PIDs and UFDs

Abstract

Support notes for the Algebra course of LMAC, on the relations between principal ideal domains and unique factorization domains.

Contents

0 Introduction **1**

1 PIDs are Noetherian rings **1**

2 Irreducible elements **2**

3 Reducible elements **3**

4 Unique factorization domains **5**

5 Complements **8**

0 Introduction

In what follows, R will always be assumed to be a fixed but arbitrary integral domain. We introduce the following notation:

$$\widetilde{R} = R^{\times} \cup \{0\}.$$

1 PIDs are Noetherian rings

This short section is only meant to establish a simple property of PIDs which will be needed below.

§1. Definition. R is *Noetherian* if for all ideals $I_1 \subset I_2 \subset I_3 \subset \cdots$ there is $n \in \mathbb{Z}_{\geq 1}$ such that $I_n = I_k$ for all $k \geq n$ (we say that every ascending sequence of ideals eventually *stabilizes*).

§2. Remark. The general definition of Noetherian ring, for noncommutative rings, applies both to left ideals and to right ideals, but in these notes we are assuming that R is an integral domain, so we are only concerned with commutative Noetherian rings.

§3. Lemma. *Every PID is Noetherian.*

Proof. Assume that R is a PID, and let $I_1 \subset I_2 \subset I_3 \subset \cdots$ be an ascending sequence of ideals. The union

$$I = \bigcup_{i_1}^{\infty} U_i$$

is itself an ideal (exercise: verify this), so there is $a \in R$ such that $I = (a)$. Then $a \in I$, so there is n such that $a \in I_n$, but then $(a) \subset I_n$, and thus $(a) = I_n = I_{n+1} = \cdots = I$. ∎

2 Irreducible elements

Let R be an integral domain.

§4. Definition. An element $r \in R \setminus \widetilde{R}$ is *irreducible* if for all $a, b \in R$ the condition $r = ab$ implies that either $a \in R^\times$ or $b \in R^\times$.

§5. Definition. An element $p \in R \setminus \widetilde{R}$ is *prime* if (p) is a prime ideal; that is, if for all $a, b \in R$ the condition $p \mid ab$ implies either $p \mid a$ or $p \mid b$.

§6. Definition. Elements $a, b \in R$ are *associated* if there is $u \in R^\times$ such that $a = ub$.

§7. Example. In $\mathbb{Z}$ the irreducible elements are of the form p or $-p$ for a prime p. Two primes p and q are associated if and only if $q = \pm p$.

§8. Lemma. *Any prime element is irreducible. If R is a PID the converse is true: any irreducible element is prime.*

Proof. Let $p \in R$ be prime, and let $p = ab$ for $a, b \in R$. Then $p \mid ab$, so either $p \mid a$ or $p \mid b$. Suppose $p \mid a$, and let $r \in R$ be such that $a = pr$. Then $p = prb$, so $1 = rb$ (because R is an integral domain), and thus $b \in R^\times$. Similarly, if $p \mid b$ we conclude that $a \in R^\times$, so p is irreducible.

Now assume that R is a PID, and assume that p is irreducible. In order to prove that p is prime we show that (p) is a prime ideal, for which it suffices to prove that (p) is a maximal ideal (indeed, (p) is prime if and only if (p) is maximal because R is a PID). Let I be an ideal such that $(p) \subset I$. Since R is a PID, let $I = (m)$ for some $m \in R$. Then $m \mid p$, so $p = mr$ for some $r \in R$, and thus either $m \in R^\times$ or $r \in R^\times$ because we are assuming that p is irreducible. If $m \in R^\times$ then $(m) = R$, and if $r \in R^\times$ then $(p) = (m)$, so (p) is indeed maximal. ∎

