13. Dedekind Domains

In the last chapter we have mainly studied 1-dimensional regular local rings, i. e. geometrically the local properties of smooth points on curves. We now want to patch these local results together to obtain global statements about 1-dimensional rings (resp. curves) that are "locally regular". The corresponding notion is that of a Dedekind domain.

Definition 13.1 (Dedekind domains)**.** An integral domain R is called **Dedekind domain** if it is Noetherian of dimension 1, and for all maximal ideals $P \trianglelefteq R$ the localization R_P is a regular local ring.

Remark 13.2 (Equivalent conditions for Dedekind domains)**.** As a Dedekind domain R is an integral domain of dimension 1, its prime ideals are exactly the zero ideal and all maximal ideals. So every localization R_P for a maximal ideal P is a 1-dimensional local ring. As these localizations are also Noetherian by Exercise 7.23, we can replace the requirement in Definition 13.1 that the local rings R_P are regular by any of the equivalent conditions in Proposition 12.14. For example, a Dedekind domain is the same as a 1-dimensional Noetherian domain such that all localizations at maximal ideals are discrete valuation rings.

This works particularly well for the normality condition as this is a local property and can thus be transferred to the whole ring:

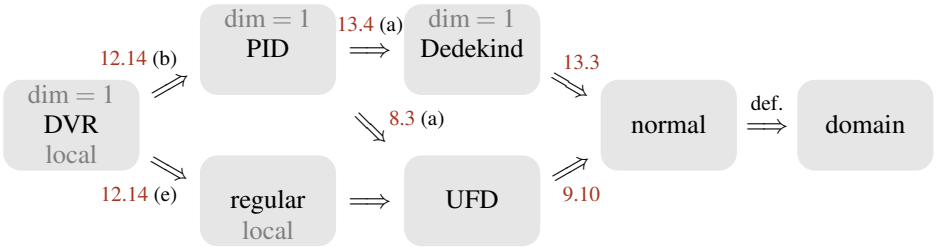
Lemma 13.3. *A 1-dimensional Noetherian domain is a Dedekind domain if and only if it is normal.*

Proof. By Remark 13.2 and Proposition 12.14, a 1-dimensional Noetherian domain R is a Dedekind domain if and only if all localizations R_P at a maximal ideal P are normal. But by Exercise 9.13 (c) this is equivalent to R being normal. □

25

Example 13.4.

(a) By Lemma 13.3, any principal ideal domain which is not a field is a Dedekind domain: it is 1-dimensional by Example 11.3 (c), clearly Noetherian, and normal by Example 9.10 since it is a unique factorization domain by Example 8.3 (a). For better visualization, the following diagram shows the implications between various properties of rings for the case of integral domains that are not fields. Rings that are always 1-dimensional and / or local are marked as such. It is true that every regular local ring is a unique factorization domain, but we have not proven this here since this requires more advanced methods — we have only shown in Proposition 11.40 that any regular local ring is an integral domain.



(b) Let X be an irreducible curve over an algebraically closed field. Assume that X is smooth, i. e. that all points of X are smooth in the sense of Example 11.37 and Definition 11.38. Then the coordinate ring $A(X)$ is a Dedekind domain: it is an integral domain by Lemma 2.3 (a) since $I(X)$ is a prime ideal by Remark 2.7 (b). It is also 1-dimensional by assumption and Noetherian by Remark 7.15. Moreover, by Hilbert's Nullstellensatz as in Remark 10.11 the

maximal ideals in $A(X)$ are exactly the ideals of points, and so our smoothness assumption is the same as saying that all localizations at maximal ideals are regular.

In fact, irreducible smooth curves over algebraically closed fields are the main geometric examples for Dedekind domains. However, there is also a large class of examples in number theory, which explains why the concept of a Dedekind domain is equally important in number theory and geometry: it turns out that the ring of integral elements in a number field, i. e. in a finite field extension of $\mathbb{Q}$, is always a Dedekind domain. Let us prove this now.

Proposition 13.5 (Integral elements in number fields)**.** *Let $\mathbb{Q} \subset K$ be a finite field extension, and let R be the integral closure of $\mathbb{Z}$ in K. Then R is a Dedekind domain.*

Proof. As a subring of a field, R is clearly an integral domain. Moreover, by Example 11.3 (c) and Lemma 11.8 we have $\dim R = \dim \mathbb{Z} = 1$. It is also easy to see that R is normal: if $a \in \operatorname{Quot} R \subset K$ is integral over R it is also integral over $\mathbb{Z}$ by transitivity as in Lemma 9.6 (b), so it is contained in the integral closure R of $\mathbb{Z}$ in K. Hence by Lemma 13.3 it only remains to show that R is Noetherian — which is in fact the hardest part of the proof. We will show this in three steps.

(a) We claim that $|R/pR| < \infty$ for all prime numbers $p \in \mathbb{Z}$.

Note that R/pR is a vector space over $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. It suffices to show that $\dim_{\mathbb{Z}_p} R/pR \leq \dim_{\mathbb{Q}} K$ since this dimension is finite by assumption. So let $\overline{a_1}, \dots, \overline{a_n} \in R/pR$ be linearly independent over $\mathbb{Z}_p$. We will show that $a_1, \dots, a_n \in K$ are also independent over $\mathbb{Q}$, so that $n \leq \dim_{\mathbb{Q}} K$. Otherwise there are $\lambda_1, \dots, \lambda_n \in \mathbb{Q}$ not all zero with $\lambda_1 a_1 + \dots + \lambda_n a_n = 0$. After multiplying these coefficients with a common scalar we may assume that all of them are integers, and not all of them are divisible by p. But then $\overline{\lambda_1}\ \overline{a_1} + \dots + \overline{\lambda_n}\ \overline{a_n} = 0$ is a non-trivial relation in R/pR with coefficients in $\mathbb{Z}_p$, in contradiction to $\overline{a_1}, \dots, \overline{a_n}$ being independent over $\mathbb{Z}_p$.

