# Commutative Algebra

Dietrich Burde

Lecture Notes 2009

# Contents

# Introduction

Commutative algebra studies commutative rings, their ideals, and modules over such rings. It has a long and fascinating genesis, and it is also a fundamental basis for algebraic geometry, invariant theory and algebraic number theory.
In the second half of the 19th century, two concrete classes of commutative rings (and their ideal theory) marked the beginning of commutative algebra: rings of integers of algebraic number fields (like $\mathbb{Z}$ in $\mathbb{Q}$), on the one hand, and polynomial rings occurring in classical algebraic geometry and invariant theory, on the other hand. In the first half of the 20th century, after the basics of abstract algebra had been established, commutative algebra was developed further by E. Noether, E. Artin, W. Krull, B. L. van der Waerden, and others. This was applied in the 1940's to classical algebraic geometry by C. Chevalley, O. Zariski, and A. Weil, creating a revolution in this field. The 1950's and 1960's saw the development of the structural theory of local rings, the foundations of algebraic multiplicity theory, Nagata's counter-examples to Hilbert's 14th problem, the introduction of homological methods into commutative algebra, and other pioneering achievements. However, the most important mark of this period was A. Grothendieck's creation of the theory of schemes, the (till now) ultimate revolution of algebraic geometry. His foundational work lead to a far-reaching alliance of commutative algebra and algebraic geometry.

Here is a (very) short list of mathematicians in this field:

Emil Artin (1898-1962),
Richard Dedekind (1831-1916),
David Hilbert (1862-1943),
Ernst Eduard Kummer (1810-1893),
Leopold Kronecker (1823-1891),
Emanuel Lasker (1868 -1941),
Emmy Noether (1882-1935),
Oscar Zariski (1899-1986),
Wolfgang Krull (1899-1971),
Alexander Grothendieck (1928-).

CHAPTER 1

# Commutative Rings and Ideals

Commutative rings are the main objects of commutative algebra. Any field $K$ is a commutative ring. Apart from this, very important and basic examples are the ring of integers $\mathbb{Z}$, the polynomial rings $K[x_1, \ldots, x_n]$ in $n$ variables over a field $K$, the subrings $\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} \mid x, y \in \mathbb{Z}\}$ of $\mathbb{C}$, and others. Of course, there are many interesting rings which are not commutative, e.g., matrix rings $M_n(R)$, $n \geq 2$ over commutative rings, Lie rings, division rings, group rings etc.

We want to start with a brief introductory example, how Kummer tried to tackle Fermat's Last Theorem, and how this started commutative algebra and algebraic number theory with the number ring $\mathbb{Z}[\zeta]$, where $\zeta$ is a $p$-th root of unity. Assume that $p \geq 5$ is a prime number, and that $x, y, z$ are nonzero integers with $p \nmid xyz$ satisfying

$$x^p + y^p = z^p.$$

The minimal polynomial for $\zeta$ over $\mathbb{Q}$ is given by $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. It is irreducible (by Eisenstein's criterion), thus $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$ forms a basis for $\mathbb{Q}(\zeta)$ as a vector space over $\mathbb{Q}$. We have $X^p - 1 = (X-1)(X-\zeta)\cdots(X-\zeta^{p-1})$, and substituting $X = -x/y$, multiplying out the $-1$'s, and clearing denominators, we have

$$x^p + y^p = (x+y)(x+\zeta y)\cdots(x+\zeta^{p-1}y).$$

We have $\zeta^{p-1} = -(1 + \zeta + \cdots + \zeta^{p-2})$, and the ring $\mathbb{Z}[\zeta]$ is given by

$$\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \mid a_i \in \mathbb{Z}\}.$$

In this ring, Fermats equation $x^p + y^p = z^p$ becomes

$$z^p = (x+y)(x+y\zeta)\cdots(x+y\zeta^{p-1}).$$

It is easy to see that the terms on the right-hand side are relatively prime in $\mathbb{Z}[\zeta]$. Suppose now for a moment (as Kummer did), that the ring $\mathbb{Z}[\zeta]$ is *factorial*. Then we could conclude that

$$x + y\zeta = u\alpha^p$$

for some $u, \alpha \in Z[\zeta]$ with $u$ a unit. We may write $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$, so that $\alpha^p \equiv a_0 + a_1 + \cdots + a_{p-2} \mod p$ by the binomial theorem and Fermat's little theorem. In particular, $\alpha^p \equiv r \mod p$ for some $r \in \mathbb{Z}$. If we knew further that $u = \pm\zeta^j$ for some $j \in \mathbb{Z}$, then $x + y\zeta = u\alpha^p \equiv \pm r\zeta^j$ for some $0 \leq j \leq p-1$. Comparing powers of $\zeta$ on both sides, and remembering $p \geq 5$, it follows that $xy \equiv 0 \mod p$, a contradiction to the assumption $p \nmid xyz$.

Unfortunately it turned out, as Kummer realized, that $\mathbb{Z}[\zeta]$ is hardly ever a factorial ring (this is true if and only if $p \leq 19$). Furthermore the units are not only of the form $\pm\zeta^j$. Nonetheless, Kummer was able to make a lot of progress towards the solution of Fermat's last Theorem by modifiying this argument suitably. He realized that even though unique factorization of elements into irreducibles often fails in $\mathbb{Z}[\zeta]$, every *ideal* still factors uniquely into a product of prime ideals. This discovery was the birth of modern algebraic number theory (and a part of commutative algebra). Kummer proved Fermat's Last Theorem for so called *regular primes*.

