Lecture 21: Local rings & ring of fractions

Recall: R commutative is a local ring if it has a unique maximal ideal.

§1 More on local rings

- 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.

Example: $R = \mathbb{K}[x]/(x^3) = \{ f_{(x)} := a_0 + a_1 \bar{x} + a_2 \bar{x}^2 \quad a_0, a_1, a_2 \in \mathbb{K} \}$

Claim: f is a unit $\iff$ $a_0 \in \mathbb{K} \setminus \{0\}$

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

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

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

Example 2: (HW7) Fix $p \in \mathbb{Z}_{\geq 2}$ prime & set

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

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

- $\frac{0}{1}, \frac{1}{1} \in R$ ✓
- $\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1b_2 + a_2b_1}{b_1b_2}$ $\quad$ $p \nmid b_1,\ p\nmid b_2 \Rightarrow p \nmid b_1 b_2$ $\Rightarrow p \nmid \frac{b_1b_2}{\gcd(c, b_1b_2)}$ $\quad c = a_1b_2 + a_2b_1$

  $\Rightarrow \frac{a_1}{b_1} + \frac{a_2}{b_2} \in R$ ✓
- $\frac{a}{b} \in R \Rightarrow \frac{-a}{b} \in R$ ✓
- $\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1a_2}{b_1b_2}$ $\quad$ $p \nmid b_1,\ p \nmid b_2 \Rightarrow p \nmid b_1 b_2$ $\Rightarrow p \nmid \frac{b_1b_2}{\gcd(c, b_1b_2)}$ $\quad c = a_1a_2$

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

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

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

§2 Ring of fractions.

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

- Equivalence relation $\sim$ on $R \times S$:

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

Def The <u>ring of fractions of R relative to S</u>, 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: $0=(0,1)$ & $1=(1,1)$

(Think of (a,s) in $R^{-1}S$ as $\frac{a}{s}$.)

<u>Special case</u>: R is an integral domain (no zero divisors)

Then $S=R\setminus\{0\}$ is a multiplicatively closed set.

Then $S^{-1}R$ is a field called the <u>field of fractions</u>

Sometimes denoted by $\mathrm{Quot}(R)$

$(a,s)\neq(0,1)$ is invertible & $(a,s)^{-1}=(s,a)$.

$(\Leftrightarrow a\neq 0)$

<u>Ex</u>: 1. $R=\mathbb{Z}$, $\mathrm{Quot}(R)=\mathbb{Q}$ $\quad (a,b)\longleftrightarrow \frac{a}{b}$

$(a,b)\sim(c,d) \iff \exists\, s\in\mathbb{Z}\setminus\{0\}$ with $s(ad-bc)=0$

But $\mathbb{Z}$ is a domain, so $ad-bc=0$ (since $s\neq 0$)

If $m=\gcd(a,b)$, $n=\gcd(d,c)$ then $\frac{a}{m}\frac{d}{n}=\frac{b}{m}\frac{c}{n}$ forces

$\frac{a}{m}=k\frac{c}{n}$ & $\frac{d}{n}=k\frac{b}{m}$ for $k\in\mathbb{Z}$

In conclusion: $\frac{a}{b}=\frac{a/m}{b/m}=\frac{c/n}{d/n}=\frac{c}{d}$.

2. $R=\mathbb{Z}[x]$, $\mathrm{Quot}(R)=\mathbb{Q}(x)=\left\{\frac{P(x)}{Q(x)} : P,Q\in\mathbb{Q}[x],\ Q\neq 0\right\}$

<u>Another special example of S</u>:

- R commutative $S=$ set of nonzero divisors of R

Then: S is multiplicatively closed

Def: $S^{-1}R$ = total ring of fractions = $\mathrm{Quot}(R)$

- **From polynomials to Laurent polynomials:**

$S = \{1, x^i : i \geq 1\} \in \mathbb{K}[x]$ is multiplicatively closed.

Thm: $S^{-1}\mathbb{K}[x] = \mathbb{K}[x, x^{-1}]$.

$(a,s) \sim (b,t) \iff x^n(at - bs) = 0 \quad n \geq 0$

Again, $at - bs = 0$, $s, t \in S$ so $s = x^k$, $t = x^\ell$

So $a = b x^{k-\ell} \in \mathbb{K}[x]$ if $k \geq \ell$

$b = a x^{\ell-k} \in \mathbb{K}[x]$ if $\ell \geq k$

$\Rightarrow \frac{a}{s} \in \mathbb{K}[x, x^{-1}]$.