(b) We will show that $|R/mR| < \infty$ for all $m \in \mathbb{Z}\backslash\{0\}$.

In fact, this follows by induction on the number of prime factors in m: for one prime factor the statement is just that of (a), and for more prime factors it follows from the exact sequence of Abelian groups

$$0 \longrightarrow R/m_1R \xrightarrow{\cdot m_2} R/m_1m_2R \longrightarrow R/m_2R \longrightarrow 0,$$

since this means that $|R/m_1m_2R| = |R/m_1R| \cdot |R/m_2R| < \infty$.

(c) Now let $I \trianglelefteq R$ be any non-zero ideal. We claim that $m \in I$ for some $m \in \mathbb{Z}\backslash\{0\}$.

Otherwise we would have

$$\dim R/I = \dim \mathbb{Z}/(I \cap \mathbb{Z}) = \dim \mathbb{Z} = 1$$

by Lemma 11.8, since R/I is integral over $\mathbb{Z}/(I \cap \mathbb{Z})$ by Lemma 9.7 (a). But $\dim R$ has to be bigger than $\dim R/I$, since a chain of prime ideals in R/I corresponds to a chain of prime ideals in R containing I, which can always be extended to a longer chain by the zero ideal since R is an integral domain. Hence $\dim R > 1$, a contradiction.

Putting everything together, we can choose a non-zero $m \in I \cap \mathbb{Z}$ by (c), so that $mR \trianglelefteq I$. Hence $|I/mR| \leq |R/mR| < \infty$ by (b), so $I/mR = \{\overline{a_1}, \dots, \overline{a_n}\}$ for some $a_1, \dots, a_n \in I$. But then the ideal $I = (a_1, \dots, a_n, m)$ is finitely generated, and hence R is Noetherian. □

Example 13.6. Consider again the ring $R = \mathbb{Z}[\sqrt{5}\,i]$ of Example 8.3 (b). By Example 9.16, it is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{5}\,i)$. Hence Proposition 13.5 shows that R is a Dedekind domain.

We see from this example that a Dedekind domain is in general not a unique factorization domain, as e. g. by Example 8.3 (b) the element 2 is irreducible, but not prime in R, so that it does not have a factorization into prime elements. However, we will prove now that a Dedekind domain always has an analogue of the unique factorization property for *ideals*, i. e. every non-zero ideal can be written uniquely as a product of non-zero prime ideals (which are then also maximal since Dedekind domains are 1-dimensional). In fact, this is the most important property of Dedekind domains in practice.

Proposition 13.7 (Prime factorization of ideals in Dedekind domains)**.** *Let R be a Dedekind domain.*

(a) *Let $P \trianglelefteq R$ be a maximal ideal, and let $Q \trianglelefteq R$ be any ideal. Then*

$$Q \text{ is } P\text{-primary} \quad \Leftrightarrow \quad Q = P^k \text{ for some } k \in \mathbb{N}_{>0}.$$

Moreover, the number k is unique in this case.

(b) *Any non-zero ideal $I \trianglelefteq R$ has a "prime factorization"*

$$I = P_1^{k_1} \cdot \ldots \cdot P_n^{k_n}$$

with $k_1, \ldots, k_n \in \mathbb{N}_{>0}$ and distinct maximal ideals $P_1, \ldots, P_n \trianglelefteq R$. It is unique up to permutation of the factors, and $P_1, \ldots, P_n$ are exactly the associated prime ideals of I.

Proof.

(a) The implication "$\Leftarrow$" holds in arbitrary rings by Lemma 8.12 (b), so let us show the opposite direction "$\Rightarrow$". Let Q be P-primary, and consider the localization map $R \to R_P$. Then Q^e is a non-zero ideal in the localization R_P, which is a discrete valuation ring by Remark 13.2. So by Corollary 12.17 we have $Q^e = (P^e)^k$ for some k, and hence $Q^e = (P^k)^e$ as extension commutes with products by Exercise 1.19 (c). Contracting this equation now gives $Q = P^k$ by Lemma 8.33, since Q and P^k are both P-primary by Lemma 8.12 (b).

The number k is unique since $P^k = P^l$ for $k \neq l$ would imply $(P^e)^k = (P^e)^l$ by extension, in contradiction to Corollary 12.17.

(b) As R is Noetherian, the ideal I has a minimal primary decomposition $I = Q_1 \cap \cdots \cap Q_n$ by Corollary 8.21. Since I is non-zero, the corresponding associated prime ideals $P_1, \ldots, P_n$ of these primary ideals are distinct and non-zero, and hence maximal as $\dim R = 1$. In particular, there are no strict inclusions among the ideals $P_1, \ldots, P_n$, and thus all of them are minimal over I. By Proposition 8.34 this means that the ideals $Q_1, \ldots, Q_n$ in our decomposition are unique.

Now by (a) we have $Q_i = P_i^{k_i}$ for unique $k_i \in \mathbb{N}_{>0}$ for $i = 1, \ldots, n$. This gives us a unique decomposition $I = P_1^{k_1} \cap \cdots \cap P_n^{k_n}$, and thus also a unique factorization $I = P_1^{k_1} \cdot \ldots \cdot P_n^{k_n}$ by Exercise 1.8 since the ideals $P_1^{k_1}, \ldots, P_n^{k_n}$ are pairwise coprime by Exercise 2.24. □