## 1.1. Basic definitions

DEFINITION 1.1.1. A *ring* $R$ is a set with two binary operations, usually called addition and multiplication such that

- $(R, +)$ is an abelian group, with zero element 0, and additive inverse $-x$ for every $x \in R$.
- The multiplication is associative, i.e., $(x, y, z) = 0$ for all $x, y, z \in R$, where $(x, y, z) = x(yz) - (xy)z$ denotes the associator.
- The distributions laws are satisfied: $x(y + z) = xy + xz$ and $(y + z)x = yx + zx$.

The ring is called *commutative*, if $xy = yx$ for all $x, y \in R$. If not said otherwise we assume that $R$ has a unit element $1 \in R$ satisfying $1x = x1 = x$ for all $x \in R$.

EXAMPLE 1.1.2. *Let $M_3(\mathbb{Z})$ denote the ring of $3 \times 3$-matrices over $\mathbb{Z}$ and*

$$R = \left\{ \begin{pmatrix} x & 0 & 0 \\ 0 & x & 0 \\ y & z & x \end{pmatrix} \mid x, y, z \in \mathbb{Z} \right\}$$

*Then $R$ is a commutative subring of $M_3(\mathbb{Z})$.*

A subset $R \subseteq S$ of a ring $S$ which is closed under the two operations, and contains the identity element of $S$ is called a *subring* of $S$. For example, $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$. It is called the *ring of Gaussian integers*. The bracket notation has the following meaning. If $R \subseteq S$ are two rings and $M \subseteq S$ is a subset of $S$, then we denote by $R[M]$ the smallest subring of $S$ containg $R$ and $M$. In other words,

$$R[M] = \bigcap \{A \subseteq S \mid A \text{ ring}, M \subseteq A, R \subseteq A\}.$$

EXAMPLE 1.1.3. *Let $d \in \mathbb{Z}$. Then $\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} \mid x, y \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$.*

For $d = -1$ we obtain $\mathbb{Z}[i]$. Another example is the ring $\mathbb{Z}[\frac{1}{2}] \subseteq \mathbb{Q}$, which is given by $\{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 0}\}$.
An important class of commutative rings is given by polynomial rings: if $R$ is a ring, then the polynomial ring $R[x]$ in one indeterminate $x$ over $R$ consists of the formal terms

$$\sum_{i=0}^{n} a_i x^i,$$

where $a_i \in \mathbb{R}$ and $n \in \mathbb{Z}_{\geq 0}$. Two such polynomials are equal if and only if the coefficients coincide. Addition is defined in the obvious way, i.e.,

$$\sum_{i \geq 0} a_i x^i + \sum_{i \geq 0} b_i x^i = \sum_{i \geq 0} (a_i + b_i) x^i,$$

whereas multiplication is given by

$$\sum_{i \geq 0} a_i x^i \cdot \sum_{j \geq 0} b_j x^j = \sum_{i \geq 0} \left( \sum_{j=0}^{i} a_j b_{i-j} \right) x^i.$$

This makes $R[x]$ a commutative ring with unit 1. By adjunction one obtains polynomial rings $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$ in $n \geq 1$ variables.

Let $R$ be a commutative ring. We define $R[[x]]$ to be the ring of all formal power series

$$\sum_{i=0}^{\infty} a_i x^i,\ a_i \in R,$$

where addition and multiplication are defined in the same way as before. We have

$$R \subset R[x] \subset R[[x]].$$

REMARK 1.1.4. The ring $R[[x]]$ can be viewd as the completion of the polynomial ring $R[x]$ with respect to the $I$-adic topology determined by the ideal $I = \langle x \rangle$ of $R[x]$. This results in a complete topological ring containing $R[x]$ as a dense subspace.

DEFINITION 1.1.5. A *ring homomorphism* is a mapping $\varphi\colon R \to S$ between two rings satisfying

(1) $f(x+y) = f(x) + f(y)$ for all $x, y \in R$,
(2) $f(xy) = f(x)f(y)$ for all $x, y \in R$,
(3) $f(1_R) = 1_S$.

In other words, $f$ is a homomorphism of the additive abelian groups, respecting the multiplication and the identity element.

DEFINITION 1.1.6. A *left ideal* $I$ of a ring $R$ is an additive subgroup satisfying $RI \subseteq I$. A *right ideal* $I$ is an additive subgroup satisfying $IR \subseteq I$.

