4. Dedekind domains.

In this section we will introduce Dedekind domains (named after Richard Dedekind, German mathematician 1831–1916). Rings of integers of number fields are important examples of Dedekind domains. We show that the ideals of a Dedekind domain admit unique factorization into prime ideals.

Definition. *A commutative ring R is called Noetherian if every ideal of R is finitely generated.*

Lemma 4.1. *Let R be a commutative ring. The following are equivalent:*
(a) R is Noetherian.
(b) Every sequence of ideals of R

$$I_1 \subset I_2 \subset \ldots \subset I_i \subset \ldots$$

stabilizes, i.e. there exists an index i_0 such that $I_i = I_{i_0}$ for all $i \geq i_0$.
(c) Every non-empty collection Ω of R-ideals contains a maximal element i.e. an ideal I such that no ideal $J \in \Omega$ contains I properly.

Proof. *(a) $\Rightarrow$ (b)* Let $I_1 \subset I_2 \subset \ldots \subset I_i \subset \ldots$ be a sequence of ideals of R. Suppose the union $I = \cup_{i \geq 1}$ is generated by $\alpha_1, \ldots, \alpha_m$. For every α_k there exists an index i such that $\alpha_k \in I_i$. Writing N for the maximum of the indices i, we see that $\alpha_k \in I_N$ for all k. Therefore $I = I_N$ and the sequences stabilizes.

(b) $\Rightarrow$ (c) Suppose Ω is a non-empty collection without maximal elements. Pick $I = I_1 \in \Omega$. Since I_1 is not maximal, there exists an ideal $I_2 \in \Omega$ such that $I_1 \subset_{\neq} I_2$. Similarly, there exists an ideal $I_3 \in \Omega$ such that $I_2 \subset_{\neq} I_3$. In this way we obtain a sequence $I_1 \subset I_2 \subset \ldots \subset I_i \subset \ldots$ that does not stabilize. This contradicts the fact that R is Noetherian

(c) $\Rightarrow$ (a) Let I be an ideal of R and let Ω be the collection of ideals $J \subset I$ which are finitely generated. Since $(0) \in \Omega$, we see that $\Omega \neq \emptyset$ and hence contains a maximal element J. If $J \neq I$, we pick $x \in I - J$ and we see that the ideal $J + (x)$ properly contains J and is in Ω. This contradicts the maximality of J. We conclude that $I = J$ and the proof of the lemma is complete.

Rings that appear in algebraic number theory and algebraic geometry are usually Noetherian (named after Emmy Noether, German mathematician 1882–1935). Every principal ideal domain is clearly Noetherian, so fields and the ring $\mathbf{Z}$ are Noetherian rings. According to Exer.4.1., any quotient ring R/I of a Noetherian ring R is again Noetherian. Finite products of Noetherian rings are Noetherian. The famous "Basissatz" of Hilbert (David Hilbert, German mathematician 1862–1943) affirms that the polynomial ring $R[T]$ is Noetherian whenever R is.

Non-Noetherian rings are often very large. For instance, the ring of continuous functions $\mathbf{R} \to \mathbf{R}$ is not Noetherian. Neither is the ring $R[X_1, X_1, X_3, \ldots]$ of polynomials in countably many variables with coefficients in a commutative ring R.

Definition. *Let $R \subset S$ be an extension of commutative rings. An element $x \in S$ is called integral over R, if there exists a monic polynomial $f(T) \in R[T]$ with $f(x) = 0$. A domain*

R is called integrally closed if every element in its field of fractions that is integral over R is actually contained in R.

Using this terminology, one can say that the integers of number fields are, in fact, integral over $\mathbf{Z}$. Let F be a number field. By Prop. 3.3, the field of fractions of the ring of integers O_F of F is equal to F. By Prop.3.6 rings of integers are integrally closed. Other examples of integrally closed rings are provided by Exer.4.3: every unique factorization domain is integrally closed.