Example 13.8. Recall from Examples 8.3 (b) and 13.6 that the element 2 in the Dedekind domain $R = \mathbb{Z}[\sqrt{5}i]$ does not admit a factorization into prime elements. But by Proposition 13.7 (b) the ideal (2) must have a decomposition as a product of maximal ideals (which cannot all be principal, as otherwise we would have decomposed the number 2 into prime factors). Concretely, we claim that this decomposition is

$$(2) = (2, 1 + \sqrt{5}i)^2.$$

To see this, note first that the ideal $(2, 1 + \sqrt{5}i)$ is maximal by Lemma 2.3 (b) since the quotient

$$\mathbb{Z}[\sqrt{5}i]/(2, 1 + \sqrt{5}i) \;\cong\; \mathbb{Z}/(2) \;\cong\; \mathbb{Z}_2$$

is a field. Moreover, we have $(2) \subset (2, 1 + \sqrt{5}i)^2$ since

$$2 = (1 + \sqrt{5}i)^2 - 2^2 - 2\sqrt{5}i(1 + \sqrt{5}i) \quad \in (2, 1 + \sqrt{5}i)^2,$$

and $(2, 1 + \sqrt{5}i)^2 \subset (2)$ as

$$2^2 \in (2), \quad 2(1 + \sqrt{5}i) \in (2), \quad \text{and } (1 + \sqrt{5}i)^2 = -4 + 2\sqrt{5}i \in (2).$$

To understand the geometric meaning of the prime factorization of ideals we need a lemma first.

Lemma 13.9 (Ideals in Dedekind domains)**.** *Let R be a Dedekind domain.*

(a) *For all distinct maximal ideals $P_1, \ldots, P_n$ of R and $k_1, \ldots, k_n, l_1, \ldots, l_n \in \mathbb{N}$ we have*

$$P_1^{k_1} \cdot \ldots \cdot P_n^{k_n} \subset P_1^{l_1} \cdot \ldots \cdot P_n^{l_n} \qquad \Leftrightarrow \qquad l_i \leq k_i \text{ for all } i = 1, \ldots, n.$$

(b) *For any $a \in R\backslash\{0\}$ we have*

$$(a) = P_1^{\nu_1(a)} \cdot \ldots \cdot P_n^{\nu_n(a)},$$

where $P_1, \ldots, P_n$ are the associated prime ideals of (a), and ν_i denotes the valuation of the discrete valuation ring R_{P_i} (restricted to R).

Proof. By Exercise 6.29 (a) ideal containment is a local property, i. e. we can check it on all localizations R_P for maximal ideals P. Moreover, products commute with localization by Exercise 1.19 (c), and the localization of P_i at a maximal ideal $P \neq P_i$ is the unit ideal by Example 6.25 (a). Hence:

(a) We have

$$\begin{aligned} P_1^{k_1} \cdot \ldots \cdot P_n^{k_n} \subset P_1^{l_1} \cdot \ldots \cdot P_n^{l_n} &\Leftrightarrow (P_i^e)^{k_i} \subset (P_i^e)^{l_i} \text{ in } R_{P_i} \text{ for all } i \\ &\Leftrightarrow l_i \leq k_i \text{ for all } i. \qquad \text{(Corollary 12.17)} \end{aligned}$$

(b) By Proposition 13.7 (b) we know that $(a) = P_1^{k_1} \cdot \ldots \cdot P_n^{k_n}$ for suitable $k_1, \ldots, k_n \in \mathbb{N}$ if $P_1, \ldots, P_n$ are the associated prime ideals of (a). To determine the exponent k_i for $i = 1, \ldots, n$, we localize at R_{P_i} to get $(a) = (P_i^e)^{k_i}$ in the discrete valuation ring R_{P_i}, and use Proposition 12.13 to conclude from this that $k_i = \nu_i(a)$. □

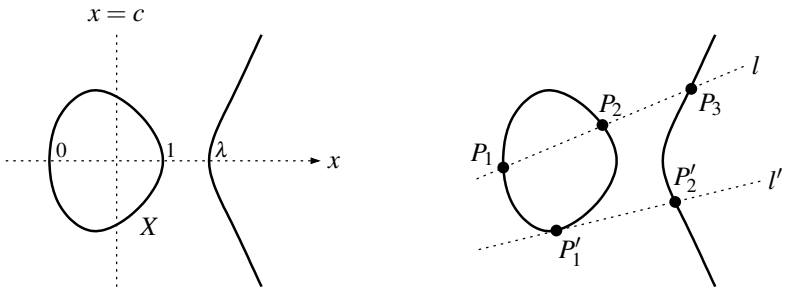
Remark 13.10. If a is a non-zero element in a Dedekind domain R and $P \trianglelefteq R$ a maximal ideal that is not an associated prime ideal of (a), the same argument as in the proof of Lemma 13.9 (b) shows that the valuation of a in the discrete valuation ring R_P is 0. Hence the ideals $P_1, \ldots, P_n$ in the statement of this lemma are exactly the maximal ideals of R so that the valuation of a in the corresponding discrete valuation ring is non-zero.

Remark 13.11 (Geometric interpretation of the prime factorization of ideals)**.** Let X be an irreducible smooth curve over an algebraically closed field, so that its coordinate ring $R = A(X)$ is a Dedekind domain by Example 13.4 (b). Now let $f \in R$ be a non-zero polynomial function on X, and let $a_1, \ldots, a_n \in X$ be the zeroes of f, with corresponding maximal ideals $P_1, \ldots, P_n \trianglelefteq R$. Moreover, for $i = 1, \ldots, n$ let k_i be the order of vanishing of f at a_i as in Remark 12.2, i. e. the valuation of f in the ring R_{P_i} of local functions on X at a_i. Then Lemma 13.9 (b) (together with Remark 13.10) states that

$$(f) = P_1^{k_1} \cdot \ldots \cdot P_n^{k_n}.$$

In other words, the prime factorization of a principal ideal (f) in the coordinate ring of X encodes the orders of vanishing of the function f at all points of X. Here is a concrete example of this construction that will also be used later on in Example 13.29.

Example 13.12. Consider the complex plane cubic curve $X = V(y^2 - x(x-1)(x-\lambda)) \subset \mathbb{A}^2_{\mathbb{C}}$ for some $\lambda \in \mathbb{C}\backslash\{0,1\}$. The picture (a) below shows approximately the real points of X in the case $\lambda \in \mathbb{R}_{>1}$: the vertical line $x = c$ for $c \in \mathbb{R}$ intersects X in two real points symmetric with respect to this axis if $0 < c < 1$ or $c > \lambda$, in exactly the point $(c,0)$ if $c \in \{0, 1, \lambda\}$, and in no real point in all other cases.



