Lecture 3. Radicals.

R a ring.

The Jacobson radical of R is the intersection of all maximal ideals. Denoted $\mathrm{rad}(R)$.

Prop. $x \in R$, $u \in R^\times$. Then $x \in \mathrm{Rad}(R) \iff u - xy$ is a unit for any $y \in R$.

Pf. Let $x \in \mathrm{rad}(R)$. Let $\mathfrak{m}$ be a max. ideal. Suppose $u - xy \in \mathfrak{m}$. Then $xy \in \mathfrak{m}$, so $u \in \mathfrak{m}$ $\Rightarrow\Leftarrow$. Thus $u - xy$ is not in any max. ideal so is a unit (as any proper ideal is cont. in a max. ideal). Conversely, supp. $u - xy$ is a unit for all y. Let $\mathfrak{m}$ be a max. ideal s.t. $x \notin \mathfrak{m}$ (assuming the contrary). Then $\langle x \rangle + \mathfrak{m} = R$. So $\exists y \in R$, $m \in \mathfrak{m}$ s.t. $xy + m = u$. So $u - xy$ is not a unit. $\Rightarrow\Leftarrow$. $\blacksquare$

Let $\mathfrak{a} \subset R$ be an ideal, $\pi : R \to R/\mathfrak{a}$ the quotient map.

Prop. If $\mathfrak{a} \subset \mathrm{Rad}(R)$ then π is injective on idempotents.

Pf. Let e, e' be idempotents in R such that $\varkappa(e) = \varkappa(e')$, so $\varkappa(e-e') = 0$. Then

$$x^3 = (e-e')^3 = e - e' = \overset{\shortparallel}{x}. \text{ So } x(1-x^2) = 0.$$

But $x \in \mathfrak{a}$, so $1-x^2$ is a unit. Hence $x = 0$, as desired. ■.

Def. A ring R is local if it has a unique maximal ideal, and semilocal if it has ~~all local~~ finitely many.

$\mathrm{rad}(\mathbb{Z}/p^n\mathbb{Z}) = p\mathbb{Z}/p^n\mathbb{Z}$, $\mathrm{rad}(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/p_1 \cdots p_m\mathbb{Z}$. p_i prim fact

Ex. $\mathrm{rad}(\mathbb{Z}) = 0$, $\mathrm{rad}(\mathbb{C}[x]) = 0$, $\mathrm{rad}(\mathbb{C}[[x]]) = x\,\mathbb{C}[[x]]$, $\mathrm{rad}(\mathbb{C}[x]/(x-\alpha_1)^{m_1} \cdots (x-\alpha_n)^{m_n}) = \langle (x-\alpha_1) \cdots (x-\alpha_n) \rangle$ if α_i are distinct.

$\mathbb{C}[[x]]$ is a local ring, so is $\mathbb{C}[x]/x^n$.
$\mathbb{C}[x]$ is not a local ring

The ring R_a of rational fns in x without pole at $a \in \mathbb{C}$ is a local ring.

$\mathbb{Z}$ is not local, but $\mathbb{Z}/p^n\mathbb{Z}$ local
$\mathbb{Z}_p$ (p-adic integers) are local.

$\mathbb{Z}/n$, $\mathbb{C}[x]/(f)$ are semilocal.

Ex. of local ring: Ring of Germs of analytic functions. (explains the terminology)

Lemma. R a ring, $\mathfrak{n} \subset R$ set of nonunits. Then R is local $\Leftrightarrow$ $\mathfrak{n}$ is an ideal (if so, $\mathfrak{n}$ is a max. ideal)

Pf. $\mathfrak{n}$ is an ideal $\Rightarrow \forall x \notin \mathfrak{n}$ is a unit, so $\langle x \rangle = R$, hence $\mathfrak{n}$ maximal. ~~Conversely~~ Also $\mathfrak{n}$ contains all other max ideals since they consist of nonunits, so they all coincide with it. Conversely, if R is local, then $\mathfrak{m} \subset R$ unique max. ideal, and as we showed, any nonunit is contained in a max ideal, so $\mathfrak{n} \subset \mathfrak{m}$. Thus $\mathfrak{n} = \mathfrak{m}$ since $\mathfrak{m}$ does not contain units.

Ex. $R' \times R''$ not local if $R', R'' \neq 0$. $(0,1)$ and $(1,0)$ nonunits but their sum is a unit.

Ex. If R is local with max ideal $\mathfrak{m}$ then $P = R[[X_1, \dots, X_n]]$ local with max ideal $\mathfrak{m} + \mathfrak{a}$, $\mathfrak{a} = \langle X_1, \dots, X_n \rangle$.

Ex. Let k be a field. Then $A = k[[X]]$ is a PID. In fact, the only proper nonzero ideals are (X^n). Namely, if $I \neq 0$ is an ideal, n = minimal order of vanishing of $f \in I$. So A is a PID.