Definition. *Let R be a commutative ring. The height of a prime ideal $P = P_0$ of R is the supremum of the integers n for which there exists a chain*

$$P_0 \subset P_1 \subset P_2 \subset \ldots \subset P_n \subset R$$

of distinct prime ideals in R. The Krull dimension of a ring is the supremum of the heights of the prime ideals of R.

For example, a field has Krull dimension 0 and the ring $\mathbf{Z}$ has dimension 1 (Wolfgang Krull, German mathematician 1899–1971). In general, principal ideal domains that are not fields, have dimension 1. It is easy to show that for every field K, the ring of polynomials $K[X_1, \ldots, X_n]$ has dimension at least n. The notion of dimension originates in algebraic geometry: the ring of regular functions on an affine variety of dimension n over a field K has Krull dimension equal to n.

Definition. *A Dedekind domain is a Noetherian, integrally closed domain of dimension at most 1.*

By Exer.4.4, every principal ideal domain R is a Dedekind domain. Its dimension is 0 if R is a field and 1 otherwise. The following proposition gives us many examples of Dedekind domains.

Proposition 4.2. *Let F be a number field. Then the ring of integers O_F of F is a Dedekind domain.*

Proof. Proposition 3.3 says that O_F is integrally closed. Proposition 3.9 (d) and (e) say that O_F is Noetherian and that every non-zero prime ideal of O_F is maximal. This implies that the dimension of O_F is at most 1 and proves the proposition.

Lemma 4.3. *Let R be a Noetherian domain. Then every non-zero ideal of R contains a product of non-zero prime ideals.*

Proof. Suppose that there exists an ideal that does not contain a product of non-zero prime ideals. So, the collection Ω of such ideals is not empty. Since R is Noetherian, we can, by Lemma 4.1 find an ideal $I \in \Omega$ such that every ideal J that properly contains I is not in Ω. Clearly I is not prime itself. Therefore there exist $x, y \notin I$ such that $xy \in I$. The ideals $I + (x)$ and $I + (y)$ are strictly larger than I and hence contain a product of non-zero prime ideals. Say $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subset I + (x)$ and $\mathfrak{p}'_1 \cdot \ldots \cdot \mathfrak{p}'_s \subset I + (y)$. Now we have $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \mathfrak{p}'_1 \cdot \ldots \cdot \mathfrak{p}'_s \subset (I + (x))(I + (y)) \subset I$ contradicting the fact that $I \in \Omega$.

This proves the Lemma.

Lemma 4.3. *Let R be a 1-dimensional Noetherian domain. Then for every proper R-ideal I there exists an element $a \in \mathrm{Frac}(R) - R$ so that aI is contained in R.*

Proof. Since I is proper, it is contained in a maximal ideal $\mathfrak{p}$. Let $x \in I$ be a non-zero element. By part (a), the ideal (x) contains a product of prime ideals. We may and do assume that this product has a *minimal* number of factors. In particular, every proper partial product is not contained in (a). So we have inclusions

$$\mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_t \quad \subset \quad (x) \quad \subset \quad I \quad \subset \quad \mathfrak{p}.$$

One of the prime ideals $\mathfrak{p}_i$ is contained in $\mathfrak{p}$. Since R has Krull domension one, we must have equality. Let's say $\mathfrak{p} = \mathfrak{p}_1$.

Next, let $y \neq 0$ be an element of $\prod_{i=2}^{t} \mathfrak{p}_i$. Then $y \notin (x)$, so that y/x is in the fraction field of R, but not in R itself. Then $a = y/x$ has the required property. Indeed, we have inclusions

$$xaI = yI \subset \mathfrak{p} \cdot \prod_{i=2}^{t} \mathfrak{p}_i \subset (x).$$

The lemma follows by dividing by x.

