

# Chapter 14

## Rings of Dimension One

Noetherian rings of dimension 0 are rather well understood: They are semilocal, and a Noetherian local ring of dimension 0 is regular if and only if it is a field. The next step is to study one-dimensional rings. In geometry, one-dimensional rings occur as coordinate rings of affine curves. In algebraic number theory, they occur as rings of algebraic integers. The final chapter of this book is devoted to rings of dimension one. We first show that a Noetherian local ring of dimension one is regular if and only if it is normal. As a consequence, we see that the process of normalization, when applied to an affine curve, amounts to desingularization.

In the second section of this chapter we look at the multiplicative theory of ideals. We extend the notion of ideals by including so-called *fractional ideals*, and ask which ideals are invertible as fractional ideals. This is closely linked having height one.

The last section is about *Dedekind domains*. These can be characterized as normal Noetherian domains of dimension  $\leq 1$ . It turns out that this is equivalent to the condition that all nonzero ideals are invertible (as fractional ideals). Yet another equivalent condition is that every ideal can be written as a product of prime ideals. If this is satisfied, then the factorization of an ideal as a product of prime ideals is unique. So ideals in Dedekind domains enjoy the unique factorization property, while elements in general do not. The extent to which a Dedekind domain fails to be factorial is measured by the *ideal class group*, which we introduce. As an application, we will see that the group law on an elliptic curve can be defined by a correspondence between points and elements of the ideal class group of the coordinate ring.

### 14.1 Regular Rings and Normal Rings

We start by taking a closer look at one-dimensional regular local rings. By definition, the maximal ideal of a one-dimensional regular local ring  $R$  is a principal ideal  $\mathfrak{m} = (\pi)$ . A generator  $\pi$  is often called a **uniformizing parameter**. It follows that  $\mathfrak{m}^n = (\pi^n)$  for all nonnegative integers  $n$ . Krull's

intersection theorem (Theorem 12.9) shows that for every nonzero  $a \in R$  there exists a maximal integer  $n$  such that  $a \in \mathfrak{m}^n$ , so  $a = u \cdot \pi^n$  with  $u \in R^\times$  an invertible element. Since  $R$  is an integral domain by Corollary 13.6(a), we can form  $K := \text{Quot}(R)$  and write every  $a \in K^\times$  ( $:=$  the multiplicative group  $K \setminus \{0\}$ ) as  $a = u \cdot \pi^n$  with  $n \in \mathbb{Z}$  and  $u \in R^\times$ . It is easy to see that  $n$  and  $u$  are unique (and  $n$  does not depend on the choice of the uniformizing parameter). A consequence is that  $R$  is factorial with exactly one prime element, up to invertible elements. (As mentioned before, it is true but much harder to show that regular local rings of any dimension are factorial.) Mapping  $a$  to  $n$  defines a map  $\nu: K^\times \rightarrow \mathbb{Z}$ . This map is a group homomorphism, and if we set  $\nu(0) := \infty$ , then  $\nu$  satisfies  $\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$  for all  $a, b \in K$ , and  $\nu(a) = \infty$  if and only if  $a = 0$ . A map with these properties is called a **discrete valuation** on  $K$ . We can retrieve  $R$  from  $K$  by means of  $\nu$ , since

$$R = \{a \in K \mid \nu(a) \geq 0\}.$$

This is usually expressed by saying that  $R$  is the **valuation ring** belonging to the valuation  $\nu$ . One also says that  $R$  is a **discrete valuation ring** (abbreviated DVR). Viewing regular local rings of dimension one as discrete valuation rings has become so common that these rings are often just referred to as DVRs. This is justified since as a converse of what we have just found, all DVRs are one-dimensional regular local rings (see Exercise 14.1).

**Theorem 14.1.** *A Noetherian local ring of dimension one is regular if and only if it is normal.*

*Proof.* Regularity implies normality by Corollary 13.6(b).

For the converse, assume that  $R$  is a one-dimensional normal Noetherian local domain with maximal ideal  $\mathfrak{m}$ . By Corollary 7.9 there exists  $a \in \mathfrak{m}$  with  $\sqrt{(a)} = \mathfrak{m}$ . By the Noether property there exists an ideal  $P$  that is maximal among all colon ideals  $(a) : (y) := \{x \in R \mid xy \in (a)\} \subseteq R$  with  $y \in R \setminus (a)$ . So  $P := (a) : (b)$  with  $b \in R \setminus (a)$ . We claim that  $P$  is a prime ideal. Indeed,  $P \neq R$  since  $b \notin (a)$ , and if  $x, y \in R \setminus P$ , then  $xb \notin (a)$  and  $(a) : (b) \subseteq (a) : (xb)$ , so  $(a) : (xb) = P$  by the maximality. Therefore  $y \notin (a) : (xb)$ , so  $xy \notin P$ . We have  $(a) \subseteq P$ , and since  $\mathfrak{m}$  is the only prime ideal of  $R$  that contains  $(a)$ , we conclude that  $\mathfrak{m} = P = (a) : (b)$ . Clearly  $a \neq 0$ , so we may consider the  $R$ -submodule

$$I := \frac{b}{a} \cdot \mathfrak{m} \subseteq \text{Quot}(R).$$

From  $\mathfrak{m} = (a) : (b)$  we get  $I \subseteq R$ , so  $I$  is an ideal. By way of contradiction assume that  $I \subseteq \mathfrak{m}$ . Then  $\mathfrak{m}$  is an  $R[\frac{b}{a}]$ -module, so by Lemma 8.3,  $b/a$  is integral over  $R$ . By hypothesis, this implies  $b/a \in R$ , so  $b \in (a)$ , a contradiction. We conclude that  $I = R$ . Multiplying this equation by  $a/b$  yields  $\mathfrak{m} = R \cdot \frac{a}{b}$ , so  $\mathfrak{m}$  is a principal ideal. Therefore  $R$  is regular.  $\square$

Exercise 12.8 shows that this result does not extend to higher dimensions. In fact, there are examples of nonregular normal Noetherian local rings of all dimensions  $\geq 2$ .

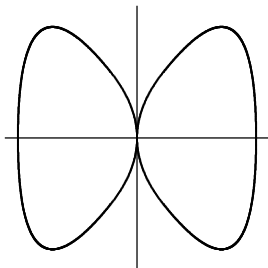
Theorem 14.1 has some nice consequences. For example, if  $R$  is a Noetherian normal ring, then  $R_P$  is normal for all  $P \in \operatorname{Spec}(R)$  by Proposition 8.10, so Theorem 14.1 says that  $R_P$  is regular for all  $P$  with  $\operatorname{ht}(P) \leq 1$ . Geometrically, this means that if  $X$  is a normal variety over an algebraically closed field, then the singular locus has codimension at least 2 in  $X$ . Both these statements are referred to as *regularity in codimension 1*. However, regularity in codimension 1 does not imply normality; a second condition, usually called “S2,” is required (see Eisenbud [17, Theorem 11.15], and Exercise 14.3 for an explicit example). The situation is better for rings of dimension 1. In fact, it follows from Proposition 8.10 and Theorem 14.1 that a one-dimensional Noetherian domain is normal if and only if it is regular, and an irreducible affine curve is normal if and only if it is nonsingular. An important point is that normality is a property that can be achieved by normalization (whereas there is no such process as “regularization” in general). So in particular, by combining Corollary 8.28 with Theorem 14.1 we get the following result.

**Corollary 14.2** (Desingularization of affine curves). *Let  $X$  be an irreducible affine curve. Then there exists an affine curve  $\tilde{X}$  with a surjective morphism  $f: \tilde{X} \rightarrow X$  such that:*

- (a)  $\tilde{X}$  is nonsingular.
- (b) All fibers of  $f$  are finite, and if  $x \in X$  is a nonsingular point, then the fiber of  $x$  consists of one point.

Generalizing Corollary 14.2, we could speak of “desingularization in codimension 1” of a higher-dimensional irreducible affine variety. Moreover, in Exercise 14.4, the corollary is generalized to arbitrary affine curves. What Corollary 14.2 does can best be pictured in the situation of a double point: The two branches of the curve that cross are taken apart by raising one to a higher dimension, thereby deleting the double point. Sometimes one also speaks of *blowing up* a singularity. Example 8.9(4) illustrates this. The example also shows that the “higher” dimension can in fact be smaller. The following is an example in which the dimension does go up.