$\mathrm{Frac}(A) = K$ is obtained by inverting nonunits and we only need to invert X. So $K = k((X))$, the field of Laurent series $\sum_{i=-m}^{\infty} a_i x^i$.

Ex. Consider $R = k[[x]][y]$. $\varphi: R \to K$, $\varphi(y) = x^{-1}$. Then φ is surjective, $\operatorname{Ker}\varphi$ is a maximal ideal. This ideal is generated by $yx-1$. Also $\langle x, y\rangle$ is a max. ideal. So R has both principal and nonprincipal max. ideals.

Ex. Can do the same with $A = \mathbb{Z}_p$, $\operatorname{Frac}(A) = K = \mathbb{Q}_p$ - p-adic field, $R = \mathbb{Z}_p[y]$, $\varphi: R \to \mathbb{Q}_p$, $\varphi(y) = \frac{1}{p}$.

Prop. R a ring, $S \subset R$ multiplicative subset, $\mathfrak{a} \subset R$ and ideal with $\mathfrak{a} \cap S = \emptyset$. Set $\mathcal{S} = \{$ideals $\mathfrak{b} \supset \mathfrak{a}$ such that $\mathfrak{b} \cap S = \emptyset\}$. Then $\mathcal{S}$ has a maximal element $\mathfrak{p}$, and any such $\mathfrak{p}$ is prime.

Ex. $S = \{$numbers coprime to $N\}$, $\mathfrak{a} = (m)$, m not coprime to N. Then $\mathfrak{p} = \langle p\rangle$, p - any prime factor of m which divides N.

Proof. Clearly, $\mathfrak{a} \in \mathcal{S}$, so $\mathcal{S} \neq \emptyset$, and $\mathcal{S}$ is partially ordered by inclusion. If $\mathfrak{b}_\lambda$ is a chain in $\mathcal{S}$, let $\mathfrak{b} = \bigcup \mathfrak{b}_\lambda$. Then $\mathfrak{b}$ is an upper bd for $\mathfrak{b}_\lambda$. So by Zorn's lemma, $\mathcal{S}$ has a maximal element. Let's show it's a prime.

Let $x, y \in R \setminus \mathfrak{p}$. Then $\mathfrak{p} + \langle x\rangle$ and $\mathfrak{p} + \langle y\rangle$ are strictly larger than $\mathfrak{p}$. So $\exists p, q \in \mathfrak{p}$ and $a, b \in R$ s.t. $p + ax \in S$, $q + by \in S$. So since S is mult,
$(p+ax)(q+by) = pq + pby + qax + abxy \in S$.

Since $pq + pby + qax \in \mathfrak{p}$, $xy \notin \mathfrak{p}$. So $\mathfrak{p}$ is prime. ∎

<u>Saturated multiplicative subsets.</u> Let R be a ring, $S \subset R$ a mult. subset. Say S is <u>saturated</u> if $\forall x, y \in R$ with $xy \in S$, we have $x, y \in S$.

<u>Ex.</u> $R^\times$, $R \setminus \mathrm{zdiv}(R)$ are saturated mult. subsets. $\{2^n, n \geq 0\}$ is saturated, but $\{4^n, n \geq 0\}$ is not. Further, if $\varphi : R \to R'$ is a ring map, and $T \subset R'$ subset then if T is saturated mult, so is $\varphi^{-1}(T)$ and converse holds for surjective φ. Also any mult. subset S is contained in a saturated one, $\bar{S} = \{x \in R : \exists y \in R \text{ s.t. } xy \in S\}$ (minimal sat. mult. subset cont. S).

<u>Lemma.</u> (Prime avoidance). R a ring, $\mathfrak{a} \subset R$ stable under $+, \cdot$, and $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ ideals s.t. $\mathfrak{p}_3, \dots, \mathfrak{p}_n$ prime. If $\mathfrak{a} \not\subset \mathfrak{p}_j$ for all j, then $\exists x \in \mathfrak{a}$ s.t. $x \notin \mathfrak{p}_j$ for all j; In other words, if $\mathfrak{a} \subset \bigcup_{i=1}^n \mathfrak{p}_i$ then $\mathfrak{a} \subset \mathfrak{p}_i$ for some i.

<u>Pf.</u> Induct on n. For $n = 1$ the assertion is trivial. Assume $n \geq 2$. By the induction assumption, $\forall i \ \exists x_i$ s.t. $x_i \notin \mathfrak{p}_j \ \forall j \neq i$. Can assume $x_i \in \mathfrak{p}_i$, otherwise we are done. If $n = 2$ then $x_1 + x_2 \notin \mathfrak{p}_j$ for $j = 1, 2$. If $n \geq 3$,

Then $x_1 \cdots x_{n-1} + x_n \notin \mathfrak{p}_j$ for all j, as, if $j=n$, then $\mathfrak{p}_n$ is prime and $x_n \in \mathfrak{p}_n$ [$x_1 \cdots x_{n-1} \neq 0$ in $R/\mathfrak{p}_n$ since $x_1, \dots, x_{n-1} \neq 0$ in $R/\mathfrak{p}_n$] and if $j<n$ then $x_n \notin \mathfrak{p}_j$ but $x_j \in \mathfrak{p}_j$. ☒

<u>Nilradical</u>. R a ring, $\mathfrak{a} \subset R$ subset.

