

# IDEAL THEORY ON PRÜFER DOMAINS

FELIX GOTTI

## 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. One can actually use Zorn's lemma to argue the following result, which is stronger than the fact that every proper ideal is contained in a maximal ideal.

**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  $R$  disjoint from  $I$ , then there exists an ideal  $P$  that is maximal in the set consisting of all ideals of  $R$  disjoint from  $M$  and containing  $I$ . Moreover,  $P$  is prime.*

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

Now we show that  $P$  is indeed a prime ideal. Suppose, by way of contradiction, that  $J_1 J_2 \subseteq P$  for ideals  $J_1$  and  $J_2$  of  $R$  none of them contained in  $P$ . Then both ideals  $J_1 + P$  and  $J_2 + P$  properly contain  $P$ , which means that they both intersect  $M$ . Take  $p_1, p_2 \in P$ ,  $j_1 \in J_1$  and  $j_2 \in J_2$  such that  $m_1 := p_1 + j_1 \in M$  and  $m_2 := p_2 + j_2 \in M$ . Thus, we see that

$$m_1 m_2 = p_1 p_2 + j_2 p_1 + j_1 p_2 + j_1 j_2 \in P + J_1 J_2 \subseteq P.$$

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

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  $R$  and  $P$  is a prime ideal containing  $I$ , then there exists a prime ideal contained in  $P$  that is minimal over all prime ideals containing  $I$ .*

*Proof.* Let  $\mathcal{P}$  be the set consisting of all prime ideals of  $R$  containing  $I$ . Since  $P \in \mathcal{P}$ , the set  $\mathcal{P}$  is nonempty. We consider  $\mathcal{P}$  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 (see Exercise 1). Therefore it follows from Zorn's lemma that  $\mathcal{P}$  has a maximal element, which is clearly a minimal prime ideal over  $I$ .  $\square$

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

**Unions and Intersections of Prime Ideals.** The following proposition on prime ideals, which is called the Prime Avoidance Lemma, is often useful.

**Proposition 5** (Prime Avoidance Lemma). *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  $j \in \llbracket 1, n \rrbracket$ .*

*Proof.* Suppose, by way of contradiction, that  $S \not\subseteq P_j$  for any  $j \in \llbracket 1, n \rrbracket$ , and further assume that  $n$  has been taken as small as possible. It is clear that  $n \geq 2$ . Then for every  $j \in \llbracket 1, n \rrbracket$ , 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  $k \in \llbracket 1, n \rrbracket$  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  $j \in \llbracket 2, n \rrbracket$ , contradicting that  $s_j \notin \bigcup_{i \neq j} P_i$ .  $\square$

A multiplicative submonoid  $S$  of  $R \setminus \{0\}$  is called *saturated* or *divisor-closed* provided that for all  $x \in S$  if  $y \in R$  divides  $x$  in  $R$ , then  $y \in S$ . It turns out that the complement of any saturated multiplicative submonoid of  $R$  is the union of prime ideals.

**Proposition 6.** *Let  $R$  be a commutative ring with identity, and let  $S$  be a subset of  $R$ . Then  $S$  is a saturated multiplicative submonoid of  $R \setminus \{0\}$  if and only if  $R \setminus S$  is the union of prime ideals.*

*Proof.* For the direct implication, suppose that  $S$  is a saturated multiplicative submonoid of  $R \setminus \{0\}$ . Now fix  $x \in R \setminus S$ . Because  $S$  is saturated  $x \notin R^\times$ , and so the principal ideal  $Rx$  is proper. Then it follows from Corollary 2 that  $x$  is contained in a prime ideal. Thus,  $R \setminus S$  is the union of prime ideals.

Conversely, suppose that  $R \setminus S$  is the union of prime ideals. Since no prime ideal contains 1, we see that  $1 \in S$ . To check that  $S$  is closed under multiplication, take  $x_1, x_2 \in R$  with  $x_1x_2 \notin S$ , then there exists a prime ideal  $P$  contained in  $R \setminus S$  such that  $x_1x_2 \in P$ , which implies that either  $x_1 \in P$  or  $x_2 \in P$ , that is, either  $x_1 \notin S$  or  $x_2 \notin S$ . Hence  $S$  is a multiplicative submonoid of  $R \setminus \{0\}$ . Finally, suppose that  $x \in S$ , and take  $y \in R$  such that  $y \mid_R x$ . Observe that if  $y \notin S$ , then there would exist a prime ideal  $P'$  disjoint from  $S$  such that  $y$ , and therefore  $x$ , belongs to  $P'$ . Hence  $S$  is saturated.  $\square$

**Example 7.** The group of units  $R^\times$  is clearly a saturated multiplicative submonoid of  $R^*$ . It is clear that the complement of  $R^\times$  is the union of prime ideals; for instance, by virtue of Corollary 2, we can take such a union to consist of all maximal ideals of  $R$ .

