1 Elements of commutative algebra

1.1 Basic definitions

Definition 1.1. A ring $A$ is a set equipped with two binary operations, addition and multiplication, such that

1. $A$ is an abelian group with respect to addition, with identity element 0.
2. $A$ is an abelian semigroup with respect to multiplication, with identity element 1.
3. Multiplication is distributive over addition:
\[ a(b + c) = ab + ac \] for all $a, b, c \in A$.

Example 1.2. 1. The ring of integers $\mathbb{Z}$.
2. Let $A$ be a ring. We denote by $A[t]$ the ring of polynomials in $t$ with coefficients in $A$
\[ A[t] = \{ a_0 + a_1 t + a_2 t^2 + \cdots | a_i \in A, \text{ all but finitely many } a_i = 0 \}, \]
with the usual addition and multiplication rules for polynomials.
3. Let $A$ be a ring. We denote by $A[[t]]$ the ring of formal power series in $t$ with coefficients in $A$
\[ A[[t]] = \{ a_0 + a_1 t + a_2 t^2 + \cdots | a_i \in A \}, \]
with the usual addition and multiplication rules for power series.
4. Let $A$ be a ring such that $1 = 0$. Then for any $a \in A$, we have $a = a \cdot 1 = a \cdot 0 = 0$, hence $A$ has only one element. The ring $A$ is called the zero ring.

Remark 1.3. The zero ring is in some sense a pathological object: in a number of definitions, we need to specifically exclude it from consideration.

Definition 1.4. An element $a$ in a ring $A$ is called a unit if there is an element $a^{-1} \in A$ such that $aa^{-1} = 1$. We denote the set of units of $A$ by $A^\times$, it is an abelian group. A nonzero ring is called a field if every nonzero element is a unit.
Example 1.5.  
1. The field of rational numbers \( \mathbb{Q} \).

2. The field of real numbers \( \mathbb{R} \).

3. The field of complex numbers \( \mathbb{C} \).

4. Let \( k \) be a field. We denote by \( k(t) \) the field of rational functions in \( t \) with coefficients in \( k \):

\[
k(t) = \left\{ \frac{f}{g} \middle| f, g \in k[t] \right\} / \sim, \quad f/g \sim f'/g' \text{ if } fg' = f'g.
\]

with the usual addition and multiplication rules for fractions (this is an example of localization, see Def. 1.70).

5. Let \( k \) be a field. We denote by \( k((t)) \) the field of formal Laurent series in \( t \) with coefficients in \( k \):

\[
k((t)) = \{ \cdots + a_{-1} t^{-1} + a_0 + a_1 t + a_2 t^2 + \cdots \middle| a_i = 0 \text{ for } i \ll 0 \},
\]

with the usual addition and multiplication rules for Laurent series.

Definition 1.6. Let \( A \) and \( B \) be rings. A ring homomorphism \( f : A \to B \) is a map preserving addition and multiplication, and sending 1 to 1.

Example 1.7.  
1. There is a unique ring homomorphism from \( \mathbb{Z} \) to any ring. We say that \( \mathbb{Z} \) is an initial object in the category of rings.

2. There is a unique ring homomorphism from any ring to the zero ring. There are no ring homomorphisms from the zero ring to any nonzero ring, because 0 = 1 in the zero ring must go to both 0 and 1.

3. The ring of polynomials \( A[t] \) is characterized by the following universal property. Given a ring homomorphism \( f : A \to B \), and an element \( b \in B \), there exists a unique ring homomorphism \( g : A[t] \to B \) such that \( g(t) = b \) and such that \( f = g \circ i \), where \( i : A \to A[t] \) is the canonical embedding sending \( a \) to \( at^0 \). If \( A \) is a subring of \( B \) and \( b \in B \) is an element, we denote by \( A[b] \) the image of this map.

Definition 1.8. Given a homomorphism of rings \( A \to B \), we also say that \( B \) is an \( A \)-algebra. If \( B \) and \( C \) are \( A \)-algebras, homomorphism of \( A \)-algebras \( f : B \to C \) is a ring homomorphism such that \( f(ab) = af(b) \) for all \( a \in A \) and all \( b \in B \), where the image of any \( a \in A \) in \( B \) and \( C \) is also denoted \( a \).
Remark 1.9. For example, the ring $\mathbb{Z}[\sqrt{2}]$ is defined as the subring of, say, $\mathbb{R}$ that is the image of the map $\mathbb{Z}[t] \to \mathbb{R}$, $t \mapsto \sqrt{2}$. Note that there is no corresponding universal property for fields: the field $\mathbb{Q}(\sqrt{2})$ is not the image of $\mathbb{Q}(t)$ under any map.

Definition 1.10. Let $A$ be a ring. An ideal $a$ of $A$ is a subgroup under addition, such that $ab \in a$ whenever $a \in a$ and $b \in A$.

Example 1.11. 1. Let $A$ be a ring. Then $A$ is also an ideal, called the unit ideal. It is to be avoided, just like the zero ring. All other ideals are called proper.

2. Let $\{a_i|i \in I\}$ be a set of elements of a ring $A$. The ideal generated by the $a_i$ is denoted $(a_i)_{i \in I}$ and consists of all finite linear combinations of the $a_i$ with coefficients in $A$:

$$(a_i)_{i \in I} = \left\{ \sum_{i \in I} a_i b_i | b_i \in A, \text{ all but finitely many } b_i = 0 \right\}.$$

For a single element $a \in A$, we also denote this ideal by $aA$, such an ideal is called principal.

Proposition 1.12. An ideal contains a unit if and only if it is the unit ideal.

Proof. Omitted.

Proposition 1.13. Let $a$ be an ideal of $A$. Then the quotient group $A/a$ has a ring structure, the canonical map $\pi : A \to A/a$ is a surjective ring homomorphism with kernel $a$, and there is a one-to-one order-preserving correspondence between the ideals of $A/a$ and the ideals of $A$ which contain $a$.

Conversely, let $f : A \to B$ be a ring homomorphism. Then Ker $f$ is an ideal of $A$, and the image of $f$ is a subring of $B$ isomorphic to $A/Ker f$. Given an ideal $a$ of $A$ contained in Ker $f$, the ring homomorphism $f$ factors uniquely through the canonical map $\pi : A \to A/a$. Note that Ker $f = A$ only when $B$ is the zero ring.

Proof. Omitted.

Definition 1.14. Let $f : A \to B$ be a ring homomorphism.
1. For an ideal \( a \subset A \), its extension \( a^e \) is the ideal of \( B \) generated by elements of the form \( f(a) \) with \( a \in A \). We also denote this by \( aB \), especially if \( f \) is injective.

2. For an ideal \( b \subset B \), its preimage \( f^{-1}(b) \) is an ideal of \( A \), called the contraction of \( b \) and denoted \( b^c \).

**Proposition 1.15.** A contraction of a prime ideal is prime.

**Proof.** Omitted. \( \square \)

**Remark 1.16.** A contraction of a maximal ideal need not be maximal, and extension does not in general preserve either property.

**Definition 1.17.** Let \( a \) and \( b \) be ideals of \( A \). Then

1. The intersection \( a \cap b \) is an ideal of \( A \).

2. The sum \( a + b = \{ a + b | a \in a, b \in b \} \) is an ideal of \( A \).

3. The product \( ab \) is the ideal generated by elements of the form \( ab \), where \( a \in a \) and \( b \in b \).

**Remark 1.18.** The union of ideals is generally not an ideal.

**Definition 1.19.** Let \( A \) be a ring, let \( a, b \in A \). We say that \( a \) divides \( b \), denoted \( a \mid b \), if there is an element \( c \in A \) such that \( b = ac \). If \( ab = 0 \) for some \( b \neq 0 \), we say that \( a \) is a zero divisor.

**Definition 1.20.** A nonzero ring is called an integral domain if it has no zero divisors aside from 0.

**Definition 1.21.** Let \( A \) be a ring. A proper ideal \( p \) is called prime if for any \( a, b \in A \), if \( ab \in p \), then \( a \in p \) or \( b \in p \).

**Proposition 1.22.** An ideal \( p \subset A \) is prime if and only if \( A/p \) is an integral domain.
Proposition 1.23. Let $p$ be a prime ideal, and let $a_1, \ldots, a_n$ be ideals such that $a_1 \cdots a_n \subset p$. Then $a_i \subset p$ for some $i$.

Proof. Omitted.

Definition 1.24. Let $A$ be a ring. An proper ideal $m$ is called maximal if no proper ideal of $A$ strictly contains $m$.

Proposition 1.25. An ideal $m \subset A$ is maximal if and only if $A/m$ is a field. In particular, a maximal ideal is prime.

Proof. Omitted.

Example 1.26. 1. Let $k$ be a field. Then the only ideals of $k$ are $(0)$ and the unit ideal. Conversely, if the only ideals of a ring $A$ are $(0)$ and the unit ideal, then $A$ is a field. Also, a ring homomorphism from a field to a nonzero ring is injective.

2. Every ideal of $\mathbb{Z}$ is equal to $(n)$ for some integer $n$, and $(n) = (m)$ if and only if $n = \pm m$. The maximal ideals are $(p)$ with $p$ prime, and the zero ideal $(0)$ is the only prime ideal that is not maximal. The quotient $\mathbb{Z}/(p)$ is the finite field with $p$ elements, denoted $\mathbb{F}_p$.

3. Let $k$ be a field. Every ideal of $k[t]$ is equal to $(f)$ for some polynomial $f \in k[t]$, and $(f) = (g)$ if and only if $f = cg$ for some nonzero $c \in k$. The maximal ideals are $(f)$ with $f$ irreducible and nonzero, and the zero ideal is the only prime ideal that is not maximal. The quotient $k[t]/(f)$ for an irreducible $f$ is a finite extension of $k$ whose degree is equal to the degree of $f$. In particular, if $k$ is algebraically closed, then the only maximal ideals of $k[t]$ are $(t - a)$ for $a \in k$.

Remark 1.27. We will prove the above statements later, see Cor. 2.21. They are our first example of the profound similarity between the ring of integers $\mathbb{Z}$ and the ring of polynomials in one variable over a field.

Proposition 1.28. Let $A$ be a ring, and let $a \in A$ be a non-unit. Then $a$ is contained in a maximal ideal of $A$. More generally, any ideal of $A$ is contained in a maximal ideal.
Proof. This is a standard application of Zorn’s lemma, see [AM] Thm. 1.3. □

Definition 1.29. Let $A_1, \ldots, A_n$ be rings. We define their product $\prod_{i=1}^n A_i$ to be the set of all sequences $(a_1, \ldots, a_n)$, with $a_i \in A_i$ and component-wise addition and multiplication. It is a commutative ring with additive identity $(0, \ldots, 0)$ and multiplicative identity $(1, \ldots, 1)$.

Theorem 1.30 (Chinese remainder theorem). Let $a_1, \ldots, a_n$ be ideals in a ring $A$ such that $a_i + a_j = A$ for all $i \neq j$, and let $a = \bigcap_{i=1}^n a_i$. Then

$$A/a \simeq \prod_{i=1}^n A/a_i.$$ 

Proof. Let $a \mod a_i$ denote the residue class of $a$ in $A/a_i$. Define

$$f : A \to \prod_{i=1}^n A/a_i, \quad a \mapsto \prod_{i=1}^n a \mod a_i,$$

then the kernel of $f$ is clearly $a$, so it remains to show that $f$ is surjective.

For $i = 2, \ldots, n$, find $a_i \in a_1$ and $b_i \in a_n$ such that $a_i + b_i = 1$, and let $x = (1 - u_2) \cdots (1 - u_n)$. Then $x = 1 \mod a_1$ and $x = 0 \mod a_i$ for $i \geq 2$, hence $f(x) = (1, 0, \ldots, 0)$. Similarly, we see that all elements of the form $(\ldots, 0, 1, 0, \ldots)$ are in the image of $f$, hence $f$ is surjective. □

Definition 1.31. A ring $A$ is called **local** if it has a unique maximal ideal.

Remark 1.32. Local rings are, generally speaking, the simplest rings to study beside fields, since by the above they have few prime ideals.

Definition 1.33. A ring $A$ is called **Noetherian** if every ideal $a$ of $A$ is finitely generated, in other words if there exist $a_1, \ldots, a_n \in a$ such that $a = (a_1, \ldots, a_n)$.

Proposition 1.34. A ring $A$ is Noetherian if and only if it satisfies one of the following equivalent conditions:
1. Given any sequence of ideals \( a_1 \subset a_2 \subset a_3 \subset \cdots \), there exists an \( N \) such that \( a_n = a_N \) for all \( n \geq N \) (this is known as the ascending chain condition).

2. Every nonempty set of ideals of \( A \) has a maximal element with respect to inclusion.

Proof. See [AM] Prop. 6.1 and Prop. 6.2.

Remark 1.35. The Noetherian property is similar to the second countability property in the definition of a manifold, its role is to exclude rings that are “too large”. Nevertheless, it is sometimes necessary to work with non-Noetherian rings. In general, neither the number of generators of an ideal nor the maximum length of a nontrivial sequence of ideals can be uniformly bounded.

Example 1.36. 1. Any field is Noetherian, because the only ideals are the zero and the unit ideals.

2. Any quotient of a Noetherian ring is Noetherian by Prop. 1.13.

3. The ring \( \mathbb{Z} \) is Noetherian because it is a PID (see Cor. 2.21).

Theorem 1.37 (Hilbert’s basis theorem). Let \( A \) be a Noetherian ring. Then the ring \( A[t] \) is also Noetherian.

Proof. See [AM] Thm. 7.5.

Remark 1.38. The only rings that we will consider in this course are polynomial rings over \( \mathbb{Z} \) or over a field, their quotients, and their localizations (see Def. 1.70). All of these rings are Noetherian, by the above results and by Cor. 1.80.

Geometric Remark 1.39. Let \( \mathbb{A}^1_{\mathbb{C}} \) denote the complex line, in other words the set of complex numbers viewed as a one-dimensional space. We view the rings \( \mathbb{C}[t] \) and \( \mathbb{C}(t) \) as, respectively, the rings of polynomial and rational functions on \( \mathbb{A}^1_{\mathbb{C}} \) (technically, a rational function with a nontrivial denominator isn’t a function on all of \( \mathbb{A}^1_{\mathbb{C}} \)). Since \( \mathbb{C} \) is algebraically closed, the maximal
ideals of \(\mathbb{C}[t]\) have the form \((t - a)\) for \(a \in \mathbb{C}\), in other words they are in one-to-one correspondence with the points of \(\mathbb{A}^1_{\mathbb{C}}\).

The central insight of scheme theory is that any commutative ring \(A\) can and should be viewed as the ring of functions on some topological space, called the spectrum of \(A\) and denoted \(\text{Spec} A\). As a set, \(\text{Spec} A\) is defined to be set of prime ideals of \(A\), and it comes equipped with the Zariski topology. An element \(a \in A\) is then viewed as a function on \(\text{Spec} A\), whose value at a point corresponding to the prime ideal \(p \in \text{Spec} A\) is the residue class of \(a\) in the quotient ring \(A/p\).

For example, the maximal ideals of \(\mathbb{C}[t]\) have the form \((t - a)\) for some \(a \in \mathbb{C}\), the quotient ring \(\mathbb{C}[t]/(t - a)\) is isomorphic to \(\mathbb{C}\), and the residue class of \(f \in \mathbb{C}[t]\) in \(\mathbb{C}[t]/(t - a)\) is identified with \(f(a)\). Similarly, the maximal ideals of \(\mathbb{Z}\) are \((p)\) for \(p\) prime, and an integer \(n\) can be viewed as a function on \(\text{Spec} \mathbb{Z}\) whose value at \((p)\) is \(n \mod p\).