We assume that $R$ is commutative, so that any left ideal is a right ideal and vice versa. We just say that $I$ is a (two-sided) ideal. The quotient group $R/I$ inherits a uniquely defined multiplication from $R$ which makes it into a ring, called the *quotient ring*, or residue-class ring $R/I$.
Recall that a *zero-divisor* in a ring $R$ is an element $x \in R$ dividing zero. This means, there is an $y \neq 0$ in $R$ such that $xy = 0$.
An element $x \in R$ is called *nilpotent*, if $x^n = 0$ for some $n \in \mathbb{N}$. If $R \neq 0$, then any nilpotent element is a zero-divisor. The converse need not to be true. For example, 3 is a zero-divisor in $R = \mathbb{Z}/6\mathbb{Z}$, since $3 \cdot 2 = 0$. But 3 is not nilpotent since $3^2 = 3$.
A *unit* in $R$ is an element $x$ which divides 1. This means, there exists an $y \in R$ such that $xy = 1$. The units of a ring $R$ form a multiplicative abelian group $E(R)$. For example, the group of units in the quotient ring $\mathbb{Z}/n\mathbb{Z}$ is given by $E(\mathbb{Z}/n\mathbb{Z}) = \{[k] \in \mathbb{Z}/n\mathbb{Z} \mid (k,n) = 1\}$, i.e. where $k$ and $n$ are coprime. Its cardinality is given by $\varphi(n)$. Here $\varphi$ is called Euler's $\varphi$-funktion. It is defined by

$$\varphi(n) = \sum_{\substack{1 \leq k \leq n \\ (k,n)=1}} 1.$$

EXAMPLE 1.1.7. *Here are a few examples of unit groups of rings $E(\mathbb{Z}[\sqrt{d}])$:*

(1) $E(\mathbb{Z}) = \{\pm 1\}$,
(2) $E(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$,
(3) $E(\mathbb{Z}[\sqrt{2}]) = \{\pm(1+\sqrt{2})^n \mid n \in \mathbb{Z}\}$,
(4) $E(\mathbb{Z}[\sqrt{163}]) = \{\pm(64080026 + 5019135\sqrt{163})^n \mid n \in \mathbb{Z}\}$.

Consider an element $x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, where $d \in \mathbb{Z}$ is not a square. Then $x + y\sqrt{d}$ is a unit in this ring if and only if $(x, y)$ is an integer solution of the Diophantine equation

$$x^2 - dy^2 = \pm 1.$$

Indeed, if $x+y\sqrt{d}$ is a unit, then there exist $u, v \in \mathbb{Z}$ such that

$$(x+y\sqrt{d})(u+v\sqrt{d}) = 1.$$

Rewriting this in the form $(xu+yvd)+(xv+yu)\sqrt{d} = 1+0\sqrt{d}$ yields

$$xv+yu = 0,$$
$$xu+yvd = 1.$$

Since $x, y$ are coprime there is an $m \in \mathbb{Z}$ such that $u = mx$ and $v = -my$. This yields $m(x^2-y^2d) = 1$, i.e., $x^2-dy^2 = \pm 1$.
Conversely this last equation implies

$$(x+y\sqrt{d})(x-y\sqrt{d}) = 1,$$

so that $x+y\sqrt{d}$ is a unit.
For $d=-1$ we obtain the equation $N(x+iy) = x^2+y^2 = \pm 1$, which has exactly 4 solutions $(x,y) = (\pm 1, 0), (0, \pm 1)$, which yields the units $\{\pm 1, \pm i\}$ in $\mathbb{Z}[i]$.
For $d \leq -2$ we obtain the equation $x^2+|d|y^2 = \pm 1$, which has only the solutions $(x,y) = (\pm 1, 0)$.
For $d \geq 2$ the Diophantine equation $x^2-dy^2 = \pm 1$ becomes quite difficult to solve. It is called *Pell's equation*, although it should be rather called *Euler's equation*. There exists a so called fundamental unit $\varepsilon$ such that $\pm\varepsilon^n$ gives infinitely many units. For example, for $\mathbb{Z}[\sqrt{2}]$, the fundamental unit is $\varepsilon = (1+\sqrt{2})$. In fact, all units here are given by

$$\pm(1+\sqrt{2})^n, \ n \in \mathbb{Z}.$$

Note that $(1+\sqrt{2})(1-\sqrt{2}) = -1$, so that $(1-\sqrt{2}) = -(1+\sqrt{2})^{-1}$ and $E(\mathbb{Z}[\sqrt{2}]) = \{\pm(1\pm\sqrt{2})^n \mid n \geq 0\}$. For example,

$$(1+\sqrt{2})^2 = 3+2\sqrt{2},$$
$$(1+\sqrt{2})^3 = 7+5\sqrt{2},$$
$$(1+\sqrt{2})^4 = 17+12\sqrt{2},$$
$$(1+\sqrt{2})^5 = 41+29\sqrt{2},$$
$$(1+\sqrt{2})^6 = 99+70\sqrt{2}.$$

For $d = 163$ the fundamental unit is already difficult to find. The rings $\mathbb{Z}[\sqrt{d}]$, $d \geq 1$ are the rings of integers in real quadratic number fields, as long as $d \equiv 2(4)$ or $d \equiv 3(4)$. A theorem of Dirichlet shows that the unit group $E(\mathcal{O}_K)$ is a finitely generated abelian group, where $K$ is a number field, and $\mathcal{O}_K$ the ring of interegs in $K$. In fact, we have

$$E(\mathcal{O}_K) \simeq \mathbb{Z}^{r+s-1} \oplus \mathbb{Z}/m\mathbb{Z},$$

where $r$ is the number of real embeddings of $K$, $s$ is half the number of complex embeddings, and $m$ is the number of roots of unity in $K$. Note that $r+2s = [K:\mathbb{Q}]$. In particular, for a real quadratic number field $K = \mathbb{Q}[\sqrt{d}]$, the unit group is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, where the fundamental unit $\varepsilon$ generates $\mathbb{Z}$.