Lemma 4.4. *Let R be a Dedekind domain. Let $I \subset R$ be an ideal containing $x \neq 0$. Then there is an ideal J of R with the property that $IJ = (x)$.*

Proof. Put $J = \{b \in R : bI \subset (x)\}$. Since it contains x, this is a non-zero R-ideal. The set $\frac{1}{x}IJ$ is also an ideal. If it were a proper ideal, we apply Lemma 4.3 and find an element $a \in \mathrm{Frac}(R) - R$ for which $\frac{a}{x}IJ \subset R$ and hence $aIJ \subset (x)$ and $aIJ \subset I$. The fact that $aIJ \subset I$ implies that elements in aJ are integral and hence in R. By definition of J it follows that $aJ \subset J$. Since R is Noetherian, J is a finitely generated R-ideal. By Exercise 0.0 the element a is integral over R and is hence contained in R. Contradiction.

So we have $\frac{1}{x}IJ = R$. Multiplying by x gives the result.

Corollary 4.5. *Let R be a Dedekind domain and let $I \subset J \subset R$ be non-zero ideals. Then there is a unique ideal $K \subset R$ for which KJ is equal to I.*

Proof. Pick a non-zero element x in I. By Lemma 4.4 there exists an ideal K such that $KJ = (x)$. Then we have $KI \subset (x)$ so that $\frac{1}{x}KI$ is an R-ideal. This ideal works. Indeed, we have $\frac{1}{x}KIJ = I$ as required.

To prove uniqueness, suppose that $K_1J = K_2J = I$ for two R-ideals K_1 and K_2. By Lemma 4.6 there is a non-zero $y \in J$ and and ideal J' so that $JJ' = (y)$. This implies $yK_1 = JJ'K_1 = J'K_2J = yK_2$ and hence $K_1 = K_2$.

Theorem 4.6. *Let R be a Dedekind domain. Then every non-zero R-ideal is a product of prime ideals. Moreover, the product is unique up to order of the factors.*

Proof. Existence: let I be a non-zero R-ideal. If $I = R$, it is equal to an empty product of prime ideals. If $I \neq R$, it is contained in a maximal ideal $\mathfrak{p}_1$. By Corollary 4.5 there exists a non-zero ideal I_1 for which $I = I_1\mathfrak{p}_1$. We have $I \subset I_1$ and this inclusion is proper. Indeed,

if $I = I_1$ we get $I = I\mathfrak{p}_1$. By Lemma 4.6 there is an ideal J so that $IJ = (x)$ for some non-zero $x \in I$. Multiplying by J we get $(x) = x\mathfrak{p}_1$ and hence $\mathfrak{p}_1 = R$, a contradiction.

If $I_1 = R$ we have $I = \mathfrak{p}_1$ and we are done. If not, it is contained in a maximal ideal $\mathfrak{p}_2$. There exists a non-zero ideal I_2 for which $I_1 = I_2\mathfrak{p}_1$. We have $I_1 \subset I_2$. If $I_2 = R$, we have $I_1 = \mathfrak{p}_2$ and hence $I = \mathfrak{p}_1\mathfrak{p}_2$ and we are done. If not, I_2 is contained in a maximal ideal $\mathfrak{p}_3$ ... etcetera. Since R is Noetherian, the sequence of ideals $I \subset I_1 \subset I_2 \subset \ldots$ stabilizes. Since the inclusions are proper, this means that I_k is equal to R when k is sufficiently large.

Uniqueness: if two products $\mathfrak{p}_1 \cdots \mathfrak{p}_t$ and $\mathfrak{q}_1 \cdots \mathfrak{q}_s$ of prime ideals are equal, then we have an inclusion $\mathfrak{p}_1 \cdots \mathfrak{p}_t \subset \mathfrak{q}_1$. this means that $\mathfrak{p}_j \subset \mathfrak{q}_1$ for some index j. We may assume that $j = 1$. Since R has dimension 1, it follows that $\mathfrak{p}_1 = \mathfrak{q}_1$. By Lemma 4.6 there is an ideal J of R for which $J\mathfrak{p}_1 = (x)$ for some element $x \in \mathfrak{p}_1$. Multiplying by J and then dividing by x gives the relation $\mathfrak{p}_2 \cdots \mathfrak{p}_t = \mathfrak{q}_2 \cdots \mathfrak{q}_s$ involving fewer prime ideals. The uniqueness therefore follows by induction.