This perspective turns out to be very fruitful. For example, given a continuous map of topological spaces \(X \to Y\) and a continuous function on \(Y\), we can pull it back to a continuous function on \(X\). With schemes we can go in the other direction: a homomorphism of rings \(f : A \to B\) corresponds to a continuous map \(f^\# : \text{Spec} B \to \text{Spec} A\) defined by sending a prime ideal \(p \subset B\) to its contraction under \(f\) (see Prop. 1.15). Pulling back functions on \(\text{Spec} A\) (i.e. elements of \(A\)) to functions on \(\text{Spec} B\) (i.e. elements of \(B\)) via \(f^\#\) is then just applying the map \(f\).

We will not define schemes in this course, but many results of algebraic number theory have elegant interpretations in terms of schemes and maps between them.

### 1.2 Modules

Modules are to rings what vector spaces are to fields.

**Definition 1.40.** Let \(A\) be a ring. An \(A\)-module, or a module over \(A\), is an abelian group \(M\) with an operation \(A \times M \to M\), denoted \((a, m) \mapsto am\), such that

1. \(a(x + y) = ax + ay\) for all \(a \in A, x, y \in M\),
2. \((a + b)x = ax + bx\) for all \(a, b \in A, x \in M\),
3. \((ab)x = a(bx)\) for all \(a, b \in A, x \in M\),
4. $1x = x$ for all $x \in M$.

**Remark 1.41.** An equivalent definition is the following: an $A$-module is an abelian group $M$ and a ring homomorphism from $A$ to the ring of endomorphisms of $M$.

**Example 1.42.**
  1. Any abelian group is also a $\mathbb{Z}$-module.
  2. A module over $\mathbb{Z}[t]$ is an abelian group together with an endomorphism.
  3. A module over a field $k$ is a vector space over $k$.
  4. A module over $k[x]$ is a $k$-vector space together with a $k$-linear map.
  5. Let $G$ be a group, and let $k[G]$ be the group algebra over a field $k$ (note that $k[G]$ is commutative only if $G$ is). Then a $k[G]$-module is a $k$-representation of $G$.

**Definition 1.43.** Let $M$ and $N$ be $A$-modules. A **homomorphism of $A$-modules** $f : M \to N$ is a group homomorphism such that

$$f(ax) = af(x) \text{ for all } a \in A, x \in M.$$ 

All of the standard definitions for abelian groups translate to modules:

**Definition 1.44.**
  1. Let $M$ be an $A$-module. An **$A$-submodule** $N \subset M$ is an abelian subgroup preserved by multiplication by $A$.
  2. Let $N \subset M$ be $A$-modules. The quotient group $M/N$ has the structure of an $A$-module, called the **quotient module**.
  3. Let $f : M \to N$ be an $A$-module homomorphism. Then the **kernel** $\text{Ker}f$ and **image** $\text{Im}f$ are $A$-submodules of $M$ and $N$, respectively. The **cokernel** $\text{Coker}f$ is $N/\text{Im}f$.
  4. Let $M$ and $N$ be $A$-modules. Then the set $\text{Hom}_A(M, N)$ of $A$-module homomorphisms from $M$ to $N$ has the structure of an $A$-module.
  5. Let $M_i$ be $A$-modules with $i \in I$. Then their **intersection** $\bigcap_{i \in I} M_i$, their **product** $\prod_{i \in I} M_i$, and their **sum**

$$\bigoplus_{i \in I} M_i = \left\{(x_i) \in \prod_{i \in I} M_i \mid \text{all but finitely many } x_i = 0 \right\}$$
are $A$-modules.

The standard theorems of algebra generalize to modules:

**Proposition 1.45.**

1. Let $f : M \to N$ be a homomorphism of $A$-modules, then $\text{Im } f \cong M/\text{Ker } f$.

2. Let $M_1, M_2$ be submodules of an $A$-module $M$, and let $M_1 + M_2 = \{x_1 + x_2 \mid x_i \in M_i\}$. Then $M_1 + M_2$ is an $A$-submodule of $M$, and

   $$(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2).$$

3. Let $M \subset N \subset P$ be $A$-modules, then

   $$P/M \cong (P/N)/(N/M).$$

**Proof.** Omitted.

**Remark 1.46.** Any ring $A$ is a module over itself, and an ideal $a \subset A$ is an $A$-submodule of $A$.

**Definition 1.47.** An $A$-module $M$ is called free if there exists an $A$-module isomorphism $f : \bigoplus_{i \in I} A \to M$. The images of elements of the form $(\ldots, 0, 1, 0, \ldots)$ form a basis of $M$.

**Definition 1.48.** An $A$-module $M$ is called finitely generated (alternatively, finite) if there exists a surjective $A$-module homomorphism $A^n \to M$ for some $n$, where

$$A^n = A \oplus \cdots \oplus A.$$

A ring $A$ is Noetherian if and only if any $A$-submodule of $A$ is finitely generated. More generally, we have the following result:

**Proposition 1.49.** A submodule of a finitely generated module over a Noetherian ring is finitely generated.

**Proof.** See [AM], Prop. 6.2 and 6.5.
**Definition 1.50.** Let $A$ be a ring, let $a$ be an ideal, and let $M$ be an $A$-module. We define the submodule $aM \subset M$ as

$$aM = \left\{ \sum a_i m_i \mid a_i \in A, m_i \in M \right\}.$$ 

The goal of your mathematical career should be to prove a lemma that bears your name (not a theorem).

**Lemma 1.51** (Nakayama’s lemma). Let $A$ be a local ring, let $a$ be a proper ideal, and let $M$ be a finitely generated module.

1. If $aM = M$, then $M = 0$.
2. If $N \subset M$ is a submodule and $aM + N = M$, then $M = N$.

**Proof.** If $M \neq 0$, let $m_1, \ldots, m_n$ be a minimal set of generators of $M$. If $aM = M$, then there exist $a_1, \ldots, a_n \in a$ such that

$$m_1 = a_1 m_1 + \cdots + a_n m_n \quad \rightarrow \quad -(1 - a_1)m_1 = a_2 m_2 + \cdots + a_n m_n.$$ 

Since $a_1 \in a$, the element $1 - a_1$ does not lie in the maximal ideal of $M$, and is therefore invertible. Hence $m_1$ lies in the submodule of $M$ generated by $m_2, \ldots, m_n$, contradicting the minimality.

For (2), we note that $a(M/N) = (aM + N)/N = M/N$, hence by (1) $M/N = 0$.

**Remark 1.52.** The assumption that $M$ is finitely generated is crucial. For example, take $A$ to be any local domain, and $M$ its quotient field. Then for any nonzero ideal $a$ we have $aM = M$.

The following result is usually proved in undergraduate algebra courses for $A = \mathbb{Z}$, in other words for finitely generated abelian groups. The proof only uses the fact that $\mathbb{Z}$ is a PID, and can be generalized as follows:

**Theorem 1.53** (Structure theorem for finitely generated modules over a PID). Let $A$ be a principal ideal domain, and let $M$ be a finitely generated module over $A$. Then there exist prime elements $p_1, \ldots, p_k$ and integers $n, a_1, \ldots, a_k$ such that

$$M \cong A^n \oplus A/(p_1^{a_1}) \oplus \cdots \oplus A/(p_k^{a_k}),$$

and the elements $n, p_i, a_i$ are uniquely determined.
Proof. See Chapter 3.7 in [LA].

Geometric Remark 1.54. In the previous section, we discussed that to every ring \( A \) we can associate a geometric object \( \text{Spec} \ A \). Roughly speaking, an \( A \)-module \( M \) corresponds to a vector bundle on \( \text{Spec} \ A \).

1.3 Fields

The kernel of a ring homomorphism to a nonzero is a proper ideal, hence ring homomorphisms between fields are injective, and are usually called field extensions. Given field extensions \( K \subset L \) and \( K \subset L' \), a \( K \)-homomorphism from \( L \to L' \) is a map of fields \( L \to L' \) which is trivial on \( K \).

Definition 1.55. Let \( K \) be a field, and let \( i : \mathbb{Z} \to K \) be the canonical map. Then \( \ker i \) is a prime ideal, which is either \((0)\) or \((p)\) for a positive prime \( p \). In the former case we say that \( K \) has characteristic zero, in the latter \( K \) that has characteristic \( p \).

Hence, any field is an extension of either the rational numbers \( \mathbb{Q} \) or the finite field \( \mathbb{F}_p \).

Definition 1.56. Let \( K \subset L \) be a field extension. An element \( x \in L \) is called algebraic if the canonical map \( K[t] \to L \) sending \( t \) to \( x \) has a nontrivial kernel, and transcendental if it is injective. If \( x \) is algebraic, then the kernel of \( K[t] \to L \) is a principal ideal. Its unique monic generator is called the minimal polynomial of \( x \) over \( K \) and is denoted \( p_x(t) \). In either case, we denote \( K(x) \) to be the smallest subfield of \( L \) containing \( K \) and \( x \).

Remark 1.57. Let \( K \subset L \) be a field extension. Then \( x \in L \) is algebraic if and only if \( K[x] \), which is defined as the image of \( K[t] \) under \( t \mapsto x \), is a field, in other words if \( K[x] = K(x) \). Indeed, if the kernel is nontrivial, then it is a prime ideal since \( K[x] \) is an integral domain, hence maximal. If \( p_x(t) \) is the minimal polynomial of \( x \) over \( K \), then \( p_x(x) = 0 \), and \( f(x) = 0 \) implies that \( p_x(t) \) divides \( f(t) \). Also note that \( x \in L \) is algebraic if and only if \( K[x] \) is a finite-dimensional \( K \)-vector space.

Definition 1.58. A field extension \( K \subset L \) is called algebraic if every element of \( L \) is algebraic over \( K \), finitely generated if there exist \( x_1, \ldots, x_n \in L \) such that \( L = K(x_1, \ldots, x_n) \), and finite if \( L \) is a finite dimensional \( K \)-vector space. The degree \( [L : K] \) of a finite extension is \( \dim_K L \).
Proposition 1.59. A field extension is finite if and only if it is finitely generated and algebraic.

Proof. Omitted.

Given an irreducible polynomial \( f(t) \) over a field \( K \), we can form the field \( K_1 = K[t]/(f) \) in which \( f \) factors into terms of smaller degree. We can repeat this process: let \( f_1 \) be an irreducible factor of \( f \) in \( K_1[t] \), and form \( K_2 = K_1[t]/(f_2) \), and so on. In the end, we obtain a field, called the splitting field of \( f \), over which it factors into linear terms. It is possible to do all this for all polynomials at the same time.

Definition 1.60. A field \( K \) is called algebraically closed if all irreducible polynomials in \( K[t] \) have degree one.

Remark 1.61. Equivalently, a field \( K \) is algebraically closed if there does not exist a finite extension \( K \subset L \).

Proposition 1.62. Let \( K \) be a field. Then there exists a field \( \overline{K} \supset K \), called the algebraic closure of \( K \), such \( K \subset \overline{K} \) is an algebraic extension and such that \( \overline{K} \) is algebraically closed. Any two algebraic closures of \( K \) are isomorphic over \( K \).

Proof. See Exercise 1.13 in [AM].

Funny things can happen in infinite fields of positive characteristic: an irreducible polynomial may have multiple roots. For example, consider the polynomial \( f(t) = t^p - x \) over the field \( \mathbb{F}_p(x) \). It is irreducible, but over the algebraic closure \( \overline{\mathbb{F}_p(x)} \) it factors as
\[
t^p - x = (t - x^{1/p})^p.
\]
Note also that the derivative of \( f(t) \) is identically zero. This sort of behavior turns out to be problematic, and we will try to avoid it, which will not be difficult since we are mostly working in characteristic zero.

Definition 1.63. An irreducible polynomial \( p(t) \in K[t] \) over a field \( K \) is called separable if it factors into distinct linear factors in an algebraic closure of \( K \). A field extension \( K \subset L \) is called separable if the irreducible polynomial of every \( x \in L \) is separable. A field \( K \) is called perfect if every finite extension of \( K \) is separable.
Proposition 1.64. Any field of characteristic zero is perfect. Any finite field is perfect.

Proof. Omitted. □

Proposition 1.65 (The primitive element theorem). Let $K \subset L$ be a finite separable extension. Then there exists an element $x \in L$ such that $L = K(x)$.

Proof. See Theorem 4.6 in [LA]. □

Example 1.66. Consider the field extension $\mathbb{F}_p(x, y) \subset \mathbb{F}_p(x, y)[x^{1/p}, y^{1/p}]$. It has degree $p^2$, but it is easy to check that $f^p \in \mathbb{F}_p(x, y)$ for any $f \in \mathbb{F}_p(x, y)[x^{1/p}, y^{1/p}]$, hence any element generates a subfield of degree at most $p$, and there is no primitive element.

Proposition 1.67. Let $K \subset L$ be a finite separable extension of degree $n$. Then there are exactly $n$ $K$-homomorphisms of $L$ into $\overline{K}$.

Proof. Let $x \in L$ be a primitive element, so that $L = K[x]$. A map $\sigma : L \to \overline{K}$ that is trivial on $K$ is uniquely determined by the image of $x$. If $p_x(t)$ is the minimal polynomial of $x$ over $K$, then $\deg p_x = n$ and $p_x(t)$ has $n$ distinct roots $x_1, \ldots, x_n$ in $\overline{K}$. Since $\sigma(x) = x_i$, there are exactly $n$ such maps. □

1.4 Localization

Given a ring $A$, it is convenient to be able to invert some of its nonzero elements. For example, the field $\mathbb{Q}$ is obtained by inverting the nonzero elements in $\mathbb{Z}$, while the field of rational functions $k(t)$ is obtained by inverting nonzero polynomials in $k[t]$.

Here is a more detailed example. We consider the field $\mathbb{C}(t)$ as the field of rational functions on the complex line $\mathbb{A}_C^1$. A rational function $f(t)/g(t)$ is defined at a point $a \in \mathbb{A}_C^1$ if and only if $g(a) \neq 0$, in other words if $g$ does not belong to the maximal ideal $(t - a)$. By continuity, any such function is actually defined on some neighborhood of $a$. Hence, we can consider the ring

$$\{f(t)/g(t) \mid g(t) \notin (t - a)\} \subset \mathbb{C}(t), \quad (1)$$
which consists of rational functions that are defined near \( a \). An element \( f(t) \in \mathbb{C}[t] \) is invertible in this ring if and only if \( f \notin (t - a) \). All these constructions are examples of localization, which we now define.

Given a ring \( A \) and a subset \( S \), we want to construct a ring in which all elements of \( S \) are invertible.

**Definition 1.68.** Let \( A \) be a ring. A subset \( S \subseteq A \) is called a multiplicative subset if \( 1 \in S \) and \( ab \in S \) whenever \( a,b \in S \).

**Remark 1.69.** The condition \( 1 \in S \) is not strictly necessary, but it makes the definitions cleaner.

**Definition 1.70.** Let \( A \) be a ring and let \( S \) be a multiplicative subset. The localization of \( A \) with respect to \( S \), denoted \( S^{-1}A \), is constructed as follows. As a set, \( S^{-1}A = \{(a,s) | a \in A, s \in S\} / \sim \), where

\[(a,s) \sim (a',s') \text{ if there is a } t \in S \text{ such that } (as' - a's)t = 0.\]

We denote the equivalence class of \((a,s)\) by \( a/s \). We define a ring structure on \( S^{-1}A \) using the sum and product rule for fractions:

\[
\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}, \quad \frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}. 
\]

**Proposition 1.71.** The relation \( \sim \) defined above is an equivalence relation. The set \( S^{-1}A \) with the operations defined above is a ring with additive identity \( 0/1 \) and multiplicative identity \( 1/1 \). The map \( f : A \rightarrow S^{-1}A \) given by \( f(a) = a/1 \) is a ring homomorphism, and for any \( s \in S \), \( f(s) \) is invertible with inverse \( 1/s \). Moreover, \( f \) satisfies the following universal property: given any ring homomorphism \( g : A \rightarrow B \) such that \( g(s) \) is invertible for any \( s \in S \), there exists a unique ring homomorphism \( h : S^{-1} \rightarrow B \) such that \( g = h \circ f \).

