IDEAL THEORY AND PRÜFER DOMAINS

FELIX GOTTI

Radical and Primary Ideals

In this lecture, we will discuss two generalizations of prime ideals, namely, radical and primary ideals. Although radical and primary ideals have intrinsic value by themselves, the main purpose of this lecture is to settle the ground for the Noether-Lasker Theorem on primary decompositions, which we shall prove in the next lecture. Throughout this lecture, R is a commutative ring with identity.

Radical Ideals. Recall that every proper ideal of R is contained in a maximal ideal. The *radical* (or *nilradical*) of a proper ideal I of R, denoted by $\operatorname{Rad} I$, is the intersection of all prime ideals of R containing I. In addition, $\operatorname{Rad} R = R$. The ideal I is *radical* if $\operatorname{Rad} I = I$. Clearly, every prime ideal is radical. The converse does not hold: indeed, $6\mathbb{Z}$ is a radical ideal of $\mathbb{Z}$ that is not prime.

Example 1. In $\mathbb{Z}$, the radical of $18\mathbb{Z}$ is $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$ and the radical of both $9\mathbb{Z}$ and $27\mathbb{Z}$ is the ideal $3\mathbb{Z}$.

Proposition 2. *Let R be a commutative ring with identity, and let $I, I_1, \dots, I_n$ be ideals of R. Then the following statements hold.*

(1) $\operatorname{Rad} I = \{r \in R : r^n \in I \text{ for some } n \in \mathbb{N}\}$.

(2) $\operatorname{Rad}(\operatorname{Rad} I) = \operatorname{Rad} I$.

(3) $\operatorname{Rad} I_1 \cdots I_n = \operatorname{Rad}\left(\bigcap_{j=1}^n I_j\right) = \bigcap_{j=1}^n \operatorname{Rad} I_j$, *and so* $\operatorname{Rad} I^n = \operatorname{Rad} I$.

Proof. (1) If $I = R$, then the desired equality clearly holds. So we assume that I is a proper ideal. Set $J := \{r \in R : r^n \in I \text{ for some } n \in \mathbb{N}\}$, and let us verify that $J = \operatorname{Rad} I$. If $r \in J$, then for every prime ideal P containing I, there is an $n \in \mathbb{N}$ such that $r^n \in P$ and, therefore, $r \in P$. This implies that $J \subseteq \operatorname{Rad} I$. To argue the reverse inclusion, take $r \in R \setminus J$. Now set $M := \{r^n + a \mid n \in \mathbb{N} \text{ and } a \in I\}$, and note that M is a multiplicative subset of R that is disjoint from I. Therefore I is contained in a prime ideal P that is disjoint from M. Observe that $r \notin P$, which implies that $r \notin \operatorname{Rad} I$. As a result, $\operatorname{Rad} I \subseteq J$.

(2) If $r \in \operatorname{Rad}(\operatorname{Rad} I)$, then it follows from part (1) that $r^m \in \operatorname{Rad} I$ for some $m \in \mathbb{N}$ and also that $r^{mn} = (r^m)^n \in I$ for some $n \in \mathbb{N}$, whence $r \in \operatorname{Rad} I$. Thus, $\operatorname{Rad}(\operatorname{Rad} I) \subseteq \operatorname{Rad} I$. The reverse inclusion follows from the fact that $I \subseteq \operatorname{Rad} I$.

