## IV.C. Primes and radicals

Returning to the commutative setting, let $\mathcal{S} \subset R$ be a multiplicative subset, and $\mathcal{I} \subset R$ a (necessarily proper) ideal with $\mathcal{I} \cap \mathcal{S} = \emptyset$. The set

$$\mathbb{S} := \{J \subset R \text{ ideal} \mid J \cap \mathcal{S} = \emptyset,\ J \supset \mathcal{I}\}$$

contains $\mathcal{I}$, so is nonempty. We have the following key

IV.C.1. LEMMA. *$\mathbb{S}$ has a maximal element $P$, and it is prime.*

PROOF. The maximal element exists by Zorn (straightforward), but why is it prime? Let $I_1, I_2 \subset R$ be ideals with $I_1 I_2 \subset P$, but $I_1, I_2 \not\subset P$. Then $I_j + P \supsetneq P$ and $I_j + P \supset \mathcal{I}$, so $(I_j + P) \cap \mathcal{S} \neq \emptyset$ by maximality of $P$. Write $\imath_j + p_j \in (I_j + P) \cap \mathcal{S}$ for $j = 1, 2$, and observe that $(\imath_1 + p_1)(\imath_2 + p_2)$ belongs to $\mathcal{S}$ (by multiplicativity) and also to $I_1 I_2 + P = P$. This contradicts $P \cap \mathcal{S} = \emptyset$. □

This has the immediate

IV.C.2. COROLLARY. *$R$ has a prime ideal disjoint from $\mathcal{S}$.*

PROOF. Since $0 \notin \mathcal{S}$, we can apply the Lemma with $\mathcal{I} = \{0\}$. □

This is admittedly not very interesting if $R$ is a domain, since then $\{0\}$ is prime. It also wastes the power of the Lemma, which is a broad generalization of the existence of maximal ideals (the $\mathcal{S} = \{1\}$ case). For a better application, we first need a

IV.C.3. DEFINITION. The **radical** of an ideal $I \subsetneq R$ is

$$\sqrt{I} \ \text{ or } \ \mathrm{Rad}(I) := \bigcap_{\substack{P \supset I \\ \text{prime}}} P.$$

This is a proper ideal containing $I$.[2] (Note that the intersection is nonempty, since a proper ideal is contained in a maximal, *a fortiori*

[2] The process of taking the radical is called "radicalization". Whereas normal people might be radicalized *by* their ideals, algebraists are so extreme (and apparently immune to normal English syntax) that they *radicalize their ideals*.

prime, ideal.) The **nilradical** of $R$ is the special case

$$N(R) := \mathrm{Rad}(\{0\}) = \bigcap_{P \text{ prime}} P.$$

If $I = \mathrm{Rad}(I)$, then we call $I$ a **radical ideal**. Of course, if $I$ is prime, then it is radical. (As a special case, if $R$ is a domain, then $\{0\}$ is a prime ideal, and the nilradical is zero.) But radical ideals are a larger class than prime ideals.

IV.C.4. EXAMPLE. In $R = \mathbb{Z}$, if $p_1, \ldots, p_r$ are distinct prime numbers, then $\mathrm{Rad}((p_1^{m_1} \cdots p_r^{m_r})) = (p_1) \cap \cdots \cap (p_r) = (p_1 \cdots p_r)$. So the nonzero radical ideals are precisely the ideals generated by square-free integers.

IV.C.5. THEOREM. $\mathrm{Rad}(I) = \{r \in R \mid r^n \in I \textit{ for some } n \in \mathbb{N}\}$.

PROOF. $\underline{(\supseteq)}$: If $r^n \in I$ and $P$ is a prime containing $I$, then $r^n \in P \implies r \in P \implies r \in \mathrm{Rad}(I)$.