**Proof.** Omitted.
Remark 1.72. The ordinary rule for comparing fractions, say in \( \mathbb{Q} \), is that 
\[ \frac{a}{s} = \frac{a'}{s'} \] 
if \( as = a's \). However, this rule may fail to be an equivalence relation if the ring \( A \) is not an integral domain, and we need the more complicated rule above.

Example 1.73. Let \( A \) be ring, and let \( p \) be a prime ideal. Then \( S = A - p \) is a multiplicative subset, and the localization \( S^{-1}A \) is denoted by \( A_p \). For example, the ring defined in (1) is \( C[t]_{(t-a)} \).

Example 1.74. Let \( A \) be an integral domain. Then \( (0) \) is a prime ideal, and \( A_{(0)} \) is called the fraction field of \( A \) and is denoted \( K(A) \). As an example, if \( k \) is a field, then \( k(t) \) is the fraction field of \( k[t] \). Note that any localization \( S^{-1}A \) of \( A \) is naturally a subring of \( K(A) \).

Example 1.75. Let \( A \) be a ring, let \( t \in A \) be an element, and let \( S = \{1, t, t^2, \ldots \} \). The localization \( S^{-1}A \) is denoted \( A_t \). Note that if \( (t) \) is a prime ideal, then \( A_t \) and \( A_{(t)} \) have different, and essentially complementary, meanings: in \( A_t \) we invert all powers of \( t \), while in \( A_{(t)} \) we invert all elements relatively prime to \( t \).

Remark 1.76. Two localizations \( S^{-1}A \) and \( S'^{-1}A \) may be isomorphic even if \( S \) and \( S' \) are different. For example, if \( u = t^k \), then the localized rings \( A_u \) and \( A_t \) are the same, because we can write
\[
\frac{a}{t} = \frac{at^{k-1}}{u}
\]

The ideals of \( S^{-1}A \) are easy to describe in terms of the ideals of \( A \). Given an ideal \( a \subset A \), denote \( S^{-1}a \) its extension to \( S^{-1}A \). It is easy to see that
\[
S^{-1}a = \{(a, s) | a \in a, s \in S \} \subset S^{-1}A.
\]

Proposition 1.77. Every ideal of \( S^{-1}A \) is of the form \( S^{-1}a \) for some ideal \( a \) of \( A \). The map \( a \mapsto S^{-1}a \) defines a one-to-one order-preserving correspondence between the prime ideals of \( A \) that do not meet \( S \) and the prime ideals of \( S^{-1}A \).

Proof. Omitted.

Example 1.78. Let \( A \) be a ring and let \( p \) be a prime ideal. Then the proposition above implies that the image of \( p \) in \( A_p \) is the unique maximal ideal, hence \( A_p \) is a local ring.
Remark 1.79. Given a ring $A$ and a prime ideal $\mathfrak{p}$, we can form two rings: the quotient $A/\mathfrak{p}$ and the localization $A_\mathfrak{p}$. These constructions are complementary: for example, by Prop. 1.13 and Prop. 1.15, the prime ideals of $A/\mathfrak{p}$ correspond to the prime ideals of $A$ containing $\mathfrak{p}$, while by Prop. 1.15 the prime ideals of $A_\mathfrak{p}$ correspond to the prime ideals of $A$ contained in $\mathfrak{p}$.

For the integers, the notational situation is even worse. Given a prime $p \in \mathbb{Z}$, we can form four completely different objects:

1. The localization of $\mathbb{Z}$ with respect to the prime ideal $(p)$, which is denoted $\mathbb{Z}_{(p)}$.
2. The localization of $\mathbb{Z}$ with respect to $\{1, p, p^2, \ldots\}$, which should be denoted $\mathbb{Z}_p$. However, this should be avoided.
3. The ring of $p$-adic integers, denoted $\mathbb{Z}_p$.
4. The quotient field $\mathbb{Z}/p\mathbb{Z}$, which is also denoted $\mathbb{Z}/p$, $\mathbb{Z}_p$ and $\mathbb{F}_p$.

Corollary 1.80. A localization of a Noetherian ring is Noetherian.

Proof. Omitted.

Given a ring $A$, a multiplicative subset $S$, and an $A$-module $M$, we can also localize $M$ and obtain the $S^{-1}A$-module $S^{-1}M$.

Definition 1.81. Let $A$ be a ring, let $S$ be a multiplicative subset, and let $M$ be an $A$-module. The localization of $M$ with respect to $S$, denoted $S^{-1}M$, is constructed as follows. As a set, $S^{-1}M$ consists of pairs $(m, s)$, with $m \in A$ and $s \in S$, modulo an equivalence relation

$$S^{-1}M = \{(a, s) | a \in M, s \in S\}/\sim,$$

where

$$(m, s) \sim (m', s')$$

if there is a $t \in S$ such that $(as' - a's)t = 0$.

We denote the equivalence class of $(m, s)$ by $m/s$. We define the structure of an $S^{-1}A$-module on $S^{-1}M$ as follows:

$$\frac{m}{s} + \frac{m'}{s'} = \frac{ms' + m's}{ss'}, \quad \frac{m}{s} \cdot \frac{a'}{s'} = \frac{ma'}{ss'}, \quad \frac{m}{s}, \frac{m'}{s'} \in S^{-1}M, \quad \frac{a'}{s'} \in S^{-1}A.$$
Remark 1.82. Given a localization map $A 	o S^{-1}A$ and an ideal $a \subset A$, the extension of $a$ to $S^{-1}A$ is the same as the localization $S^{-1}a$ of $a$ viewed as an $A$-module.

Localization at $S$ defines a functor from $A$-modules to $S^{-1}A$-modules:

**Definition 1.83.** Let $f : M \to N$ be a homomorphism of $A$-modules. We define the homomorphism $S^{-1}f : S^{-1}M \to S^{-1}N$ of $S^{-1}A$-modules by

$$S^{-1}f(m/a) = f(m)/a.$$ 

The key property of this functor is that it is exact:

**Proposition 1.84.** If the sequence $M' \to M \to M''$ is exact at $M$, then the sequence $S^{-1}M' \to S^{-1}M \to S^{-1}M''$ is exact at $S^{-1}M$.

*Proof.* Omitted.

It follows that localization commutes with most module operations:

**Proposition 1.85.** Let $N$ and $P$ be submodules of an $A$-module $M$, and let $S$ be a multiplicative subset. Then

1. $S^{-1}(N + P) = S^{-1}N + S^{-1}P$.
2. $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$.
3. $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.

2 Unique factorization

2.1 Basic definitions

In this section, we will study the ways in which the fundamental theorem of arithmetic for $\mathbb{Z}$ can be generalized to other rings, in particular, to the rings of integers of algebraic number fields. In this section we will always assume that all rings are integral domains.

The fundamental theorem of arithmetic has two parts:

1. Every integer can be written as a product of prime numbers.
2. Any two factorizations of an integer into a product of prime numbers are the same, up the order of the factors.

The fundamental theorem relies on two properties of prime numbers, which are equivalent and uniquely characterize them:

1. If \( p \) is a prime number and \( p = ab \) for some \( a, b \in \mathbb{Z} \), then either \( a \) or \( b \) is a unit, in other words either \( a = \pm 1 \) or \( b = \pm 1 \).

2. If \( p \) is a prime number and \( p|ab \) for some \( a, b \in \mathbb{Z} \), then either \( p|a \) or \( p|b \).

The first property of prime numbers assures us that, when we factor an integer into smaller factors, we eventually get to a point where we cannot factor any further. The second is then used to show that any two factorizations are the same, up to order. We will see that the generalizations of these two properties of prime numbers to other rings are, in general, not equivalent, and this is the main reason why unique factorization may fail.

**Definition 2.1.** An element \( a \in A \) is called *irreducible* if it is not a unit, and if for any \( b, c \in A \) such that \( a = bc \), either \( b \) or \( c \) is a unit.

**Definition 2.2.** An element \( p \in A \) is called *prime* if it is not a unit, and for any \( a, b \in A \), \( p|ab \) implies that \( p|a \) or \( p|b \).

We first note that the second property is stronger than the first:

**Proposition 2.3.** Prime elements are irreducible.

*Proof.* Suppose that \( p \in A \) is prime, and suppose that \( p = ab \). Then \( p|ab \), so without loss of generality \( p|a \), hence \( a = pc \). Then

\[
p = ab = pbc \quad \rightarrow \quad bc = 1,
\]

so \( b \) is a unit.

\[\Box\]

We now state the definition of unique factorization.

**Definition 2.4.** We say that elements \( a, b \in A \) are *associated* if there is a unit \( c \) such that \( a = bc \).
Definition 2.5. An integral domain $A$ is called a unique factorization domain (UFD), if the following conditions hold:

1. Every element $a \in A$ can be written as a product of irreducible elements.

2. For any $a \in A$, given two representations of $a$ as a product of irreducible elements

   \[ a = p_1 \cdots p_n = q_1 \cdots q_m, \]

   we have that $m = n$ and, after reordering, $q_i$ is associated to $p_i$.

We will soon see that the first property is satisfied under fairly broad assumptions, namely when $A$ is Noetherian. The second, however, fails more frequently, precisely because irreducible elements may fail to be prime.

First, we state some properties of the associativity relation.

Proposition 2.6. Associativity is an equivalence relation on the elements of $A$. Furthermore, if $a$ and $b$ are associated, then

1. For any $c \in A$, $a|c$ if and only if $b|c$.

2. $a$ is irreducible if and only if $b$ is irreducible.

3. $a$ is prime if and only if $b$ is prime.

4. $a$ is a unit if and only if $b$ is a unit.

Proof. Omitted.

Proposition 2.7. An integral domain $A$ is a UFD if and only if

1. Every element $a \in A$ can be written as a product of irreducible elements.

2. Every irreducible element of $A$ is prime.
Proof. Suppose that the first property holds, and that every irreducible element of $A$ is prime. Let

$$a = p_1 \cdots p_n = q_1 \cdots q_m$$

be two factorizations of $a \in A$ into irreducibles. Since $p_1$ is prime, then $p_1 | q_1 \cdots q_m$ implies that $p_1 | q_1$ or $p_1 | q_2 \cdots q_m$. Proceeding further and reordering if necessary, we can assume that $p_1 | q_1$, in other words that $q_1 = p_1 u$. But $q_1$ is irreducible, hence $u$ is a unit, so cancelling by $p_1$ and rolling $u$ into, say, $q_2$, we see that

$$p_2 \cdots p_n = q_2 \cdots q_m.$$  

Continuing in this manner, we see that each $p_i$ is associated to $q_i$. If $n = m$, we are done. If $n \neq m$, then without loss of generality $n > m$, and we obtain

$$p_{m+1} \cdots p_n = 1,$$

which is a contradiction since each $p_i$ is assumed to be irreducible and hence not a unit.

Conversely, suppose that $A$ is a UFD, and let $a \in A$ be an irreducible element. Suppose that $a | bc$ for some $b, c \in A$, in other words suppose that $ad = bc$ for some $d \in A$. Factor $b, c$ and $d$ into irreducibles:

$$b = p_1 \cdots p_l, \quad c = q_1 \cdots q_m, \quad d = r_1 \cdots r_n.$$  

Then we have two factorizations of $ad = bc$ into irreducibles:

$$ar_1 \cdots r_n = ad = bc = p_1 \cdots p_l \cdot q_1 \cdots q_m.$$  

Since $A$ is a UFD, $a$ is associated either to one of the $p_i$ or to one of the $q_j$, hence $a | b$ or $a | c$. We conclude that $a$ is prime.

\[ \square \]

### 2.2 Factorization into ideals

A key insight of algebraic number theory is that is more convenient to work with the ideals of $A$ than with the elements. The elements of $A$ correspond to the principal ideals of $A$.

**Definition 2.8.** A proper ideal $a$ of $A$ is called *principal* if it is generated by one element, in other words if there is an $a \in A$ such that $a = (a)$.
First, we observe that the set of equivalence classes of elements of $A$ modulo associativity is the set of principal ideals, and many properties of elements correspond to the respective properties of ideals:

**Proposition 2.9.** Let $A$ be an integral domain. Then

1. Two elements $a, b \in A$ are associates if and only if $(a) = (b)$.
2. For any $a, b \in A$, $(ab) = (a)(b)$.
3. For any $a, b \in A$, $a|b$ if and only if $(b) \subset (a)$.
4. For any $a, b \in A$, $(a) \subsetneq (b)$ if and only if there exists a principal ideal $(c)$ such that $(b) = (a)(c)$.
5. An element $a \in A$ is irreducible if and only if $(a)$ is maximal among the principal ideals of $A$, in other words, if $(a) \subset (b)$ implies $(a) = (b)$.
6. An element $a \in A$ is prime if and only if $(a)$ is a prime ideal.
7. An element $a \in A$ is a unit if and only if $(a)$ is the unit ideal.

**Proof.** Omitted. \hfill \Box

**Remark 2.10.** Associativity does not respect addition, and $(a) + (b)$ in general strictly contains $(a + b)$.

We now reformulate unique factorization in terms of ideals.

**Proposition 2.11.** A ring $A$ is a unique factorization domain if and only if the following conditions hold:

1. Every principal ideal $(a)$ of $A$ admits a factorization

   $$(a) = (p_1) \cdots (p_n),$$

   where each ideal $(p_i)$ is maximal among principal ideals.
2. Every ideal of $A$ that is maximal among principal ideals is prime.
Proof. This follows directly from Prop. 2.7 and Prop. 2.9.

Remark 2.12. We don’t have a good name for principal ideals generated by irreducible elements. We can’t call them irreducible, because that means something else, and we can’t call them maximal principal, because they are in general not maximal.

Our first application of ideals is to show that factorization into irreducibles holds in a Noetherian ring.

**Proposition 2.13.** Let $A$ be a Noetherian ring. Then any principal ideal $(a)$ admits a factorization

$$ (a) = (p_1) \cdots (p_n), $$

where each ideal $(p_i)$ is maximal among principal ideals.

Proof. Consider the set $\mathfrak{M}$ of principal ideals of $A$ that fail to satisfy the factorization property. If it is nonempty, then by Prop. 1.34 it contains a maximal element $(x)$. By assumption $(x)$ is not maximal among all principal ideals (otherwise $(x) = (x)$ is the desired factorization), hence $(x) \subsetneq (y)$ for some principal ideal $(y)$. It follows that $(x) = (y)(z)$ with $(x) \subsetneq (z)$. By assumption $(y)$ and $(z)$ are not in $\mathfrak{M}$, so

$$ (y) = (p_1) \cdots (p_n), \quad (z) = (q_1) \cdots (q_m), $$

where the ideals $(p_i)$ and $(q_j)$ are maximal among principal ideals. Hence $(x)$ also factors:

$$ (x) = (p_1) \cdots (p_n)(q_1) \cdots (q_m), $$

which is a contradiction.

2.3 Euclidean domains

We now describe a class of rings which admit unique factorization.

**Definition 2.14.** An integral domain $A$ is called a principal ideal domain (PID) if every ideal of $A$ is principal.

We now show that any PID is a UFD. By using the language of ideals, we can provide a very short proof; all of the pieces are already in place.
Theorem 2.15. A principal ideal domain is a unique factorization domain.

Proof. Let $A$ be a PID. We prove that it satisfies the two conditions of Prop. 2.11. The first follows from Prop. 2.13 because $A$ is Noetherian. The second is also clear: in a PID, an ideal maximal among principal ideals is maximal among all ideals, hence is prime by Prop. 1.25.

Two important examples of PIDs are the ring of integers $\mathbb{Z}$ and the ring of polynomials $k[t]$ over a field $k$. The reason that these rings are PIDs is that they admit division with remainder, which we now formalize.