(3) Since $I_1 \cdots I_n \subseteq \bigcap_{j=1}^n I_j$, we see that $\operatorname{Rad} I_1 \cdots I_n \subseteq \operatorname{Rad}\big(\bigcap_{j=1}^n I_j\big)$. In addition, as $\bigcap_{j=1}^n I_j \subseteq I_i$ for every $i \in \mathbb{N}$, the inclusion $\operatorname{Rad}\big(\bigcap_{j=1}^n I_j\big) \subseteq \bigcap_{j=1}^n \operatorname{Rad} I_j$ holds. Finally, if $r \in \bigcap_{j=1}^n \operatorname{Rad} I_j$, then part (1) ensures the existence of $m_1, \dots, m_n \in \mathbb{N}$ such that $r^{m_j} \in I_j$ for every $j \in [\![1, n]\!]$, and so $r^{m_1 + \cdots + m_n} \in I_1 \cdots I_n$, which implies that $r \in \operatorname{Rad} I_1 \cdots I_n$. Hence $\bigcap_{j=1}^n \operatorname{Rad} I_j \subseteq \operatorname{Rad} I_1 \cdots I_n$. The second statement is a special case of the first one. □

As a consequence of part (1) of Proposition 2, we obtain the following corollary.

Corollary 3. *Let R be a Noetherian commutative ring with identity. Then for every ideal I there exists $n \in \mathbb{N}$ such that $(\operatorname{Rad} I)^n \subseteq I$.*

Proof. Let I be an ideal of R. Since R is a Noetherian ring, we can write $\operatorname{Rad} I = Ra_1 + \cdots + Ra_k$ for some $a_1, \dots, a_k \in \operatorname{Rad} I$. By virtue of Proposition 2, we can take $n_1, \dots, n_k$ such that $a_1^{n_1}, \dots, a_k^{n_k} \in I$. Set $n = n_1 + \cdots + n_k$. Observe that every element of $(\operatorname{Rad} I)^n$ is generated by elements of the form $a_1^{m_1} \cdots a_k^{m_k}$ for some $m_1, \dots, m_k \in \mathbb{N}_0$ with $m_1 + \cdots + m_k = n$, in which case, $m_i \ge n_i$ for some $i \in [\![1, k]\!]$ and so $a_1^{m_1} \cdots a_k^{m_k} \in Ra_i^{n_i} \subseteq I$. Hence $(\operatorname{Rad} I)^n \subseteq I$. □

It follows as an immediate consequence of Corollary 3 that in a Noetherian ring with identity every ideal contains a power of its radical. Here is a related result.

Proposition 4. *Let R be a Noetherian ring with identity. Then every radical ideal of R is the intersection of finitely many prime ideals.*

Proof. Suppose, by way of contradiction, that the set $\mathscr{S}$ consisting of each radical ideal of R that cannot be written as an intersection of finitely many prime ideals is nonempty. Since R is a Noetherian ring, there is a maximal element I in $\mathscr{S}$. Clearly, I cannot be a prime ideal. So we can take $x, y \in R \setminus I$ such that $xy \in I$, and then we can easily argue that $I = \operatorname{Rad}(I + Rx) \cap \operatorname{Rad}(I + Ry)$ (see Exercise 3). Since both $\operatorname{Rad}(I + Rx)$ and $\operatorname{Rad}(I + Ry)$ strictly contain I, neither $\operatorname{Rad}(I + Rx)$ nor $\operatorname{Rad}(I + Ry)$ belong to $\mathscr{S}$, and so they are both intersections of finitely many prime ideals. This implies that I can also be written as an intersection of finitely many prime ideals, contradicting that I is an element of $\mathscr{S}$. □

Recall that $r \in R$ is called *nilpotent* if $r^n = 0$ for some $n \in \mathbb{N}$. The ring R is called *reduced* if its only nilpotent element is 0. The following corollary can be easily deduced from Proposition 2(1).

Proposition 5. *Let R be a commutative ring with identity. An ideal I of R is radical if and only if R/I is a reduced ring.*

Proof. This follows immediately as for all $r \in R$ and $n \in \mathbb{N}$, the equality $(r + I)^n = I$ holds if and only if $r^n \in I$. □

Radicals are preserved under localization, as the following proposition indicates.

Proposition 6. *Let R be a commutative ring with identity, and let S be a multiplicative subset of R. Then* $\operatorname{Rad} S^{-1}I = S^{-1}\operatorname{Rad} I$.