(a) (b)

It is easy to check as in Example 11.39 (b) that all points of X are smooth, so that the coordinate ring $R = \mathbb{C}[x,y]/(y^2 - x(x-1)(x-\lambda))$ of X is a Dedekind domain by Example 13.4 (b).

Now let $l \in R$ be a general linear function as in picture (b) above. On the curve X it vanishes at three points (to order 1) since the cubic equation $y^2 = x(x-1)(x-\lambda)$ together with a general linear equation in x and y will have three solutions. If P_1, P_2, and P_3 are the maximal ideals in R corresponding to these points, Remark 13.11 shows that $(l) = P_1 \cdot P_2 \cdot P_3$ in R.

Note that for special linear functions it might happen that some of these points coincide, as in the case of l' above which vanishes to order 2 at the point P_1'. Consequently, in this case we get $(l') = P_1'^2 \cdot P_2$.

For computational purposes, the unique factorization property for ideals allows us to perform calculations with ideals in Dedekind domains very much in the same way as in principal ideal domains. For example, the following Proposition 13.13 is entirely analogous (both in its statement and in its proof) to Example 1.4.

Proposition 13.13 (Operations on ideals in Dedekind domains)**.** *Let I and J be two non-zero ideals in a Dedekind domain, with prime factorizations*

$$I = P_1^{k_1} \cdot \ldots \cdot P_n^{k_n} \quad \text{and} \quad J = P_1^{l_1} \cdot \ldots \cdot P_n^{l_n}$$

as in Proposition 13.7, where $P_1, \ldots, P_n$ are distinct maximal ideals and $k_1, \ldots, k_n, l_1, \ldots, l_n \in \mathbb{N}$. Then

$$\begin{aligned} I + J &= P_1^{m_1} \cdot \ldots \cdot P_n^{m_n} && \text{with } m_i = \min(k_i, l_i), \\ I \cap J &= P_1^{m_1} \cdot \ldots \cdot P_n^{m_n} && \text{with } m_i = \max(k_i, l_i), \\ I \cdot J &= P_1^{m_1} \cdot \ldots \cdot P_n^{m_n} && \text{with } m_i = k_i + l_i \end{aligned}$$

for $i = 1, \ldots, n$. In particular, $I \cdot J = (I+J) \cdot (I \cap J)$.

Proof. By Proposition 13.7 (b) we can write all three ideals as $P_1^{m_1} \cdot \ldots \cdot P_n^{m_n}$ for suitable $m_1, \ldots, m_n$ (if we possibly enlarge the set of maximal ideals occurring in the factorizations). So it only remains to determine the numbers $m_1, \ldots, m_n$ for the three cases.

The ideal $I + J$ is the smallest ideal containing both I and J. By Lemma 13.9 (a) this means that m_i is the biggest number less than or equal to both k_i and l_i, i. e. $\min(k_i, l_i)$. Analogously, the intersection $I \cap J$ is the biggest ideal contained in both I and J, so in this case m_i is the smallest number greater than or equal to both k_i and l_i, i. e. $\max(k_i, l_i)$. The exponents $m_i = k_i + l_i$ for the product are obvious. □

As a Dedekind domain is in general not a unique factorization domain, it clearly follows from Example 8.3 (a) that it is usually not a principal ideal domain either. However, a surprising result following from the computational rules in Proposition 13.13 is that every ideal in a Dedekind domain can be generated by *two* elements. In fact, there is an even stronger statement:

Proposition 13.14. *Let R be a Dedekind domain, and let a be a non-zero element in an ideal $I \trianglelefteq R$. Then there is an element $b \in R$ such that $I = (a,b)$.*

In particular, every ideal in R can be generated by two elements.

Proof. By assumption $(a) \subset I$ are non-zero ideals, so we know by Proposition 13.7 (b) and Lemma 13.9 (a) that

$$(a) = P_1^{k_1} \cdot \ldots \cdot P_n^{k_n} \qquad \text{and} \qquad I = P_1^{l_1} \cdot \ldots \cdot P_n^{l_n}$$

for suitable distinct maximal ideals $P_1, \ldots, P_n \trianglelefteq R$ and natural numbers $l_i \leq k_i$ for all $i = 1, \ldots, n$. By the uniqueness part of Proposition 13.7 (b) we can pick elements

$$b_i \in P_1^{l_1+1} \cdot \ldots \cdot P_i^{l_i} \cdot \ldots \cdot P_n^{l_n+1} \setminus P_1^{l_1+1} \cdot \ldots \cdot P_i^{l_i+1} \cdot \ldots \cdot P_n^{l_n+1} \quad \subset I$$

for all i. Then $b_i \in P_j^{l_j+1}$ for all $j \neq i$, but $b_i \notin P_i^{l_i+1}$, since otherwise by Proposition 13.13

$$b_i \in P_i^{l_i+1} \cap \left(P_1^{l_1+1} \cdot \ldots \cdot P_i^{l_i} \cdot \ldots \cdot P_n^{l_n+1}\right) = P_1^{l_1+1} \cdot \ldots \cdot P_n^{l_n+1}$$

in contradiction to our choice of b_i. Hence

$$b := b_1 + \cdots + b_n \quad \notin P_i^{l_i+1}$$

for all i, but certainly $b \in I$. We now claim that $I = (a,b)$. To see this, note first that by Proposition 13.13 the prime factorization of $(a,b) = (a)+(b)$ can contain at most the maximal ideals occurring in (a), so we can write $(a,b) = P_1^{m_1} \cdot \cdots \cdot P_n^{m_n}$ for suitable $m_1, \ldots, m_n$. But by Lemma 13.9 (a) we see that:

- $l_i \leq m_i$ for all i since $(a,b) \subset I$;
- $m_i \leq l_i$ for all i since $b \notin P_i^{l_i+1}$, and hence $(a,b) \not\subset P_i^{l_i+1}$.