Definition. *Let R be a Dedekind domain and let I be a non-zero ideal. We let*

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}},$$

where $\mathfrak{p}$ runs over the non-zero prime ideals of R and the exponents $m_{\mathfrak{p}}$ are in $\mathbf{Z}_{\geq 0}$. Only finitely many exponents are non-zero. We put

$$\mathrm{ord}_{\mathfrak{p}}(I) = m_{\mathfrak{p}}.$$

Theorem 4.6 implies

$$\mathrm{ord}_{\mathfrak{p}}(IJ) = \mathrm{ord}_{\mathfrak{p}}(I) + \mathrm{ord}_{\mathfrak{p}}(J)$$

for non-zero ideals I and J and a non-zero prime ideal $\mathfrak{p}$. We would like to say that the $\mathrm{ord}_{\mathfrak{p}}$-function is a group homomorphism, but even though ideal multiplication is associative and commutative with neutral element R, the ideals do not form a group because there are no inverses. Therefore we extend the notion of ideal.

Definition. *Let R be a Dedekind domain with field of fractions K. A fractional ideal of R (or K) is an additive subgroup I of K with the property that for some $\alpha \in K^*$ the group αI is a non-zero ideal of R.*

Ideals of R are clearly fractional ideals. For every $\alpha \in K^*$, the set $(\alpha) = \{\lambda\alpha : \lambda \in R\}$ is a fractional ideal. Ideals of this type are called *principal* ideals.

Proposition 4.7. *Let R be a Dedekind domain with field of fractions K. Then*

(a) Every non-zero ideal of R is a fractional ideal.

(b) If I and J are fractional ideals, then the product IJ defined by

$$IJ = \{\textit{finite sums of products } \alpha_i\beta_i \textit{ with } \alpha_i \in I \textit{ and } \beta_i \in J\}$$

is a fractional ideal.

(c) For every fractional ideal I, the set $I^{-1} = \{\alpha \in K : \alpha I \subset R\}$ is a fractional ideal.

(d) *The fractional ideals form a group $Id(R)$ under multiplication. The neutral element is R and the inverse of a fractional ideal I is I^{-1}.*
(e) *For every $\alpha \in K^*$ the set $(\alpha) = \alpha R = \{\alpha r : r \in R\}$ is a fractional ideal. Fractional ideals of this form are called principal fractional ideals. They form a subgroup.*

Proof. *(a)* is obvious.
(b) If $\alpha, \beta \in R$ satisfy $\alpha I \subset R$ and $\beta J \in R$ then $\alpha\beta IJ \subset R$.
(c) Let $\alpha \neq 0$ be any element in I. Then $\alpha I^{-1} \subset R$ is an ideal. This proves (c).
(d) We only need to show that $I^{-1}I = R$. If it is not, then $I^{-1}I$ is a proper ideal of R. By Lemma 4.3 there exists an element $a \in \mathrm{Frac}(R) - R$ for which we have $xI^{-1}I \subset R$. This implies $xI^{-1} \subset I^{-1}$. Since I^{-1} is finitely generated over R, this implies that x is integral and hence an element of R. Contradiction.
(e) This is clear.

Proposition 4.8. *Let R be a Dedekind domain. Then*
(a) Every fractional ideal I of R can be written in a unique way as

$$I \quad = \quad \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}},$$

where the product runs over the prime ideals of R and the exponents $m_{\mathfrak{p}}$ are integers, almost all of which are zero. The exponents satisfy $m_{\mathfrak{p}} \geq 0$ for all $\mathfrak{p}$ if and only if I is an R-ideal.
(b) The map

$$Id(R) \xrightarrow{\cong} \bigoplus_{\mathfrak{p}} \mathbf{Z}$$

that sends I to the vector of exponents $m_{\mathfrak{p}}$, is an isomorphism of groups.