*Example 14.3.* We wish to desingularize the plane complex curve  $X \subseteq \mathbb{C}^2$  given by the equation  $x_1^4 + x_2^4 - x_1^2 = 0$ , which is irreducible by the Eisenstein criterion (see Lang [33, Chapter V, Theorem 7.1]). The curve  $X$  is shown in Fig. 14.1. The idea is to desingularize  $X$  by forming the normalization of the coordinate ring  $A := \mathbb{C}[X]$ . How can we find quotients of elements of  $A$  that are integral over  $A$ ? The Jacobian criterion (Theorem 13.10) yields  $(0, 0)$  as the only singular point. By Theorem 14.1, the localization of the coordinate ring  $A = \mathbb{C}[X]$  is normal at all points except  $(0, 0)$ . So the normalization  $\tilde{A}$  is contained in all  $A_x$  with  $x \neq (0, 0)$ . This means that an  $f/g \in \tilde{A}$  satisfies  $g(x) \neq 0$  for  $x \neq (0, 0)$ . From this it is straightforward to try the residue class



**Fig. 14.1.** A “butterfly” curve

of  $x_1$  as the denominator  $g$ . By trial and error, we find that  $a := \bar{x}_2^2/\bar{x}_1$  (with  $\bar{x}_i := x_i + (x_1^4 + x_2^4 - x_1^2) \in A$ ) is integral over  $A$ , since dividing the defining equation by  $x_1^2$  yields  $\bar{x}_1^2 + a^2 - 1 = 0$ . Putting this equation together with the defining equation for  $a$ , we consider the variety

$$\tilde{X} := \{(\xi_1, \xi_2, \xi_3) \in \mathbb{C}^3 \mid \xi_1^2 + \xi_3^2 - 1 = \xi_1\xi_3 - \xi_2^2 = 0\} \subset \mathbb{C}^3.$$

We hope and guess that  $\tilde{X}$  is the desired desingularization. To verify this, we first check that

$$f: \tilde{X} \rightarrow X, (\xi_1, \xi_2, \xi_3) \mapsto (\xi_1, \xi_2),$$

is a morphism, since  $(\xi_1, \xi_2, \xi_3) \in \tilde{X}$  obviously implies  $\xi_1^4 + \xi_2^4 - \xi_1^2 = 0$ . Secondly, every point  $(\xi_1, \xi_2) \in X \setminus \{(0, 0)\}$  has the unique preimage  $(\xi_1, \xi_2, \xi_2^2/\xi_1)$ , and the singular point  $(0, 0)$  has two preimages:  $(0, 0, 1)$  and  $(0, 0, -1)$ . Finally, the Jacobian matrix of  $\tilde{X}$  is

$$J = \begin{pmatrix} 2x_1 & 0 & 2x_3 \\ x_3 & -2x_2 & x_1 \end{pmatrix}.$$

For points  $(\xi_1, \xi_2, \xi_3) \in \tilde{X}$  with  $\xi_2 \neq 0$ , also  $\xi_1$  and  $\xi_3$  are nonzero, so  $J(\xi_1, \xi_2, \xi_3)$  has rank 2. On the other hand, if  $\xi_2 = 0$ , then  $\xi_1$  or  $\xi_3$ , but not both, are zero, and again  $\text{rank}(J(\xi_1, \xi_2, \xi_3)) = 2$ . By the Jacobian criterion, this shows that  $\tilde{X}$  is nonsingular. So we have indeed found a desingularization. With a bit more work (i.e., by verifying that the equations for  $\tilde{X}$  define a prime ideal) we could also establish that  $\tilde{X}$  is exactly the normalization of  $X$ .

This example shows very nicely what happens: The original plane curve is wound around the cylinder given by the equation  $\xi_1^4 + \xi_3^2 - 1 = 0$  in such a way that the branches of the curve are on different sides of the cylinder. In this way the double point is blown up.  $\triangleleft$

More examples are contained in Exercise 14.5.

In dimension greater than one, the existence and calculation of a desingularization is a much harder problem. In fact, in positive characteristic the existence problem is still open. For a good overview and an in-depth treatment, readers should turn to Cutkosky [14].

## 14.2 Multiplicative Ideal Theory

For any ring  $R$ , the set of ideals together with the ideal product forms an abelian monoid with  $R$  as neutral element. The only invertible element in this monoid is  $R$  itself. The situation becomes more interesting if we enlarge our view by including *fractional ideals*, according to the following definition.

**Definition 14.4.** *Let  $R$  be an integral domain and  $K := \text{Quot}(R)$  its field of fractions.*

- (a) *A **fractional ideal** is an  $R$ -submodule  $I \subseteq K$ . The product of two fractional ideals is defined as the product of ordinary ideals (see Definition 2.5), making the set of fractional ideals into an abelian monoid with neutral element  $R$ . (It should be noted that some authors require fractional ideals to be nonzero, and/or impose the additional condition that there exist a nonzero  $a \in R$  with  $aI \subseteq R$ .)*
- (b) *A fractional ideal is called **invertible** if there exists a fractional ideal  $J$  with  $I \cdot J = R$ . So the invertible fractional ideals form an abelian group, which we write as  $C(R)$ . (We will give an explanation for the choice of the letter  $C$  on page 205.)*

It is possible to generalize the above definition to rings that need not be integral domains by considering the total ring of fractions instead of the field of fractions. However, almost none of the theory that we will develop here carries over to this case. So we continue to assume that  $R$  is an integral domain.

If a product  $I \cdot J$  of fractional ideals is invertible then so are  $I$  and  $J$  (multiply the inverse of  $I \cdot J$  by  $J$  and by  $I$ ), and conversely. For every nonzero  $a \in K$ , the principal fractional ideal  $(a)_R$  is invertible (with inverse  $(a^{-1})_R$ ). This gives a homomorphism from  $K^\times$  into  $C(R)$  with kernel  $R^\times$ . In general, this is not surjective, i.e., there may exist nonprincipal invertible ideals, as the following example shows.

*Example 14.5.* In the ring  $R := \mathbb{Z}[\sqrt{-5}] \subseteq \mathbb{C}$ , consider the ideal  $I = (2, 1 + \sqrt{-5})_R \subseteq R$ . If  $J := \left(1, \frac{1 - \sqrt{-5}}{2}\right)_R \subseteq \text{Quot}(R)$ , then

$$I \cdot J = (2, 1 - \sqrt{-5}, 1 + \sqrt{-5}, 3)_R = R,$$

so  $I$  is invertible. But  $I$  is not a principal ideal. Indeed, from the assumption  $I = (z)_R$  with  $z = a + b\sqrt{-5}$ ,  $a, b \in \mathbb{Z}$ , we deduce that  $a^2 + 5b^2$  (the norm of  $z$ , which by definition is the product of  $z$  and its complex conjugate) divides 4 and 6, the norms of 2 and of  $1 + \sqrt{-5}$ . This implies  $a = \pm 1$  and  $b = 0$ , so  $I = R$ . But  $I = \{x + y\sqrt{-5} \mid x, y \in \mathbb{Z}, x \equiv y \pmod{2}\} \neq R$ .

We have already studied this ring  $R$  in Example 8.9(3), and seen that it is normal but not factorial.  $\triangleleft$

So invertible ideals generalize principal ideals. But they are not very far away from being principal, as the following result shows.

**Proposition 14.6** (Invertible ideals are locally principal). *Let  $R$  be an integral domain and  $I \subseteq K := \text{Quot}(R)$  a fractional ideal. Then the following statements are equivalent:*

- (a)  $I$  is invertible.
- (b) If  $I' := \{a \in K \mid aI \subseteq R\}$ , then  $I \cdot I' = R$ .
- (c)  $I$  is nonzero, finitely generated, and for every prime ideal  $P \in \text{Spec}(R)$  there exists  $a \in I$  such that the localization of  $I$  satisfies

$$I_P = (a)_{R_P}.$$

We describe the latter property of  $I$  by saying that  $I$  is locally principal.

