Lecture XLVI: Nilradicals & Coming Attractions

Recall: R commutative ring, S = multiplicatively closed

$$\left\{\begin{matrix}\text{Prime ideals } \mathfrak{P} \\ \text{of } R \text{ with } \mathfrak{P}\cap S = \emptyset\end{matrix}\right\} \xleftrightarrow{\text{1-to-1}} \left\{\begin{matrix}\text{Prime ideals} \\ \text{of } S^{-1}R\end{matrix}\right\}$$

$$\mathfrak{P} \longmapsto \tilde{\mathfrak{P}} = S^{-1}\mathfrak{P}$$

$$j^*(\tilde{\mathfrak{P}}) \longleftarrow \tilde{\mathfrak{P}}$$

§46.1 An application: the Nilradical of R:

Assume R is a commutative ring.

Definition: An element $a \in R$ is <u>nilpotent</u> if $\exists\, n \gneq 0$ with $a^n = 0$.

Set $\boxed{\mathcal{N} := \{a \in R : a \text{ is nilpotent}\}}$

Remark: as we do not allow 0 to be in our multiplicatively closed set, for a given $a \in R$, we have:

$$\{1, a, a^2, a^3, \ldots\} \text{ is multiplicatively closed} \iff a \notin \mathcal{N}.$$

Proposition: (1) $\mathcal{N} \subsetneq R$ is an ideal

(2) $\mathcal{N} \subset \mathfrak{P}$ for any prime ideal $\mathfrak{P} \subsetneq R$.

(3) $$\bigcap_{\substack{\mathfrak{P}\subsetneq R \\ \text{prime}}} \mathfrak{P} = \mathcal{N}$$

Definition: $\mathcal{N}$ is called the <u>nilradical</u> of R.

Proof: (1) was a homework problem ("$a, b \in \mathcal{N} \Rightarrow a+b \in \mathcal{N}$" uses Binomial Theorem: $a^n = 0$ & $b^m = 0 \Rightarrow (a+b)^{n+m} = 0$)

(2) $a \in \mathcal{N} \Rightarrow a^n = 0$ for some $n \gneq 0$

Since $a^n = 0 \in \mathfrak{P}$ & $\mathfrak{P}$ is prime, then $a \in \mathfrak{P}$.

(3) By (2) $\mathcal{N} \subseteq \bigcap_{\substack{\mathfrak{P}\subsetneq R \\ \text{prime}}} \mathfrak{P}$, so it suffices to prove the reverse inclusion:

If $a \notin \mathcal{N}$, then $S = \{1, a, a^2, \dots\} \subseteq R$ is a multiplicatively closed set. Consider the ring homomorphism:

$$j : R \longrightarrow S^{-1}R$$

Take any prime ideal $\tilde{\mathfrak{P}} \subsetneq S^{-1}R$ (such ideals exist because $\exists\, M \subseteq S^{-1}R$ maximal ideal, and maximal ideals are prime).

Set $\mathfrak{P} = j^*(\tilde{\mathfrak{P}}) \subsetneq R$ prime ideal. By Theorem §45.2, $\mathfrak{P} \cap S = \emptyset$ so $a \notin \mathfrak{P}$.

This shows: $a \notin \mathcal{N} \implies \exists$ prime ideal $\mathfrak{P} \subsetneq R$ with $a \notin \mathfrak{P}$.

Hence: $\displaystyle\bigcap_{\substack{\mathfrak{P} \subsetneq R \\ \text{prime}}} \mathfrak{P} \subseteq \mathcal{N}$. $\square$

§46.2 Jacobson radical:

Let R be a commutative ring. Define:

$$\mathcal{J} := \bigcap_{\substack{M \subsetneq R \\ \text{maximal ideal}}} M \qquad (\text{Name: Jacobson radical of } R)$$

Recall analogy: $\displaystyle \mathcal{N} = \{a \in R : a \text{ is nilpotent}\} = \bigcap_{\substack{\mathfrak{P} \subsetneq R \\ \text{prime ideal}}} \mathfrak{P}$

Name: nilradical ideal of R

Remark: Since $M \subsetneq R$ maximal ideal $\Rightarrow$ M is a prime ideal, we get $\boxed{\mathcal{N} \subseteq \mathcal{J}}$.

Proposition: $\mathcal{J} = \{a \in R : 1 - xa \in R^\times \ \forall x \in R\}$

Proof: Consider the set $K := \{a \in R : 1 - xa \in R^\times \ \forall x \in R\}$. We want to prove that $\mathcal{J} = K$.