Therefore we get $m_i = l_i$ for all i, which means that $I = (a,b)$. □

26

We have now studied prime factorizations of ideals in Dedekind domains in some detail. However, recall that the underlying valuations on the local rings are defined originally not only on these discrete valuation rings, but also on their quotient field. Geometrically, this means that we can equally well consider orders of rational functions, i. e. quotients of polynomials, at a smooth point of a curve. These orders can then be positive (if the function has a zero), negative (if it has a pole), or zero (if the function has a non-zero value at the given point). Let us now transfer this extension to the quotient field to the global case of a Dedekind domain R. Instead of ideals we then have to consider corresponding structures (i. e. R-submodules) that do not lie in R itself, but in its quotient field $\operatorname{Quot} R$.

Definition 13.15 (Fractional ideals)**.** Let R be an integral domain with quotient field $K = \operatorname{Quot} R$.

(a) A **fractional ideal** of R is an R-submodule I of K such that $aI \subset R$ for some $a \in R \setminus \{0\}$.

(b) For $a_1, \ldots, a_n \in K$ we set as expected

$$(a_1, \ldots, a_n) := Ra_1 + \cdots + Ra_n$$

and call this the fractional ideal generated by $a_1, \ldots, a_n$ (note that this is in fact a fractional ideal since we can take for a in (a) the product of the denominators of $a_1, \ldots, a_n$).

Example 13.16.

(a) A subset I of an integral domain R is a fractional ideal of R if and only if it is an ideal in R (the condition in Definition 13.15 (a) that $aI \subset R$ for some a is vacuous in this case since we can always take $a = 1$).

(b) $\left(\frac{1}{2}\right) = \frac{1}{2}\mathbb{Z} \subset \mathbb{Q}$ is a fractional ideal of $\mathbb{Z}$. In contrast, the localization $\mathbb{Z}_{(2)} \subset \mathbb{Q}$ of Example 6.5 (d) is not a fractional ideal of $\mathbb{Z}$: it is a $\mathbb{Z}$-submodule of $\mathbb{Q}$, but there is no non-zero integer a such that $a\mathbb{Z}_{(2)} \subset \mathbb{Z}$.

Remark 13.17. Let R be an integral domain with quotient field K.

(a) Let I be a fractional ideal of R. The condition $aI \subset R$ of Definition 13.15 (a) ensures that I is finitely generated if R is Noetherian: as aI is an R-submodule in R it is actually an ideal in R, and hence of the form $aI = (a_1, \ldots, a_n)$ for some $a_1, \ldots, a_n \in R$. But then also $I = \left(\frac{a_1}{a}, \ldots, \frac{a_n}{a}\right)$ is finitely generated.

(b) The standard operations on ideals of Construction 1.1 can easily be extended to fractional ideals, or more generally to R-submodules of K. In the following, we will mainly need products and quotients: for two R-submodules I and J of K we set

$$IJ := \left\{ \sum_{i=1}^{n} a_i b_i : n \in \mathbb{N},\ a_1, \ldots, a_n \in I,\ b_1, \ldots, b_n \in J \right\},$$
$$I :_K J := \{a \in K : aJ \subset I\}.$$

Note that IJ is just the smallest R-submodule of K containing all products ab for $a \in I$ and $b \in J$, as expected. The index K in the notation of the quotient $I :_K J$ distinguishes this construction from the ordinary ideal quotient $I : J = \{a \in R : aJ \subset I\}$ — note that both quotients are defined but different in general if both I and J are ordinary ideals in R.

Exercise 13.18. Let K be the quotient field of a Noetherian integral domain R. Prove that for any two fractional ideals I and J of R and any multiplicatively closed subset $S \subset R$ we have:

(a) $S^{-1}(IJ) = S^{-1}I \cdot S^{-1}J$,

(b) $S^{-1}(I :_K J) = S^{-1}I :_K S^{-1}J$.

Our goal in the following will be to check whether the multiplication as in Remark 13.17 (b) defines a group structure on the set of all non-zero fractional ideals of an integral domain R. As associativity and the existence of the neutral element R are obvious, the only remaining question is the existence of inverse elements, i. e. whether for a given non-zero fractional ideal I there is always another fractional ideal J with $IJ = R$. We will see now that this is indeed the case for Dedekind domains, but not in general integral domains.

Definition 13.19 (Invertible and principal ideals)**.** Let R be an integral domain, and let I be an R-submodule of $K = \operatorname{Quot} R$.

(a) I is called an **invertible ideal** or **(Cartier) divisor** if there is an R-submodule of J of K such that $IJ = R$.

(b) I is called **principal** if $I = (a)$ for some $a \in K$.

Lemma 13.20. *As above, let K be the quotient field of an integral domain R, and let I be an R-submodule of K.*

(a) *If I is an invertible ideal with $IJ = R$, then $J = R :_K I$.*

(b) *We have the implications*

$$I \text{ non-zero principal} \quad \Rightarrow \quad I \text{ invertible} \quad \Rightarrow \quad I \text{ fractional}.$$

Proof.

(a) By definition of the quotient, $IJ = R$ implies $R = IJ \subset I(R :_K I) \subset R$, so we have equality $IJ = I(R :_K I)$. Multiplication by J now gives the desired result $J = R :_K I$.

(b) If $I = (a)$ is principal with $a \in K^*$ then $(a) \cdot \left(\frac{1}{a}\right) = R$, hence I is invertible.

