IDEAL THEORY ON PRÜFER DOMAINS

FELIX GOTTI

Lecture 1: Prime and Maximal Ideals

Let R be a commutative ring with identity. Recall that a proper ideal P of R is prime if whenever $IJ \subseteq P$ for ideals I and J in R, either $I \subseteq P$ or $J \subseteq P$. In addition, a proper ideal M of R is maximal if for any ideal I with $M \subseteq I \subseteq R$, either $I = M$ or $I = R$.

Proposition 1. *Let R be a commutative ring with identity, and let I be an ideal of R. Then the following statements hold.*

(1) *I is prime if and only if R/I is an integral domain.*
(2) *I is maximal if and only if R/I is a field.*

Proof. Exercise. □

Corollary 2. *Every maximal ideal is prime.*

Not every prime ideal, however, is maximal.

Example 3. The ideal (x) is prime in the ring $\mathbb{Z}[x]$. However, (x) is not a maximal ideal because (x) is strictly contained in the ideal $(x, 2)$, which is a proper ideal of $\mathbb{Z}[x]$.

For a commutative ring with identity, every proper ideal is contained in a maximal ideal (Corollary 5). 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 chain in S has an upper bound.

Theorem 4. *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 $\{I_\gamma : \gamma \in \Gamma\}$ is a chain in $\mathscr{S}$, 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 the given chain 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 $m_2 := p_2 + k \in M$. As a consequence,

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

Since M is closed under multiplication, $m_1 m_2 \in P \cap M$. However, this contradicts that P is disjoint from M. Therefore we can conclude that P is a prime ideal. □

As an immediate consequence of Theorem 4, we obtain the following result.

Corollary 5. *Let R be a commutative ring with identity. Then every proper ideal of R is contained in a maximal ideal.*

The following proposition on prime ideals is often useful.

Proposition 6. *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. Exercise. □

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 7. *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 $\mathscr{S}$. □

Remark 8. PIDs are among the most tractable and understood Prüfer domains, as we shall see in further lectures (unlike PIDs, UFDs are not Prüfer domains).

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