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. $\operatorname{Rad} I = \{r \in R : r^n \in I$ *for some* $n \in \mathbb{N}\}$.
2. $\operatorname{Rad}(\operatorname{Rad} I) = \operatorname{Rad} I$.
3. $\operatorname{Rad} I_1 \cdots I_n = \operatorname{Rad}\big(\bigcap_{j=1}^n I_j\big) = \bigcap_{j=1}^n \operatorname{Rad} I_j$, *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 $r \in R \setminus J$, and then take $r \in J$ such that $r^n \notin$. 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 $\text{Rad}\, I_1 \cdots I_n \subseteq \text{Rad}\left(\bigcap_{j=1}^n I_j\right)$. In addition, as $\bigcap_{j=1}^n I_j \subseteq I_i$ for every $i \in \mathbb{N}$, the inclusion $\text{Rad}\left(\bigcap_{j=1}^n I_j\right) \subseteq \bigcap_{j=1}^n \text{Rad}\, I_j$ holds. Finally, if $r \in \bigcap_{j=1}^n \text{Rad}\, I_j$, 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 $r \in \text{Rad}\, I_1 \cdots I_n$. Hence $\bigcap_{j=1}^n \text{Rad}\, I_j \subseteq \text{Rad}\, I_1 \cdots I_n$. 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 commutative ring with identity. If I is a finitely generated ideal of R, then there is a power of* $\text{Rad}\, I$ *contained in 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 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 $I = \text{Rad}(I + Rx) \cap \text{Rad}(I + Ry)$ (see Exercise 3). Since both $\text{Rad}(I + Rx)$ and $\text{Rad}(I + Ry)$ strictly contain I, neither $\text{Rad}(I + Rx)$ nor $\text{Rad}(I + Ry)$ 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).

Corollary 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.*

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* $\text{Rad}\, S^{-1}I = S^{-1}\text{Rad}\, I$.

Proof. Exercise. □

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. However, observe that $\operatorname{Rad} 4\mathbb{Z} = 2\mathbb{Z}$, which is a prime ideal. In contrast to Corollary 5, observe that an ideal Q of R is primary if and only if each zero-divisor in R/Q is nilpotent.

Proposition 7. *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). ☐

From Proposition 7, we immediately deduce the following.

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

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

Proposition 9. *If $Q_1, \dots, Q_n$ are P-primary ideals of R for some prime ideal P, then $\bigcap_{j=1}^n Q_j$ is also a P-primary ideal.*

Proof. Set $I := \bigcap_{j=1}^n Q_j$, and let us verify that $\operatorname{Rad} I = P$. Since $Q_i \subseteq P$ for every $i \in [\![1, n]\!]$, it follows that $I \subseteq P$, which implies that $\operatorname{Rad} I \subseteq P$. To argue the reverse inclusion, take a prime ideal P' containing I. Since $Q_1 \cdots Q_n \subseteq I \subseteq P'$, it follows that $Q_i \subseteq P'$ for some $i \in [\![1, n]\!]$. Thus, $P = \operatorname{Rad} Q_i \subseteq P'$. As a consequence, $P \subseteq \operatorname{Rad} I$. Hence $\operatorname{Rad} I = P$, which means that $\bigcap_{j=1}^n Q_j$ is a P-primary ideal. ☐

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 10. *Let R be a commutative ring with identity, and let S be a multiplicative subset of R. Then the following statements hold.*

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

Proof. Exercise. □

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.*
(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, and let S be a multiplicative subset of R. Prove that $\operatorname{Rad} S^{-1}I = S^{-1}\operatorname{Rad} I$.*

Exercise 5. *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.*

Exercise 6. *Let R be a commutative ring with identity, and let S be a multiplicative subset of R. Prove the following statements.*

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

(2) *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 $S^{-1}R$.*

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