Now let I be an invertible ideal, i. e. $I(R :_K I) = R$ by (a). This means that

$$\sum_{i=1}^{n} a_i b_i = 1$$

for some $n \in \mathbb{N}$ and $a_1, \dots, a_n \in I$ and $b_1, \dots, b_n \in R :_K I$. Then we have for all $b \in I$

$$b = \sum_{i=1}^{n} a_i \underbrace{b_i b}_{\in R}.$$

So if we let $a \in R$ be the product of the denominators of $a_1, \dots, a_n$, we get $ab \in R$. Therefore $aI \subset R$, i. e. I is fractional. □

Example 13.21.

(a) Let R be a principal ideal domain. Then every non-zero fractional ideal I of R is principal: we have $aI \subset R$ for some $a \in \operatorname{Quot} R \backslash \{0\}$. This is an ideal in R, so of the form (b) for some $b \in R \backslash \{0\}$. It follows that $I = \left(\frac{b}{a}\right)$, i. e. I is principal.

In particular, Lemma 13.20 (b) implies that the notions of principal, invertible, and fractional ideals all agree for non-zero ideals in a principal ideal domain.

(b) The ideal $I = (x, y)$ in the ring $R = \mathbb{R}[x, y]$ is not invertible: setting $K = \operatorname{Quot} R = \mathbb{R}(x, y)$ we have

$$R :_K I = \{f \in \mathbb{R}(x, y) : xf \in \mathbb{R}[x, y] \text{ and } yf \in \mathbb{R}[x, y]\} = \mathbb{R}[x, y].$$

But $I(R :_K I) = (x, y)\mathbb{R}[x, y] \neq R$, and hence I is not invertible by Lemma 13.20 (a).

Proposition 13.22 (Invertible = fractional ideals in Dedekind domains)**.** *In a Dedekind domain, every non-zero fractional ideal is invertible.*

Proof. Let I be a non-zero fractional ideal of a Dedekind domain R. Assume that I is not invertible, which means by Lemma 13.20 (a) that $I\,(R:_K I) \neq R$. As the inclusion $I\,(R:_K I) \subset R$ is obvious, this means that $I\,(R:_K I)$ is a proper ideal of R. It must therefore be contained in a maximal ideal P by Corollary 2.17.

Extending this inclusion by the localization map $R \to R_P$ then gives $I^e\,(R_P:_K I^e) \subset P^e$ by Exercise 13.18. This means by Lemma 13.20 (a) that I^e is not invertible in R_P. But R_P is a discrete valuation ring by Remark 13.2, hence a principal ideal domain by Proposition 12.14, and so I^e cannot be a fractional ideal either by Example 13.21 (a). This is clearly a contradiction, since I is assumed to be fractional. □

Remark 13.23. By construction, the invertible ideals of an integral domain R form an Abelian group under multiplication, with neutral element R. As expected, we will write the inverse $R:_K I$ of an invertible ideal I as in Lemma 13.20 (a) also as I^{-1}. Proposition 13.22 tells us that for Dedekind domains this group of invertible ideals can also be thought of as the group of non-zero fractional ideals.

Moreover, it is obvious that the non-zero principal fractional ideals form a subgroup:

- every non-zero principal fractional ideal is invertible by Lemma 13.20 (b);
- the neutral element $R = (1)$ is principal;
- for two non-zero principal fractional ideals (a) and (b) their product (ab) is principal;
- for any non-zero principal fractional ideal (a) its inverse (a^{-1}) is also principal.

So we can define the following groups that are naturally attached to any integral domain.

Definition 13.24 (Ideal class groups)**.** Let R be an integral domain.

(a) The group of all invertible ideals of R (under multiplication) is called the **ideal group** or **group of (Cartier) divisors** of R. We denote it by $\operatorname{Div} R$.

(b) We denote by $\operatorname{Prin} R \leq \operatorname{Div} R$ the subgroup of (non-zero) principal ideals.

(c) The quotient $\operatorname{Pic} R := \operatorname{Div} R / \operatorname{Prin} R$ of all invertible ideals modulo principal ideals is called the **ideal class group**, or **group of (Cartier) divisor classes**, or **Picard group** of R.

Let us restrict the study of these groups to Dedekind domains. In this case, the structure of the ideal group is easy to understand with the following proposition.

Proposition 13.25 (Prime factorization for invertible ideals)**.** *Let I be an invertible ideal in a Dedekind domain R. Then $I = P_1^{k_1} \cdot \dots \cdot P_n^{k_n}$ for suitable distinct maximal ideals $P_1, \dots, P_n$ and $k_1, \dots, k_n \in \mathbb{Z}$, and this representation is unique up to permutation of the factors.*

Proof. By Lemma 13.20 (b) we know that aI is an ideal in R for a suitable $a \in R \backslash \{0\}$. Now by Proposition 13.7 (b) we have $aI = P_1^{r_1} \cdot \dots \cdot P_n^{r_n}$ and $(a) = P_1^{s_1} \cdot \dots \cdot P_n^{s_n}$ for suitable distinct maximal ideals $P_1, \dots, P_n$ and $r_1, \dots, r_n, s_1, \dots, s_n \in \mathbb{N}$, and so we get a factorization

$$I = (a)^{-1} \cdot aI = P_1^{r_1 - s_1} \cdot \dots \cdot P_n^{r_n - s_n}$$

as desired. Moreover, if we have two such factorizations $P_1^{k_1} \cdot \dots \cdot P_n^{k_n} = P_1^{l_1} \cdot \dots \cdot P_n^{l_n}$ with $k_1, \dots, k_n, l_1, \dots, l_n \in \mathbb{Z}$, we can multiply this equation with suitable powers of $P_1, \dots, P_n$ so that the exponents become non-negative. The uniqueness statement then follows from the corresponding one in Proposition 13.7 (b). □

Remark 13.26. Let R be a Dedekind domain. Proposition 13.25 states that the ideal group $\operatorname{Div} R$ is in fact easy to describe: we have an isomorphism

$$\operatorname{Div} R \to \{\varphi : \operatorname{mSpec} R \to \mathbb{Z} : \varphi \text{ is non-zero only on finitely many maximal ideals}\}$$

sending any invertible ideal $P_1^{k_1} \cdot \dots \cdot P_n^{k_n}$ to the map $\varphi : \operatorname{mSpec} R \to \mathbb{Z}$ with only non-zero values $\varphi(P_i) = k_i$ for $i = 1, \dots, n$. This is usually called the *free Abelian group* generated by $\operatorname{mSpec} R$ (since the maximal ideals generate this group, and there are no non-trivial relations among these generators).