Proof. There exists an element $\alpha \in K^*$ so that $J = \alpha I$ is an R-ideal. By Theorem 4.6. the ideals J and (α) admit a factorization into products of non-zero prime ideals. From the factorizations $J = \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}}$ and $(\alpha) = \prod_{\mathfrak{p}} \mathfrak{p}^{b_{\mathfrak{p}}}$, we obtain

$$I \quad = \quad \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}} - b_{\mathfrak{p}}}$$

as required. By Theorem 4.6 the exponents $m_{\mathfrak{p}} = a_{\mathfrak{p}} - b_{\mathfrak{p}}$ are well defined and unique. They do not depend on the choice of α. The fact that I is an R-ideal if and only if the exponents $m_{\mathfrak{p}}$ are ≥ 0 for all $\mathfrak{p}$ also follows from Theorem 4.6.

This implies (a). Part (b) follows from the formula $\mathrm{ord}_{\mathfrak{p}}(IJ) = \mathrm{ord}_{\mathfrak{p}}(I) + \mathrm{ord}_{\mathfrak{p}}(J)$

Definition. *Let R be a Dedekind domain and let I be a fractional ideal. We let*

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}},$$

where $\mathfrak{p}$ runs over the non-zero prime ideals of R as in Proposition 4.8. We put

$$\mathrm{ord}_{\mathfrak{p}}(I) = m_{\mathfrak{p}}.$$

Every rational number is ± 1 times a product of primes with exponents in $\mathbf{Z}$, almost all of which are zero. In fact, we have the following sequence of abelian groups

$$0 \longrightarrow \{\pm 1\} \longrightarrow \mathbf{Q}^* \longrightarrow \bigoplus_p \mathbf{Z} \longrightarrow 0.$$

Here $\alpha \in \mathbf{Q}^*$ is mapped to the vector m_p of exponents in the factorization $\alpha = \pm \prod_p p^{m_p}$. We generalize this sequence to Dedekind domains and their fields of fractions.

Definition. *Let R be a Dedekind domain with field of fractions K. We define a map*

$$\theta : K^* \longrightarrow \mathrm{Id}(R)$$

by $\theta(\alpha) = (\alpha)$.

The image of θ is the subgroup $PId(R)$ of $Id(R)$ of principal ideals. The kernel of θ is precisely the group of units R^* of R. The cokernel of θ is called the *class group* of R:

$$Cl(R) = \mathrm{cok}(\theta) = Id(R)/PId(R).$$

In other words, there is an exact sequence

$$0 \longrightarrow R^* \longrightarrow K^* \xrightarrow{\theta} Id(R) \longrightarrow Cl(R) \longrightarrow 0.$$

The kernel and the cokernel of θ measure the difference between the group K^* and the free group $Id(R)$. The class group measures how far R is from being a principal ideal domain. Fields and, more generally, principal ideal domains have trivial class groups. The analogue of the class group in algebraic geometry is the *Picard group*. For a smooth algebraic curve this is the divisor group modulo its subgroup of principal divisors [30].

One can show [14], that *every* abelian group is isomorphic to the class group $Cl(R)$ of some Dedekind domain R. We will show in section 7 that the class group of the ring of integer of a number field is always a *finite* group

Proposition 4.9. *let R be a Dedekind domain. The following are equivalent:*
(a) The class group $Cl(R)$ is trivial.
(b) Every fractional ideal of R is principal.
(c) R is a principal ideal domain.
(d) R is a unique factorization domain.

Proof. The implications *(a)* $\Rightarrow$ *(b)* $\Rightarrow$ *(c)* $\Rightarrow$ *(d)* are easy or standard. To prove that *(d)* $\Rightarrow$ *(a)* we first note that by Theorem 4.6 it suffices to show that every *prime* ideal is principal. Let, therefore, $\mathfrak{p}$ be a non-zero prime ideal and let $0 \neq \pi \in \mathfrak{p}$. Writing π as a product of irreducible elements and observing that $\mathfrak{p}$ is prime, we see that $\mathfrak{p}$ contains an irreducible element π'. The ideal (π') is a prime ideal. Since the ring R is a Dedekind domain, it has Krull dimension 1. It follows that $\mathfrak{p} = (\pi')$ and hence that $\mathfrak{p}$ is principal, as required.