*Proof.* We start by showing that (a) implies (c). So we assume that there exists a fractional ideal  $J \subseteq K$  with  $I \cdot J = R$ . In particular, we have  $1 = \sum_{i=1}^n a_i b_i$  with  $a_i \in I$  and  $b_i \in J$ . So every  $x \in I$  satisfies  $x = \sum_{i=1}^n x b_i a_i$ , and  $x b_i \in I \cdot J = R$ . Therefore  $I$  is generated by  $a_1, \dots, a_n$ . Clearly  $I$  is nonzero. Moreover, for every  $P \in \text{Spec}(R)$  there exist  $a \in I$  and  $y \in J$  with  $ay \in R \setminus P$  (otherwise,  $I \cdot J$  would be contained in  $P$ ). So for a general element  $b/u \in I_P$  (with  $b \in I$  and  $u \in R \setminus P$ ) we have

$$\frac{b}{u} = \frac{by}{uay} \cdot a \in (a)_{R_P},$$

since  $by \in I \cdot J = R$  and  $uay \in R \setminus P$ . So  $I$  is locally principal.

Now we assume (c) and wish to deduce (b). By the definition of  $I'$ ,  $I \cdot I' \subseteq R$  is an ideal. By way of contradiction, assume that it is proper. Then there exists a maximal ideal  $P \in \text{Spec}(R)$  with  $I \cdot I' \subseteq P$ . (This conclusion requires Zorn's lemma.) By hypothesis we have  $a \in I$  with  $I_P = (a)_{R_P}$ , and  $I = (a_1, \dots, a_n)$ . It follows that there exists  $u \in R \setminus P$  with  $ua_i \in (a)_R$  for all  $i$ , so  $uI \subseteq (a)_R$ . Since  $I \neq \{0\}$ ,  $a$  is nonzero, and it follows that  $u/a \in I'$ , so  $u = a \cdot u/a \in I \cdot I'$ , in contradiction to  $I \cdot I' \subseteq P$ . Therefore (b) holds.

Finally, (b) implies (a) since  $I'$  is a fractional ideal, and we are done. Let us add that (b) can easily be deduced directly from (a).  $\square$

In view of part (b) of the above proposition, we define

$$I^{-1} := \{a \in \text{Quot}(R) \mid aI \subseteq R\}$$

for any fractional ideal of an integral domain.

The finiteness condition in part (c) cannot be omitted: Although it may seem unlikely, there are examples of Noetherian domains with fractional ideals that are locally principal but not finitely generated (see Exercise 14.6).

We draw a few consequences from Proposition 14.6.

**Corollary 14.7** (Properties of invertible ideals). *Let  $I \in C(R)$  be an invertible fractional ideal of a Noetherian domain  $R$ .*

- (a) *There exist invertible ideals  $J_1, J_2 \subseteq R$  with  $I = J_1 \cdot J_2^{-1}$ .*
- (b) *If  $I \subseteq R$ , then every prime ideal  $P \in \text{Spec}(R)$  that is minimal over  $I$  has height 1.*
- (c) *If  $I =: P$  is a prime ideal of  $R$ , then  $P$  has height 1 and  $R_P$  is regular.*

*Proof.* (a) By Proposition 14.6,  $I$  is finitely generated. If  $a \in R \setminus \{0\}$  is a common denominator of all elements in a generating set, then  $J_1 := I \cdot (a) \subseteq R$  and  $I = J_1 \cdot (a)^{-1}$ . Since  $J_2 := (a)$  and  $I$  are invertible, the same holds for  $J_1$ .

(b) Let  $P \in \text{Spec}(R)$  be minimal over  $I$ . Then  $P_P$  is minimal over  $I_P$ , which by Proposition 14.6 is a principal ideal. So  $\text{ht}(P_P) \leq 1$  by the principal ideal theorem (Theorem 7.4). Since  $\{0\} \neq I \subseteq P_P$ , the height must be equal to 1. So  $\text{ht}(P) = \text{ht}(P_P) = 1$ .

(c) By part (b),  $P$  has height 1, so  $\dim(R_P) = 1$ . By Proposition 14.6, the maximal ideal of  $R_P$  is principal, so  $R_P$  is regular.  $\square$

So we cannot hope that prime ideals of height other than 1 are invertible. But when are all height-one prime ideals invertible? By the corollary, a necessary condition for this is regularity in codimension 1. So a normal Noetherian domain would be a good candidate. However, in Exercise 14.7 we find an example of a normal Noetherian domain with a prime ideal of height 1 that is *not* invertible. So more is required. Recall that by Proposition 8.8, factoriality is a stronger condition than normality, and by Proposition 8.10, the condition that every localization at a prime ideal is factorial lies between the two. We call an integral domain  $R$  **locally factorial** if  $R_P$  is factorial for every  $P \in \text{Spec}(R)$ .

**Theorem 14.8** (Invertible ideals in a locally factorial ring). *Let  $R$  be a Noetherian domain.*

- (a) *If  $R$  is locally factorial, then every height-one prime ideal of  $R$  is invertible.*
- (b) *If every height-one prime ideal of  $R$  is invertible, then an ideal  $I \subseteq R$  is invertible if and only if it is a finite product of prime ideals of height 1 (where  $I = R$  occurs as the empty product).*

**Remark.** As mentioned before, every regular ring is locally factorial. (We have proved this only for rings of dimension at most 1; see page 197.) So all regular domains lie within the scope of the theorem.  $\triangleleft$

*Proof of Theorem 14.8.* (a) Let  $Q \subset R$  be a prime ideal of height 1. We use Proposition 14.6. Clearly  $Q$  is finitely generated and nonzero, so we need to show only that  $Q_P \subseteq R_P$  is a principal ideal for every  $P \in \text{Spec}(R)$ . If  $Q \not\subseteq P$ , then  $Q$  contains elements that are invertible in  $R_P$ , so  $Q_P = (1)_{R_P}$  is a principal ideal. On the other hand, if  $Q \subseteq P$ , then by Theorem 6.5,  $Q_P$  is a prime ideal of  $R_P$  of height 1. Since  $R_P$  is factorial, it follows by Lemma 5.14 that  $Q_P$  is a principal ideal in this case, too.

(b) It follows from the hypothesis that every product of height-one prime ideals is also invertible. We prove the converse by Noetherian induction. So assume that there exists an invertible ideal that is *not* a product of height-one prime ideals. By the Noether property we can choose  $I$  be maximal among all counterexamples. Since  $R$  is not a counterexample,  $I \neq R$ , and therefore there exists a prime ideal  $P \in \text{Spec}(R)$  that is minimal over  $I$ . By Corollary 14.7(b),  $P$  has height 1, so it is invertible. Using Lemma 14.9 below, we obtain  $I \subsetneq J := I \cdot P^{-1} \subseteq R$ . Since  $I$  is invertible, so is  $J$ . With the maximality of  $I$ , this implies that  $J$  is a product of height-one prime ideals. So the same holds for  $I$ , and we are done.  $\square$

In the proof we have used the following lemma.

**Lemma 14.9.** *Let  $R$  be a Noetherian domain and let  $I \subseteq R$  be a nonzero ideal that is contained in an invertible prime ideal  $P$ . Then  $I \subsetneq I \cdot P^{-1} \subseteq R$ .*

*Proof.* From  $I \subseteq P$  it follows that  $J := I \cdot P^{-1} \subseteq P \cdot P^{-1} = R$ . Moreover,  $I = J \cdot P \subseteq J$ . Assume that  $I = J$ . Then  $I = P \cdot I$ . This localizes to  $I_P = P_P \cdot I_P$ , which by Nakayama's lemma (Theorem 7.3) gives  $I_P = \{0\}$ . Since there are no zero divisors, we obtain  $I = \{0\}$ , contradicting the hypothesis.  $\square$

Theorem 14.8(b) becomes even more interesting if we combine it with the following unique factorization result.