The <u>radical</u> of $\mathfrak{a}$ is the set $\sqrt{\mathfrak{a}}$ defined by $\sqrt{\mathfrak{a}} = \{x \in R \mid x^n \in \mathfrak{a} \text{ for some } n \geq 1\}$.

So $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$. Also, if $\mathfrak{a} = \bigcap_\alpha \mathfrak{p}_\alpha$, $\mathfrak{p}_\alpha$ prime ideals, then $\sqrt{\mathfrak{a}} = \mathfrak{a}$.

Nilradical $nil(R) = \sqrt{\{0\}} = \{$nilpotent elements$\}$.

$x^n = 0 \Rightarrow x^n \in \mathfrak{m}$ for any max. ideal $\mathfrak{m}$.
$\Rightarrow x \in \mathfrak{m}$ since $\mathfrak{m}$ prime, so $nil(R) \subset rad(R)$.
And $nil(R)$ is an ideal.

R reduced in $nil(R) = \{0\}$.

<u>Ex.</u> Domains are reduced. Non-reduced ~~dom~~ ring $R = \mathbb{Z}/p^n\mathbb{Z}$ $nil(R) = rad(R) = (p)$.
Also $k[x]/(x^n)$. $k[x,y]/(xy)$ reduced, but not a domain. $k \times k$, k a field reduced.
$k[[x]]$ reduced. $nil(R) = 0 \neq rad(R)$.

<u>Thm.</u> (Scheinnullstellensatz) $R \supset \mathfrak{a}$ ideal. Then $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$, $\mathfrak{p}$ prime. (agree that empty int. $= R$).

Pf. $x \notin \sqrt{\mathfrak{a}}$. let $S = \langle 1, x, x^2, \ldots \rangle$

Then S is mult., and $\mathfrak{a} \cap S = \emptyset$.
So by the above, $\exists$ a prime ideal
$\mathfrak{p} \supset \mathfrak{a}$ ~~with~~ $\mathfrak{p} \cap S = \emptyset$
with $x \notin \mathfrak{p}$. So $x \notin \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$.
Conversely, if $x \in \sqrt{\mathfrak{a}}$ ~~and~~ then $x^n \in \mathfrak{a} < \mathfrak{p}$;
so $x^n \in \mathfrak{p}$ and hence $x \in \mathfrak{p}$.

Prop. R ring, $\mathfrak{a} \subset R$ ideal $\Rightarrow \sqrt{\mathfrak{a}}$ ideal.

Pf. $\underset{\substack{x^n \in \mathfrak{a} \\ y^m \in \mathfrak{a}}}{x, y \in \sqrt{\mathfrak{a}}} \Rightarrow (x+y)^{n+m} \in \mathfrak{a} \Rightarrow x + y \in \sqrt{\mathfrak{a}}$.

$(ax)^n \in \mathfrak{a} \Rightarrow ax \in \sqrt{\mathfrak{a}}$. | Another pf: intersection of ideals is an ideal.

Prop. R reduced, has a unique min prime $\Leftrightarrow$ a domain.

Pf. R domain $\Rightarrow \langle 0 \rangle$ prime $\Rightarrow$ reduced + unique min. prime. Conversely, let R be reduced, ~~and~~ then $\langle 0 \rangle = \sqrt{\langle 0 \rangle}$, and so $\langle 0 \rangle = \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p}$.

Lemma: Any prime $\mathfrak{p}$ contains a minimal prime for the property that $\mathfrak{p} \supset S$.

Pf. These are ordered by inclusion. Now if q_λ is a chain, then can cons $\bar{q} = \bigcap_{\text{all}} q_\lambda$. $xy \in \bar{q}$ $\Rightarrow xy \in q_\lambda$ for ~~some~~ all λ, so $x \in q_\lambda$ or $y \in q_\lambda$ for all λ. ~~The~~ Supp. $\exists \mu$ s.t. $\forall q_\lambda \subsetneq q_\mu$, $x \notin q_\lambda$. Then $y \in q_\lambda$, so $y \in \bar{q}$. Otherwise, $\forall \mu$, $x \in q_\mu$, so $x \in \bar{q}$. ~~Now apply Zorn.~~

So by lemma $q \subseteq$ all p, so $q = \langle 0 \rangle$

So $\langle 0 \rangle$ is a prime $\Rightarrow$ R domain.