In a field $K$, every non-zero element is a unit. For $x \in R$ the set $(x) = \{yx \mid y \in R\}$ is an ideal. Such ideals are called *principal ideals*.

PROPOSITION 1.1.8. *Let $R$ be a non-trivial commutative ring. Then the following are equivalent:*

(1) *$R$ is a field.*
(2) *The only ideals in $R$ are $(0)$ and $(1) = R$.*
(3) *Every ring homomorphism $\varphi\colon R \to S$ into a non-zero commutative ring $S$ is injective.*

PROOF. (1) $\Rightarrow$ (2): Let $I \neq 0$ be an ideal in $R$. Then $I$ contains a non-zero element $x \in R$, which must be a unit. Hence $I \supseteq (x) = (1)$ and $I = (1)$.
(2) $\Rightarrow$ (3): Since $\ker(\varphi)$ is an ideal different from (1) in $R$ it has to be zero. Hence $\varphi$ is injective.
(3) $\Rightarrow$ (1): Let $x$ be an element of $R$ which is not a unit. Then $(x) \neq (1)$, so that $S = R/(x)$ is not the zero ring. Let $\pi\colon R \to S$ be the natural ring epimorphism, with kernel $(x)$. By hypothesis, $\pi$ is injective, hence $(x) = 0$ and $x = 0$. □

DEFINITION 1.1.9. Let $R$ be a commutative ring. Then $R$ is called an *integral domain* if it has no zero divisors. It is called a *principal ideal domain*, or *PID*, if every ideal is a principal ideal. An integral domain $R$ together with a map $d\colon R \setminus 0 \to \mathbb{N}$ is called an *Euclidean ring*, if for all $a, b \in R, b \neq 0$ there exist $q, r \in R$ with $a = qb + r$, such that $r = 0$ or $d(r) < d(b)$.

The following examples show that these properties are not always obvious.

EXAMPLE 1.1.10. *The ring $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean ring and a PID. The ring $\mathbb{Z}[\sqrt{-5}]$ is not Euclidean and not a PID. The ring $\mathcal{O}_{-19} = \mathbb{Z} \oplus \mathbb{Z}(\frac{1+\sqrt{-19}}{2})$ is a PID, but not a Euclidean ring.*

Before we can explain these examples we need some basic results.

PROPOSITION 1.1.11. *Every Euclidean ring $R$ is a PID.*

PROOF. Let $I \neq 0$ be an ideal in $R$. Then the set $\{d(b) \mid b \in I \setminus 0\}$ of non-negative integers has a minimal element $a \neq 0$, i.e., we have $d(a) \leq d(b)$ for all $b \in I \setminus 0$. By assumption, for every $b \in I$ there exist $q, r \in R$ with $b = qa + r$ such that $r = 0$ or $d(r) < d(a)$. The last case is impossible, since $r = b - qa \in I$ and $a$ was minimal. Hence $r = 0$ and $b = qa \in (a)$. It follows $(a) \subset I \subset (a)$, hence $I = (a)$. □

Let us give some easy examples of Euclidean rings. First of all, $R = \mathbb{Z}$ together with $d(n) = |n|$ is a Euclidean ring. It is also a PID, as we know. The polynomial ring $K[x]$ for a field $K$ and $d(f) = \deg(f)$ is also Euclidean, via the well known polynomial divison. In particular $\mathbb{Q}[x]$ is Euclidean. Note that $\mathbb{Z}[x]$ is not Euclidean. Hence a subring of a Euclidean ring need not be Euclidean. On the other hand, the rings $K[x_1, \ldots, x_n]$ are not Euclidean for $n \geq 2$. To see this, we may assume that $n = 2$ and $R = K[x, y]$. Let $I = (x, y)$ be the ideal generated by $x$ and $y$. Suppose that $I$ is principal, i.e., $(x, y) = (f(x, y))$ for some non-zero polynomial $f \in K[x, y]$. Then there exist polynomials $g, h \in R$ such that $x = gf$ and $y = hf$. Denote by $\deg_x$ and $\deg_y$ the degree functions for the polynomial rings $K[y][x]$ resp. $K[x][y]$. Then

$$0 = \deg_y(x) = \deg_y(g) + \deg_y(f),$$
$$0 = \deg_x(y) = \deg_x(h) + \deg_x(f).$$

Since the degree function is non-negative, $f$ has zero degree in $x$ and $y$. This means, $f(x, y) = c \neq 0$ for some constant $c \in K^\times$, i.e.,

$$(x, y) = (f(x, y)) = (1) = R.$$

This is impossible, since all polynomials $g \in (x, y)$ satisfy $g(0, 0) = 0$, but $f(0, 0) = c \neq 0$. Hence $K[x, y]$ is not a PID, and hence not Euclidean.
Let $d$ be a squarefree integer, i.e., which is not divisible by any square integer $\neq 1$. Consider the quadratic number fields

$$\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} \in \mathbb{C} \mid x, y \in \mathbb{Q}\}.$$