**Proposition 14.10** (Unique factorization of invertible ideals). *Let  $R$  be an integral domain and let  $I \subseteq R$  be an invertible ideal that has a factorization*

$$I = P_1 \cdots P_n$$

*with  $P_i$  prime ideals (where  $n = 0$  occurs if  $I = R$ ). Then this factorization is unique up to the order of the factors.*

*Proof.* We use induction on  $n$ . Let  $I = Q_1 \cdots Q_m$  be another factorization with  $Q_i \in \text{Spec}(R)$ . If  $n = 0$  then  $m = 0$ , since otherwise  $I \subseteq Q_1 \subsetneq R = I$ . Consider the case  $n > 0$ . By renumbering, we may assume that  $P_1$  is minimal among the  $P_i$ . Since  $Q_1 \cdots Q_m \subseteq P_1$ , there exists  $i$  with  $Q_i \subseteq P_1$ . By renumbering, we may assume  $i = 1$ . Since  $P_1 \cdots P_n \subseteq Q_1$ , there exists  $j$  with  $P_j \subseteq Q_1$ , so  $P_j \subseteq Q_1 \subseteq P_1$ . With the minimality of  $P_1$ , this implies  $P_1 = Q_1$ . Since  $I$  is invertible, so are all  $P_i$ . Multiplying by  $P_1^{-1} = Q_1^{-1}$  gives  $P_2 \cdots P_n = Q_2 \cdots Q_m$ , and the result follows by induction.  $\square$



Assume that  $R$  is a locally factorial Noetherian domain, or more generally a Noetherian domain in which all height-one prime ideals are invertible. We can extend Theorem 14.8(b) and Proposition 14.10 to invertible *fractional* ideals. In fact, if  $I \subseteq \text{Quot}(R)$  is an invertible fractional ideal, then it follows by Corollary 14.7(a) and Theorem 14.8(b) that  $I$  can be written as a product of height-one prime ideals and inverses of height-one prime ideals. Conversely, it follows from the group property of  $C(R)$  that every such product is invertible. More formally, let  $\mathcal{M} \subseteq \text{Spec}(R)$  be the set of all prime ideals of height 1. Then a fractional ideal  $I$  is invertible if and only if it can be written as

$$I = \prod_{Q \in \mathcal{M}} Q^{e_{I,Q}} \quad (14.1)$$

with  $e_{I,Q} \in \mathbb{Z}$ , and all but finitely many  $e_{I,Q}$  equal to 0. It follows from Proposition 14.10 that the  $e_{I,Q}$  are unique. In fact, if there existed two different factorizations, we could multiply both by height-one prime ideals until we obtained two different factorizations of a nonfractional ideal, contradicting Proposition 14.10. It also follows that  $I \subseteq R$  if and only if all  $e_{I,Q}$  are nonnegative.

If we multiply two invertible ideals, the corresponding exponents  $e_{I,Q}$  in (14.1) get added. So our results can be expressed by saying that the group  $C(R)$  of invertible fractional ideals is isomorphic to the free abelian group generated by the height-one prime ideals. This motivates the following definition. For any ring  $R$ , the group  $\text{Div}(R)$  of **Weil divisors** is defined to be the free abelian group generated by the height-one prime ideals of  $R$ . In contrast to  $C(R)$ , the group of Weil divisors is usually written additively, so a Weil divisor is a “formal”  $\mathbb{Z}$ -linear combination of height-one prime ideals. In particular, if  $R$  is the coordinate ring of an affine curve, a Weil divisor can be written as a formal  $\mathbb{Z}$ -linear combination of points.

In this context, an invertible ideal of an integral domain  $R$  is called a **Cartier divisor**, and  $C(R)$  is the group of Cartier divisors. This explains the use of the letter  $C$ . (It should be noted that the standard definition of Cartier divisors in algebraic geometry is different; see Hartshorne [26, page 141].) So if  $R$  is a locally factorial Noetherian domain (or, more generally, a Noetherian domain in which all height-one prime ideals are invertible), we have  $C(R) \cong \text{Div}(R)$ . Using the isomorphism, we can speak of the Weil divisor associated to an invertible ideal or to a nonzero element  $a \in R$ : The latter is  $\sum_{i=1}^n e_i \cdot P_i$  if  $(a) = \prod_{i=1}^n P_i^{e_i}$ . The situation becomes less nice when we relax the conditions on  $R$ . Exercise 14.8 deals with the case that  $R$  is a normal Noetherian domain.

### 14.3 Dedekind Domains

In this theory, the best-behaved domains are those in which every nonzero ideal is invertible. We will study these rings now, and see that the invertibility of nonzero ideals is equivalent to various other interesting conditions.

**Theorem 14.11** (Rings with a perfect multiplicative ideal theory). *For an integral domain  $R$ , the following statements are equivalent:*

- (a) *Every nonzero ideal of  $R$  is invertible.*
- (b)  *$R$  is Noetherian and every ideal of  $R$  is locally principal.*
- (c)  *$R$  is Noetherian and normal and has dimension at most 1.*
- (d) *Every ideal  $I \subseteq R$  is a finite product of prime ideals (where  $I = R$  occurs as the empty product).*

*If these conditions are satisfied, then the factorization of a nonzero ideal as a product of prime ideals is unique up to the order of the factors. Moreover, every finitely generated, nonzero fractional ideal has a unique factorization as (14.1).*

*Proof.* It follows from Proposition 14.6 that (a) implies (b).

We now assume (b) and wish to deduce (c). It follows that for every  $P \in \text{Spec}(R)$ ,  $P_P \subseteq R_P$  is a principal ideal. If  $\text{ht}(P) = 0$ , then  $P = \{0\}$  and  $R_P = \text{Quot}(R)$  is regular. Otherwise, it follows that  $R_P$  is one-dimensional and regular. Therefore  $R$  is regular (and hence normal by Corollary 13.6(b) and Proposition 8.10) and of dimension at most 1. So we have deduced (c).

Next we assume (c) and wish to prove (d). By (c),  $R$  is locally factorial since for every  $P \in \text{Spec}(R)$ , the local ring  $R_P$  is a field (in the case  $P = \{0\}$ ) or a discrete valuation ring (by Theorem 14.1 and the discussion preceding it). So by Theorem 14.8(a), every height-one prime ideal of  $R$  is invertible. By way of contradiction, assume that there exists an ideal  $I \subseteq R$  that is not a finite product of prime ideals. Since  $R$  is Noetherian, we may assume  $I$  to be maximal with this property. We have  $\{0\} \neq I \subsetneq R$ , so there exists a prime ideal  $P$  that contains  $I$ . Since  $\dim(R) \leq 1$  and  $P \neq \{0\}$ ,  $P$  must have height 1, so it is invertible. Lemma 14.9 yields  $I \subsetneq I \cdot P^{-1} \subseteq R$ , so by the maximality of  $I$ ,  $I \cdot P^{-1}$  is a finite product of prime ideals. Therefore the same is true for  $I$ .

The most work is required for deducing (a) from (d). We will first show that (under the assumption (d)) every invertible prime ideal is maximal. From this we will draw the (at first sight surprising) consequence that every nonzero prime ideal is invertible, which together with the hypothesis (d) implies (a) directly. So let  $P \subseteq R$  be an invertible prime ideal. To show that  $P$  is maximal, we need to prove that  $P + (a) = R$  for every  $a \in R \setminus P$ . We have factorizations

$$P + (a) = P_1 \cdots P_n \quad \text{and} \quad P + (a^2) = P'_1 \cdots P'_m$$

as products of prime ideals. Computing modulo  $P$  and writing  $\bar{a} := a + P \in \bar{R} := R/P$ , we get

$$(\bar{a})_{\bar{R}} = \bar{P}_1 \cdots \bar{P}_n \quad \text{and} \quad (\bar{a}^2)_{\bar{R}} = \bar{P}'_1 \cdots \bar{P}'_m.$$

This gives two factorizations of  $(\bar{a}^2)$ , which is an invertible ideal of  $\bar{R}$ . By Proposition 14.10 it follows that  $m = 2n$  and, after renumbering,  $\bar{P}_i = \bar{P}'_{2i-1} = \bar{P}'_{2i}$  for  $i = 1, \dots, n$ . By Lemma 1.22, the same holds for the original  $P_i$  and  $P'_j$ , and we conclude that  $P + (a^2) = (P + (a))^2$ . In particular, every  $x \in P$  can be written as  $x = y + az + a^2w$  with  $y \in P^2$ ,  $z \in P$ , and  $w \in R$ . But then  $w \in P$  since  $a^2w = x - y - az \in P$  and  $a^2 \notin P$ . So  $x \in P^2 + a \cdot P$ , and we obtain

$$P \subseteq P \cdot (P + (a)) \subseteq P.$$

Multiplying by  $P^{-1}$  yields  $P + (a) = R$ , as claimed.