Proof. By definition, $\operatorname{Rad} S^{-1}I$ is the intersection of all the prime ideals in $S^{-1}R$ containing the ideal $S^{-1}I$, that is, all prime ideals of the form $S^{-1}P$, where $P \in \operatorname{Spec}(R)$ with $I \subseteq P$ (as $S^{-1}I \subseteq S^{-1}P$ if and only if $I \subseteq P$). Now the fact that localization preserves intersections guarantees that

$$S^{-1}\operatorname{Rad} I = S^{-1}\Big(\bigcap_{\substack{P \in \operatorname{Spec}(R) \\ I \subseteq P}} P \Big) = \bigcap_{\substack{P \in \operatorname{Spec}(R) \\ I \subseteq P}} S^{-1}P = \operatorname{Rad} S^{-1}I.$$

□

Primary Ideals. A proper ideal Q of R is called *primary* if whenever $rs \in Q$ for some $r, s \in R$, the fact that $r \notin Q$ implies that $s^n \in Q$ for some $n \in \mathbb{N}$. Clearly, every prime ideal is primary. The converse does not hold even in $\mathbb{Z}$; for instance, $4\mathbb{Z}$ is a primary ideal that is not prime. We can easily characterize primary ideals in terms of their quotients.

Proposition 7. *Let R be a commutative ring with identity. A proper ideal Q of R is primary if and only if each zero-divisor in R/Q is nilpotent.*

Proof. Fix a proper ideal Q of R. If Q is not a primary ideal, then we can take $r, s \in R$ with $rs \in Q$ and $r \notin Q$ such that $s^n \notin Q$ for any $n \in \mathbb{N}$. In this case, it is clear that $s + Q$ is a zero-divisor in R/Q that is not nilpotent. On the other hand, if for some $s \in R$, the element $s + Q$ of R/Q is a zero-divisor that is not nilpotent, then after taking $r \in R \setminus Q$ with $(r + Q)(s + Q) = Q$, we see that $rs \in Q$ but $r \notin Q$ and $s^n \notin Q$ for any $n \in \mathbb{N}$, whence Q is not a primary ideal. □

Proposition 7, in tandem with Proposition 5, immediately implies the following.

Corollary 8. *In a commutative ring with identity, an ideal is prime if and only if it is primary and radical.*

Example 9. Let $m\mathbb{Z}$ be a primary ideal of $\mathbb{Z}$, and let p be a prime dividing m. Write $m = p^k m'$ for some $k \in \mathbb{N}$ such that $p \nmid m'$. Observe that $p^k m' \in m\mathbb{Z}$ and $m' \notin m\mathbb{Z}$. Thus, the fact that $m\mathbb{Z}$ is primary ensures that some power of p^k belongs to $m\mathbb{Z}$; that is, m divides a power of p^k. This implies that $m = p^k$. Hence each primary ideal of $\mathbb{Z}$ has the form $p^k\mathbb{Z}$ for some $p \in \mathbb{P}$ and $k \in \mathbb{N}$. On the other hand, it is clear that all ideals of the form $p^k\mathbb{Z}$, where $p \in \mathbb{P}$ and $k \in \mathbb{N}$, are primary.

Take a primary ideal in $\mathbb{Z}$, namely $p^k\mathbb{Z}$, where $p \in \mathbb{P}$ and $k \in \mathbb{N}$. Observe that $\operatorname{Rad} p^k\mathbb{Z} = p\mathbb{Z}$, which is a prime ideal. This is not a coincidence, as the following proposition indicates.

