IDEAL THEORY ON PRÜFER DOMAINS

FELIX GOTTI

Miscellaneous on Prime Ideals

Throughout this lecture, we assume that R is a commutative ring with identity.

Existence of Prime Ideals. Every proper ideal of R is contained in a maximal ideal (Corollary 2). To argue such a result, one needs to appeal to Zorn's lemma, which is a statement equivalent to the Axiom of Choice. Zorn's lemma states that a nonempty partially ordered set (poset) S contains a maximal element provided that every totally ordered subset of S has an upper bound.

Theorem 1. *Let R be a commutative ring with identity, and let I be a proper ideal of R. If M is a multiplicative submonoid of $(R \setminus \{0\}, \cdot)$ disjoint from I, then there exists an ideal P that is maximal in the set of all ideals of R disjoint from M and containing I. Moreover, P is prime.*

Proof. Let $\mathscr{S}$ be the set of all ideals of R disjoint from M and containing I. The set $\mathscr{S}$ is nonempty because $I \in \mathscr{S}$. Clearly, $\mathscr{S}$ is a partially ordered set (under inclusion). In addition, if $\mathscr{T} := \{I_\gamma : \gamma \in \Gamma\}$ is a totally ordered subset of $\mathscr{S}$, then it is not hard to verify that $J = \bigcup_{\gamma \in \Gamma} I_\gamma$ is a proper ideal of R disjoint from M and containing I. Thus, J is an upper bound of $\mathscr{T}$ in $\mathscr{S}$. Now Zorn's lemma guarantees the existence of a maximal element P in $\mathscr{S}$, which yields the first part of the theorem.

Now we show that P is indeed a prime ideal. Suppose, by way of contradiction, that $JK \subseteq P$ for ideals J and K of R none of them contained in P. So both ideals $J + P$ and $K + P$ properly contain P, which means that they both intersect M. Take $p_1, p_2 \in P$, $j \in J$ and $k \in K$ such that $m_1 := p_1 + j \in M$ and $m_2 := p_2 + k \in M$. Then we see that

$$m_1 m_2 = p_1 p_2 + k p_1 + j p_2 + jk \in P + JK \subseteq P.$$

Since M is closed under multiplication, $m_1 m_2 \in P \cap M$, contradicting that P is disjoint from M. Thus, P is a prime ideal. □

As an immediate consequence of Theorem 1, we obtain the following result.

Corollary 2. *Let R be a commutative ring with identity. Then every proper ideal of R is contained in a maximal ideal.*

Given a proper ideal I of R, a *minimal prime ideal over* I is an ideal that is minimal in the set of all prime ideals of R containing I. A *minimal prime ideal* is, by definition, a minimal prime ideal over the zero ideal. Minimal prime ideals over a given ideal always exist.

Proposition 3. *Let R be a commutative ring with identity. If I is a proper ideal of R, then there exists a prime ideal that is minimal over I.*

Proof. Since I is a proper ideal, it follows from Corollary 2 that I is contained in a maximal ideal of R and, therefore, the set $\mathscr{P}$ consisting of all prime ideals of R containing I is nonempty. We consider $\mathscr{P}$ as a poset under reverse inclusion. One can easily verify that the intersection of all the ideals in a decreasing chain of prime ideals is also a prime ideal. Therefore it follows from Zorn's lemma that $\mathscr{P}$ has a maximal element, which is clearly a minimal prime ideal over I. □

Corollary 4. *Every commutative ring with identity contains a minimal prime ideal.*

On Union of Prime Ideals. The following proposition on prime ideals is often useful.

Proposition 5. *Let R be a commutative ring with identity, and let S be a subring of R. If for prime ideals $P_1, \dots, P_n$ the inclusion $S \subseteq \bigcup_{i=1}^n P_i$ holds, then $S \subseteq P_j$ for some $j \in [\![1, n]\!]$.*

Proof. Suppose, by way of contradiction, that $S \nsubseteq P_j$ for any $j \in [\![1, n]\!]$, and further assume that n has been taken as small as possible. It is clear that $n \ge 2$. Then for every $j \in [\![1, n]\!]$, we can take $s_j \in S$ such that $s_j \notin \bigcup_{i \neq j} P_i$. Since $s_1 + s_2 \cdots s_n \in S \subseteq \bigcup_{i=1}^n P_i$, there is a $k \in [\![1, n]\!]$ such that $s_1 + s_2 \cdots s_n \in P_k$. The fact that $s_1 \notin \bigcup_{i=2}^n P_i$ ensures that $k = 1$. This implies that $s_2 \cdots s_n \in P_1$. Because P_1 is a prime ideal, $s_j \in P_1$ for some $j \in [\![2, n]\!]$, contradicting that $s_j \notin \bigcup_{i \neq j} P_i$. □

A Characterization of PIDs. In a PID, by definition, every ideal is principal. We can actually characterize PIDs by imposing the condition of being principal only to the prime ideals.

Theorem 6. *For an integral domain R, the following statements are equivalent.*

(a) *R is a PID.*

(b) *Every prime ideal of R is principal.*

Proof. (a) $\Rightarrow$ (b): It is obvious.

(b) $\Rightarrow$ (a): Suppose that every prime ideal of R is principal. Assume, by way of contradiction, that R is not a PID, and so that there is an ideal of R that is not principal. Then the set $\mathscr{S}$ consisting of all non-principal ideals of R is a nonempty partially ordered set. Suppose that $\{I_\gamma : \gamma \in \Gamma\}$ is a chain in $\mathscr{S}$. It is not hard to verify that $I := \bigcup_{\gamma \in \Gamma} I_\gamma$ is a non-principal ideal of R and, therefore, an upper bound for the given chain. Then $\mathscr{S}$ contains a maximal element M by Zorn's lemma.

Since M is not principal, it cannot be prime. Thus, there exist $x, x' \in R \setminus M$ such that $xx' \in M$. Since the ideals $I := M + (x)$ and $I' := M + (x')$ properly contain M, the maximality of M in $\mathscr{S}$ guarantees the existence of $\alpha \in R$ such that $I = (\alpha)$. Define $K := (M : I) = \{r \in R : rI \subseteq M\}$. One can easily check that $I' \subseteq K$, and so $M \subsetneq K$. So K must be principal, and we can take $\beta \in R$ such that $K = (\beta)$.

It follows from the definition of K that $KI \subseteq M$. We claim that the reverse inclusion also holds. To show this, take $a \in M$. Since $M \subseteq I$, we can write $a = r\alpha$ for some $r \in R$. Observe that $r \in K$ and, therefore, $a = r\alpha \in KI$. Hence $M \subseteq KI$. Thus, $M = KI = (\alpha\beta)$, contradicting the fact that M belongs to $\mathscr{S}$. □

Exercises

Exercise 1. *Let R be a commutative ring with identity. Prove the following statements.*

1. *If $a \in R$ and I is an ideal of R such that $I + Ra$ and $(I : Ra)$ are finitely generated, then I is finitely generated.*
2. *If the collection $\mathscr{S}$ of all ideals of R that are not finitely generated is nonempty, then $\mathscr{S}$ has a maximal element.*
3. *If such a maximal element from the previous statement exists, then it is a prime ideal of R.*
4. *Cohen's theorem: R is a Noetherian ring if and only if every prime ideal of R is finitely generated.*

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