The group $\operatorname{Div} R$ is therefore very "big", and also at the same time not very interesting since its structure is so simple. In contrast, the ideal class group $\operatorname{Pic} R = \operatorname{Div} R / \operatorname{Prin} R$ is usually much smaller, and contains a lot of information on R. It is of great importance both in geometry and number theory. It is out of the scope of this course to study it in detail, but we will at least give one interesting example in each of these areas. But first let us note that the ideal class group can be thought of as measuring "how far away R is from being a principal ideal domain":

Proposition 13.27. *For a Dedekind domain R the following statements are equivalent:*

(a) *R is a principal ideal domain.*

(b) *R is a unique factorization domain.*

(c) *$\operatorname{Pic} R$ is the trivial group, i. e. $|\operatorname{Pic} R| = 1$.*

Proof.

(a) $\Rightarrow$ (b) is Example 8.3 (a).

(b) $\Rightarrow$ (c): By Exercise 8.32 (b) every maximal ideal $P \trianglelefteq R$ (which is also a minimal non-zero prime ideal as $\dim R = 1$) is principal. But these maximal ideals generate the group $\operatorname{Div} R$ by Proposition 13.25, and so we have $\operatorname{Prin} R = \operatorname{Div} R$, i. e. $|\operatorname{Pic} R| = 1$.

(c) $\Rightarrow$ (a): By Definition 13.24 the assumption $|\operatorname{Pic} R| = 1$ means that every invertible ideal is principal. But every non-zero ideal of R is invertible by Proposition 13.22, so the result follows. □

Example 13.28 (A non-trivial Picard group in number theory)**.** Let $R = \mathbb{Z}[\sqrt{5}\,i]$ be the integral closure of $\mathbb{Z}$ in $K = \mathbb{Q}(\sqrt{5}\,i)$ as in Examples 8.3 (b) and 13.6. We have seen there already that R is a Dedekind domain but not a principal ideal domain: the ideal $I_1 := (2, 1 + \sqrt{5}\,i)$ is not principal. In particular, the class of I_1 in the Picard group $\operatorname{Pic} R$ is non-trivial. We will now show that this is the only non-trivial element in $\operatorname{Pic} R$, i. e. that $|\operatorname{Pic} R| = 2$ and thus necessarily $\operatorname{Pic} R \cong \mathbb{Z}/2\mathbb{Z}$ as a group, with the two elements given by the classes of the ideals $I_0 := (1)$ and I_1. Unwinding Definition 13.24, we therefore claim that every invertible ideal of R is of the form aI_0 or aI_1 for some $a \in K^*$.

So let I be an invertible ideal of R. Then I is also a non-zero fractional ideal by Lemma 13.20 (b), and thus there is a number $b \in K^*$ with $bI \subset R$. But note that

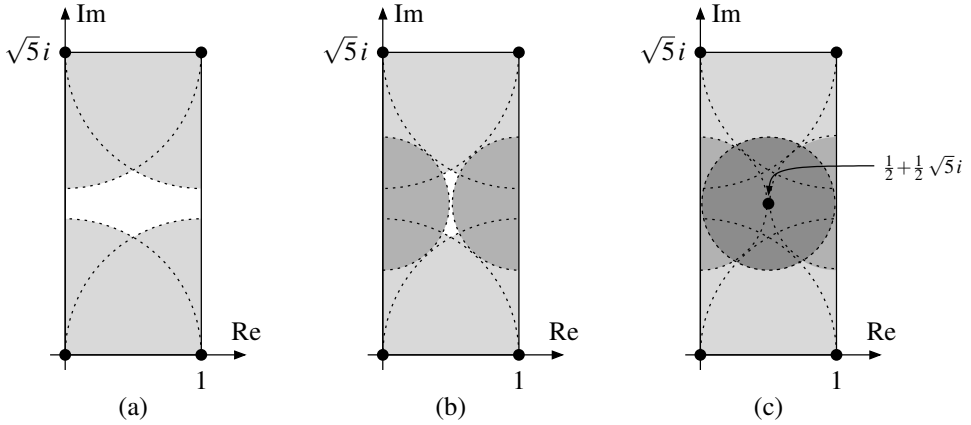
$$R = \mathbb{Z}[\sqrt{5}\,i] = \{m + n\sqrt{5}\,i : m, n \in \mathbb{Z}\}$$

is just a rectangular lattice in the complex plane, and so there is an element $c \in bI \subset K$ of minimal non-zero absolute value. Replacing I by $\frac{b}{c} I$ (which is an equivalent element in the Picard group) we can therefore assume that I is an invertible ideal with $1 \in I$, hence $R \subset I$, and that 1 is a non-zero element of minimal absolute value in I.

Let us find out whether I can contain more elements except the ones of R. To do this, it suffices to consider points in the rectangle with corners 0, 1, $\sqrt{5}\,i$, and $1 + \sqrt{5}\,i$ shown in the pictures below: I is an additive subgroup of $\mathbb{C}$ containing R, and so the complete set of points in I will just be an R-periodic repeated copy of the points in this rectangle.

To figure out if I contains more points in this rectangle, we proceed in three steps illustrated below.

(a) By construction, I contains no points of absolute value less than 1 except the origin, i. e. no points in the open disc $U_1(0)$ with radius 1 and center point 0. Likewise, because of the R-periodicity of I, the ideal also does not contain any points in the open unit discs around the other corners of the rectangle, except these corner points themselves. In other words, the shaded area in picture (a) below cannot contain any points of I except the corner points.