We want to show that for any given element $a \in R$:

$$1 - ax \in R^\times \ \forall x \in R \iff a \in M \ \forall M \text{ maximal ideal } M \subsetneq R.$$

Equivalently,

$\exists M$ maximal ideal of R, $M \subsetneq R$ with $a \notin M$ $\iff$ $\exists y \in R : 1-ay \notin R^\times$

($\Rightarrow$) Since $a \notin M$ & M is maximal, we have $(M,a) = M+(a) = R$

ideal generated by M and a

ie $\exists m \in M$ & $y \in R$ with $1 = m+ya$ $\Rightarrow$ $1-ay = m \in M$, so $1-ay \notin R^\times$ as we wanted to show

($\Leftarrow$) Assume $\exists y \in R$ with $1-ay \notin R^\times$

Then $(1-ay) = I \subsetneq R$ is a proper ideal of R.

By Proposition 1 §41.2, $\exists$ a maximal ideal $M \subsetneq R$ s.t. $(1-ay) \subseteq M$.

This implies $a \notin M$ because otherwise $\begin{matrix} 1-ay \in M \\ a \in M \end{matrix}$ $\Rightarrow 1 = 1-ay + ay \in M$ Contradiction!

$\square$

§46.3 Operations on ideals:

Recall the basic operations with rings and their ideals

Input	Output	Ideals
R_1, R_2: Two (commutative) rings	$R_1 \times R_2$ (direct product) and ring homomorphisms $R_1 \xleftarrow{\pi_1} R_1 \times R_2 \xrightarrow{\pi_2} R_2$, $r_1 \longleftarrow\!\shortmid (r_1, r_2) \longmapsto r_2$	Ideals of $R_1 \times R_2$ $= \{ I_1 \times I_2 \mid I_1 \subset R_1, I_2 \subset R_2 \text{ ideals} \}$
R (commutative) ring	Ring Homomorphisms $R[x] \hookleftarrow R$, $R[\![x]\!] \hookleftarrow R$ (constants)	When $R = K$ is a field, we know • every ideal is principal • $K[\![x]\!]$ is local with maximal ideal (x)
$R \supsetneq I$, R comm. ring, I ideal (proper)	R/I : quotient ring $\pi : R \longrightarrow R/I$ ring hom.	Ideals of R/I $= \{ \underset{\pi(J)}{\overset{\shortparallel}{J/I}} : J \subseteq R \text{ ideal with } I \subseteq J \}$

Input	Output	Ideals
R : comm. ring $S \subsetneq R$: mult closed set $(0 \notin S,\ 1 \in S,$ $a, b \in S \Rightarrow a\cdot b \in S)$	$S^{-1}R$: ring of fractions $j: R \longrightarrow S^{-1}R$ ring hom. $r \longmapsto \frac{r}{1}$	$\underset{\text{ideal}}{I \subseteq R} \rightsquigarrow S^{-1}I \subseteq S^{-1}R$ $S^{-1}I = \{\frac{a}{s} : a \in I, s \in S\}$ $\underset{\text{ideal}}{j^*(\tilde{I}) \subseteq R} \leftsquigarrow \underset{\text{ideal}}{\tilde{I} \subseteq S^{-1}R}$ $j^*(\tilde{I}) = \{a : j(a) \in \tilde{I}\}$ $S^{-1}(j^*(\tilde{I})) = \tilde{I} \quad \forall \tilde{I} \subseteq S^{-1}R$ ideal $j^*(S^{-1}I) \underset{\text{typical}}{\supsetneq} I$ even if $I \cap S = \emptyset$ Eg: $R = K[x,y]$, $I = (xy)$, $S = R \setminus (x)$ $\Rightarrow j^*(S^{-1}I) = (x) \supsetneq (xy)$

§ 46.5 Landscape of rings we'll study:

In the next few lectures we'll study certain classes of commutative rings, which are of interest in Geometry and Number Theory, namely Noetherian ones (every ideal is finitely generated). They will be classified according to their dimension which can be viewed as the "number of parameters" needed to describe them, in analogy with the dimension of a vector space.

$\dim R = -1 + (\text{maximal length of a chain of prime ideals } \mathfrak{P}_1 \subsetneq \mathfrak{P}_2 \subsetneq \cdots \subsetneq \mathfrak{P}_\ell \text{ in } R)$

	Unique Factorization Domains (eg K field, $n \in \mathbb{N}$) $K[x_1, x_2, \ldots, x_n]$	
"dim" = 1	Dedekind domains Principal Ideal domains Euclidean domains	"Singular Curves"  $= \mathbb{C}[x,y]/(y^2-x^3-x^2)$  $= \mathbb{C}[x,y]/(x^2-y^3)$
"dim" = 0	FIELDS	ARTINIAN RINGS
	Noetherian domains	Noetherian rings with zero-divisors

"dim"$(R)=0$ means every prime ideal is maximal

"dim"$(R)=1$ & R is an integral domain means every non-zero prime ideal is maximal.