Definition 2.16. Let $A$ be an integral domain. A Euclidean function on $A$ is a function $\phi : A\setminus\{0\} \to \mathbb{Z}_{\geq 0}$ satisfying the following properties:

1. If $a, b \in A\setminus\{0\}$ and $a | b$, then $\phi(a) \leq \phi(b)$.

2. If $a, b \in A\setminus\{0\}$, then there exist $q, r \in A$ such that $a = bq + r$, where either $r = 0$ or $\phi(r) < \phi(b)$.

Definition 2.17. An integral domain is called a Euclidean domain if it admits a Euclidean function.

Example 2.18. 1. The absolute value function $|a|$ is a Euclidean function on $\mathbb{Z}$.

2. The degree function is a Euclidean function on $k[t]$ for any field $k$.

We will show that any Euclidean ring is a PID.

Theorem 2.19. A Euclidean domain is a principal ideal domain.

Proof. Let $A$ be Euclidean with function $\phi$, and let $a$ be a nonzero ideal. Let $a \in a$ be such that $\phi(a) \leq \phi(b)$ for all $b \in a\setminus\{0\}$. I claim that $a = (a)$. Indeed, given $b \in a\setminus\{0\}$, write $b = aq + r$. Then $r = b - aq \in a$, and therefore $\phi(r) < \phi(a)$ is not possible, hence $r = 0$ and $b = aq$.

Corollary 2.20. A Euclidean domain is a unique factorization domain.

Corollary 2.21. The rings $\mathbb{Z}$ and $k[t]$ are principal ideal domains and hence unique factorization domains, where $k$ is any field.
We now consider our first negative example.

**Geometric Example 2.22.** Consider the ring \( \mathbb{C}[t^2, t^3] \subset \mathbb{C}[t] \) consisting of polynomials in \( t \) with no linear term. I claim that \( \mathbb{C}[t^2, t^3] \) is not a UFD. Indeed, denote \( x = t^2 \) and \( y = t^3 \). It is easy to see that \( x \) and \( y \) are irreducible. Indeed, the units of \( \mathbb{C}[t^2, t^3] \) are the polynomials of degree zero, and there are no polynomials of degree one, so neither \( x \) nor \( y \) can be factored. However, we have a relation

\[
x^3 = y^2,
\]

which gives two non-equivalent factorizations of \( t^6 \).

It follows that \( \mathbb{C}[t^2, t^3] \) is neither Euclidean nor a PID, and it is instructive to see why. Indeed, we cannot write \( y = qx + r \) for any \( q, r \in \mathbb{C}[t^2, t^3] \), hence the ring is not Euclidean. In addition, the ideal \( (x, y) \) is not principal.

This example may seem contrived, but in fact it appears quite naturally in a geometric setting. Consider the affine plane \( \mathbb{A}^2_\mathbb{C} = \{ (a, b) | a, b \in \mathbb{C} \} \), let \( f(x, y) = x^3 - y^2 \), and let

\[
C = \{ (a, b) \in \mathbb{A}^2_\mathbb{C} | f(a, b) = 0 \}
\]

be the curve cut out by the equation \( f(x, y) = 0 \), called the *cuspidal cubic*. We define the *coordinate ring* \( \mathbb{C}[C] \) of \( C \) to be the ring of polynomials \( \mathbb{C}[x, y] \) modulo those that vanish on \( C \), in other words \( \mathbb{C}[C] = \mathbb{C}[x, y]/(x^3 - y^2) \). Define a map \( \mathbb{C}[x, y] \to \mathbb{C}[t] \) by \( x \mapsto t^2 \) and \( y \mapsto t^3 \), its kernel is \( (f) \), while its image is \( \mathbb{C}[t^2, t^3] \), hence our ring is the coordinate ring of \( C \). As we will see, the failure of \( \mathbb{C}[t^2, t^3] \) to be a UFD is a consequence of the curve \( C \) being singular at the origin. Note also that \( \mathbb{C}[x, y] \) and hence \( \mathbb{C}[t^2, t^3] \) are Noetherian by Thm. 1.37.

### 2.4 Quadratic fields

We are now ready to study a family of examples.

**Definition 2.23.** Let \( d \) be an integer that is not a square, and let \( \mathbb{Z}[\sqrt{d}] \) be the ring

\[
\mathbb{Z}[\sqrt{d}] = \{ a + b\sqrt{d} | a, b \in \mathbb{Z} \} \subset \mathbb{C}.
\]

The *norm map* \( \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}_{\geq 0} \) is defined by

\[
N(a + b\sqrt{d}) = a^2 - b^2d.
\]
The norm map will be our main tool for studying divisibility and factorization in $\mathbb{Z}[\sqrt{d}]$. We first prove some elementary properties:

**Proposition 2.24.**

1. For any $x, y \in \mathbb{Z}[\sqrt{d}]$, we have $N(xy) = N(x)N(y)$.
2. $N(x) = 0$ if and only if $x = 0$.
3. $N(x) = 1$ if and only if $x$ is a unit in $\mathbb{Z}[\sqrt{d}]$. Furthermore, if $d < 0$, then the units of $\mathbb{Z}[\sqrt{d}]$ are $\pm 1$ and $\pm \sqrt{-1}$ if $d = -1$ and $\pm 1$ if $d \leq -2$.
4. If $d < 0$, then $N(x) = |x|^2$ for any $x \in \mathbb{Z}[\sqrt{d}]$.

**Proof.** Omitted.

We first consider several examples with $d < 0$.

### 2.4.1 $d = -1$.

The ring $\mathbb{Z}[\sqrt{-1}]$ is called the ring of Gaussian integers. It is a Euclidean domain.

**Proposition 2.25.** The ring $\mathbb{Z}[\sqrt{-1}]$ is a Euclidean domain with respect to the norm function $N$.

**Proof.** Let $a, b \in \mathbb{Z}[\sqrt{-1}]$. The set of elements $qb$ with $q \in \mathbb{Z}[\sqrt{-1}]$ is a square lattice with side equal to $|b|$. The point $a$ lies in one of the squares (or on the boundary), and any point inside a square with side $|b|$ is at most $|b|/\sqrt{2}$ units away from a vertex. Hence there is an $r \in \mathbb{Z}[\sqrt{-1}]$ such that

$$a = qb + r, \quad |r| \leq \frac{|b|}{\sqrt{2}}.$$  

Since $|b| = \sqrt{N(b)}$, the proof is complete.

**Corollary 2.26.** The ring $\mathbb{Z}[\sqrt{-1}]$ is a UFD.

**Proof.** This follows from Cor. 2.20.
We now ask the following two related questions, which turn out to be closely related (note that it is not a priori obvious why this should be the case):

1. What are the prime elements of $\mathbb{Z}[\sqrt{-1}]$?
2. How do prime elements of $\mathbb{Z}$ factor in $\mathbb{Z}[\sqrt{-1}]$?

The complete answer is given by the following theorem.

**Theorem 2.27.** The following is a complete list of primes in $\mathbb{Z}[\sqrt{-1}]$, and none of these primes are associated to one another:

1. For every prime $p \equiv 1 \mod 4$ in $\mathbb{Z}$, there exist unique integers $a, b \in \mathbb{Z}$ such that $a > b > 0$ and $a^2 + b^2 = p$. The elements $a + b\sqrt{-1}$ and $a - b\sqrt{-1}$ are prime in $\mathbb{Z}[\sqrt{-1}]$.
2. The element $1 + \sqrt{-1}$ is prime in $\mathbb{Z}[\sqrt{-1}]$.
3. Every prime $p \equiv 3 \mod 4$ in $\mathbb{Z}$ is also a prime in $\mathbb{Z}[\sqrt{-1}]$.

A prime ideal $(p) \subset \mathbb{Z}$ factors into prime ideals in $\mathbb{Z}[\sqrt{-1}]$ as follows:

\[
(p) = \begin{cases} 
(a + b\sqrt{-1})(a - b\sqrt{-1}), & p \equiv 1 \mod 4, \quad p = a^2 + b^2, \\
(1 + \sqrt{-1})^2, & p = 2, \\
(p), & p \equiv 3 \mod 4.
\end{cases}
\]

**Proof.** First, we consider whether or not a prime $p \in \mathbb{Z}$ remains prime in $\mathbb{Z}[\sqrt{-1}]$. If $p$ factors as $p = xy$, then $p^2 = N(p) = N(x)N(y)$. If $x$ and $y$ are non-units, then $N(x) = N(y) = p$. Let $x = a + b\sqrt{-1}$, then we are trying to solve the equation

\[ a^2 + b^2 = p, \quad a, b \in \mathbb{Z}. \]

We consider this equation mod 4. For any $a \in \mathbb{Z}$, $a^2$ is either 0 or 1 mod 4, hence the equation does not have solutions if $p \equiv 3 \mod 4$. Hence a prime $p \in \mathbb{Z}$ that is 3 mod 4 is also prime in $\mathbb{Z}[\sqrt{-1}]$. If $p = 2$, the equation does have a solution, and 2 factors as $(1 + \sqrt{-1})(1 - \sqrt{-1})$, with the two elements being associated.

Now let $p = 4k + 1$. I claim that $p$ is not prime in $\mathbb{Z}[\sqrt{-1}]$. Indeed, consider the equation

\[ a^2 + 1 \equiv 0 \mod p. \]
The multiplicative group of a finite field is cyclic, and if \( \zeta \) is a generator for \( \mathbb{F}_p^* \), then \( a = \zeta^k \) is a solution. Hence there exists \( a \in \mathbb{Z} \) such that \( p|a^2 + 1 \). But clearly \( p \nmid (a \pm \sqrt{-1}) \), hence \( p \) is not prime in \( \mathbb{Z}[\sqrt{-1}] \), so there exists a factorization \( p = (a + b\sqrt{-1})(a - b\sqrt{-1}) \). Multiplying by units as necessary, we can assume that \( a > b > 0 \), and the elements \( a \pm b\sqrt{-1} \) are prime because they have prime norm.

I claim that we have found all primes in \( \mathbb{Z}[\sqrt{-1}] \). Let \( \pi \in \mathbb{Z}[\sqrt{-1}] \) be prime. We decompose \( N(\pi) \) into integer primes:

\[
N(\pi) = \pi \pi = p_1 \cdots p_k.
\]

Viewing this as an equation in \( \mathbb{Z}[\sqrt{-1}] \), we see that \( \pi | p \) for some \( p = p_i \). Taking norms again, we see that \( N(\pi)|N(p) = p^2 \), so either \( N(\pi) = p \) or \( N(\pi) = p^2 \). In the first case, we see that \( \pi = a + b\sqrt{-1} \) and \( p \equiv 1 \mod 4 \) or \( p = 2 \), while in the second case \( \pi \) and \( p \) are associated because they have the same norm, and \( p \equiv 3 \mod 4 \).

Geometric Remark 2.28. Consider the map \( f : \mathbb{A}^1_\mathbb{C} \to \mathbb{A}^1_\mathbb{C} \) defined by \( f(a) = a^2 \). This is a two-sheeted branched cover of the complex line by itself. Let’s count the number of preimages of a point

\[
\#f^{-1}(b) = \begin{cases} 
2, & b \neq 0 \\
1, & b = 0.
\end{cases}
\]

This answer is unsatisfying: we want the number of preimages to always be equal to two. For example, the function \( \#f^{-1}(b) \) is not continuous in \( b \). Intuitively, the point 0 is special for the map \( f \), and should be counted with multiplicity two.

There is a way of making this precise in terms of scheme theory. Namely, consider the inclusion of rings \( \iota : \mathbb{C}[t] \to \mathbb{C}[u] \) defined by \( \iota(t) = u^2 \). By Prop. 1.15, the contraction of a prime ideal is prime, and it is easy to check that \( (u - a)^c = (t - a^2) \). The complex line \( \mathbb{A}^1_\mathbb{C} \) is the spectrum of \( \mathbb{C}[t] \), and the map of spectra defined above is the dual map of the ring inclusion \( \mathbb{C}[t] \subset \mathbb{C}[u] \). Let \( (t - a) \) be a prime ideal of \( \mathbb{C}[t] \). Then it factors as a product of prime ideals of \( \mathbb{C}[u] \) in the following way:

\[
(t - b) = \begin{cases} 
(u - a)(u + a), & a = \sqrt{b}, \quad b \neq 0, \\
(u)^2, & b = 0.
\end{cases}
\]
We see that the number of factors in the product is always two.

I now claim that the inclusion \( \mathbb{Z} \subset \mathbb{Z}[\sqrt{-1}] \) should be viewed as a two-sheeted branched cover of \( \text{Spec} \mathbb{Z} \) by \( \text{Spec} \mathbb{Z}[\sqrt{-1}] \). It might seem that the point-counting argument fails: according to (2), \( (p) \) splits as only prime if \( p \equiv 3 \mod 4 \). We fix this by introducing another type of multiplicity. Namely, we observe that

\[
\mathbb{Z}[\sqrt{-1}]/(a + b\sqrt{-1}) \simeq \mathbb{F}_p \quad \text{when} \quad p \equiv 1 \mod 4, \quad p = a^2 + b^2,
\]

but

\[
\mathbb{Z}[\sqrt{-1}]/(p) \simeq \mathbb{F}_{p^2} \quad \text{when} \quad p \equiv 3 \mod 4.
\]

Hence \( \mathbb{Z}[\sqrt{-1}]/(a+b\sqrt{-1}) \) is a one-dimensional vector space over \( \mathbb{Z}/(p) \) when \( p \equiv 1 \mod 4 \), but \( \mathbb{Z}[\sqrt{-1}]/(p) \) is a two-dimensional vector space over \( \mathbb{Z}/(p) \) when \( p \equiv 3 \mod 4 \).

2.4.2 \( d = -2 \).

The ring \( \mathbb{Z}[\sqrt{-2}] \) is also Euclidean, and hence a UFD.

**Proposition 2.29.** The ring \( \mathbb{Z}[\sqrt{-2}] \) is a Euclidean domain with respect to the norm function \( N \).

**Proof.** The proof is the same as in Prop. 2.25. For \( b \in \mathbb{Z}[\sqrt{-2}] \), the set of elements \( qb \) with \( q \in \mathbb{Z}[\sqrt{-2}] \) is a rectangular lattice with sides equal to \( |b| \) and \( |b|\sqrt{2} \). Any point in such a rectangle is at most \( |b|\sqrt{3}/2 \) units away from a vertex, hence for any \( a \in \mathbb{Z}[\sqrt{-2}] \) we can find \( q \) and \( r \) such that

\[
a = qb + r, \quad |r| \leq \frac{|b|\sqrt{3}}{2},
\]

which completes the proof. \( \square \)

We have a similar classification of primes in \( \mathbb{Z}[\sqrt{-2}] \), which we state without proof.

**Theorem 2.30.** The following is a complete list of primes in \( \mathbb{Z}[\sqrt{-2}] \), and none of these primes are associated to one another:

1. For every prime \( p \equiv 1 \mod 8 \) or \( p \equiv 3 \mod 8 \) in \( \mathbb{Z} \), there exist unique integers \( a, b \in \mathbb{Z} \) such that \( a, b > 0 \) and \( a^2 + 2b^2 = p \). The elements \( a + b\sqrt{-2} \) and \( a - b\sqrt{-2} \) are prime in \( \mathbb{Z}[\sqrt{-2}] \).
2. The element $\sqrt{-2}$ is prime in $\mathbb{Z}[\sqrt{-2}]$.

3. Every prime $p \equiv 5 \mod 8$ and $p \equiv 7 \mod 8$ in $\mathbb{Z}$ is also a prime in $\mathbb{Z}[\sqrt{-2}]$.

A prime ideal $(p) \subset \mathbb{Z}$ factors into prime ideals in $\mathbb{Z}[\sqrt{-2}]$ as follows:

$$(p) = \begin{cases} 
(a + b\sqrt{-2})(a - b\sqrt{-2}), & p \equiv 1, 3 \mod 8, \ p = a^2 + 2b^2, \\
(\sqrt{-2})^2, & p = 2, \\
(p), & p \equiv 5, 7 \mod 8. 
\end{cases} \tag{3}$$

2.4.3 $d = -3$.