§9. EXAMPLE. In $\mathbb{Z}[\sqrt{-5}]$ there are irreducible elements which are not prime. For instance, $9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, so 3 divides the product $(2 + \sqrt{-5})(2 - \sqrt{-5})$. But 3 does not divide either of the factors, so it is not prime. However, it is irreducible. In order to verify the latter assertion, let $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ and assume that 3 is factored as $3 = \alpha\beta$. Then, for the usual norm on $\mathbb{Z}[\sqrt{-5}]$, we have $9 = N(\alpha)N(\beta)$. Let $\beta = a + b\sqrt{-5}$. Then $N(\beta) = a^2 + 5b^2$, so we obtain

$$9 = N(\alpha)(a^2 + 5b^2)$$

and there are only three possibilities compatible with the factorization of 9 into primes:

1. $a^2 + 5b^2 = 1$, in which case $a = \pm 1$ and $b = 0$, so $\beta \in R^\times$;
2. $a^2 + 5b^2 = 3$, which is impossible;
3. $a^2 + 5b^2 = 9$, in which case $N(\alpha) = 1$, so $\alpha = \pm 1 \in R^\times$.

This shows that 3 is irreducible, despite not being prime. In particular, this implies that $\mathbb{Z}[\sqrt{-5}]$ is not a PID.

§10. EXERCISE. Can there be an irreducible element which is not prime in $\mathbb{Z}[\sqrt{-1}]$?

3 Reducible elements

Let again R be an integral domain.

§11. Definition. An element $r \in R \setminus \widetilde{R}$ is *reducible* if it is not irreducible. Let us also say that the reducible element r is *finitely reducible* if r has a factorization $p_1 \cdots p_n$ for irreducible elements $p_1, \ldots, p_n$, and that it is *infinitely reducible* otherwise.

§12. Note. Note that an element r is reducible if and only if $r = r_1 r_2$ for some $r_1, r_2 \in R \setminus \widetilde{R}$.

§13. Lemma. *The set of finitely reducible elements of R is closed under multiplication.*

Proof. If both r and s are finitely reducible there are factorizations into irreducibles $r = r_1 \cdots r_n$ and $s = s_1 \cdots s_m$, and thus rs has the factorization $r_1 \cdots r_n s_1 \cdots s_m$, so it is finitely reducible. ∎

§14. Lemma. *If $r \in R \setminus \widetilde{R}$ is infinitely reducible there is another infinitely reducible element $s \in R \setminus \widetilde{R}$ such that $(r) \subsetneq (s)$.*

Proof. Let r be infinitely reducible. Since r is reducible, it is a product $r = ss'$ with both $s, s' \in R \setminus \widetilde{R}$. By the previous lemma, one of s and s' needs to be infinitely reducible, so we may assume that s is infinitely reducible. Since $s \mid r$, we have $(r) \subset (s)$. If we had $(r) = (s)$ the elements r and s would be associated, i.e., there would be an element $u \in R^\times$ such that $r = su$, and therefore $r = ss' = su$, which in turn implies $s' = u$ because R is an integral domain. But this is a contradiction because $s' \in R \setminus \widetilde{R}$ and $u \in R^\times$, so we must have $(r) \neq (s)$. ∎

§15. Theorem. *If R is Noetherian then its reducible elements are finitely reducible.*

Proof. We shall prove that if R has an infinitely reducible element then it cannot be Noetherian. Let r_1 is an infinitely reducible element. By the previous lemma there is another infinitely reducible element r_2 such that $(r_1) \subsetneq (r_2)$. In turn, again by the lemma, there is another infinitely reducible element r_3 such that $(r_2) \subsetneq (r_3)$, etc. We thus obtain a sequence $(r_n)_{n \in \mathbb{Z}_{\geq 1}}$ of elements of R such that

$$(r_i) \subsetneq (r_{i+1})$$

for all $i \in \mathbb{Z}_{\geq 1}$. This is a sequence of ideals that never stabilizes, and thus R is not Noetherian. ∎

§16. Corollary. *If R is a PID then its reducible elements are finitely reducible.*