**Example 8.** Let  $R$  be an integral domain, and let  $S$  be the subset of  $R$  consisting of all elements that can be written as a product of primes. It is an easy exercise to verify that  $S$  is a multiplicative subset, where 1 can be thought of as the empty product of primes. Then the complement of  $S$  is the union of prime ideals. Observe that when  $R$  is an integral domain the complement of  $S$  consisting only of the zero prime ideal.

**Example 9.** The set consisting of all elements of  $R$  that are not zero-divisors is easily seen to be a saturated multiplicative submonoid of  $R^*$ . The complement  $\mathcal{Z}(R)$ , that is, the set of zero-divisors of  $R$ , is then the union of prime ideals of  $R$ . The prime ideals maximal with respect to the property of being contained in  $\mathcal{Z}(R)$  will be useful in coming lectures.

**Characterizations of PIDs, UFDs, and Noetherian Rings.** We can certainly use prime ideals to characterize PIDs, UFDs, and Noetherian rings. We proceed to argue this in the next three results.

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

**Theorem 10.** *Let  $R$  be an integral domain. Then  $R$  is a PID if and only if each prime ideal of  $R$  is principal.*

*Proof.* The direct implication follows directly from the definition.

For the reverse implication, 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  $\mathcal{S}$  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  $\mathcal{S}$ . 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  $\mathcal{S}$  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  $\mathcal{S}$  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  $\mathcal{S}$ .  $\square$

As mentioned earlier, we can also characterize UFDs in terms of prime ideals.

**Theorem 11.** *Let  $R$  be an integral domain. Then  $R$  is a UFD if and only if each nonzero prime ideal contains a prime element.*

*Proof.* For the direct implication, suppose that  $R$  is a UFD, and let  $P$  be a nonzero prime ideal of  $R$ . Now take a nonzero  $r \in P$ , and use the fact that  $R$  is a UFD to write  $r = p_1 \cdots p_k$  for some prime elements  $p_1, \dots, p_k$  in  $R$ . As  $P$  is prime,  $p_j \in P$  for some  $j \in \llbracket 1, k \rrbracket$ .

Conversely, assume that every nonzero prime ideal of  $R$  contains a prime element. Let  $S$  denote the set of elements of  $R$  that can be written as a product of primes. We have seen before that  $S$  is a saturated multiplicative subset and, therefore, it follows from Proposition 6 that  $R \setminus S$  is the union of prime ideals. Now fix  $x \in R \setminus S$ . Since  $S$  is saturated, the ideal  $Rx$  is disjoint from  $S$  and, therefore, Theorem 1 ensures the existence of a prime ideal  $P$  disjoint from  $S$  such that  $Rx \subseteq P$ . As every nonzero prime ideal contains a prime element,  $P \cap S = \emptyset$  implies that  $P$  is the zero ideal, and so  $x = 0$ . Thus, every nonzero element of  $R$  is a product of primes, which means that  $R$  is a UFD.  $\square$

We conclude this lecture with the statement of a result that is often referred to as Cohen's theorem, which is a characterization of Noetherian domains in terms of prime ideals. A proof of this result is outlined as an exercise.

**Theorem 12.** *Let  $R$  be a commutative ring with identity. Then  $R$  is Noetherian if and only if each prime ideal of  $R$  is finitely generated.*

## EXERCISES

**Exercise 1.** Let  $R$  be a commutative ring with identity, and let  $\mathcal{C}$  be a chain of prime ideals of  $R$ . Prove that  $\bigcap_{I \in \mathcal{C}} I$  and  $\bigcup_{I \in \mathcal{C}} I$  are also prime ideals.

**Exercise 2.** Let  $R$  be a commutative ring with identity, and let  $p$  and  $q$  be prime elements of  $R$  such that  $p$  is not a zero-divisor. Prove that  $Rp \subseteq Rq$  implies that  $Rp = Rq$ .

**Exercise 3.** Let  $R$  be a commutative ring with identity, and let  $P$  and  $Q$  be prime ideals of  $R$  such that  $P \subsetneq Q$ . Prove that there exist prime ideals  $P'$  and  $Q'$  of  $R$  satisfying the following two conditions:

- $P' \subsetneq Q'$ , and
- if  $P' \subseteq J \subseteq Q'$  for some prime ideal  $J$ , then  $J \in \{P', Q'\}$ .

**Exercise 4.** Let  $R$  be an infinite integral domain. Prove that if  $R^\times$  is finite, then  $R$  has infinitely many maximal ideals.

**Exercise 5.** Let  $R$  be a commutative ring with identity. Prove that if  $I$  is not finitely generated (resp., not principal, not countably generated) and is maximal among all ideals of  $R$  that are not finitely generated (resp., not principal, not countably generated), then  $I$  is prime.

**Exercise 6.** 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  $\mathcal{S}$  of all ideals of  $R$  that are not finitely generated is nonempty, then  $\mathcal{S}$  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.