_1, \dots, x_m]$

Q: Find integer solutions to $P_1 = \dots = P_n = 0$.

Approach: Look for solutions over $\mathbb{Q}$, or $\mathbb{Z}_{(p)} = \{ \frac{a}{b} \mid \underset{(a:b)=1}{p \nmid b} \}$

and "patch the local solutions" (localization of $\mathbb{Z}$ at (p))

Def: Fix a commutative ring R & $S \subset R$. We say S is a <u>multiplicatively closed set</u> if:

(i) $0 \notin S$ $\rightsquigarrow$ otherwise localization gives a set with $0=1$.

(ii) $1 \in S$

(iii) $a, b \in S \Rightarrow ab \in S$.

• Next, we define an equivalence relation on $R \times S$:

$$(a,s) \sim (b,t) \iff \exists s' \in S \text{ with } s'(at - bs) = 0$$

<u>Claim</u>: $\sim$ is an equivalence relation

Pf/ Symmetric (same s') & reflexiveness ($s'=1$) are clear.

Transitivity: $(a,s) \sim (b,t)$ & $(b,t) \sim (c,u)$

To prove: $(a,s) \sim (c,u)$

From the given relations, $\exists s', s'' \in S$ such that

$$s'(at - bs) = 0 \quad \& \quad s''(bu - ct) = 0$$

$$(1)\ s'at = s'bs \qquad (2)\ s''bu = s''ct$$

Then: $(s's''t)au \underset{(1)\cdot s''u}{=} s's''bsu = s's''sbu \overset{(2)}{=} s'ss''ct = (s's''t)(sc)$

So: $(s's''t)(au - sc) = 0$ & $s's''t \in S$ because s', s'' & t do, & S is mult closed.

Motivation $\frac{a}{b} = \frac{c}{d}$ in $\mathbb{Q} \iff ad - bc = 0$

Here, we need to allow for $ad-bc$ to be a zero division but where we can only use elements of S.

Def The ring of fractions of R relative to S, denoted by $S^{-1}R$ is the set $R \times S/\sim$ with

① Addition: $(a,s) + (b,t) = (at+bs, st)$

② Multiplication: $(a,s) \cdot (b,t) = (ab, st)$

③ Neutral elements: $0 = (0,1)$

$1 = (1,1)$

Exercise: • Verify that addition and multiplication formulae given above are well-defined (ie independent of class reps.)

• Check that $S^{-1}R$ is a ring with these operations

Standard notation $(a,s) \in S^{-1}R \longleftrightarrow$ "$\frac{a}{s}$".

Note: If $0 \in S$, then $S^{-1}R = R \times S/\sim$ is reduced to a single pt since $0(at-bs) = 0$ always. $\rightsquigarrow S^{-1}R$ would be the "zero ring" which we ignored from the beginning