The second (and final) step is to show that every nonzero prime ideal is invertible. So assume that  $\{0\} \neq Q \in \text{Spec}(R)$ . Choose a nonzero  $b \in Q$ . By hypothesis, we have  $(b) = Q_1 \cdots Q_r$  with  $Q_i \in \text{Spec}(R)$ . Since  $(b)$  is invertible, the  $Q_i$  are invertible, too, so by what we have shown they are maximal. Since  $Q_1 \cdots Q_r \subseteq Q$ , there exists an  $i$  with  $Q_i \subseteq Q$ , so  $Q = Q_i$  by the maximality of  $Q_i$ . Therefore  $Q$  is invertible, and the proof of the equivalence of (a) through (d) is complete.

The uniqueness of a factorization of a nonzero ideal follows from (a), (d), and Proposition 14.10. If  $I$  is a finitely generated, nonzero fractional ideal, there exists a nonzero  $a \in R$  such that  $J := aI \subseteq R$ . Since  $J$  and  $(a)$  are products of prime ideals,  $I$  has a factorization as (14.1). If there are two such factorizations, we can multiply both by prime ideals until we obtain two factorizations of a nonfractional ideal. So the factorizations are unique after all.  $\square$

An integral domain that satisfies the equivalent conditions from Theorem 14.11 is called a **Dedekind domain**. Of these conditions, (c) is the one that tends to be easiest to verify. The condition (b) shows that Dedekind domains are not too far away from principal ideal domains. Although our investigation originated from studying condition (a), condition (d) and the unique factorization statement may be the most interesting. Notice that elements of a Dedekind domain do not always enjoy the unique factorization property that holds for ideals: consider Example 8.9(3). So ideals are “idealized” elements. Many more properties that are equivalent to  $R$  being a Dedekind domain can be found in the literature. For instance, Larsen and McCarthy [34, Theorem 6.20] list 16.

An important class of Dedekind domains comes from algebraic geometry: If  $X$  is an irreducible, nonsingular affine curve, then the coordinate ring  $K[X]$  is a Dedekind domain since it satisfies (c) from Theorem 14.11.

Another class of arguably even more importance comes from number theory: Let  $K$  be a **number field**, i.e., a finite field extension of  $\mathbb{Q}$ . Then the ring of **algebraic integers** in  $K$  is defined as the integral closure of  $\mathbb{Z}$  in  $K$ , and is written as  $\mathcal{O}_K$ . It follows from Lemma 8.27 that  $\mathcal{O}_K$  is Noetherian. Being an integral closure of a ring in a field, it is also normal. Since  $\mathcal{O}_K$  is an integral extension of  $\mathbb{Z}$ , it has dimension 1 by Corollary 8.13. So  $\mathcal{O}_K$  satisfies condition (c) and is therefore a Dedekind domain. Rings of algebraic integers are the central object of study in the field of *algebraic number theory*. Historically, much of the interest in rings of algebraic integers originated from the study of Diophantine problems. For instance, the question which integers can be represented as  $x^2 + dy^2$  (with  $x, y, d \in \mathbb{Z}$ , but  $d$  fixed) can be translated into a question about algebraic integers using the factorization  $x^2 + dy^2 = (x + y\sqrt{-d})(x - y\sqrt{-d})$ . So one is led to calculations in the ring  $\mathcal{O}_K$  of algebraic integers in the number field  $K = \mathbb{Q}(\sqrt{-d})$ . Clearly the question whether  $\mathcal{O}_K$  is factorial plays a central role in this game. The answer is yes for some  $d$  (e.g.,  $d = 1$ ), but no for most (e.g.,  $d = 5$ ; see Example 8.9(3)). Another extremely well-known Diophantine equation is the Fermat equation  $x^n + y^n = z^n$ . With  $\zeta_{2n}$  a primitive  $(2n)$ th root of unity, this translates to

$$\prod_{i=1}^n (x - \zeta_{2n}^{2i-1}y) = z^n,$$

an equation in the ring  $\mathcal{O}_K$  of algebraic integers in the cyclotomic field  $K = \mathbb{Q}(\zeta_{2n})$ . Again, the question whether  $\mathcal{O}_K$  is factorial arises naturally. In fact, there were attempts at proving Fermat's last theorem that hinged on the assumption that  $\mathcal{O}_K$  is factorial. Again, this is false for most  $n$ . The following example illustrates how the nonuniqueness of factorization in a ring of algebraic integers is resolved by turning to ideals.

*Example 14.12.* Consider the ring  $R = \mathbb{Z}[\sqrt{-5}]$ . In Example 8.9(3) we have seen that  $R$  is normal, so  $R$  is the ring of algebraic integers in  $\mathbb{Q}(\sqrt{-5})$ . There we have also exhibited an example of a nonunique factorization:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \quad (14.2)$$

How do the corresponding principal ideals  $(2)_R$ ,  $(3)_R$ , etc. factorize? In Exercise 14.9 it is shown that every ideal of a Dedekind domain is generated by two elements. With this in mind, it is not too hard to find the following factorizations, which are easy to verify:

$$\begin{aligned} (2)_R &= (2, 1 + \sqrt{-5})_R^2, \\ (3)_R &= (3, 1 + \sqrt{-5})_R (3, 1 - \sqrt{-5})_R, \\ (1 + \sqrt{-5})_R &= (2, 1 + \sqrt{-5})_R (3, 1 + \sqrt{-5})_R, \\ (1 - \sqrt{-5})_R &= (2, 1 + \sqrt{-5})_R (3, 1 - \sqrt{-5})_R. \end{aligned}$$

To see that  $(2, 1 + \sqrt{-5})_R$  and  $(3, 1 \pm \sqrt{-5})_R$  are prime ideals, observe that they are the kernels of the ring homomorphisms  $R \rightarrow \mathbb{F}_2$ ,  $a + b\sqrt{-5} \mapsto a + b \pmod 2$ , and  $R \rightarrow \mathbb{F}_3$ ,  $a + b\sqrt{-5} \mapsto a \mp b \pmod 3$ , respectively. So we get the unique factorization

$$(6)_R = (2, 1 + \sqrt{-5})_R^2 (3, 1 + \sqrt{-5})_R (3, 1 - \sqrt{-5})_R$$

of ideals, and the nonuniqueness in (14.2) is explained by regroupings of the above factors.  $\triangleleft$

We have mentioned before that for any integral domain  $R$ , the principal ideals  $(a)$  with  $a \in \text{Quot}(R) \setminus \{0\}$  form a subgroup of  $C(R)$ . The quotient group

$$\text{Cl}(R) := C(R) / \left\{ (a) \mid a \in \text{Quot}(R) \setminus \{0\} \right\}$$

is called the **ideal class group** of  $R$ . This name is most intuitive in the case that  $R$  is a Dedekind domain, and some authors restrict the definition to that case. Since  $C(R)$  and  $\text{Div}(R)$  are isomorphic if  $R$  is a Dedekind domain,  $\text{Cl}(R)$  is isomorphic to the group of equivalence classes of Weil divisors, where two Weil divisors are called **linearly equivalent** if they map to a principal fractional ideal in  $C(R)$ . For a Dedekind domain  $R$ , the ideal class group is trivial if and only if  $R$  is a principal ideal domain (which by the following theorem is equivalent to  $R$  being factorial). So  $\text{Cl}(R)$  can be viewed as quantifying the extent to which a Dedekind domain fails to be factorial.

**Theorem 14.13** (Factorial Dedekind domains). *For a Dedekind domain  $R$ , the following statements are equivalent:*

- (a)  $R$  is factorial;
- (b)  $R$  is a principal ideal domain.