Proposition 10. *Let R be a commutative ring with identity, and let Q be an ideal of R. Then the following statements hold.*

(1) *If Q is primary, then $\operatorname{Rad} Q$ is prime.*

(2) *If $\operatorname{Rad} Q$ is maximal, then Q is primary.*

(3) *If M is a maximal ideal such that $M^n \subseteq Q \subseteq M$ for some $n \in \mathbb{N}$, then Q is primary and $\operatorname{Rad} Q = M$.*

Proof. (1) Since Q is a proper ideal, so is $\operatorname{Rad} Q$. Take $r, s \in R$ such that $rs \in \operatorname{Rad} Q$ and $r \notin \operatorname{Rad} Q$. Then there is an $n \in \mathbb{N}$ with $r^n s^n \in Q$. As $r^n \notin Q$ and Q is primary, we can choose an $m \in \mathbb{N}$ with $s^{nm} = (s^n)^m \in Q$, which implies that $s \in \operatorname{Rad} Q$. Thus, $\operatorname{Rad} Q$ is prime.

(2) After replacing R by R/Q, we can assume that $M := \operatorname{Rad}(0)$ is a maximal ideal of R, and we only need to verify that every zero-divisor of R is nilpotent. Since M is contained in every prime ideal, it must be the only prime ideal of R. Now if z is a zero-divisor of R, then Rz is a proper ideal of R, and so $Rz \subseteq M$. Thus, $z \in M$, which means that z is nilpotent.

(3) Since $Q \subseteq M$, it follows that $\operatorname{Rad} Q \subseteq \operatorname{Rad} M = M$. On the other hand, $M^n \subseteq Q$ implies that $M \subseteq \operatorname{Rad} Q$ by part (1) of Proposition 2. As a result, $\operatorname{Rad} Q = M$, and so Q is primary by part (2). $\square$

Let P be a prime ideal of R. An ideal Q is called *P-primary* if Q is primary and $\operatorname{Rad} Q = P$.

For a multiplicative set S of R, we know that $I \mapsto S^{-1}I$ yields a one-to-one correspondence between the prime ideals of R disjoint from S and the prime ideals of $S^{-1}R$. A similar result holds for primary ideals.

Proposition 11. *Let R be a commutative ring with identity, and let S be a multiplicative subset of R. Prove the following statements.*

(1) *If P is a prime ideal disjoint from S and Q is a P-primary ideal of R, then $S^{-1}Q$ is an $S^{-1}P$-primary ideal of $S^{-1}R$.*

(2) *$I \mapsto S^{-1}I$ induces a bijection between the set of primary ideals of R disjoint from S and the set of primary ideals of $S^{-1}R$.*

Proof. (1) Let P be a prime ideal of R disjoint from S, and let Q be a P-primary ideal. Suppose that $(r_1/s_1)(r_2/s_2) \in S^{-1}Q$ for some $r_1, r_2 \in R$ and $s_1, s_2 \in S$ while $r_1/s_1 \notin S^{-1}Q$. Then $(r_1 r_2 s_3 - r_3 s_1 s_2)s_4 = 0$ for some $r_3 \in Q$ and $s_3, s_4 \in S$, and so $r_1 r_2 s_3 s_4 \in Q$. Therefore, as Q is primary, the fact that no positive power of $s_3 s_4$ belongs to Q ensures that $r_1 r_2 \in Q$. Thus, $r_1 \notin Q$ implies that $r_2^n \in Q$ for some $n \in \mathbb{N}$. Hence $(r_2/s_2)^n = r_2^n/s_2^n \in S^{-1}Q$. Hence $S^{-1}Q$ is a primary ideal. In addition, as Q is P-primary, it follows from Proposition 6 that $\operatorname{Rad} S^{-1}Q = S^{-1}\operatorname{Rad} Q = S^{-1}P$, whence $S^{-1}Q$ is an $S^{-1}P$-primary ideal of $S^{-1}R$.