This is our first arithmetic example of a non-UFD. Consider the equation

$$(1 + \sqrt{-3})(1 - \sqrt{-3}) = 2 \cdot 2$$

in $\mathbb{Z}[\sqrt{-3}]$. I claim that these are two nonequivalent factorizations of 4 into irreducibles. Indeed, the units are $\pm 1$, so the elements are not associated. The norms of each of the elements $1 \pm \sqrt{-3}$ and 2 are equal to 4. If, say, $2 = xy$ in $\mathbb{Z}[\sqrt{-3}]$, then $x$ and $y$ have norm 2, but the equation $a^2 + 3b^2 = 2$ clearly has no integer solutions.

We can fix the problem in the following way: add the element

$$x = \frac{1 + \sqrt{-3}}{2}$$

to our ring. Note that $\sqrt{-3} = 2x - 1$ and $x^2 = x - 1$, so

$$\mathbb{Z}[\sqrt{-3}][x] = \mathbb{Z}[x] = \{a + bx | a, b \in \mathbb{Z}\}.$$

Note that

$$N(x) = N(1 + \sqrt{-3})/N(2) = 1,$$

so $x$ is a unit, and the norm function extends to $\mathbb{Z}[x]$. In this larger ring, $1 \pm \sqrt{-3}$ and 2 are still irreducible, but they are now associated. In fact, $\mathbb{Z}[x]$ is a Euclidean ring with respect to $N$, and hence a UFD. We will see that $\mathbb{Z}[x]$ is the integral closure of $\mathbb{Z}[\sqrt{-3}]$.

It is also easy to see that the proof of Prop. 2.25 breaks down precisely for $d = -3$: the lattice $qb$ with $q \in \mathbb{Z}[\sqrt{-3}]$ is a rectangular lattice with sides equal to $|b|$ and $|b|\sqrt{3}$, and a point in the center of the rectangle is exactly
|b| units away from each vertex. Hence, for instance, we cannot divide with remainder \(1 + \sqrt{−3}\) by 2 with respect to the function \(N\), and indeed with respect to any Euclidean function. The solution is also clear, we add the centers of all the rectangles to our lattice, this is the same thing as adjoining \(x\).

2.4.4 \(d = -8\).

The ring \(\mathbb{Z}[\sqrt{-8}]\) also fails to be a UFD, for a similar reason. Consider the factorization

\[-8 = \sqrt{-8} \cdot \sqrt{-8} = (-2)(-2)(-2).\]

The corresponding norms are \(64 = 8 \cdot 8 = 4 \cdot 4 \cdot 4\), and the ring \(\mathbb{Z}[\sqrt{-8}]\) has no elements of norm 2, hence \(\sqrt{-8}\) and \(-2\) are irreducible in \(\mathbb{Z}[\sqrt{-8}]\).

It is clear that we are missing the element \(x = \sqrt{-2} = \sqrt{-8}/(-2)\). Note that \(\sqrt{-8} = -2x\) and \(x^2 = -2\), therefore adjoining \(x\) gives the ring \(\mathbb{Z}[\sqrt{-2}]\), which is a UFD. Again, \(\mathbb{Z}[\sqrt{-2}]\) is the integral closure of \(\mathbb{Z}[\sqrt{-8}]\).

2.4.5 \(d = -5\).

The ring \(\mathbb{Z}[\sqrt{-5}]\), as we shall see, is our first truly nontrivial example of a non-UFD. Consider the equation

\[(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3.\]

The corresponding norms are \(6 \cdot 6 = 4 \cdot 9\), the equations \(a^2 + 5b^2 = 2\) and \(a^2 + 5b^2 = 3\) have no solutions, hence the elements \(1 \pm \sqrt{-5}, 2\) and \(3\) are irreducible.

We can attempt to remedy this situation by adding, say, \(x = (1 + \sqrt{-5})/2\) to the ring \(\mathbb{Z}[\sqrt{-5}]\). This, however, leads to a number of interrelated problems:

1. \(N(x) = 3/2\) is not an integer.

2. The element \(x\) satisfies \(2x^2 = 2x - 3\), hence it is no longer true that \(\mathbb{Z}[\sqrt{-5}][x] = \{a + bx | a, b \in \mathbb{Z}\}\). In other words, adding \(x\) is not enough: we need to add \(x^2, x^3, \) and so on.

3. The element \(x^2 - x + 2 = 1/2\) is now in the ring, hence \(\mathbb{Z}[x]\) contains elements of arbitrarily small norm, and therefore doesn’t form a lattice in \(\mathbb{C}\).
4. The element 2 has become invertible in \( \mathbb{Z}[x] \), so we have restored unique factorization at the cost of losing a prime number.

The difference between this example and the previous is that the rings \( \mathbb{Z}[\sqrt{-3}] \) and \( \mathbb{Z}[\sqrt{-8}] \) are not integrally closed, but their integral closures are UFDs, while \( \mathbb{Z}[\sqrt{-5}] \) is integrally closed but still not a UFD.

2.4.6 \( d = 2 \).

The rings \( \mathbb{Z}[\sqrt{d}] \) with \( d > 0 \) behave quite differently, the main reason for this being that the equation

\[
N(a + b\sqrt{d}) = a^2 - b^2d = \pm 1
\]

describing the units, known as Pell’s equation, has infinitely many solutions for \( d > 0 \). It turns out that the set of units is \( \pm \varepsilon^n \), where \( n \in \mathbb{Z} \) and \( \varepsilon \) is a fundamental unit of \( \mathbb{Z} [\sqrt{d}] \). For now we prove this for \( d = 2 \):

**Proposition 2.31.** The units of \( \mathbb{Z}[\sqrt{2}] \) are \( \pm (1 + \sqrt{2})^n \) with \( n \in \mathbb{Z} \), in other words the group of units is isomorphic to \( \mu_2 \oplus \mathbb{Z} \).

**Proof.** First we check that \( N(1 + \sqrt{2}) = -1 \), so \( 1 + \sqrt{2} \) is a unit with inverse \( -1 + \sqrt{2} \). Now suppose that there is a unit \( a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \) that is not of the form \( \pm (1 + \sqrt{2})^n \). Passing to the conjugate and multiplying by \( -1 \) if necessary, we can assume that \( a, b > 0 \). Pick such a unit with smallest positive \( a \). Clearly \( a > 1 \), so \( a^2 - 2b^2 = 1 \) implies that \( 2b > a > b \). Then

\[
\frac{a + b\sqrt{2}}{1 + \sqrt{2}} = 2b - a + (a - b)\sqrt{2}.
\]

But \( 0 < 2b - a < a \), hence the unit on the right hand side is a power of \( 1 + \sqrt{2} \), which is a contradiction. \( \square \)

2.5 Integral dependence and unique factorization

We have seen that the rings \( \mathbb{Z}[\sqrt{d}] \) are not UFDs for \( d = -3 \) and \( d = -8 \). However, the failure of unique factorization is due to the absence of an element \( x \) which satisfies a monic polynomial equation with integer coefficients. This turns out to be a key property, which we need to study in detail.
**Definition 2.32.** Let $A \subset B$ be integral domains. An element $x \in B$ is said to be integral over $A$ if it is a root of a monic polynomial with coefficients in $A$, in other words if there exist $a_1, \ldots, a_n \in A$ such that

$$x^n + a_1x^{n-1} + \cdots + a_n = 0.$$ 

**Example 2.33.** Let $A = \mathbb{Z}$ and let $B = \mathbb{Q}$. Let $x = r/s$ be integral over $\mathbb{Z}$, where $r$ and $s$ are relatively prime. Clearing denominators, we see that

$$r^n + sa_1r^{n-1} + \cdots + s^na_n = 0,$$

hence $s|r^n$. It follows that $s|r$, so $s = \pm 1$.

The definition of integrality is somewhat mysterious at first, but it becomes much clearer once we reinterpret it in the language of modules.

**Proposition 2.34.** Let $A \subset B$ be integral domains. Then an element $x \in B$ is integral over $A$ if and only if the $A$-algebra $A[x]$ is finitely generated as an $A$-module.

**Remark 2.35.** If $A$ and $B$ are fields, then this implies that an element $x \in B$ is integral over $A$ if and only if it is algebraic, so integrality is the correct generalization of algebraicity from fields to rings.

We first prove a slightly different statement:

**Proposition 2.36.** Let $A \subset B$ be integral domains. Then an element $x \in B$ is integral over $A$ if and only if there exists a finitely generated nonzero $A$-module $M \subset B$ such that $xM \subset M$.

**Proof.** Suppose that $x \in B$ is integral over $A$, satisfying the equation

$$x^n + a_1x^{n-1} + \cdots + a_n = 0, \quad a_i \in A.$$ 

Let $M = A[x]$. Then clearly $xM \subset M$, and $M$ is generated as an $A$-module by $1, x, \ldots, x^{n-1}$.

Conversely, suppose that $M \subset B$ is generated as an $A$-module by $m_1, \ldots, m_n$, which we assume to be nonzero. If $xM \subset M$, then there exist elements $a_{ij} \in A$ such that

$$xm_i = \sum_{j=1}^n a_{ij}m_j, \quad i = 1, \ldots, n.$$
Let $X$ be the $n \times n$-matrix with entries $\delta_{ij}x - a_{ij}$, and let adj $X$ be its adjugate. Then

$$\text{adj } X \cdot X = I_n \det X.$$ 

Applying adj $X \cdot X$ to the vector $(m_1, \ldots, m_n)$, we see that $\det X = 0$, which gives the monic equation for $x$.

\textit{Proof of Prop. 2.34.} If $x \in B$ is integral, then by the proof of Prop. 2.36 $A[x]$ is a finitely generated $A$-module. Conversely, it is clear that $xA[x] \subset A[x]$, so if $A[x]$ is a finitely generated $A$-module, then by Prop. 2.36 $x$ is integral over $A$.

\textbf{Proposition 2.37.} Let $A \subset B$ be integral domains, and let $C$ be the set of elements of $B$ integral over $A$. Then $C$ is a subring of $B$ containing $A$.

\textit{Proof.} Every element of $A$ is integral over $A$. Let $x, y \in C$, we need to show that $x + y$ and $xy$ are in $C$. By Prop. 2.36, there exist finitely generated $A$-modules $M, N \subset B$ such that $xM \subset M$ and $yN \subset N$. Consider the $A$-submodule $MN \subset B$ generated by $m_in_j$, where $m_1, \ldots, m_k$ and $n_1, \ldots, n_l$ are generators for $M$ and $N$, respectively. It is clear that $(x + y)MN \subset MN$ and $xyMN \subset MN$, and $MN$ is nonzero because $B$ is an integral domain. Hence $x + y$ and $xy$ are integral over $A$.

\textbf{Definition 2.38.} The ring $C$ is called the \textit{integral closure} of $A$ in $B$. If $C = A$, we say that $A$ is \textit{integrally closed} in $B$. If $C = B$, we say that $B$ is \textit{integral} over $A$. If $A$ is a domain, its \textit{integral closure} is its integral closure in its fraction field. We say that an integral domain is \textit{integrally closed} if it is equal to its integral closure.

Prop. 2.34 can be generalized to extensions of rings.

\textbf{Corollary 2.39.} Let $A \subset B$ be integral domains. Then $B$ is finitely generated as an $A$-algebra and integral over $A$ if and only if $B$ is a finite $A$-module.

\textit{Proof.} Suppose that $B = A[x_1, \ldots, x_n]$, with $x_i$ integral over $A$. Then $x_n$ is integral over $A[x_1, \ldots, x_{n-1}]$, because it is integral over $A$. Hence $B$ is a finite $A[x_1, \ldots, x_{n-1}]$-module, which by induction is a finite $A$-module. Therefore $B$ is a finite $A$-module.
Remark 2.40. This is the exact analogue for rings of Prop. 1.59 for fields.

Proposition 2.41. Let $A \subset B \subset C$ be domains. If $B$ is integral over $A$ and $C$ is integral over $B$, then $C$ is integral over $A$. In particular, the integral closure of a ring is integrally closed.

Proof. Suppose that $x \in C$ satisfies

$$x^n + b_1x^{n-1} + \cdots + b_n = 0$$

for $b_j \in B$. Then $c$ is in fact integral over the subring $A[b_1, \ldots, b_n]$ of $B$. Hence $A[b_1, \ldots, b_n, c]$ is a finite $A[b_1, \ldots, b_n]$-module, which is a finite $A$-module. Therefore $A[b_1, \ldots, b_n, c]$ is a finite $A$-module, hence $c$ is integral over $A$.

Integrality is preserved under ring homomorphisms.

Proposition 2.42. Let $A \subset B$ be integral domains, and let $\sigma$ be a ring homomorphism of $B$. If $B$ is integral over $A$, then $\sigma(B)$ is integral over $\sigma(A)$.

Proof. Omitted.

Example 2.43. 1. Let $A \subset B$ be integral domains, let $q$ be a prime ideal of $B$, and let $p = A \cap q$ be the contraction. If $B$ is integral over $A$, then $B/q$ is integral over $A/p$.

2. Let $A$ be an integral domain with fraction field $K$, let $L$ be an extension of $K$, and let $\sigma : L \to L$ be an isomorphism of $L$ over $K$. Then $x \in L$ is integral over $A$ if and only if $\sigma(x)$ is integral over $A$.

Integrality is also preserved under localization.

Proposition 2.44. Let $A \subset B$ be integral domains, let $C$ be the integral closure of $A$ in $B$, and let $S$ be a multiplicative subset of $A$. Then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.

Proof. The proof is similar to Prop. 3.5. If $x \in C$, then

$$x^n + a_1x^{n-1} + \cdots + a_n = 0$$
for some \(a_i \in A\). Then for any \(s \in S\), we have
\[
\left(\frac{x}{s}\right)^n + \frac{a_1}{s} \left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{a_n}{s^n} = 0,
\]
hence \(x/s\) is integral over \(S^{-1}A\). Conversely, suppose that \(x \in S^{-1}B\) is integral over \(S^{-1}A\), then
\[
x^n + \frac{a_1}{s_1} x^{n-1} + \cdots + \frac{a_n}{s_n} = 0
\]
for some \(a_i \in A\), \(s_i \in S\). Let \(s = s_1 \cdots s_n\), multiplying by \(s^n\) we see that
\[
(sx)^n + b_2(sx)^{n-1} + \cdots + b_n = 0
\]
for some \(b_i \in A\). Hence \(sx \in C\), therefore \(x \in S^{-1}C\).

We also prove the following result, which has geometric significance, and illustrates the technique of localization.

**Theorem 2.45** (The going-up theorem). Let \(A \subset B\) be domains, with \(B\) integral over \(A\). Let \(p\) be a prime ideal of \(A\). Then there exists a prime ideal \(\mathfrak{p} \subset B\) such that \(A \cap \mathfrak{p} = p\).

The idea of the proof is to remove from consideration all prime ideals containing and contained in \(p\).

**Proposition 2.46.** Let \(A \subset B\) be integral domains, with \(B\) integral over \(A\). Then \(A\) is a field if and only if \(B\) is a field.

**Proof.** Suppose that \(A\) is a field. Any nonzero \(b \in B\) satisfies an equation
\[
b^n + a_1 b^{-1} + \cdots + a_n = b(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) + a_n = 0
\]
with \(a_i \in A\), and hence has inverse \(- (b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1})/a_n\). Conversely, if \(B\) is a field, then for any nonzero \(a \in A\), the element \(a^{-1} \in B\) is integral over \(A\) and satisfies
\[
a^{-n} + a_1 a^{-n+1} + \cdots + a_n = 0
\]
for some \(a_i \in A\). But then \(a^{-1} = -(a_1 + a_2 a + \cdots + a_n a^{n-1}) \in A\). \(\square\)
Corollary 2.47. Let $A \subset B$ be integral domains, with $B$ integral over $A$.