*Proof.* First assume that  $R$  is factorial. By Lemma 5.14, it follows that every prime ideal of height 1 is principal. Since every nonzero ideal is a product of height-one prime ideals, this implies (b).

The fact that every principal ideal domain is factorial is usually part of an abstract algebra course (see Lang [33, Chapter II, Theorem 4.2]). We give a (shorter) proof for the case of Dedekind domains here. Let  $a \in R$  be a nonzero, noninvertible element. Then  $(a) = P_1 \cdots P_n$  with  $P_i$  prime ideals. By assumption, we have  $P_i = (p_i)$  with  $p_i \in R$  prime elements. Multiplying  $p_1$  by an invertible element if necessary, we can achieve that  $a = p_1 \cdots p_n$ . Now suppose that we have another factorization  $a = q_1 \cdots q_m$  with  $q_j \in R$  irreducible. Since  $p_1$  is a prime element that divides the product of the  $q_j$ , it divides one of the  $q_j$ , say  $q_1$ . Therefore we can achieve  $q_1 = p_1$  by multiplying  $q_1$  by an invertible element if necessary. Continuing in this way, we end up with  $p_i = q_i$  for  $i = 1, \dots, n$  and  $1 = q_{n+1} \cdots q_m$ , so  $m = n$ . This proves the uniqueness of factorization.  $\square$

A generalization of Theorem 14.13 is given in Exercise 14.10.

How large can ideal class groups become? For rings  $\mathcal{O}_K$  of algebraic integers in a number field, the answer is that the ideal class group is finite. Its order is called the *class number*. This is one of the central results of algebraic number theory. For a proof, see Neukirch [42, Chapter I, Theorem 6.3]. This is in sharp contrast to the behavior in more general cases. In fact, we will see in the following example that for a nonsingular, irreducible affine curve  $X$ ,  $\text{Cl}(K[X])$  can become infinite. (In fact, it is finite only in exceptional cases.) Moreover, Claborn [10] proved that any abelian group whatsoever is isomorphic to the ideal class group of a suitable Dedekind domain.

We finish this chapter with an example that shows how the ideal class group can be used to give an elliptic curve the structure of an abelian group.

*Example 14.14* (The group law on an elliptic curve). Let  $E \subseteq K^2$  be an elliptic curve over an algebraically closed field  $K$  of characteristic not equal to 2, given by the equation

$$x_2^2 = x_1^3 + ax_1 + b$$

with  $a, b \in K$  such that  $4a^3 + 27b^2 \neq 0$  (see Exercise 13.10). The goal of this example is to give  $E$  (enriched by a point at infinity) the structure of an abelian group, which is isomorphic to the ideal class group of the coordinate ring  $R := K[E]$ . For some details and proofs we will refer to the exercises. By Exercise 13.10,  $E$  is nonsingular, so  $R$  is a Dedekind domain. For two points  $P_1, P_2 \in E$ , let  $L$  be the line passing through  $P_1$  and  $P_2$ . If  $P_1 = P_2$ , take the tangent line to  $E$  through  $P_1$ . (The remark at the end of Exercise 14.11 says exactly how this is done.) If  $L$  is not parallel to the  $x_2$ -axis, then  $L$  meets  $E$  at another point  $P_3$ . This is shown in Fig. 14.2, and proved in Exercise 14.11. Notice that  $P_3$  may be equal to  $P_1$  or to  $P_2$  if  $P_1 \neq P_2$  and  $L$  is tangent to  $E$  at this point, or if  $P_1 = P_2$  is an inflection point of  $E$ . If  $l \in K[x_1, x_2]$  is a polynomial of degree 1 defining  $L$  and  $\bar{l} \in R$  is the corresponding regular function on  $X$ , then  $\bar{l}$  vanishes at the points  $P_i$ , so it lies in

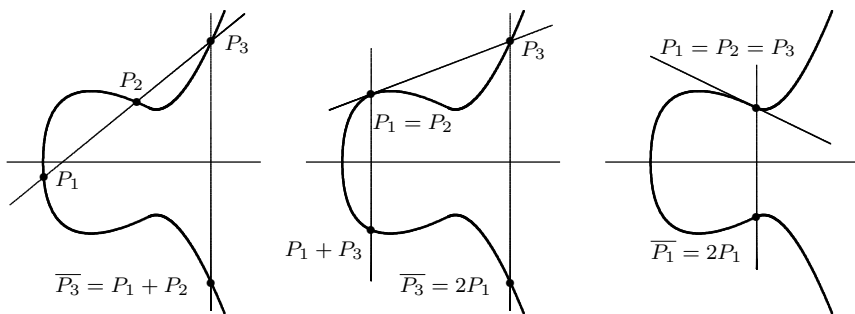


Fig. 14.2. The group law on the elliptic curve  $y^2 = x^3 - x + 1$

the corresponding maximal ideals  $\mathfrak{m}_{P_i} \in \text{Spec}_{\max}(R)$ . It is very plausible that  $(\bar{l})_R = \mathfrak{m}_{P_1} \mathfrak{m}_{P_2} \mathfrak{m}_{P_3}$ . Exercise 14.11 gives an exact proof. (The subtlety lies in the multiplicities in the case that some  $P_i$  coincide.) So the Weil divisor  $P_1 + P_2 + P_3$  is linearly equivalent to 0. We write this as

$$P_1 + P_2 + P_3 \sim 0. \quad (14.3)$$

Next we consider the case that  $L$  is parallel to the  $x_2$ -axis. This happens if and only if  $P_2 = \bar{P}_1$ , where for any point  $P = (\xi_1, \xi_2)$  we write  $\bar{P} := (\xi_1, -\xi_2)$ . In this case,  $P_1$  and  $\bar{P}_1$  are the only intersections of  $L$  and  $E$ . So for every  $P \in E$  we obtain

$$P + \bar{P} \sim 0. \quad (14.4)$$

Putting this together with (14.3) yields

$$P_1 + P_2 \sim \bar{P}_3. \quad (14.5)$$

This already looks like an addition on  $E$ . To show that it really defines a group law, consider the map

$$\varphi: E \rightarrow \text{Cl}(R), \quad P \mapsto [\mathfrak{m}_P] \quad (\text{the class of } \mathfrak{m}_P \text{ in } \text{Cl}(R)).$$

So in terms of Weil divisors,  $\varphi$  maps every point to its equivalence class. Let  $d = \sum_{i=1}^m n_i P_i \in \text{Div}(R)$  (with coefficients  $n_i \in \mathbb{Z}$  and  $P_i \in E$ ) be a Weil divisor. We obtain another Weil divisor  $\bar{d} = \sum_{i=1}^m k_i Q_i$  by substituting every  $P_i$  with  $n_i < 0$  in  $d$  by  $-\bar{P}_i$ . Then  $d \sim \bar{d}$  by (14.4), and all coefficients  $k_i$  in  $\bar{d}$  are nonnegative. If the coefficient sum of  $\bar{d}$  is greater than 2, we can use (14.5) to find a Weil divisor that is linearly equivalent to  $\bar{d}$ , but has coefficient sum one smaller than that of  $\bar{d}$ . So by induction on the coefficient sum, we see that every Weil divisor is linearly equivalent to a point  $P \in E$  or to 0. We conclude that every nontrivial element of  $\text{Cl}(R)$  lies in the image of  $\varphi$ .