(2) It suffices to fix a prime ideal P of R disjoint from S and show that the extension map e induces a bijection from the set $\mathscr{I}$ consisting of P-primary ideals of R to the set $\mathscr{J}$ consisting of $S^{-1}P$-primary ideals of $S^{-1}R$. It follows from part (1) that the map $e\colon \mathscr{I} \to \mathscr{J}$ is well defined. In addition, the contraction map $c\colon \mathscr{J} \to \mathscr{I}$ is also well defined because being primary is preserved under taking homomorphic inverse images (check this!). As $e \circ c$ is the identity of $\mathscr{J}$, we are done once we argue that $c \circ e$ is the identity of $\mathscr{I}$. To do so, fix $Q \in \mathscr{I}$. We already know that $Q \subseteq c(e(Q))$. For the reverse inclusion, take $r \in c(e(Q))$ and write $r/1 = q/s$ for some $q \in Q$ and $s \in S$. Then $s'(sr - q) = 0$ for some $s' \in S$, and so $(s's)r \in Q$. Since no power of $s's$ belongs to Q, the fact that Q is primary ensures that $r \in Q$. Hence $c \circ e$ is the identity of $\mathscr{I}$, as desired. □

Exercises

Exercise 1. *Let R be a commutative ring with identity. Prove that*

$$\operatorname{Rad}(I + J) = \operatorname{Rad}(\operatorname{Rad} I + \operatorname{Rad} J)$$

for any ideals I and J of R.

Exercise 2. *Let k be a field. Consider the ideals $I = (x^2 - y)$ and $J = (x^2 + y)$ of the polynomial ring $k[x, y]$.*

(1) *Argue that both I and J are prime ideals.*

(2) *Argue that $I + J$ is not a radical ideal provided that k has characteristic zero (or different from 2).*

(3) *Conclude that the addition of radical ideals may not be a radical ideal, even inside a Noetherian ring.*

Exercise 3. *Let R be a commutative ring with identity, and let I be a radical ideal of R. Show that for any $x, y \in R$ with $xy \in I$, the following equality holds:*

$$I = \operatorname{Rad}(I + Rx) \cap \operatorname{Rad}(I + Ry).$$

Exercise 4. *Let R be a commutative ring with identity. For any ideal I of R, prove that the following conditions are equivalent.*

(a) *I is a radical ideals.*

(b) *For each $r \in R$, if $r^2 \in I$, then $r \in I$.*

Deduce that if R is a UFD, a nontrivial principal ideal (a) is radical if and only if a is a squarefree.

Exercise 5. *Let R be a commutative ring with identity, and let I be a proper ideal of R. Prove that the following conditions are equivalent.*

(a) $\operatorname{Rad} I$ *is a prime ideal of* R.

(b) *There exists a unique minimal prime ideal over* I.

(c) *For all* $r, s \in R$ *with* $rs \in I$, *there exists* $n \in \mathbb{N}$ *such that either* $r^n \in I$ *or* $s^n \in I$.

If I satisfies the previous conditions, then I is called semiprimary*. Assuming that R is a UFD and $x \in R$ is a nonzero nonunit, prove that the ideal (x) is semiprimary if and only if x is associate to a power of a prime element of R.*

Exercise 6. *Let k be a field, and consider the ideal $I = (x, y^2)$ of $k[x, y]$.*

(1) *Prove that I is a primary ideal with* $\operatorname{Rad} I = (x, y)$.

(2) *Argue that I is not a power of (x, y).*

(3) *Deduce that primary ideal may not be a power of a prime ideal (even in the context of Noetherian rings).*

Exercise 7. *Let k be a field, and consider the ideal $I = (x^2, xy)$ of $k[x, y]$.*

(1) *Prove that* $\operatorname{Rad} I = (x)$.

(2) *Argue that I is not a primary ideal.*

(3) *Deduce that ideals with prime radical may not be primary (even in the context of Noetherian rings).*

Exercise 8. *Let R be the subring of all polynomials in $\mathbb{Z}[x]$ having their coefficients corresponding to x divisible by 3. Show that $P = (3x, x^2, x^3)$ is a prime ideal of R satisfying that P^2 is not primary. Deduce that powers of prime ideals may not be primary.*

Department of Mathematics, MIT, Cambridge, MA 02139
Email address: fgotti@mit.edu