1. If $q$ is a prime ideal of $B$ and $p = A \cap q$, then $q$ is maximal if and only if $p$ is maximal.

2. If $q$ and $q'$ are two prime ideals of $B$ such that $q \subset q'$ and $A \cap q = A \cap q'$, then $q = q'$

Proof. For part 1, note that $B/q$ is integral over $A/p$ by Prop. 2.42, and use Prop. 2.46. For part 2, we localize at $p$. By Prop. 2.44, $B_p$ is integral over $A_p$, which is a local ring with maximal ideal $m = pA_p$. Denote $n = qB_p$, $n' = q'B_p$, then by Part 1 the ideals $n$ and $n'$ are maximal and hence $n = n'$. But then $q = q'$ by Prop. 1.77.

Proof of Thm. 2.45. We localize at $p$. The ring $B_p$ is integral over $A_p$. Let $n$ be maximal ideal of $B_p$, then by the above $n \cap A_p$ is a maximal ideal of $A_p$, so it must be $pA_p$. Therefore the contraction $\mathfrak{P}$ of $n$ to $B$ is a prime ideal such that $\mathfrak{P} \cap A = p$.

We now consider several examples. In the beginning of this section, we saw that $\mathbb{Z}$ is integrally closed. This is a general phenomenon:

Proposition 2.48. A unique factorization domain is integrally closed.

Proof. Let $A$ be a unique factorization domain with fraction field $K$. Let $a/b \in K$, with $a$ and $b$ relatively prime, satisfy the equation

$$\left(\frac{a}{b}\right)^n + c_1 \left(\frac{a}{b}\right)^{n-1} + \cdots + c_n = 0,$$

with $c_1, \ldots, c_n \in A$. Clearing denominators, we get

$$a^n + c_1a^{n-1}b + \cdots + c_nb^n = 0.$$

Hence $b|a^n$, so if $p$ is a prime element dividing $b$, then $p|a$, which is a contradiction.

It follows that, before studying a ring for unique factorization, we should first pass to the integral closure. For example, let’s compute the integral closure of $\mathbb{Z}[\sqrt{d}]$. 

37
Proposition 2.49. Let $d$ be a square-free integer. Then the integral closure of $\mathbb{Z}[\sqrt{d}]$ is equal to

$$
\mathbb{Z}[(1 + \sqrt{d})/2], \quad d \equiv 1 \text{ mod } 4,
$$

$$
\mathbb{Z}[\sqrt{d}], \quad d \equiv 2, 3 \text{ mod } 4.
$$

Proof. Let $x = (p + q\sqrt{d})/r$ be an element in the fraction field $\mathbb{Q}(\sqrt{d})$ of $\mathbb{Z}[\sqrt{d}]$, where we assume that $\gcd(p, q, r) = 1$. Then by Prop. 3.17 $x$ is integral if and only if the coefficients of its minimal polynomial

$$
(t - \frac{p + q\sqrt{d}}{r})(t - \frac{p - q\sqrt{d}}{r}) = t^2 - \frac{2p}{r}t + \frac{p^2 - q^2d}{r^2}
$$

are integers. Suppose that $p$ and $r$ have a common prime factor $s$, then since $s^2 \nmid d$ we see that $s|q$, which is a contradiction. Hence either $r = 1$ or $r = 2$. If $r = 1$, then $x \in \mathbb{Z}[\sqrt{d}]$. If $r = 2$, then $p^2 - q^2d \equiv 0 \text{ mod } 4$. Since $4 \nmid d$ this implies that $p$ and $q$ are odd, in which case $p^2, q^2$ and hence $d$ are $1 \text{ mod } 4$. This completes the proof.

Remark 2.50. If $d = p_1^{e_1} \cdots p_k^{e_k}$ is not a square, then the integral closure of $\mathbb{Z}[\sqrt{d}]$ is the same as the integral closure of $\mathbb{Z}[\sqrt{d'}]$, where $d' = p_1 \cdots p_k$ is the square-free part. Hence we will only consider $\mathbb{Z}[\sqrt{d}]$ with $d$ square-free.

Geometric Example 2.51. The ring $\mathbb{C}[t^2, t^3]$ of Ex. 2.22 is not integrally closed, because its field of fractions is $\mathbb{C}(t)$, and the element $t$ satisfies the monic equation $z^2 - t^2 = 0$. In fact, the integral closure of $\mathbb{C}[t^2, t^3]$ is $\mathbb{C}[t]$, and the ring inclusion $\mathbb{C}[t^2, t^3] \subset \mathbb{C}[t]$ corresponds to the normalization of the cuspidal cubic by the smooth curve $\mathbb{A}^1 = \text{Spec } \mathbb{C}[t]$.

3 The ring of integers of a number field

We are now ready to give the main definition of our course.

Definition 3.1. Let $K$ be a number field, in other words a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}$ is called the ring of algebraic integers of $K$ and is denoted $\mathfrak{O}_K$.
Example 3.2. We have seen in the previous section that $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$.

Our goal is the following structure theorem.

**Theorem 3.3.** Let $K$ be a number field of degree $n$. Then $\mathcal{O}_K \simeq \mathbb{Z}^n$, in other works $\mathcal{O}_K$ is a finitely generated free abelian group of rank $n$.

We will prove a more general statement.

**Proposition 3.4.** Let $A$ be a Noetherian integrally closed integral domain with fraction field $K$, and let $L$ be a finite separable extension of $K$. Then the integral closure $B$ of $A$ in $L$ is a finite $A$-module.

First, we determine the relationship between $B$ and $L$:

**Proposition 3.5.** Let $A$ be an integral domain, let $K$ be its fraction field, and let $L$ be an extension of $K$. If $x \in L$ is algebraic over $K$, then there exists a nonzero $d \in A$ such that $ax$ is integral over $A$.

*Proof.* Suppose that $x \in L$ is algebraic over $K$, then it satisfies an equation

$$x^n + a_1x^{n-1} + \cdots + a_n = 0,$$

where $a_i \in K$. Choose $d$ to be a common denominator for all $a_i$, then $da_i \in A$ for all $i$. Multiplying by $d^n$, we get

$$(dx)^n + da_1(dx)^{n-1} + \cdots + d^na_n = 0,$$

so $dx$ is integral over $A$ because $d^na_i \in A$ for all $i$.

**Corollary 3.6.** Let $A$ be an integral domain, let $K$ be its fraction field, let $L$ be an extension of $K$, and let $B$ be the integral closure of $A$ in $L$. If $L$ is algebraic over $K$, then $L$ is the field of fractions of $B$.

*Proof.* Omitted.
3.1 Trace, norm, discriminant, and the trace pairing

**Definition 3.7.** Let $K$ be a field, and let $L$ be a finite extension of degree $n$. Let $x \in L$, and let $T_x : L \to L$ be the $K$-linear map $T_x(y) = xy$. We define

1. The **trace** $\text{Tr}_{L/K}(x) = \text{tr} T_x$.
2. The **norm** $\text{Nm}_{L/K}(x) = \det T_x$.
3. The characteristic polynomial $c_{x,L/K}(t) = \det(tI_n - T_x)$ of $T_x$.

**Remark 3.8.** Note that trace is an additive homomorphism from $L$ to $K$, while the norm is a multiplicative homomorphism from $L^*$ to $K^*$. Note that the trace and norm of an element $x \in L$ is defined only relative to a subfield $K$ of finite index.

**Proposition 3.9.** Let $L$ be a finite extension of $K$, let $x \in L$, let $p_x(t)$ be the minimum polynomial of $x$, and let $x_1, \ldots, x_m$ be the roots of $p_x(t)$ in $\mathcal{K}$. Then

$$c_{x,L/K}(t) = p_x(t)^d, \quad \text{Tr}_{L/K}(x) = d \sum_{i=1}^m x_i, \quad \text{Nm}_{L/K}(x) = \left( \prod_{i=1}^m x_i \right)^d,$$

where $d = [L : K(x)]$.

**Proof.** Let

$$p_x(t) = t^m + c_1 t^{m-1} + \cdots + c_m.$$

Let $1, x, \ldots, x^{m-1}$ be a basis of $K(x)$ over $K$, with respect to this basis the map $T_x|_{K(x)} : K(x) \to K(x)$ has matrix

$$A_x = \begin{pmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 1 \\
-c_m & -c_{m-1} & -c_{m-2} & \cdots & -c_1
\end{pmatrix},$$

whose characteristic polynomial is $p_x(t)$. Let $\alpha_1, \ldots, \alpha_d$ be a basis of $L$ over $K(x)$, and let $\alpha_i x^j$ be the corresponding basis of $L$ over $K$, then the matrix of $T_x : L \to L$ with respect to our basis is block-diagonal with $d$ blocks equal to $A_x$, hence its characteristic polynomial is $p_x(t)^d$. The second and third formulas follow immediately. □
For separable extensions, we can give a Galois-theoretic interpretation of the above result.

**Proposition 3.10.** Let $K$ be a field, let $L$ be a separable extension of $K$ of degree $n$, and let $\sigma_1, \ldots, \sigma_n$ be $K$-homomorphisms of $L$ into $\overline{K}$. Let $x \in L$. Then

$$c_{x,L/K}(t) = \prod_{i=1}^n (t - \sigma_i(x)), \quad \text{Tr}_{L/K}(x) = \sum_{i=1}^n \sigma_i(x), \quad \text{Nm}_{L/K}(x) = \prod_{i=1}^n \sigma_i(x).$$

*Proof.* Omitted. $\square$

**Remark 3.11.** This was Dedekind’s original definition of trace and norm.

**Proposition 3.12.** Let $K \subset L \subset M$ be a tower of finite separable extensions. Then

$$\text{Tr}_{L/K} \circ \text{Tr}_{M/L} = \text{Tr}_{M/K}, \quad \text{Nm}_{L/K} \circ \text{Nm}_{M/L} = \text{Nm}_{M/K}.$$

*Proof.* Omitted. $\square$

**Remark 3.13.** This follows easily from the above proposition, but is in fact true for inseparable extensions as well.

**Definition 3.14.** Let $K \subset L$ be a finite extension. The *trace pairing* is the symmetric bilinear $K$-valued pairing $L \times L \to K$ defined by

$$(x, y) \mapsto \text{Tr}_{L/K}(xy).$$

**Definition 3.15.** Let $K \subset L$ be a finite separable extension, let $x_1, \ldots, x_n$ be a $K$-basis of $L$, and let $\sigma_1, \ldots, \sigma_n$ be the $K$-homomorphisms of $L$ into an algebraic closure $\overline{K}$ of $K$. The *discriminant* of $x_1, \ldots, x_n$ is defined by

$$d(x_1, \ldots, x_n) = \det(\sigma_ix_j)^2.$$

**Proposition 3.16.** Let $K \subset L$ be a finite separable extension. Then the trace pairing on $L$ is nondegenerate, and if $x_1, \ldots, x_n$ is a $K$-basis of $L$, then

$$d(x_1, \ldots, x_n) \neq 0.$$
Proof. Let \( \sigma_1, \ldots, \sigma_n \) be the \( K \)-homomorphisms of \( L \) into \( \overline{K} \), and let \( x_1, \ldots, x_n \) be a \( K \)-basis of \( L \). Then by Prop. 3.10 we have

\[
\text{Tr}_{L/K}(x_i x_j) = \sum_{k=1}^{n} \sigma_k(x_i) \sigma_k(x_j),
\]

so the matrix \( \text{Tr}_{L/K}(x_i x_j) \) is a product of the matrices \( (\sigma_k x_i)^t \) and \( (\sigma_k x_j) \), hence

\[
d(x_1, \ldots, x_n) = \det(\text{Tr}_{L/K}(x_i x_j)).
\]

Now let \( x \in L \) be a primitive element, and consider the corresponding \( K \)-basis \( y_i = x^{i-1} \). Let \( z_i = \sigma_i(x) \). Then

\[
\det(\sigma_i y_j) = \begin{pmatrix}
1 & z_1 & \cdots & z_1^{n-1} \\
1 & z_2 & \cdots & z_2^{n-1} \\
\vdots & \vdots & \ddots & \vdots \\
1 & z_n & \cdots & z_n^{n-1}
\end{pmatrix} = \prod_{1 \leq i < j \leq n} (z_j - z_i) \neq 0,
\]

hence

\[
\det(\text{Tr}_{L/K}(y_i y_j)) = d(y_1, \ldots, y_n) = \prod_{1 \leq i < j \leq n} (z_j - z_i)^2
\]

is nonzero, so \( \text{Tr}_{L/K} \) is a nondegenerate pairing. Finally, if \( x_1, \ldots, x_n \) is an arbitrary \( K \)-basis of \( L \), then \( d(x_1, \ldots, x_n) \) differs from \( d(y_1, \ldots, y_n) \) by the square of the determinant of the change of basis matrix, hence is also nonzero. \( \square \)

### 3.2 Finiteness of integral closure

We are now ready to prove Thm. 3.3 and Prop. 3.4. First, let’s prove a related result.

**Proposition 3.17.** Let \( A \) be an integrally closed integral domain with field of fractions \( K \), and let \( L \) be a finite extension of \( K \). An element \( x \in L \) is integral over \( A \) if and only if the coefficients of its minimal polynomial \( p_x \) lie in \( A \), in which case \( \text{Tr}_{L/K}(x) \) and \( \text{Nm}_{L/K}(x) \) also lie in \( A \).

**Proof.** Let \( x \in L \), and let \( p_x(t) \) be its minimal polynomial. It is monic by definition, so if \( p_x(t) \in A[t] \) then \( x \) is integral over \( A \).

Conversely, suppose that \( x \) is integral over \( A \), then \( g(x) = 0 \) for some monic polynomial \( g \in A[t] \). Then \( p_x \) divides \( g \) in \( K[t] \), hence each root
$x_i \in \overline{K}$ of $p_x$ is also a root of $g$, hence each $x_i$ is integral over $A$. The coefficients of $p_x$ are symmetric functions of its roots, so by Prop. 2.37 they are integral over $A$. However, they lie in $K$, and since $A$ is integrally closed they lie in $A$. Finally, by Prop. 3.9, $\text{Tr}_{L/K}(x)$ and $\text{Nm}_{L/K}(x)$ are also integral over $A$, hence are in $A$.

Proof of Prop. 3.4. Let $x_1, \ldots, x_n$ be a $K$-basis of $L$. By Prop. 3.5, we can assume that $x_i \in B$. By Prop. 3.16, the trace pairing $\text{Tr}(xy)$ is a non-degenerate $K$-valued bilinear form on $L$. Let $y_1, \ldots, y_n$ be a dual basis of $L$ with respect to this pairing, so that

$$\text{Tr}(x_i y_j) = \delta_{ij}.$$ 

Pick an element $a \in A$ such that $ay_i \in B$ for all $i$. Given an element $z \in B$, write

$$z = b_1 x_1 + \cdots + b_n x_n$$

with $b_i \in K$. Since $ay_i \in B$, we have $zay_i \in B$ and hence $\text{Tr}(zay_i) = ab_i \in B$. But $ab_i \in K$, hence $ab_i \in A$. Hence $z$, and therefore $B$, is contained in the $A$-submodule of $L$ spanned by the $a^{-1}x_i$. But $A$ is Noetherian, hence by Prop. 1.49 $B$ is a finitely generated $A$-module.

Proof of Thm. 3.3. By Prop. 3.4, $\mathfrak{O}_K$ is a finitely generated $\mathbb{Z}$-module. But $\mathbb{Z}$ is a principal ideal domain, and any finitely generated torsion-free module over a PID is free.

Definition 3.18. Let $K$ be a number field of degree $n$. A basis of $\mathfrak{O}_K$ over $\mathbb{Z}$ is called an integral basis of $K$. The discriminant of an integral basis is called the discriminant of $K$.

Remark 3.19. If $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ are two integral bases, then by the proof of Prop. 3.16 their discriminants satisfy

$$d(x_1, \ldots, x_n) = d(y_1, \ldots, y_n)(\det C)^2,$$

where $C$ is the change-of-basis matrix. However, $C$ is an invertible matrix with integer coefficients, hence $\det C = \pm 1$, therefore the discriminant does not depend on the choice of integral basis.