For every element $z = x + y\sqrt{d}$ define the norm

$$N(z) = z\overline{z} = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2.$$

For two elements $v, w \in \mathbb{Q}(\sqrt{d})$ we have $\overline{vw} = \overline{v} \cdot \overline{w}$ and $N(vw) = N(v)N(w)$. Let

$$\omega_d = \begin{cases} \sqrt{d}, & \text{if } d \equiv 2, 3(4), \\ \frac{1}{2}(1 + \sqrt{d}), & \text{if } d \equiv 1(4). \end{cases}$$

Then $\mathcal{O}_d = \mathbb{Z} \oplus \mathbb{Z}\omega_d = \{a + b\omega_d \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{Q}(\sqrt{d})$ which is an integral domain. It is called the *ring of integers* in the quadratic number field $\mathbb{Q}(\sqrt{d})$.

PROPOSITION 1.1.12. *The ring $\mathcal{O}_d$ is norm-Euclidean, i.e., with respect to $d(z) = |N(z)|$ if and only if*

$$d = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

PROOF. We cannot give a proof here. It is easy to show that the rings $\mathcal{O}_d$ are norm-Euclidean for the values listed. To show the "only if" part is much more difficult. Let us at least give an argument for the "if" part for $d = -2, -1, 2, 3$. For the general case see [**3**]. Suppose $z, w \in \mathcal{O}_d$ are given with $w \neq 0$. Then

$$zw^{-1} = u + v\sqrt{d}$$

for some $u, v \in \mathbb{Q}$. Choose $n, m \in \mathbb{Z}$ such that $|u - m| \leq 1/2$ and $|v - n| \leq 1/2$. Let $\alpha = u - m$, $\beta = v - n$ and $q = m + n\sqrt{d}$. We have $z = wq + r$ with $r = w(\alpha + \beta\sqrt{d}) \in \mathcal{O}_d$. We have $r = 0$ or

$$|N(r)| = |N(w)N(\alpha + \beta\sqrt{d})| = |N(w)||\alpha^2 - d\beta^2| < |N(w)|,$$

since $|\alpha^2 - d\beta^2| \leq \alpha^2 + 2\beta^2 \leq 3/4$ for $|d| \leq 2$, and $|\alpha^2 - 3\beta^2| \leq \max\{\alpha^2, 3\beta^2\} \leq 3/4$ for $d = 3$. □

REMARK 1.1.13. The result shows that there are only finitely many rings $\mathcal{O}_d$ which are norm-Euclidean. It does not say whether there are other rings which are Euclidean but not norm-Euclidean. In fact, M. Harper [**4**] showed that the ring of integers $\mathcal{O}_{14}$ is Euclidean but not norm-Euclidean.

REMARK 1.1.14. Harper and Murty proved the following result: let $K/\mathbb{Q}$ be a finite Galois extension of degree $n \geq 9$. Then the ring $\mathcal{O}_K$ is Euclidean if and only if $\mathcal{O}_K$ is a PID.

DEFINITION 1.1.15. Let $R$ be a commutative ring with 1. A non-zero element $p \in R$ is called *prime*, if it is not a unit and $p \mid ab$ implies $p \mid a$ or $p \mid b$. It is called *irreducible*, if it is not a unit and there is no factorization $p = ab$ with $a, b \in R \setminus E(R)$.

In an integral domain, every prime element is irreducible. The converse however holds only in unique factorization domains (UFD's).

DEFINITION 1.1.16. A UFD, or factorial ring $R$, is an integral domain $R$ in which every non-zero non-unit $x$ of $R$ can be written uniquely (up to permutation and units) as a product of irreducible elements of $R$.

We recall that every PID is a factorial ring. The converse is not true in general, since the polynomial ring $K[x_1, \ldots, x_n]$ is a factorial ring, but not a PID for $n \geq 2$.

EXAMPLE 1.1.17. *The ring $\mathbb{Z}[\sqrt{-5}]$ is not factorial, hence not a PID.*

Indeed, let $N\colon \mathcal{O}_{-5} \to \mathbb{Z}$ be the norm map, and $z = a + b\sqrt{-5}$. Then $N(z) = a^2 + 5b^2 > 0$ for all $z \neq 0$. Hence $z$ is a unit in $\mathcal{O}_{-5}$ iff $N(z) = 1$, i.e., iff $z = \pm 1$. Furthermore we have $N(z) \equiv 0, 1, 4(5)$ for all $z$ in $\mathcal{O}_{-5}$. Suppose that $u$ is one of the elements

$$3, 2 + \sqrt{-5}, 2 - \sqrt{-5}.$$

Then $N(u) = 9$. If $u = ab$ with $a, b \in \mathcal{O}_{-5}$ then

$$9 = N(u) = N(a)N(b).$$

The norm of $a, b$ cannot be 3, so that $N(a) = 1$ or $N(b) = 1$. This means, either $a$ or $b$ is a unit. It follows that the above three elements $u$ are irreducible. Furthermore, they do not divide each other in some way. Now the integer 9 has two different factorizations in $\mathcal{O}_{-5}$:

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$$

We also see that an irreducible element need not be prime in this ring. Indeed, $2 + \sqrt{-5}$ divides $9 = 3 \cdot 3$, but does not divide 3.