4 Unique factorization domains

§17. Definition. R is said to be a *unique factorization domain* (UFD) if for all $r \in R \setminus \widetilde{R}$ the following conditions hold:

1. There are irreducible elements $p_1, \ldots, p_n$ such that $r = p_1 \cdots p_n$;
2. This factorization is unique up to multiplication by invertibles; that is, if $r = q_1 \cdots q_m$ for irreducible elements $q_1, \ldots, q_m$ then $m = n$ and there is a permutation $\sigma \in S_n$ such that for all $i = 1, \ldots, n$ the irreducibles p_i and $q_{\sigma(i)}$ are associated.

§18. Example. Any field is a UFD.

§19. Example. It can be proved (but we will not see it here) that if R is a UFD then so is $R[x]$. In particular, as is well known, $\mathbb{Z}[x]$ is a UFD.

§20. Theorem. *Any PID is a UFD.*

Proof. Assume that R is a PID, and let us prove that it is a UFD. Let $r \in R \setminus \widetilde{R}$. By the previous corollary, r is either irreducible or finitely reducible, so r can be factored as a product of irreducibles

$$r = p_1 \cdots p_n$$

with $n \geq 1$. Now let us prove the uniqueness of this factorization. Let there be another factorization into irreducibles

$$r = q_1 \cdots q_m.$$

Now we use the fact that in a PID the irreducibles are primes (cf. §8). Each p_i divides r, so it must divide some q_j because p_i is prime. This means that $q_j = p_i a$ for some $a \in R$, but the fact that q_j is irreducible forces a to be invertible (p_i cannot be invertible because it is irreducible), so q_j and p_i are associated. So for each i the irreducible p_i is associated to some q_j. Similarly, for each j the irreducible q_j is associated to some p_i.

Let us now finish the proof by induction on n.

The induction base is the case $n = 1$, in which $r = p_1$. Then $m \geq 1$ because p_1 must be associated to at least one q_j, but $m > 1$ is impossible because then p_1 would not be irreducible, a contradiction. Hence, $m = 1$ and q_1 is associated to p_1, which finishes the induction base.

Now the induction step. As induction hypothesis let $n \in \mathbb{Z}_{\geq 1}$ and assume that if r has a factorization into irreducibles $r = p_1 \cdots p_n$ then for any other factorization into irreducibles $r = q_1 \cdots q_m$ we have $m = n$ and there is a permutation $\upsilon \in S_n$ such that for all i the irreducible p_i is associated to $q_{\upsilon(i)}$. Let there be two factorizations into irreducibles

$$r = p_1 \cdots p_{n+1} = q_1 \cdots q_m.$$

There is j such that p_{n+1} and q_j are associated. Let $\tau = (j\ m) \in S_m$, and for each $k = 1, \ldots, m$ define $s_k = q_{\tau(k)}$. So we have

$$r = p_1 \cdots p_{n+1} = s_1 \cdots s_m,$$

and p_{n+1} and s_m are associated, so there is $u \in R^\times$ such that $s_m = up_{n+1}$, and thus

$$p_1 \cdots p_{n+1} = us_1 \cdots s_{m-1} p_{n+1}.$$

Since R is an integral domain it follows that

$$p_1 \cdots p_n = us_1 \cdots s_{m-1},$$

and thus, using the induction hypothesis, we obtain $m - 1 = n$ and there is a permutation $\upsilon \in S_n$ such that p_i is associated to $s_{\upsilon(i)}$ for each $i = 1, \ldots, n$. Finally, define $\sigma \in S_{n+1}$ as follows:

$$\sigma(i) = \begin{cases} \tau(\upsilon(i)) & \text{if } i \leq n, \\ j & \text{if } i = n + 1. \end{cases}$$

So for each $i = 1, \ldots, n + 1$ the irreducibles p_i and $q_{\sigma(i)}$ are associated, thus ending the proof. ∎

Since $\mathbb{Z}$ is a PID, its primes coincide with its irreducibles, and the conclusion that $\mathbb{Z}$ is also a UFD shows that every integer has a unique factorization into primes (up to signs). In other words, the fundamental theorem of arithmetic is a corollary of the above theorem.