43
Let’s consider our main example.

**Proposition 3.20.** Let \( d \) be a square-free integer. Then the discriminant of \( \mathbb{Q}(\sqrt{d}) \) is equal to \( d \) if \( d \equiv 1 \mod 4 \) and \( 4d \) if \( d \equiv 2, 3 \mod 4 \).

**Proof.** Prop. 2.49 states that an integral basis of \( \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \) is \( \{1, (1 + \sqrt{d})/2\} \) if \( d \equiv 1 \mod 4 \) and \( \{1, d\} \) if \( d \equiv 2, 3 \mod 4 \), and the proof is a direct calculation.

\[ \square \]

## 4 Dedekind domains

We have seen that

\[ (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3 \]

are two non-equivalent factorizations of 6 in the ring \( \mathbb{Z}[\sqrt{-5}] \). In Sec. 2.2, we interpreted factorization of elements in a domain \( A \) in terms of factorization of the corresponding principal ideals, and saw that the basic concepts of factorization, such as divisibility and prime elements, have an ideal-theoretic interpretation. The solution to the unique factorization problem now presents itself: instead of looking at factorization into only *principal* ideals of \( A \), we use all ideals instead. Under certain assumptions, any ideal, in particular any principal ideal, can be uniquely written as a product of prime ideals.

For example, we will see that there exist prime ideals \( p_1, \ldots, p_4 \subset \mathbb{Z}[\sqrt{-5}] \) such that

\[ (1 + \sqrt{-5}) = p_1p_2, \quad (1 - \sqrt{-5}) = p_3p_4, \quad (2) = p_1p_3, \quad (3) = p_2p_4, \]

and that \( p_1p_2p_3p_4 \) is the unique factorization of the ideal \( (6) \) into prime ideals.

### 4.1 Unique factorization into prime ideals

We are looking for a class of integral domains \( A \) with the property that any ideal can be factored uniquely as a product of prime ideals. Let’s make a list of the properties that \( A \) should have.

1. The Noetherian hypothesis is sufficient to guarantee that an element factors into irreducibles, and to exclude rings that are too large.
2. We have seen that a UFD is integrally closed (but not vice versa), so it makes sense to require $A$ to be integrally closed.

3. For elements $a, b$ in a ring, $a | b$ corresponds to $(b) \subset (a)$. It doesn’t make sense for nonzero prime ideals to divide each other, so we assume that every prime ideal of $A$ that is not the zero ideal is also maximal.

It turns out that these conditions are exactly what we need:

**Definition 4.1.** An integral domain $A$ is called a Dedekind domain if it is Noetherian, integrally closed, and if every nonzero prime ideal of $A$ is maximal, and if it is not a field.

**Remark 4.2.** The Krull dimension $\text{dim} \ A$ of a ring $A$ is defined to be the maximum number $n$ such that there exists a strictly ascending chain of prime ideals of length $n + 1$ in $A$:

$$p_0 \subsetneq p_1 \subsetneq \cdots \subsetneq p_n$$

This notion is intimately related to the geometric interpretation of $A$. For example, if $A$ is an integral domain, then the zero ideal is prime. If $\text{dim} \ A = 0$, then it is also maximal, hence $A$ is a field. In other words, a field should be viewed as a zero-dimensional object, or a “point”. More generally, the Krull dimension of the ring $k[x_1, \ldots, x_n]$ is $n$, corresponding to the fact that it is the ring of functions on an $n$-dimensional space $\mathbb{A}_k^n$.

A Dedekind domain is thus a Noetherian, integrally closed domain of Krull dimension one.

First, we construct a family of Dedekind domains.

**Theorem 4.3.** Let $A$ be a Dedekind domain with fraction field $K$, let $L$ be a finite separable extension of $K$, and let $B$ be the integral closure of $A$ in $L$. Then $B$ is a Dedekind domain.

**Proof.** Since $A$ is Noetherian, $B$ is contained in a finitely generated $A$-module by Prop. 3.4, hence is also Noetherian. It is integrally closed by definition. Finally, let $p$ be a nonzero prime ideal of $B$, let $q = A \cap p$, and let $b \in p$ be a nonzero element. Consider an equation

$$b^n + a_1b^{n-1} + \cdots + a_n = 0$$
with \(a_i \in A\) of the lowest possible degree \(n\). In this case \(a_n \neq 0\), and \(a_n \in q\) implies that \(q\) is a nonzero prime ideal of \(A\). Then \(A/q\) is a field because \(q\) is maximal, and \(B/p\) is integral over \(A/q\) by Prop. 2.42, hence \(B/p\) is a field by Prop. 2.46 and \(p\) is maximal.

\[\blacksquare\]

**Corollary 4.4.** The ring of integers \(\mathfrak{O}_K\) of a number field \(K\) is a Dedekind domain.

We now show that in a Dedekind domain, every ideal factors uniquely as a product of prime ideals. First, we show that any nonzero ideal is divisible by a product of prime ideals.

**Lemma 4.5.** Let \(\mathfrak{O}\) be a Dedekind domain, and let \(\mathfrak{a}\) be a nonzero ideal. Then there exist nonzero prime ideals \(\mathfrak{p}_i\) such that

\[\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset \mathfrak{a}\]

**Proof.** The proof is very similar to that of Prop. 2.13. Consider the set \(\mathfrak{M}\) of ideals of \(\mathfrak{O}\) that fail to satisfy this property. If it is non-empty, then it contains a maximal element \(\mathfrak{a}\), because \(\mathfrak{O}\) is Noetherian. The ideal \(\mathfrak{a}\) is not prime, because any prime ideal is not in \(\mathfrak{M}\), hence there exist \(a_1, a_2\) such that \(a_1, a_2 \in \mathfrak{a}\) but \(a_1, a_2 \notin \mathfrak{a}\). Let \(a_1 = (a_1) + \mathfrak{a}\), \(a_2 = (a_2) + \mathfrak{a}\). Then \(a_1\) and \(a_2\) are not in \(\mathfrak{M}\), so they each contain a product of prime ideals. But hence so does \(\mathfrak{a}\), because \(a_1a_2 \subset \mathfrak{a}\), which is a contradiction.

\[\blacksquare\]

In an integral domain such as \(\mathfrak{O}\), we can divide by nonzero elements, and we want to be able to do the same with ideals. We will later make this precise when we talk about fractional ideals, but the basic idea is simple: instead of studying ideals, which are \(\mathfrak{O}\)-submodules of \(\mathfrak{O}\), we also study \(\mathfrak{O}\)-submodules of the fraction field \(K\) of \(\mathfrak{O}\).

**Lemma 4.6.** Let \(\mathfrak{O}\) be a Dedekind domain with fraction field \(K\). For a prime ideal \(\mathfrak{p}\) of \(\mathfrak{O}\) define the following \(\mathfrak{O}\)-submodule of \(K\):

\[\mathfrak{p}^{-1} = \{x \in K | \mathfrak{p}x \subset \mathfrak{O}\}\]

Then \(\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{O}\), and for every nonzero ideal \(\mathfrak{a}\) of \(\mathfrak{O}\) we have \(\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1}\).
Proof. First, note that for any ideal \( a \subset \mathfrak{p} \), the \( \mathfrak{O} \)-submodule \( \mathfrak{a} \mathfrak{p}^{-1} \) of \( K \) is actually a submodule of \( \mathfrak{O} \), i.e. it is an ideal.

We now show that \( \mathfrak{O} \not\subseteq \mathfrak{p}^{-1} \). Indeed, let \( a \in \mathfrak{p} \) be a nonzero element. Choose \( n \) to be the smallest integer such that there exist prime ideals \( \mathfrak{p}_1, \ldots, \mathfrak{p}_n \) such that \( \mathfrak{p}_1 \cdots \mathfrak{p}_n \subset (a) \). By Prop. 1.23 one of the \( \mathfrak{p}_i \) is contained in \( \mathfrak{p} \), say \( \mathfrak{p}_1 \), in which case \( \mathfrak{p}_1 = \mathfrak{p} \) because all nonzero prime ideals are maximal. By the minimality of \( n \) there exists \( b \in \mathfrak{p}_2 \cdots \mathfrak{p}_n \) such that \( b / \in (a) \), hence \( a^{-1}b / \in \mathfrak{O} \). On the other hand, \( a^{-1}b \in \mathfrak{p}^{-1} \), because \( b \mathfrak{p} = b \mathfrak{p}_1 \subset (a) \), hence \( a^{-1}b \mathfrak{p} \subset \mathfrak{O} \) and therefore \( a^{-1}b \in \mathfrak{p}^{-1} \).

Now let \( \mathfrak{a} \) be a nonzero ideal of \( \mathfrak{O} \) such that \( \mathfrak{a} \mathfrak{p}^{-1} = \mathfrak{a} \). Then for each \( x \in \mathfrak{p}^{-1} \) we have \( xa \subset \mathfrak{a} \). But \( \mathfrak{O} \) is Noetherian and integrally closed, hence \( \mathfrak{a} \) is a finitely generated \( \mathfrak{O} \)-submodule of \( K \) and by Prop. 2.36 we have \( x \in \mathfrak{O} \).

Now let \( \mathfrak{M} \) be the set of proper ideals of \( \mathfrak{O} \) which do not admit such a factorization, and let \( \mathfrak{a} \) be a maximal element. Let \( \mathfrak{p} \) be a maximal ideal containing \( \mathfrak{a} \), and consider the ideal \( \mathfrak{a} \mathfrak{p}^{-1} \). If \( \mathfrak{a} \mathfrak{p}^{-1} = \mathfrak{O} \), then \( \mathfrak{a} = \mathfrak{a} \mathfrak{p}^{-1} \mathfrak{p} = \mathfrak{O} \mathfrak{p} = \mathfrak{p} \), which is impossible because \( \mathfrak{p} / \in \mathfrak{M} \). On the other hand \( \mathfrak{a} \not\subset \mathfrak{a} \mathfrak{p}^{-1} \), hence \( \mathfrak{a} \mathfrak{p}^{-1} \) admits a factorization

\[
\mathfrak{a} \mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_n.
\]

But then so does \( \mathfrak{a} = \mathfrak{a} \mathfrak{p}^{-1} \mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{p} \), a contradiction.

Now suppose that

\[
\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m
\]

are two prime ideal factorizations of \( \mathfrak{a} \). By Prop. 1.23 we have \( \mathfrak{p}_1 \subset \mathfrak{q}_i \) for some \( i \), hence \( \mathfrak{p}_1 = \mathfrak{q}_i \). Multiplying by \( \mathfrak{p}_1^{-1} \) and using that \( \mathfrak{p}_1 \mathfrak{p}_1^{-1} = \mathfrak{O} \), we cancel \( \mathfrak{p}_1 \) on both sides, and continuing in this manner we see that the factorizations are the same after a reordering.

\[\square\]
4.2 Local characterization of Dedekind domains

Let \( U \) be an open subset of the complex plane \( \mathbb{C} \), and let \( \mathcal{O}(U) \) denote the ring of holomorphic functions on \( U \). A function \( f \in \mathcal{O}(U) \) is the zero function if and only if \( f(a) = 0 \) for all \( a \in U \). In other words, being zero is a local property. A slightly less obvious fact is the following: \( f \in \mathcal{O}(U) \) is a unit if and only if \( f(a) \neq 0 \) for all \( a \in U \), in other words if and only if \( f(a) \in \mathbb{C} \) is a unit for all \( a \in U \). Hence being a unit is also a local property.

Now suppose that \( g \in \mathcal{O}(U) \), and we pose the problem of finding a function \( f \in \mathcal{O}(U) \) satisfying the differential equation

\[
\frac{df}{dz} = g. \tag{4}
\]

Locally, we can always do this: for any \( a \in U \), we can find a neighborhood \( a \in V \subset U \) in which \( g \) is given by a convergent Taylor series

\[
g(z) = c_0 + c_1(z-a) + \frac{1}{2}c_2(z-a)^2 + \cdots,
\]

and then the Taylor series

\[
f(z) = c_0(z-a) + \frac{1}{2}c_1(z-a)^2 + \frac{1}{6}c_2(z-a)^3 + \cdots
\]

is also convergent on \( V \) and solves (4). Alternatively, if \( V \) is simply connected, we define

\[
f(z) = \int_a^z g(w) \, dw.
\]

However, there might be no solution of (4) on all of \( U \). For example, if \( U = \mathbb{C} \setminus \{0\} \) and \( g(z) = 1/z \), then the general solution of (4) is the multivalued function \( \log z + C \), which is not in \( \mathcal{O}(U) \).

We see that a solution of (4) on \( U \) may exist locally but not globally, and this failure is related to the global geometry of \( U \). In fact, we can make a precise characterization (4) has a global solution on \( U \) if and only if \( g(z) \, dz \) represents a nonzero cohomology class in \( H^1_{dR}(U, \mathbb{C}) \), and hence (4) has a solution for all \( g \) if and only if \( H^1_{dR}(U, \mathbb{C}) = 0 \). There are several equivalent characterizations of such \( U \), for example we may require that \( H_1(U, \mathbb{Z}) = 0 \) or \( \pi_1(U) = 0 \).

A ring \( A \) corresponds to a geometric object \( \text{Spec} A \), whose points correspond to the prime ideals of \( A \). Given a prime ideal \( p \) of \( A \), we can form
the localization $A_p$, which is usually a simpler object to study because it is a local ring.

As a first example, being zero and being a unit are local properties:

**Proposition 4.8.** Let $A$ be a ring, and let $a \in A$ be an element. Then $a$ is zero (resp. a unit) in $A$ if and only if for any maximal ideal $m$, the element $a/1$ is zero (resp. a unit) in $A_m$.

**Proof.** The element $0/1$ is zero in $A_m$ for any $m$. Conversely, for $a \in A$ let $D = \{ s \in A | as = 0 \}$, and let $a$ be the ideal generated by $D$. If $a = (1)$, then $1 = a_1s_1 + \cdots + a_ns_n$ for some $a_i \in A$ and $s_i \in S$, implying that

$$a = a \cdot 1 = a(a_1s_1 + \cdots + a_ns_n) = 0.$$ 

If $a$ is not the unit ideal, then it is contained in a maximal ideal $m$. Then $as \neq 0$ for any $s \in A \setminus m$, hence $a/1 \neq 0/1$ in $A_m$.

Similarly, if $ab = 1$ in $A$, then $a/1 \cdot b/1 = 1/1$ in any $A_m$. If $a \in A$ is not a unit, then it is contained in some maximal ideal $m$. If $a/1 \cdot b/c = 1/1$ in $A_m$, then for some $t \notin m$ we have $(ab - c)t = 0$, hence $ct \in m$, which is impossible because $c, t \notin m$. □

Similarly, exactness of $A$-module homomorphisms is a local property:

**Proposition 4.9.** Let $f : M \to N$ be an $A$-module homomorphism, and for any maximal ideal $m$ of $A$ let $f_m : M_m \to N_m$ be the corresponding homomorphism of $A_m$-modules. Then $f$ is injective (resp. surjective) if and only if $f_m$ is injective (resp. surjective) for all maximal ideals $m$.

**Proof.** This follows from Prop. 1.84. □

A much more interesting result is that being integrally closed is a local property:

**Proposition 4.10.** Let $A$ be a integral domain. Then $A$ is integrally closed if and only if $A_m$ is integrally closed for any maximal ideal $m$.

**Proof.** Let $C$ be the integral closure of $A$ in its fraction field $K$, then for any maximal ideal $m$, the integral closure of $A_m$ is $C_m$ by Prop. 2.44. Therefore $A$ integrally closed if and only if the map $f : A \to C$ is surjective, which by Prop. 4.9 holds if and only if each $f_m : A_m \to C_m$ is surjective, i.e. if and only if each $A_m$ is integrally closed. □
This suggests that we study Dedekind domains locally.