REMARK 1.1.18. The ring of integers in a number field is a so called *Dedekind ring*, see chapter 5. A Dedekind ring is a PID if and only if it is factorial. In particular, the rings $\mathcal{O}_d$ are factorial if and only if they are PIDs.

PROPOSITION 1.1.19. *Let $d$ be a squarefree integer. If $d < 0$ then the ring $\mathcal{O}_d$ is factorial (resp. a PID) if and only if*

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

*If $d > 0$ then Gauß conjectured that $\mathcal{O}_d$ is factorial (resp. a PID) for infinitely many $d$, starting with $d = 1, 2, 3, 5, 6, 7, 11, 13, 14$.*

DEFINITION 1.1.20. An ideal $P$ in a commutative ring $R$ is called *prime ideal*, if $P \neq R$ and for all $x, y \in R$ with $xy \in P$ it follows $x \in P$ or $y \in P$. An ideal $M$ in $R$ is called *maximal*, if $M \neq R$, and if for every ideal $I$ in $R$ the relation $M \subseteq I \subseteq R$ implies $I = M$ or $I = R$.

PROPOSITION 1.1.21. *Let $R$ be a commutative ring. Then $P$ is a prime ideal if and only if the quotient ring $R/P$ is an integral domain. Furthermore $M$ is a maximal ideal if and only if $R/M$ is a field.*

PROOF. Let $P$ be a prime ideal of $R$, and $(a + P)(b + P) = 0 + P$. Then $ab \in P$, and at least one of $a, b$ is in $P$ which means that either $a + P = 0 + P$, or $b + P = 0 + P$. Thus, $R/P$ is an integral domain. Conversely, let $R/I$ be an integral domain. If $ab \in I$ then $(a + I)(b + I) = I = 0 + I$, hence either $a + I = I$ and so $a \in I$, or $b + I = I$ and so $b \in I$. Thus, $I$ is a prime ideal of $R$.
If $M$ is a maximal ideal then $R/M$ has no proper ideals, hence it is a field. This works also in the converse direction. □

COROLLARY 1.1.22. *Every maximal ideal in $R$ is prime, and $P = (0)$ is prime if and only if $R$ is an integral domain.*

PROPOSITION 1.1.23. *Every non-trivial commutative ring $R$ has at least one maximal ideal.*

PROOF. The set $M$ of all ideals $I \neq R$ in $R$ is non-empty, since $(0) \in M$. It is partially ordered by inclusion. The claim follows from Zorn's lemma, which says that if every chain in $M$ has an upper bound, then $M$ has at least one maximal element.
Suppose that $T$ is such a chain. Define

$$I_0 := \bigcup_{I \in T} I.$$

This is an ideal in $R$ since for all $x, y \in I_0$ there is an $I \in T$ such that $x, y \in I$, hence $x - y \in I$ and $ax \in I$ for all $a \in I$. We have $1 \notin I_0$, since $1 \notin I$ for all $a \in T$. This means that $I_0 \in M$, and $I_0$ is an upper bound for the chain $T$. □

COROLLARY 1.1.24. *If $I$ is a proper ideal in $R$, there exists a maximal ideal $M$ of $R$ such that $I \subset M$.*

PROOF. Consider the ring $R/I$ instead of $R$ in the proposition, and recall that there is a $1-1$ correspondence between ideals $M$ of $R$ which contain $I$ and ideals $\overline{M}$ of $R/I$. □

EXAMPLE 1.1.25. *Let $R = \mathbb{Z}$. Then every prime ideal is of the form $(p) = p\mathbb{Z}$ for a prime $p$, or $0$.*

All ideals $(p)$ are maximal, since $\mathbb{Z}/(p)$ is a field. Another argument is, that all prime ideals $P \neq 0$ in a PID are also maximal ideals.

EXAMPLE 1.1.26. *Let $R = K[x_1, \ldots, x_n]$, where $K$ is a field. Then all ideals*

$$(x_1) \subset (x_1, x_2) \subset \ldots \subset (x_1, \ldots, x_n)$$

*are prime ideals. The last one is also a maximal ideal in $R$.*

Indeed, $R/(x_{m+1}, \ldots, x_n) \simeq K[x_1, \ldots x_m]$ is an integral domain for $m \geq 0$.
If $S$ is a commutative ring, and $a \in S$, then $\varphi\colon S[x] \to S$, $\varphi(x) = a$ is a surjective ring homomorphisms with kernel $(x - a)$. It follows

$$S[x]/(x - a) \simeq S.$$

By induction we have $S[x_1, \ldots, x_n]/(x_{m+1}, \ldots, x_n) \simeq S[x_1, \ldots, x_m]$.

DEFINITION 1.1.27. Two ideals $I, J$ in $R$ are called *coprime*, if $I + J = R$.

Equivalently, there exist $a \in I$ and $b \in J$ such that $a + b = 1$. For example, in $R = \mathbb{Z}$ the two ideals $n\mathbb{Z}$ and $m\mathbb{Z}$ are coprime if and only if $(n, m) = 1$, i.e., $nx + my = 1$ for some $n, m \in \mathbb{Z}$.