- **A degenerate example:**

$R = \mathbb{Z}/_{6\mathbb{Z}} \supset S = \{1, 2, 4\}$ mult. closed

In $S^{-1}R$ $\frac{r}{s} = 0 \left(= \frac{0}{1}\right) \iff \exists t \in S$ with $t(r \cdot 1 - s \cdot 0) = 0$
$tr = 0$

So $\frac{3}{s} = 0 \quad \forall s \in S \quad (2 \cdot 3 = 0)$

$\frac{1}{s} \neq 0, \quad \frac{2}{s} \neq 0, \quad \frac{4}{s} \neq 0, \quad \frac{5}{s} \neq 0$

Claim: $S^{-1}R = \{0, 1, \frac{1}{2}\}$ (HW7)

§3. Universal Properties:

Fix R commutative ring & $S \subset R$ multiplicatively closed

Proposition: We have a natural ring homomorphism

$$j_S : \begin{array}{ccc} R & \longrightarrow & S^{-1}R \\ a & \longmapsto & \frac{a}{1} \end{array} \quad (= \text{class of } (a,1))$$

such that for every $t \in S$, $j_S(t)$ is invertible in $S^{-1}R$ (its inverse is $\frac{1}{t}$)

Proof: Definition of the ring structure on $S^{-1}R$ makes j_S a ring homomorphism.

- $\left(\frac{t}{1}\right)^{-1} = \frac{1}{t}$ because $(t,1)\cdot(1,t) = (t,t) = (1,1)$

Lemma: $\operatorname{Ker}(j_S) = \{ a \in R : \exists s \in S \text{ with } sa = 0 \}$

Pf/ $j_S(a) = \frac{a}{1} = \frac{0}{1} \iff \exists s \in S$ st $s(a\cdot 1 - 0\cdot 1) = 0$, ie $sa = 0$ $\square$

- Next, we state the universal property satisfied by $S^{-1}R$:

Theorem: Fix B another commutative ring & let $f: R \longrightarrow B$ be a ring homomorphism such that $\forall t \in S$: $f(t) \in B$ is invertible. Then, there exists a unique ring homomorphism $\tilde{f}: S^{-1}R \longrightarrow B$ making $\tilde{f} \circ j_S = f$.

Proof Want to show

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "j_S"'] \arrow[dr, phantom, "\circlearrowleft"] & B \\ S^{-1}R \arrow[ur, dashed, "\exists ! \tilde{f}"'] & \end{tikzcd}$$

Set $\boxed{\tilde{f}\left(\frac{a}{s}\right) := f(a)\, f(s)^{-1}}$

- Well-defined: $\frac{a}{s} = \frac{b}{t} \iff \exists s' \in S$ with $s'(at - bs) = 0$

Then $\underset{B^*}{\underset{\cap}{f(s)}}\big(f(a)f(t) - f(b)f(s)\big) = 0$

$\Rightarrow f(a)f(t) = f(b)f(s)$

So $f(a)\,f(s)^{-1} = f(b)\,f(t)^{-1}$ in B

- Ring homomorphism:
  - $\tilde{f}\left(\frac{a}{s}+\frac{b}{t}\right) = f\left(\frac{at+bs}{st}\right) = f(at+bs)\,f(st)^{-1}$
  $= \left(f(a)f(t) + f(b)f(s)\right) f(s)^{-1} f(t)^{-1}$
  $= f(a)f(s)^{-1} + f(b)f(t)^{-1} = \tilde{f}\left(\frac{a}{s}\right) + \tilde{f}\left(\frac{b}{t}\right)$
  - $\tilde{f}\left(\frac{a}{s}\frac{b}{t}\right) = \tilde{f}\left(\frac{ab}{st}\right) = f(ab)\,f(st)^{-1}$
  $= f(a)f(b)f(s)^{-1}f(t)^{-1} = f(a)f(s)^{-1}f(b)f(t)^{-1}$
  $= \tilde{f}\left(\frac{a}{s}\right)\tilde{f}\left(\frac{b}{t}\right).$
  - $\tilde{f}(1) = \tilde{f}\left(\frac{1}{1}\right) = f(1)f(1)^{-1} = 1\cdot 1^{-1} = 1.$
- $\tilde{f}\circ j_S(a) = \tilde{f}\left(\frac{a}{1}\right) = f(a)f(1)^{-1} = f(a)1^{-1} = f(a).$ $\square$

Note: All these constructions can be done for modules (modules of fractions relative to S are modules ($S^{-1}M$) over $S^{-1}R$ build over of R-modules (M)). See HW7.