**Proposition 4.11.** Let $A$ be a Noetherian integral domain. Then $A$ is a Dedekind domain if and only if $A_m$ is Dedekind domain for all maximal ideals $m$ of $A$.

**Proof.** Suppose that $A$ is a Dedekind domain. Then for any $m$, $A_m$ is Noetherian by 1.80, integrally closed by 4.10, and by Prop. 1.77 the only prime ideals of $A_m$ are $(0)$ and $mA_m$. Hence $A_m$ is a Dedekind domain.

Conversely, suppose $A$ is a Noetherian integral domain. If each $A_m$ is a Dedekind domain, then $A$ is integrally closed by Prop. 4.10. If there exists a non-zero, non-maximal prime ideal $p$ in $A$, then it is contained in some maximal ideal $m$, and by Prop. 1.77 and Prop. 4.9 the strict inclusion $(0) \subsetneq p \subsetneq m$ holds in $A_m$ as well, which is impossible since $A_m$ is a Dedekind domain. Hence every nonzero prime ideal of $A$ is maximal, so $A$ is a Dedekind domain.

**Remark 4.12.** It is clear that dimension is a local property. However, being Noetherian is not a local property. A localization of a Noetherian ring is Noetherian by Prop. 1.80, but there are examples of non-Noetherian rings whose localization at every maximal ideal is Noetherian. The converse is true if we assume that every element of the ring is contained in finitely many maximal ideals.

Local Dedekind domains are the simplest rings to study after fields.

**Definition 4.13.** Let $K$ be a field. A discrete valuation on $K$ is a mapping $v : K^* \rightarrow \mathbb{Z}$ satisfying

1. $v(xy) = v(x) + v(y)$ for all $x, y \in K^*$.
2. $v(x + y) \geq \min(v(x), v(y))$.

For a discrete valuation $v$ on $K$, we formally define $v(0) = +\infty$.

**Proposition 4.14.** Let $K$ be a field with a discrete valuation $K$. Then the set $A = \{x \in K|v(x) \geq 0\}$, called the valuation ring of $K$, is a subring of $K$ with maximal ideal $m = \{x \in K|v(x) > 0\}$. The field $K$ is the field of fractions of $A$.

**Proof.** Omitted.
Remark 4.15. It is possible to study more general valuation rings with \( v \) taking values in \( \mathbb{R} \) instead of \( \mathbb{Z} \), but these rings are never Noetherian.

Definition 4.16. A local integral domain \( A \) is called a discrete valuation ring if it is the valuation ring of its field of fractions \( K \) with respect to some discrete valuation. The field \( k = A/\mathfrak{m} \) is called the residue field of \( A \).

It turns out that a DVR is the same thing as a local Dedekind domain.

Proposition 4.17. Let \( A \) be a Noetherian local domain of dimension one with maximal ideal \( \mathfrak{m} \), and let \( k = A/\mathfrak{m} \). Then the following conditions are equivalent:

1. \( A \) is a discrete valuation ring.
2. \( A \) is a Dedekind domain.
3. Every non-zero ideal of \( A \) is a power of \( \mathfrak{m} \).

Proof. Let \( A \) be a discrete valuation ring with fraction field \( K \), valuation \( v \) and maximal ideal \( \mathfrak{m} \). We first observe that \( A \) is a Euclidean domain with respect to \( v \). Indeed, let \( a, b \in A \). If \( v(a) \geq v(b) \), then \( v(a/b) \geq 0 \) so \( a/b \in A \), so \( a = a/b \cdot b \) and we can divide \( a \) by \( b \) without remainder. It follows by Thm. 2.19 that \( A \) is a PID, hence Noetherian, and a UFD, hence integrally closed (by Cor. 2.20 and Thm. 2.48). This proves that (1) implies (2).

If \( A \) is a Dedekind domain, then by Thm. 4.7 every ideal of \( A \) factors into prime ideals, and \( \mathfrak{m} \) is the only nonzero prime ideal, hence (2) implies (3). Finally, if (3) holds, then \( \mathfrak{m}^n \neq \mathfrak{m}^{n+1} \) for all \( n \) by Nakayama’s lemma. Therefore for each nonzero \( x \in A \) there is a unique \( n \) such that \( (x) = \mathfrak{m}^n \).

Define \( v(x) = n \). It is clear that \( v(xy) = v(x) + v(y) \). Similarly, if \( v(x) \geq v(y) \), then \( x \in (y) \), hence \( (x + y) \subset (y) \) and therefore \( v(x + y) \geq v(y) \). Therefore \( v \) is a discrete valuation on \( A \).

\[ \square \]

Definition 4.18. If \( A \) is a DVR with maximal ideal \( \mathfrak{m} \), then a generator \( x \) of \( \mathfrak{m} \) is called a uniformizer of \( A \). It is the only prime element of \( A \) up to associates.

There are two fundamental examples of DVRs.
Example 4.19. Let $K = \mathbb{Q}$, and let $p$ be a prime. Any rational number $x \in \mathbb{Q}$ can be uniquely written as $x = p^{v_p(x)}y$, where the numerator and denominator of $y$ are not divisible by $p$. The function $v_p$ is a valuation on $\mathbb{Q}$, with valuation ring $\mathbb{Z}(p)$ and residue field $\mathbb{F}_p$.

Example 4.20. Let $k$ be a field, let $K = k(t)$, and let $a \in k$. Any rational function $f \in k(t)$ can be uniquely written as $f(t) = (t-a)^{v_a(f)}g(t)$, where $g(a) \neq 0$. The function $v_a$ is a valuation on $k(t)$, with valuation ring $k[t][t-a]$ and residue field $k$.

We conclude by noting that there are several other equivalent ways of characterizing DVRs.

Proposition 4.21. Let $A$ be a Noetherian local integral domain of dimension one with maximal ideal $m$, and let $k = A/m$ be the residue field. Then the following statements are equivalent:

1. $A$ is a discrete valuation ring.
2. $A$ is a principal ideal domain.
3. The $k$-vector space $m/m^2$ is one-dimensional.
4. Every ideal of $A$ is a power of $m$.
5. There exists $x \in A$ such that every nonzero ideal of $A$ has the form $(x^k)$ for $k \geq 0$.

Proof. See [AM] Thm. 9.2.

\hfill \Box

4.3 Fractional ideals

We have seen that being a Dedekind domain is a local property. However, being a UFD is not a local property: any Dedekind domain is locally a DVR (Prop. 4.11) and hence locally a UFD (Prop. 4.17), but not every Dedekind domain is a UFD (for example, we have seen that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD).

We have seen that any principal ideal domain is a unique factorization domain, so having non-principal ideals may be an obstruction to unique factorization. For Dedekind domains, this is the only obstruction:
Proposition 4.22. A Dedekind domain is a UFD if and only if it is a PID.

Proof. A PID is a UFD by Prop. 2.15. Conversely, suppose that $A$ is a Dedekind domain that is a UFD. Since by Thm. 4.7 every ideal of $A$ is a product of prime ideals, it is enough to show that every prime ideal is principal. Let $p$ be a nonzero prime ideal, let $a \in p$ be a nonzero element, and let $a = p_1 \cdots p_n$ be a prime factorization of $a$. Since $p$ is prime, one of the $p_i$ lies in $p$. But then $(p_i)$ is a nonzero prime ideal contained in $p$, and by the Dedekind property $p = (p_i)$. Therefore, we can measure the failure of a Dedekind domain $A$ to be a unique factorization domain by an appropriate quotient of the prime ideals of $A$ modulo the principal ideals, just as the measure of the failure of the solvability of Eq. 4 on $U \subset \mathbb{C}$ is the quotient $H^1_{dR}(U, \mathbb{C})$ of the closed 1-forms on $U$ by the exact 1-forms.

The nonzero ideals of a ring $A$ form an abelian semigroup with respect to multiplication, with the unit ideal as the identity element. However, this semigroup is a group only if $A$ is a field, because $ab = (1)$ implies that $1 \in a$ and $1 \in b$, hence $a = b = (1)$. We cannot in general form quotients in a semigroup, so we need to define inverses of ideals. Recalling that ideals are $A$-submodules of $A$, the solution is evident: we also consider $A$-submodules of the quotient field $K$ of $A$.

Definition 4.23. Let $A$ be an integral domain with fraction field $K$, viewed as an $A$-module. A nonzero $A$-submodule $a \subset K$ is called a fractional ideal if there exists an element $a \in A$ such that $ab \in A$ for all $b \in a$. Any ideal $a \subset A$ is also a fractional ideal; we now call these integral ideals.

Remark 4.24. The condition that $ab \in A$ for all $b \in a$ implies that elements of a fractional ideal $a$ have a uniformly bounded denominator $a$, so for example $K$ itself is not a fractional ideal unless it is finite. We also denote this condition by $a \subset a^{-1}A$. Also, any ideal $a \subset A$ is also a fractional ideal.

Proposition 4.25. Let $A$ be an integral domain. Then any finitely generated $A$-submodule of $K$ is a fractional ideal. Conversely, if $A$ is Noetherian, any fractional ideal is finitely generated.

Proof. Omitted.
Definition 4.26. A principal fractional ideal is an $A$-submodule $(x)$ of $K$ generated by a nonzero element $x \in K$.

Proposition 4.27. Let $A$ be an integral domain with fraction field $K$, and let $a \subset a^{-1}A$ and $b \subset b^{-1}A$ be fractional ideals. Define the $A$-submodules $a \cap b$ and $a + b$ of $K$, and define

$$ab = \left\{ \sum a_i b_i \bigg| a_i \in a, b_i \in b \right\}.$$ 

Then $a \cap b$, $a + b$ and $ab$ are fractional ideals of $A$ contained in $(ab)^{-1}A$.

Proof. Omitted.

We want the fractional ideals of $A$ to form a group under multiplication, with (1) being the identity. This turns out to be a subtle matter.

Definition 4.28. Let $A$ be an integral domain with fraction field $K$. We say that an $A$-submodule $a \subset K$ is an invertible ideal if there exists an $A$-submodule $b \subset K$ such that $ab = (1)$. We call $b$ an inverse of $a$.

Proposition 4.29. Let $A$ be an integral domain with fraction field $K$. If an $A$-submodule $a \subset K$ is invertible, then it is finitely generated and hence a fractional ideal. Moreover, its inverse is unique and equal to

$$a^{-1} = \{ x \in K | xa \subset A \},$$

and it is also a finitely generated fractional ideal.

Proof. Suppose that $ab = A$. Then

$$b \subset a^{-1} = a^{-1}ab \subset Ab = b,$$

hence $b = a^{-1}$.

The condition $aa^{-1} = A$ implies that $1 = x_1 y_1 + \cdots + x_n y_n$ for some $x_i \in a$ and $y_i \in a^{-1}$. Hence for any $x \in a$ we have

$$x = (xy_1)x_1 + \cdots + (xy_n)x_n,$$

and since $xy_i \in A$ for all $i$ it follows that $x_1, \ldots, x_n$ generate $a$, so by Prop. 4.25 it is a fractional ideal.

Finally, note that $aa^{-1} = A$ implies that $a$ is an inverse of $a^{-1}$, hence $a^{-1}$ is also a fractional ideal.
Remark 4.30. The invertible fractional ideals of $A$ form a group under multiplication. A principal fractional ideal $(x)$ is invertible with inverse $(x^{-1})$, and the principal ideals form a subgroup of all invertible ideals.

It turns out that invertibility of fractional ideals is equivalent to the Dedekind property.

Theorem 4.31. Let $A$ be an integral domain. Then $A$ is a Dedekind domain if and only if every fractional ideal of $A$ is invertible.

We prove this theorem by reducing it to a local calculation.

Proposition 4.32. Let $A$ be an integral domain with fraction field $K$, and let $a \subseteq K$ be a fractional ideal. Then $a$ is invertible if and only if $a$ is finitely generated and, for each maximal ideal $m$, $a_m$ is invertible as a fractional ideal over $A_m$.

Proof. If $a$ is invertible, then by Prop. 4.25 it is finitely generated, and a direct calculation shows that $A = aa^{-1}$ implies $A_m = a_m(a^{-1})_m$ for all $m$, so each $a_m$ is invertible.

Conversely, suppose that $a$ is finitely generated. Let $b = aa^{-1}$, where $a^{-1}$ is defined in Prop. 4.29. Then $b$ is an integral ideal of $A$, and for any maximal ideal $m$ we have $b_m = a_m(a^{-1})_m$. It is an exercise to show that for any finitely generated fractional ideal we have $(a^{-1})_m = (a_m)^{-1}$. It follows that for each maximal ideal $m$ we have $b_m = a_m(a_m)^{-1} = A_m$, hence by Prop. 1.77 $b_m \nsubseteq m$. Therefore $b = A$ and hence $a$ is invertible. 

Proposition 4.33. Let $A$ be a local integral domain with maximal ideal $m$. Then $A$ is a discrete valuation ring if and only if every fractional ideal of $A$ is invertible.

Proof. Let $A$ be a DVR with uniformizer $x$ and fraction field $K$, and let $a \subseteq K$ be a fractional ideal. Then there exists $y \in K$ such that $ya$ is an integral ideal, which by Prop. 4.17 is equal to $(x^n)$ for some $n$. But then $a = (x^{n-v(y)})$ is a principal fractional ideal, and hence invertible.

Conversely, suppose that every nonzero fractional ideal of $A$ is invertible. An invertible ideal is finitely generated by Prop. 4.29, so in particular every integral ideal of $A$ is finitely generated and $A$ is Noetherian. Let $\mathfrak{M}$ be the set of nonzero integral ideals of $A$ that are not powers of $m$. If it is not empty,
it contains a maximal element \(a\). Then \(a \subsetneq m\), hence \(m^{-1}a \subsetneq m^{-1}m = A\) is a proper integral ideal containing \(a\). If \(m^{-1}a = a\), then \(a = ma\) and hence \(a = 0\) by Nakayama’s lemma. But if \(m^{-1}a \supsetneq a\), then \(m^{-1}a \notin M\), and therefore \(m-1a\) and hence \(a\) are powers of \(m\). Therefore every integral ideal of \(A\) is a power of \(m\), so \(A\) is a Dedekind domain by Prop. 4.17.

**Proof of Th. 4.31.** Suppose that \(A\) is a Dedekind domain, and let \(a\) be a fractional ideal of \(A\). For any maximal ideal \(m\) of \(A\), the ring \(A_m\) is a Dedekind domain, and the ideal \(a_m\) is invertible by Prop. 4.33. The ideal \(a\) is finitely generated by Prop. 4.29, hence it is invertible by Prop. 4.32.

Conversely, suppose that every fractional ideal of \(A\) is invertible. Then every integral ideal of \(A\) is finitely generated by Prop. 4.29, hence \(A\) is Noetherian. Let \(m\) be a maximal ideal of \(A\), and let \(b\) be a nonzero fractional ideal of \(A_m\). Then by Prop. 1.77 \(b = a_m\) for some fractional ideal \(a\) of \(A\), hence \(b\) is invertible by Prop. 4.32. Hence \(A_m\) is a DVR by Prop. 4.33, so \(A\) is a Dedekind domain.

**Definition 4.34.** Let \(A\) be a Dedekind domain. The non-zero fractional ideals of \(A\) form an abelian group under multiplication, called the *ideal group* \(I\) of \(A\). The principal fractional ideals form a subgroup \(P\), and the quotient \(H = I/P\) is called the *ideal class group* of \(A\).

We summarize all this information in a theorem.

**Theorem 4.35.** Let \(A\) be a Dedekind domain with fraction field \(K\), let \(U\) be the group of units of \(A\), let \(I\) be the ideal group and let \(H\) be the ideal class group. Then there exists an exact sequence of abelian groups

\[1 \rightarrow U \rightarrow K^* \rightarrow I \rightarrow H \rightarrow 1,\]

where the middle map associates to an element \(x \in K^*\) the principal fractional ideal \((x)\), and \(A\) is a unique factorization domain if and only if \(H = 1\).

**References**


56