The most difficult part of this discussion is to prove that  $\varphi$  is injective, i.e., that for two distinct points  $P, Q \in E$ , there exists no  $f \in \text{Quot}(R)$  with  $(f)_R = \mathfrak{m}_P \cdot \mathfrak{m}_Q^{-1}$ . This is the content of Exercise 14.12. In this exercise, it is also shown that the trivial class is not in the image of  $\varphi$ , i.e., there exists no  $f \in \text{Quot}(R)$  such that  $(f)_R = \mathfrak{m}_P$  with  $P \in E$ . With this, we can extend  $\varphi$  to a bijection between  $\hat{E} := E \cup \{\infty\}$  and  $\text{Cl}(R)$  by mapping  $\infty$  to the trivial class. The geometric interpretation of the additional point  $\infty$  is that it is the point at infinity. This makes sense since we can think of the line through  $P$  and  $\bar{P}$  as meeting  $E$  at infinity. Having a bijection between  $\hat{E}$  and the abelian group  $\text{Cl}(R)$ , we can use this to transfer the group law from  $\text{Cl}(R)$  to  $\hat{E}$ . With this, (14.5) indeed defines the sum of two points  $P_1, P_2 \in E$  as given by the following recipe: Draw the line through  $P_1$  and  $P_2$  and take the third point  $P_3$  of  $E$  meeting this line (always counting intersections with multiplicities). Then reflect  $P_3$  in the  $x_1$ -axis to obtain the desired point  $\bar{P}_3 = P_1 + P_2$ . Special cases apply:  $P + \infty := P$ , and  $P + \bar{P} := \infty$ .

It is of course possible to define the addition on  $\widehat{E}$  directly by this recipe. Then the main difficulty is to verify the associative law (e.g., this takes 12 pages in the book of Washington [52]). But by using the bijection with  $\text{Cl}(R)$ , we get the associative law automatically. This approach also gives a conceptual explanation of why the group law is defined in such a seemingly arbitrary way. On the other hand, it provides the ideal class group  $\text{Cl}(R)$  with the structure of a projective variety. In this way, elliptic curves act as the first significant example for the theories of Jacobian varieties and abelian varieties, which are deep and fascinating subjects in algebraic geometry.

Another important aspect is rational points. Suppose that  $k \subseteq K$  is a subfield with  $a, b \in k$  (i.e., the equation defining  $E$  lies in  $k[x_1, x_2]$ ). A point  $P \in E(k) := k^2 \cap E$  is called **( $k$ -)rational**. If  $P$  is a rational point, then clearly the same is true for  $-P = \bar{P}$ . Moreover, if  $P_1, P_2 \in E(k)$  with  $P_1 \neq -P_2$ , then substituting a parametrization of the line through  $P_1$  and  $P_2$  into the equation defining  $E$  gives a polynomial of degree 3 with coefficients in  $k$ . (Exercise 14.11 has more details.) Since this polynomial has two zeros in  $k$ , corresponding to the points  $P_1$  and  $P_2$  (or a double zero if  $P_1 = P_2$ ), its third zero lies in  $k$ , too. This means that  $P_1 + P_2$  is also a rational point. So we have seen that  $\widehat{E}(k) := E(k) \cup \{\infty\}$  is a subgroup of  $\widehat{E}$ .

This has applications in cryptography. In fact, if  $k$  is a (large) finite field, then  $\widehat{E}(k)$  provides a finite group  $G$  in which the *discrete logarithm problem* (i.e., determining  $n$  from the given data  $g$  and  $g^n$ , with  $g \in G$ , written multiplicatively) is supposedly very hard. This gives rise to public-key cryptosystems. In this business, the choice of the elliptic curve and of a “base point”  $P \in E$  with large order are crucial for the security of the cryptosystem. Applications to cryptography are among the reasons why elliptic curves have become very fashionable (and useful) in recent years. See Washington [52] for a good introduction to elliptic curves and their use in cryptography.  $\triangleleft$

## Exercises for Chapter 14

**14.1 (Discrete valuation rings).** Let  $K$  be a field and let  $\nu: K \rightarrow \mathbb{Z} \cup \{\infty\}$  be a discrete valuation. Assume that  $\nu$  is *nontrivial*, i.e.,  $\text{im}(\nu) \neq \{0, \infty\}$ . Show that the valuation ring  $R := \{a \in K \mid \nu(a) \geq 0\}$  is a one-dimensional regular local ring.

**14.2 (Discrete valuations on the rational function field).** Let  $K(x)$  be the rational function field over a field. Classify all nontrivial discrete valuations on  $K(x)$  that vanish on  $K^\times$ .

*Hint:* You will find that the valuation rings are in bijective correspondence with the set of all monic irreducible polynomials in  $K[x]$  together with one extra element, usually written as  $\infty$  (why?).



**14.3 (Regular in codimension 1 does not imply normal).** This exercise deals with an example of an affine domain that is regular in codimension 1 but not normal. The example is drawn from Shafarevich [46, Chapter II, §5.1], where it appears in geometric terms. The example is the subalgebra

$$A := K[f_1, f_2, f_3, f_4] \subseteq K[x_1, x_2]$$

with

$$f_1 = x_1, \quad f_2 = x_1x_2, \quad f_3 = x_2(x_2 - 1), \quad f_4 = x_2^2(x_2 - 1),$$

where  $K[x_1, x_2]$  is the polynomial algebra in two indeterminates over a field.

- (a) Show that  $K[x_1, x_2]$  is the normalization of  $A$ .
- (b) Show that there exist two maximal ideals  $\mathfrak{n}_1, \mathfrak{n}_2 \in \text{Spec}_{\max}(K[x_1, x_2])$  with  $A \cap \mathfrak{n}_i = (f_1, f_2, f_3, f_4)_A =: \mathfrak{m}$ .
- \*(c) Show that  $K[x_1, x_2] \subseteq A_P$  for all  $P \in \text{Spec}(A) \setminus \{\mathfrak{m}\}$ , and conclude that there exists  $Q \in \text{Spec}(K[x_1, x_2])$  with  $A_P = K[x_1, x_2]_Q$ . *Hint:* Two of the relations of the  $f_i$  are  $f_1^2 f_3 + f_2(f_1 - f_2) = 0$  and  $f_3^3 + f_4(f_3 - f_4) = 0$ .
- (d) Conclude that  $A$  is a two-dimensional nonnormal domain such that the singular locus in  $\text{Spec}(A)$  is  $\{\mathfrak{m}\}$ , so regularity in codimension 1 holds.

**14.4 (Desingularization of nonirreducible curves).** Show that Corollary 14.2 holds for all (not necessarily irreducible) affine curves.

*Hint:* Use Exercises 4.3 and 6.6.

**14.5 (Examples of desingularization).** Find desingularizations of the plane complex curves given by the following equations.

- (a)  $x_1^3 - x_2^2 = 0$  (the cubic curve with a cusp shown in Fig. 12.1)
- (b)  $x_1^4 - x_1^2 + x_2^2 = 0$  (lemniscate of Gerono, an  $\infty$ -shaped curve)
- (c)  $x_1^6 + x_2^6 - x_1^2 = 0$  (butterfly-shaped, similar to Fig. 14.1)
- (d)  $x_1^4 + x_2^4 - x_1x_2 = 0$  (another figure-eight curve, but tilted by  $45^\circ$  and with perpendicular crossing)

*Hint:* It may be hard to do (d) by hand. If you have access to MAGMA [5] you can use the function `Normalization`.

- 14.6 (Finite generation of fractional ideals).**
- (a) Give an example of a fractional  $\mathbb{Z}$ -ideal  $I \subseteq \mathbb{Q}$  that is locally principal but not finitely generated.
  - (b) Show that for a nonzero fractional ideal  $I \subseteq \text{Quot}(R)$  of a Noetherian domain  $R$ ,  $I^{-1}$  is finitely generated.
  - (c) For your example in (a), what are  $I^{-1}$ ,  $I \cdot I^{-1}$ , and  $(I^{-1})^{-1}$ ?

**14.7 (A noninvertible prime ideal of height 1).** This example is taken from Hutchins [28, Example 47] (with a slight modification), and due to Gilmer [20, page 554, Exercise 2]. Consider the ring  $R = \mathbb{Z}[x, x^2/2] \subset \mathbb{Q}[x]$ .

- (a) Show that  $R$  is a normal Noetherian domain. *Hint:* For this part, it may lead to a nicer notation to consider the isomorphic ring  $S := \mathbb{Z}[x, \sqrt{2x}]$ . You may look at Example 8.9(3) for inspiration.
- (b) Show that the ideal  $P := (x, x^2/2)_R$  is a prime ideal of height 1.
- (c) Show that  $P$  is not invertible.