§21. Example. Since $\mathbb{Z}[x]$ is a UFD but not a PID (because $(2, x)$ is not principal), we conclude that the class of UFDs is strictly larger than that of PIDs.

Notice that in the proof of the above theorem we needed to use the fact that in a PID the irreducibles are prime, but it turns out that UFDs have the same property:

§22. LEMMA. *Assume that R is a UFD and let $p \in R \setminus \widetilde{R}$. Then p is prime if and only if p is irreducible.*

Proof. Since in an integral domain any prime is irreducible, we only need to prove the converse. So assume that p is irreducible, and let us prove that it is prime. Let $p \mid ab$, and let $r \in R$ be such that $ab = pr$. Let the factorizations of a and b into irreducibles be given by

$$a = a_1 \cdots a_n \quad \text{and} \quad b = b_1 \cdots b_m.$$

Then, since R is a UFD, there is either i such that p and a_i and associated or there is j such that p and b_j are associated. Therefore we either have $p \mid a$ or $p \mid b$, which proves that p is prime. ∎

§23. WARNING! We have proved that every PID is a UFD and that in every UFD the primes coincide with the irreducibles, from which it seems to logically follow that in every PID the primes coincide with the irreducibles. Therefore the independent proof of the latter fact that we gave earlier might appear to be redundant. However, it is not redundant because we needed to use it in order to prove that PIDs are UFDs.

§24. EXAMPLE. We have seen above that 3 is irreducible in the ring $\mathbb{Z}[\sqrt{-5}]$ but it is not prime, and noted that, due to this, $\mathbb{Z}[\sqrt{-5}]$ is not a PID. But the previous lemma also shows that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, thus showing that the class of integral domains is strictly larger than that of UFDs.

It could also be seen directly from the definition of UFD that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, by noting that 6 has two distinct factorizations into irreducibles:

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

§25. EXAMPLE. $\mathbb{Z}[2i]$ is not a UFD because 4 has two distinct factorizations:

$$4 = 2 \times 2 = 2i \times (-2i).$$

Notice that the factorizations really are distinct because the invertible element that would make 2 and $2i$ associated exists in $\mathbb{Z}[i]$ but not in $\mathbb{Z}[2i]$.

5 Complements

We have seen that there are the following inclusions of classes:

$$\text{fields} \subset \text{EDs} \subset \text{PIDs} \subset \text{UFDs} \subset \text{integral domains}.$$

All the inclusions are strict, and examples that prove the strictness of the inclusions are:

- fields $\neq$ EDs — $\mathbb{Z}$ is an ED but not a field; similarly for $F[x]$ with F a field.
- PIDs $\neq$ UFDs — $\mathbb{Z}[x]$ is a UFD but not a PID (not even a Bezout domain, because the ideal $(2, x)$ is not principal).
- UFDs $\neq$ integral domains — $\mathbb{Z}[\sqrt{-4}]$ is an integral domain (because it is contained in the field $\mathbb{Q}(\sqrt{-4})$) but it is not a UFD (this was seen in one of the above examples); similarly for $\mathbb{Z}[\sqrt{-5}]$.
- EDs $\neq$ PIDs — a separating example is the ring of quadratic integers

  $$\mathcal{O}_{\mathbb{Q}(\sqrt{-19})} = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right],$$

  which is a PID but not a euclidean domain. The proof of this was omitted in these notes, but it can be found in Dummit&Foote's book on pages 276 (last two lines) and 277, which prove that $\mathcal{O}_{\mathbb{Q}(\sqrt{-19})}$ is not a euclidean domain, and on pages 281 and 282, which prove that it is a PID.