Exercises.

4.1 Show: If A is a Noetherian ring and $I \subset A$ is an ideal, then A/I is also Noetherian.

4.2 Show that the ring $C^\infty(\mathbf{R}) = \{f : \mathbf{R} \to \mathbf{R} : f \text{ is a continuous function}\}$ is not Noetherian.

4.3 Show that every unique factorization domain is integrally closed.

4.4 Prove that every principal ideal domain is a Dedekind domain.

4.5 (Hilbert's Basissatz) Let A be a Noetherian ring and let $I \subset A[X]$ be an ideal. For every $n \geq 0$ let $J_n \subset A$ be the set containing 0 and the leading coefficients of polynomials in I of degree at most n.

(a) Show that the J_n form an ascending sequence of A-ideals.
For each n let $S_n \subset I$ be a finite set of polynomials of degree $\leq n$ in I whose leading coefficients generate J_n.

(b) Let $N \geq 0$ be such that $J_n = J_N$ for all $n \geq N$. Show that $\underset{n \leq N}{\cup} S_n$ generates the $A[X]$-ideal I.

(c) Conclude that $A[X]$ is Noetherian.

4.6 Let R be an integrally closed ring and let $f \in R[X]$ be irreducible over K, the field of fractions of R. Then f is irreducible over R.

4.7 Prove the Chinese Remainder Theorem: let R be a commutative ring and suppose that I and J are two ideals of R that are relatively prime i.e. $I + J = R$. Then the canonical homomorphism

$$R/IJ \longrightarrow R/I \times R/J$$

4.8 Consider the properties "Noetherian", "integrally closed" and "of Krull dimension 1" that characterize Dedekind domains. Give examples of rings that have two of these properties, but not the third. is an isomorphism.

4.9 Let I and J be two fractional ideals of a Dedekind domain.

(i) Show that $I \cap J$ and $I + J$ are fractional ideals.

(ii) Show that $I^{-1} + J^{-1} = (I \cap J)^{-1}$ and that $I^{-1} \cap J^{-1} = (I + J)^{-1}$.

(iii) Show that $I \subset J$ if and only if $J^{-1} \subset I^{-1}$.

4.10 Let R be a Dedekind domain. Show:

(a) a fractional ideal contained in R is an ideal of R.

(b) for $\alpha \in R$ and a fractional ideal I one has that $\alpha I \subset I$.

(c) every fractional ideal I is of the form $m^{-1}J$ where $m \in \mathbf{Z}$ and J is an ideal of R.

(d) if $I = (x)$ is a principal fractional ideal, then $I^{-1} = (x^{-1})$.

4.11 Let I and J be fractional ideals of a Dedekind domain R. Let $n_\mathfrak{p}$ and $m_\mathfrak{p}$ be the exponents in their respective prime decompositions. Show that $I \subset J \Leftrightarrow n_\mathfrak{p} \geq m_\mathfrak{p}$ for all primes $\mathfrak{p}$.

4.12 Let R be a Dedekind domain with only finitely many prime ideals. Show that R is a principal ideal domain.

4.13 Show that in a Dedekind domain every ideal can be generated by at most two elements.

4.14 Let R be a Dedekind domain. Let S be a set of prime ideals of R. Let R' be the subset of the quotient field K of R defined by

$$R' = \{x \in K^* : (x) = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}} \quad \text{with } n_\mathfrak{p} \geq 0 \text{ for all } \mathfrak{p} \notin S\} \cup \{0\}.$$

Show that R' is a Dedekind domain.

4.15 Let R be a Dedekind domain and let $\mathfrak{p}$ and $\mathfrak{p}'$ be two different non-zero prime ideals of R. Show that $\mathfrak{p} + \mathfrak{p}' = R$.

4.16 Let R be a Dedekind domain and let x be in the field of fractions of R. Show that if we have $xJ \subset J$ for some fractional ideal J of R, then x is contained in R