$\underline{(\subseteq)}$: Let $r \in R$, with $r^n \notin I$ $(\forall n \in \mathbb{N})$. [We need to show that $r \notin \mathrm{Rad}(I)$.] The set $\mathcal{S} := \{r^n \mid n \in \mathbb{N}\}$ is multiplicative, and $\mathcal{S} \cap I = \emptyset$. By Lemma IV.C.1, there exists a prime ideal $\mathcal{P}$ with $\mathcal{P} \cap \mathcal{S} = \emptyset$ and $\mathcal{P} \supset I$. Clearly $r \notin \mathcal{P}$ (since $r \in \mathcal{S}$), and so $r \notin \mathrm{Rad}(I)$. □

IV.C.6. COROLLARY. *The nilradical of R consists of its nilpotent elements:* $N(R) = \{r \in R \mid r^n = 0 \textit{ for some } n \in \mathbb{N}\}$.

We summarize some properties of the radical:

IV.C.7. COROLLARY. (i) $\mathrm{Rad}(\mathrm{Rad}(I)) = \mathrm{Rad}(I)$
(ii) $\mathrm{Rad}(I_1 I_2 \cdots I_n) = \mathrm{Rad}(\cap_j I_j) = \cap_j \mathrm{Rad}(I_j)$
(iii) $\mathrm{Rad}(I^n) = \mathrm{Rad}(I)$.
(iv) $\mathrm{Rad}(P) = P$ *for P prime.*

PROOF. (i) By IV.C.5, the LHS comprises elements with a power in $\mathrm{Rad}(I)$, which is equivalent to having a power in $I$.

(ii) An element $r$ in the RHS is one with $r^{m_j} \in I_j$ for some $m_j \in \mathbb{N}$ (for each $j$), hence with $r^{\sum_j m_j} \in I_1 \cdots I_n$ ($\implies r \in$ LHS). An element in the LHS belongs to the middle term since $I_1 \cdots I_n \subset I_1 \cap \cdots \cap I_n$.

An element $r$ in the middle term has $r^m \in \cap_j I_j$ hence belongs to the RHS.

(iii) We have LHS $\subset$ RHS since $I^m \subset I$. For the converse, if $r^m \in I$ then $r^{mn} \in I^n$. (iv) is obvious. □

For one more result related to IV.C.1, consider the case where the multiplicative subset $\mathcal{S}$ is the intersection of complements of prime ideals $P_1, \ldots, P_n$. Then it turns out that the maximal elements of $\mathbb{S}$ are precisely the $P_i$:

IV.C.8. PROPOSITION ("Prime avoidance lemma"). *Given prime ideals $P_1, \ldots, P_n \subset R$, any ideal $I \subset P_1 \cup \cdots \cup P_n$ is contained in some $P_j$.*

PROOF. Inductively assume the result for fewer than $n$ primes. Then the only way it can fail for $n$ primes is if $I \not\subset \mathsf{U}_j := \cup_{i \neq j} P_i$ for each $j$. Suppose this, pick elements $\imath_j \in I \backslash (I \cap \mathsf{U}_j) \subset I \cap P_j$ ("only in $P_j$"), and put $\imath := \imath_1 \cdots \imath_{n-1} + \imath_n \in I \subset P_1 \cup \cdots \cup P_n$. Clearly $\imath \in P_{i_0}$ for some $i_0$. If $i_0 < n$, then $(\imath_1 \cdots \imath_{n-1} \in P_{i_0} \implies)$ $\imath_n \in P_{i_0}$ yields a contradiction. If $i_0 = n$, then we get $\imath_1 \cdots \imath_{n-1} \in P_n$, which contradicts primality of $P_n$ (since it doesn't contain $\imath_1, \ldots, \imath_{n-1}$). □

IV.C.9. REMARK. The reason for the name is the contrapositive statement: if $I \not\subset P_1, \ldots, P_n$, then there exists $a \in I$ avoiding all the primes: $a \notin P_1 \cup \cdots \cup P_n$.

To get a feel for what this says in an "algebro-geometric" setting, think of $R = \mathbb{C}[x_1, \ldots, x_n]$ as the "ring of regular functions on $\mathbb{C}^n$", and let $I$ be an ideal comprising functions whose common vanishing locus is a curve $C \subset \mathbb{C}^n$ (1-dimensional variety). If each $P_j$ is (say) a maximal ideal, comprising functions whose common vanishing locus is a single point $q_j \in \mathbb{C}^n$, then $I \not\subset P_j$ means that there is a function $f_j$ vanishing on $C$ that doesn't vanish on $q_j$, i.e. $q_j \notin C$. What IV.C.8 then tells us is that there exists a *single* function $f$ vanishing on $C$ with $f(q_i) \neq 0$ $(\forall i)$.