§46.4 Euclidean Domains:

Definition: A Euclidean domain is an integral domain R such that there exists a function

$$N : R \longrightarrow \mathbb{Z}_{\geq 0} \quad \text{(optimal: } N(0)=0 \text{ or define } N: R\smallsetminus\{0\} \longrightarrow \mathbb{Z}_{\geq 0})$$

such that for every $a, b \in R$, $b \neq 0$ we can find $q, r \in R$ such that:

$$a = qb + r \qquad \text{AND} \qquad N(r) < N(b) \text{ if } r \neq 0$$

Main examples (from §39.2):

① $R=\mathbb{Z}$; $N(l) = |l| \quad \forall l \in \mathbb{Z}$

② $R=K[x]$ for K a field, $N(f(x)) = \text{degree of } f(x) \quad \forall f(x) \in K[x]\smallsetminus\{0\}$

Convention: Set $N(0)=0$ although for other reasons we wanted $N(0)=-\infty$

③ $R=\mathbb{Z}[i]=\mathbb{Z}[\sqrt{-1}]$ Gauss Integers $N(a+bi) = a^2+b^2 = |a+bi|^2 \quad \forall a,b\in\mathbb{Z}$

§46.5 Euclidean Domains are PIDs:

Recall: A PID is an integral domain R where each ideal is principal (ie can be generated by 1 element).

The three examples above are PIDs. This is true in general:

Lemma: Let R be a Euclidean domain. Then R is a principal ideal domain.

Proof: Let $N: R \longrightarrow \mathbb{Z}_{\geq 0}$ be the function on R given by the definition of a Euclidean domain.

Let $I \subseteq R$ be a nonzero ideal. Choose $b \in I\smallsetminus\{0\}$ with $N(b) = \min \underbrace{\{N(b) : b \in I\smallsetminus\{0\}\}}_{\subseteq \mathbb{N} \text{ (is well-ordered)}}$

Claim: $I=(b)$

Pf/ For $a\in I$, write it as $a = q\cdot b + r$ with $r=0$ or $r\neq 0$ and $N(r)<N(b)$

But $r = a - qb \in I$. So if $r\neq 0$ we get $N(r) \geq N(b)$ Contr!

$\Rightarrow$ Only option is $r=0$ ie $I \subseteq (b) \underset{b\in I}{\subseteq} I$ giving $I=(b)$ □

§46.6 Quadratic field extensions:

Definition: Consider $D \in \mathbb{Z} \setminus \{0,1\}$ with $\sqrt{D} \notin \mathbb{Z}$. A quadratic field extension of $\mathbb{Q}$ is a field of the form $R = \mathbb{Q}(\sqrt{D}) \subseteq \mathbb{C}$. Here $\mathbb{Q}(\sqrt{D})$ is the smallest subfield of $\mathbb{C}$ containing $\sqrt{D} \in \mathbb{C}$.

Remark 1: $R \ni \sqrt{D}$, $R \ni 1$ and it is a subfield $\Rightarrow R \supseteq \mathbb{Z}$ $(\mathbb{Z} = \langle 1 \rangle)$ & so $R \supseteq \mathbb{Q}$.
(R field)

Lemma 1: We can assume D is square free ie $D = \pm p_1 \cdots p_\ell$ for $p_1 \cdots p_\ell \in \mathbb{Z}_{\geq 2}$ distinct primes

Proof: By the unique factorization of D into prime factors, we can write

$$D = \pm p_1^{\ell_1} \cdots p_r^{\ell_r} = \pm M^2 \, p_{i_1} \cdots p_{i_s} \qquad \text{with } M \in \mathbb{Z}$$

(Indeed: $\ell_i = 2k_i$ or $\ell_i = 2k_i + 1$ $\forall i \Rightarrow$ Take $M = \prod_{i=1}^{n} p_i^{2k_i}$)

Then $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\underset{\substack{\cap \\ \mathbb{Z}}}{M} \sqrt{\pm p_{i_1} \cdots p_{i_s}}) = \mathbb{Q}(\sqrt{\pm p_{i_1} \cdots p_{i_s}})$

(A field contains $\mathbb{Q}$ & $\sqrt{D}$ $\Leftrightarrow$ it contains $\mathbb{Q}$ & $\sqrt{D'}$ where $D' = \pm p_{i_1} \cdots p_{i_s}$ is square-free)

⚠ -1 is square free. ($\ell = 0$ in the definition)