THEOREM 1.1.28. *Let $R$ be a commutative ring and $I_1, \ldots I_n$ pairwise coprime ideals in $R$.*

1. *Each ideal $I_i$ is coprime to the ideal $\prod_{j \neq i} I_j$.*
2. *We have $\prod_{j=1}^n I_j = \bigcap_{j=1}^n I_j$.*
3. *The ring homomorphism $\varphi\colon R \to \prod_{j=1}^n (R/I_j)$, given by $x \mapsto (x + I_1, \ldots, x + I_n)$ induces a ring isomorphism*

$$R/(I_1 \cdots I_n) \simeq R/I_1 \times \cdots \times R/I_n.$$

PROOF. (1): Because for fixed $i$ the ideal $I_i$ is coprime to all $I_j$ for $j \neq i$, we have $x_j \in I_i$ and $y_j \in I_j$ such that $1 = x_j + y_j$. It follows that

$$1 = \prod_{j \neq i}(x_j + y_j) = y_1 \dots y_{i-1} y_{i+1} \cdots y_n + a,$$

for some $a \in I_i$.
(2): We prove this with induction on $n \geq 2$. Clearly, $I_1 I_2 \subset I_1 \cap I_2$. Conversely, let $x \in I_1 \cap I_2$. There are $a \in I_1$ and $b \in I_2$ such that $a + b = 1$. Then $x = x \cdot 1 = xa + xb \in I_1 I_2 + I_1 I_2 = I_1 I_2$, and hence $I_1 \cap I_2 \subset I_1 I_2$. Now suppose $n > 2$. Assume that the claim holds for $I_1, \dots, I_{n-1}$, i.e., $\prod_{j=1}^{n-1} I_j = \bigcap_{j=1}^{n-1} I_j := J$. Then

$$\prod_{j=1}^{n} I_j = J I_n = J \cap I_n = \bigcap_{j=1}^{n} I_j,$$

since $J$ and $I_n$ are coprime by (1).
(3) Let $x_1, \dots, x_n \in R$. For every $j = 1, \dots, n$ there are ideals $I_j$ and $\prod_{i \neq j} I_i$ are coprime. Hence there are elements $u_j \in I_j$ and $v_j \in \prod_{i \neq j} I_i$ such that $u_j + v_j = 1$. Then $v_j \equiv \delta_{ij} \mod I_i$. Setting

$$x := \sum_{j=1}^{n} v_j x_j$$

we obtain $x \equiv x_j \mod I_j$ for all $j$, and the map $\varphi \colon R \to \prod(R/I_j)$ is surjective. The kernel of $\varphi$ is given by $\bigcap I_j = \prod I_j$. □

The last part is called the *Chinese Remainder Theorem*: for pairwise coprime ideals $I_1, \dots, I_n$ and elements $x_1, \dots, x_n$ in $R$ we can solve the system of congruences $X \equiv x_j \mod I_j$. For a solution $x$ the residue class $x + \bigcap_j I_j$ is the set of all solutions. To find a solution, one has to construct elements $v_j \in \prod_{i \neq j} I_i$ and $u_j \in I_j$ such that $u_j + v_j = 1$.
For $R = \mathbb{Z}$ and $n = p_1^{e_1} \cdots p_r^{e_r}$ the above isomorphism gives

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$$

as rings. If the ideals are not coprime, the result need not be true. Consider for example $I = J = p\mathbb{Z}$. Then $\mathbb{Z}/IJ \simeq \mathbb{Z}/p^2\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/I \times \mathbb{Z}/J \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

## 1.2. Localization of Rings

A subset $S$ of $R$ is said to be *multiplicatively closed*, if it satisfies the following:

(1) $1 \in S$.
(2) If $a \in S$ and $b \in S$ then $ab \in S$.

If $R$ is an integral domain, then $R^\times = R \setminus 0$ is multiplicatively closed. More generally, the set of all nonzerodivisors in $R$ is a multiplicatively closed. Also, the set of units $E(R)$ in a ring is a multiplicatively closed subset of $R$. Here is another important example:

EXAMPLE 1.2.1. *If $P$ is a prime ideal of $R$, then $R \setminus P$ is multiplicatively closed.*

In fact, for any ideal $I$ in $R$ the set $R \setminus I$ is multiplicatively closed if and only if $I$ is a prime ideal.

DEFINITION 1.2.2. Let $I$ be an ideal in $R$. Then the *radical* of $I$ is defined by

$$\sqrt{I} := \{a \in R \mid a^n \in I \text{ for some } n \geq 1\}.$$

One says that $I$ is a *radical ideal* if $\sqrt{I} = I$.