**Primes and finite generation.**

IV.C.10. PROPOSITION. *An ideal which is maximal in the set of non-finitely-generated ideals is prime.*

PROOF. Suppose $P$ is maximal in this set, $a_1, a_2 \notin P$, and $a_1 a_2 \in P$; we aim for a contradiction. By maximality of $P$, $P + (a_j)$ is finitely generated, taking the form $(p_{1j} + r_{1j}a_j, \ldots, p_{nj} + r_{nj}a_j)$ with $p_{ij} \in P$.

Define an ideal $J := \{r \in R \mid ra_1 \in P\}$; since $a_1 a_2 \in P$, we have $(p_{i2} + r_{i2}a_2)a_1 = p_{i2}a_1 + r_{i2}a_2 a_1 \in P \; (\forall i) \implies (P \subsetneq)\, P + (a_2) \subset J$. By maximality of $P$, $J$ is finitely generated; write $J = (\jmath_1, \ldots, \jmath_m)$.

Given $x \in P$, we have $x \in P + (a_1)$

$$\begin{aligned}
&\implies \exists \{s_i\}_{i=1}^{n} \subset R \text{ s.t. } x = \textstyle\sum_i s_i(p_{i1} + r_{i1}a_1) = \sum_i s_i p_{i1} + \sum_i s_i r_{i1} a_1 \\
&\implies (\textstyle\sum_i s_i r_{i1}) a_1 = x - \sum_i s_i p_{i1} \in P \\
&\implies \textstyle\sum_i s_i r_{i1} \in J \text{ (by defn of } J\text{)} \\
&\implies \exists \{t_k\}_{k=1}^{m} \in R \text{ s.t. } \textstyle\sum_i s_i r_{i1} = \sum_k t_k \jmath_k \\
&\implies x = \textstyle\sum_i s_i p_{i1} + \sum_k t_k \jmath_k a_1,
\end{aligned}$$

whence $P = (p_{11}, \ldots, p_{n1}, \jmath_1 a_1, \ldots, \jmath_m a_1)$, which is absurd. □

This last result allows us to connect prime ideals to the ACC, strengthening the equivalence between Noetherianity and finite generation of *all* ideals in IV.B.10:

IV.C.11. THEOREM (Cohen). *$R$ is Noetherian $\iff$ every prime ideal is finitely generated.*

PROOF. [Prefatory note: only the " $\Longleftarrow$ " direction is new. Intuitively, we might expect it to be true (from our experience with number rings) by decomposing arbitrary ideals as products of prime ideals, obtaining f.g. of the former from f.g. of the latter, and applying IV.B.10. But this doesn't work, because general ideals in fairly simple Noetherian rings like $\mathbb{C}[x, y]$ fail to decompose as products of primes. So the proof looks completely different.]

Assume that all primes are f.g., and suppose the set $\mathbb{S} := \{I \subset R \mid I \text{ non-f.g.}\}$ is nonempty. Then it is partially ordered by inclusion; and for any chain $\{I_\alpha\} \subset \mathbb{S}$, the union $\cup_\alpha I_\alpha =: I$ is an ideal containing every $I_\alpha$.

Suppose $I$ is f.g.: if $I = (r_1, \ldots, r_k)$, then each generator is in some $I_\alpha$. By the total ordering on ideals in the chain, the $\{r_k\}$ all belong to some $I_{\alpha_0}$. But then $I$ lies inside that $I_{\alpha_0}$, so $I = I_{\alpha_0}$ is not f.g., a contradiction.

So every chain in $\mathbb{S}$ has an upper bound *in* $\mathbb{S}$, and we may apply Zorn to obtain a maximal element $P \in \mathbb{S}$. This is prime by IV.C.10. But then by hypothesis, it is f.g., a contradiction. So $\mathbb{S} = \emptyset$. □