**14.8 (Cartier divisors and Weil divisors).** Let  $R$  be a normal Noetherian domain. The goal of this exercise is to construct an injective homomorphism  $C(R) \rightarrow \text{Div}(R)$ . Write  $\mathcal{M}$  for the set of height-one prime ideals of  $R$ , and write  $\mathcal{F}$  for the set of all finitely generated nonzero fractional ideals. For each  $Q \in \mathcal{M}$ ,  $R_Q$  is a Dedekind domain, so for  $I \in \mathcal{F}$  there exists a unique  $e_{I,Q} \in \mathbb{Z}$  with  $I_Q = Q_Q^{e_{I,Q}}$ .

- (a) Show that

$$\Phi: \mathcal{F} \rightarrow \text{Div}(R), \quad I \mapsto \sum_{Q \in \mathcal{M}} e_{I,Q} \cdot Q,$$

defines a homomorphism of monoids. *Hint:* The hardest part is to show that  $e_{I,Q} = 0$  for all but finitely many  $Q$ .

- (b) Show that the restriction

$$\Psi := \Phi|_{C(R)}: C(R) \rightarrow \text{Div}(R)$$

of  $\Phi$  to  $C(R)$  is an injective group homomorphism. *Hint:* Use Exercise 8.3.

- (c) Show that  $\Psi$  is surjective if and only if every  $P \in \mathcal{M}$  is invertible. In this case,  $\Psi$  coincides with the isomorphism described on page 205. *Hint:* If  $\Psi(I) = P \in \mathcal{M}$ , consider  $P \cdot I^{-1}$ .

*Remark:* It follows that Exercise 14.7 gives an example in which  $\Psi$  is not surjective.

**\*14.9 (Properties of Dedekind domains).** Let  $R$  be a Dedekind domain. Prove the following.

- (a) If  $P_1, \dots, P_n \in \text{Spec}(R)$  are pairwise distinct nonzero prime ideals and  $e_1, \dots, e_n$  are nonnegative integers, there exists  $a \in R \setminus \{0\}$  such that

$$(a) = P_1^{e_1} \cdots P_n^{e_n} \cdot J$$

with  $J \subseteq R$  an ideal in whose factorization none of the  $P_i$  appear.

- (b) Every ideal of  $R$  is generated by at most two elements.

**14.10 (Factorial rings).** Show that for an integral domain  $R$ , the following statements are equivalent:

- (a)  $R$  is factorial of dimension  $\leq 1$ .
- (b)  $R$  is a principal ideal domain.

If these conditions are satisfied, then  $R$  is Noetherian. Is it true that every factorial ring is Noetherian?

Exercises 14.11 and 14.12 fill the gaps in Example 14.14. Together with the example, they form a nice application project of our methods.

**14.11 (Divisor of a line intersecting a curve).** In this exercise we study a situation that seems rather special, but is general enough to handle elliptic curves, for example. Let  $K$  be an algebraically closed field and let  $X \subset K^2$  be a nonsingular, irreducible affine curve. So  $\mathcal{I}(X) = (g)$  with  $g \in K[x_1, x_2]$  irreducible (see Theorem 5.13). Consider a line

$$L = \{(a\xi + b, c\xi + d) \mid \xi \in K\} \subset K^2 \quad (\text{with } a, b, c, d \in K, a \text{ or } c \text{ nonzero}),$$

and assume  $L \neq X$ . With  $t$  a new indeterminate, set  $f := g(at + b, ct + d) \in K[t]$  and let  $f = a_n \cdot \prod_{i=1}^n (t - \xi_i)$  with  $a_n \in K \setminus \{0\}$  and  $\xi_i \in K$ , not necessarily distinct. So the  $P_i := (a\xi_i + b, c\xi_i + d)$  are the points of the intersection  $L \cap X$ , counted with “multiplicities.” Multiplicity greater than one means that  $L$  is “tangent” to  $X$  in  $P_i$ . Let  $\mathfrak{m}_i \in \text{Spec}_{\max}(K[X])$  be the maximal ideal belonging to  $P_i$ . Furthermore, let  $l := cx_1 - ax_2 + ad - bc$  (which defines  $L$ ), and let  $\bar{l} := l + (g) \in K[X]$  be the corresponding regular function on  $X$ . Show that

$$(\bar{l}) = \mathfrak{m}_1 \cdots \mathfrak{m}_n.$$

So the Weil divisor  $P_1 + \cdots + P_n$  is linearly equivalent to 0.

*Remark:* If  $X$  is an elliptic curve defined as in Example 14.14, then  $f$  has degree 3 if  $a \neq 0$ , i.e., if  $L$  is not parallel to the  $x_2$ -axis. So in this case we get three points whose sum is linearly equivalent to 0. Otherwise,  $f$  has degree 2, so the sum of two points is linearly equivalent to 0. It is also clear that (for general  $X$ ) if  $P$  is a point of  $X$ , then by setting  $a := \frac{\partial g}{\partial x_2}(P)$ ,  $b := -\frac{\partial g}{\partial x_1}(P)$ , and  $(b, d) := P$ , one achieves that the polynomial  $f$  will become divisible by  $t^2$ , which geometrically means that  $L$  is tangent to  $X$  in  $P$ . (Solution on page 231)

**\*14.12 (Rational functions on an elliptic curve).** Let  $K$  be an algebraically closed field of characteristic not equal to 2, and let  $E \subset K^2$  be an elliptic curve given by the equation

$$x_2^2 = x_1^3 + ax_1 + b$$

with  $a, b \in K$ ,  $4a^3 + 27b^2 \neq 0$  (see Exercise 13.10). Let  $R := K[E]$  be the coordinate ring and  $L := \text{Quot}(R)$  the *field of rational functions* on  $E$ . By a **place** of  $L$  we mean a discrete valuation ring  $\mathcal{O}$  such that  $K \subset \mathcal{O} \subset L$  and  $\text{Quot}(\mathcal{O}) = L$ . So giving a place of  $L$  is the same as giving a nontrivial discrete valuation on  $L$  that vanishes on  $K^\times$  (see Exercise 14.1).

- (a) Show that  $L$  has the following places: (1) the localizations  $R_P =: \mathcal{O}_P$  of  $R$  at points  $P \in E$ , and (2) one further place, which we will write as  $\mathcal{O}_\infty$ . We will write the maximal ideals of the places as  $\mathfrak{p}_P$  and  $\mathfrak{p}_\infty$ . Also show that  $R \cap \mathfrak{p}_\infty = \{0\}$ . *Hint:* The last statement can be proved by using a suitable  $K$ -automorphism  $\varphi: L \rightarrow L$ .
- (b) Show that  $L$  is not isomorphic (as a  $K$ -algebra) to the rational function field  $K(x)$ . This result is usually expressed by saying that  $E$  is not a *rational curve*. *Hint:* This can be done by giving a  $K$ -automorphism  $\varphi: L \rightarrow L$  that fixes four places of  $L$  (in the sense that  $\varphi(\mathcal{O}) = \mathcal{O}$ ), and showing that  $K(x)$  has no such automorphism.
- (c) Assume that there exists  $f \in L$  such that  $(f)_R = \mathfrak{m}_P \cdot \mathfrak{m}_Q^{-1}$  with  $P, Q \in E$  distinct points, or  $(f)_R = \mathfrak{m}_P$  ( $:=$  the maximal ideal of  $R$  belonging to  $P$ ). In other words, assume that as a Weil divisor,  $P$  is linearly equivalent to  $Q$  or to 0. Show that this implies  $L \cong K(f)$ , contradicting (b). *Hint:* Consider the integral closure  $A$  of  $K[f]$  in  $L$ . Apply the structure theorem for finitely generated modules over a principal ideal domain (see Lang [33, Chapter XV, Theorem 2.2]) to  $A$ .

*Remark:* Part (c) shows that for a nonrational, nonsingular, irreducible affine curve that has only one point at infinity, no point is linearly equivalent to another point or to 0. In this context, it would be more natural to consider *projective curves*. Then zeros and poles at infinity would be included in the divisor of a rational function, and the hypothesis on the number of points at infinity would vanish. (*Solution on page 232*)



<http://www.springer.com/978-3-642-03544-9>

A Course in Commutative Algebra

Kemper, G.

2011, XII, 248 p., Hardcover

ISBN: 978-3-642-03544-9