(b) Now consider the open disc $U_{\frac{1}{2}}(\frac{1}{2}\sqrt{5}i)$, whose intersection with our rectangle is the left dark half-circle in picture (b) above. Again, it cannot contain any points of I except its center: as I is an R-module, any non-center point $a \in I$ in this disc would lead to a non-center point $2a \in I$ in the disc $U_1(\sqrt{5}i)$, which we excluded already in (a). But in fact the center point $\frac{1}{2}\sqrt{5}i$ cannot lie in I either, since then we would have

$$\sqrt{5}i \cdot \frac{1}{2}\sqrt{5}i + 3 \cdot 1 = \frac{1}{2} \in I$$

as well, in contradiction to (a). In the same way we see that the open disc $U_{\frac{1}{2}}(1+\frac{1}{2}\sqrt{5}i)$ does not contain any points of I either. Hence the complete shaded area in picture (b) is excluded now for points of I.

(c) Finally, consider the open disc $U_{\frac{1}{2}}(\frac{1}{2}+\frac{1}{2}\sqrt{5}i)$, shown in picture (c) above in dark color. For the same reason as in (b), no point in this disc except the center can lie in I. As our discs now cover the complete rectangle, this means that the only point in our rectangle except the corners that can be in I is $\frac{1}{2}+\frac{1}{2}\sqrt{5}i$. This leads to exactly two possibilities for I:

$$\text{either} \quad I = R = I_0 \qquad \text{or} \quad I = \left(1, \frac{1}{2}+\frac{1}{2}\sqrt{5}i\right) = \frac{1}{2}I_1.$$

In fact, we know already that this last case $\frac{1}{2}I_1$ is an invertible ideal of R, so that this time (in contrast to (b) above) it does not lead to a contradiction if the center point of the disc lies in I.

Altogether, we thus conclude that $|\operatorname{Pic} R| = 2$, i. e. $\operatorname{Pic} R \cong \mathbb{Z}/2\mathbb{Z}$, with the class of I_0 being neutral and I_1 being the unique other element. We have indeed also checked already that I_1 is its own inverse in $\operatorname{Pic} R$, since by Example 13.8

$$I_1 \cdot I_1 = (2)$$

is principal, and hence the neutral element in $\operatorname{Pic} R$.

Example 13.29 (A non-trivial Picard group in geometry)**.** Consider again the complex plane cubic curve $X = V(y^2 - x(x-1)(x-\lambda)) \subset \mathbb{A}^2_{\mathbb{C}}$ for some $\lambda \in \mathbb{C}\backslash\{0,1\}$ as in Example 13.12. We have already seen that its coordinate ring $R = A(X)$ is a Dedekind domain. Let us now study its ideal class group $\operatorname{Pic} R$.

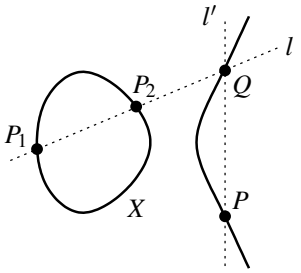
Note that there is an obvious map

$$\varphi : X \to \operatorname{Pic} R, \quad a \mapsto \overline{I(a)}$$

that assigns to each point of X the class of its maximal ideal in $\operatorname{Pic} R = \operatorname{Div} R / \operatorname{Prin} R$. The surprising fact is that this map φ is injective with its image equal to $\operatorname{Pic} R \backslash \{\overline{(1)}\}$, i. e. to $\operatorname{Pic} R$ without its neutral element. We can therefore make it bijective by adding a "point at infinity" to X that is mapped to the missing point $\overline{(1)}$ of $\operatorname{Pic} R$. This is particularly interesting as we then have a bijection between

two completely different algebraic structures: X is a variety (but a priori not a group) and $\operatorname{Pic} R$ is a group (but a priori not a variety). So we can use the bijection φ to make the cubic curve $X \cup \{\infty\}$ into a group, and the group $\operatorname{Pic} R$ into a variety.

We cannot prove this statement or study its consequences here since this would require methods that we have not covered in this course — this is usually done in the "Algebraic Geometry" class. However, we can use our definition of the Picard group and the map φ above to describe the group structure on the curve $X \cup \{\infty\}$ explicitly. To do this, consider two points on the curve with maximal ideals P_1 and P_2, as shown in the picture on the right. Draw the line through these two points; it will intersect X in one more point Q since the cubic equation $y^2 = x(x-1)(x-\lambda)$ together with a linear equation in x and y will have three solutions. By Example 13.12, this means algebraically that there is a linear polynomial $l \in R$ (whose zero locus is this line) such that $(l) = P_1 \cdot P_2 \cdot Q$.



Next, draw the vertical line through Q. By the symmetry of X, it will intersect X in one more point P. Similarly to the above, it follows that there is a linear polynomial l' such that $(l') = Q \cdot P$. But in the Picard group $\operatorname{Pic} R$ this means that

$$\overline{P_1} \cdot \overline{P_2} \cdot \overline{Q} = \overline{(l)} = \overline{(l')} = \overline{Q} \cdot \overline{P}$$

(note that (l) and (l') both define the neutral element in $\operatorname{Pic} R$), and thus that $\overline{P_1} \cdot \overline{P_2} = \overline{P}$. Hence the above geometric construction of P from P_1 and P_2 describes the group structure on $X \cup \{\infty\}$ mentioned above.

Note that it is quite obvious without much theory behind it that this geometric two-line construction can be used to associate to any two points on X (corresponding to P_1 and P_2 above) a third point on X (corresponding to P). The surprising statement here (which is very hard to prove without using Picard groups) is that this gives rise to a group structure on $X \cup \{\infty\}$; in particular that this operation is associative. The neutral element is the additional point ∞ (corresponding to the class of principal ideals in $\operatorname{Pic} R$), and the inverse of a point in X is the other intersection point of the vertical line through this point with X (so that e. g. in the above picture we have $\overline{P}^{-1} = \overline{Q}$).

27