LEMMA 1.2.3. *The radical $\sqrt{I}$ of an ideal $I$ of $R$ is again an ideal of $R$.*

PROOF. Let $a, b \in \sqrt{I}$. Then, for some positive integers $m, n$ we have $a^n, b^m \in I$. We will first show that $a + b \in \sqrt{I}$. By the binomial theorem we have

$$(a+b)^{n+m-1} = \sum_{i=0}^{n+m-1} \binom{n+m-1}{i} a^i b^{n+m-1-i}.$$

For each $i$ we have either $i \geq n$ or $n + m - 1 - i \geq m$. This says that in each expression $a^i b^{n+m-1-i}$, either the exponent of $a$ will be large enough to make this power of $a$ be in $I$, or the exponent of $b$ will be large enough to make this power of $b$ be in $I$. Since the product of an element in $I$ with an element in $R$ is in $I$, this product expression will be in $I$, and then $(a+b)^{n+m-1}$ is in $I$, therefore $a + b$ is in $\sqrt{I}$.
Now let $a \in \sqrt{I}$ with $a^n \in I$, and $r \in R$ an arbitrary element in $R$. Then $(ra)^n = r^n a^n \in I$, so that $ra \in \sqrt{I}$. □

EXAMPLE 1.2.4. *Every prime ideal $P$ of $R$ is a radical ideal.*

For $R = \mathbb{Z}$ let $I = p\mathbb{Z}$. Then $\sqrt{I} = \{k \in \mathbb{Z} \mid k^n \in p\mathbb{Z}\} = p\mathbb{Z} = I$. However, for example $\sqrt{4\mathbb{Z}} = 2\mathbb{Z}$.

DEFINITION 1.2.5. Denote the set of all prime ideals in $R$ by $\mathrm{Spec}(R)$, and the set of all maximal ideals in $R$ by $\mathrm{Max}(R)$.

If $R = 0$ then $\mathrm{Spec}(R) = \mathrm{Max}(R) = \emptyset$. If $R$ is a field then $\mathrm{Spec}(R) = \mathrm{Max}(R) = \{0\}$. For $R = \mathbb{Z}$ we have $\mathrm{Spec}(R) = \{0\} \cup \{(p)\}$, for $p \in \mathbb{P}$, and $\mathrm{Max}(R) = \{(p)\}$.

DEFINITION 1.2.6. For $I = 0$ the radical $\sqrt{0}$ is the ideal of all nilpotent elements in $R$, the so called *nilradical* of $R$.

The nilradical of $R$ is the intersection of all prime ideals of $R$. To show this we need a lemma:

LEMMA 1.2.7. *If $I \lhd R$ and $S$ is a multiplicatively closed subset of $R$ such that $I \cap S = \emptyset$, then there exists a prime ideal $P$ of $R$ such that $I \subseteq P$ and $P \cap S = \emptyset$. Moreover $P$ is maximal among the family of ideals $J$ of $R$ satisfying $I \subseteq J$ and $J \cap S = \emptyset$.*

PROOF. Consider the family $\{J \mid J \lhd R, I \subseteq J, J \cap S = \emptyset\}$ and Zornify, i.e., apply Zorn's lemma as before in proposition 1.1.23. □

Note that we obtain corollary 1.1.24 if we take $S = \{1\}$ and $I \neq (1)$.

PROPOSITION 1.2.8. *Let $R$ be a ring and $I$ be an ideal of $R$. Then*

$$\sqrt{I} = \bigcap_{\substack{P \in \mathrm{Spec}(R) \\ I \subseteq P}} P.$$

*In particular we have $\sqrt{0} = \bigcap_{P \in \mathrm{Spec}(R)} P$.*

PROOF. Let $P$ be a prime ideal containg $I$ and $a \in \sqrt{I}$. Then $a^n \in I \subseteq P$, so that $a \in P$ since $P$ is prime. It follows that $\sqrt{I} \subseteq P$. On the other hand, suppose that $a \in P$ for every $P \in \mathrm{Spec}(R)$ with $I \subseteq P$. Then we want to show that $a \in \sqrt{I}$. Assume that $a^n \notin I$ for all $n \in \mathbb{N}$. Then apply the above lemma to the set $S := \{a^n \mid n \in \mathbb{N}\}$ to obatin a contradiction. □

DEFINITION 1.2.9. Define the *Jacobson radical* of $R$ by

$$\mathcal{J}(R) := \bigcap_{M \in \mathrm{Max}(R)} M.$$

The Jacobson radical can be characterized as follows.

PROPOSITION 1.2.10. *One has $\mathcal{J}(R) = \{a \in R \mid 1 - ab \in E(R)$ for every $b \in R\}$.*

PROOF. Let $a \in \mathcal{J}(R)$. Suppose that $1 - ab$ is a non-unit. Then, by corollary 1.1.24 there is a maximal ideal $M$ of $R$ containing $1 - ab$. But $a \in \mathcal{J}(R) \subseteq M$, hence $ab \in M$ and therefore $1 \in M$, which is absurd. Hence $1 - ab$ is a unit in $R$.
Conversely, suppose that $a \notin M$ for some maximal ideal in $R$. Then $M$ and $a$ generate the unit ideal $(1) = R$, so that we have $u + ab = 1$ for some $u \in M$ and some $b \in R$. Hence $1 - ab \in M$, which is therefore not a unit. □

Now we come to the process of *localization* which generalizes the well-known construction of a field of fractions of an integral domain (which in turn is a generalization of the formal construction of the rational numbers $\mathbb{Q}$ from the integers $\mathbb{Z}$).
Let $S$ be a multiplicatively closed subset of $R$. Define an equivalence relation on the set of all ordered pairs of $R \times S$ as follows: given any $(a, s), (b, t) \in R \times S$,

$$(a, s) \sim (b, t) \iff u(at - bs) = 0 \text{ for some } u \in S.$$

We show that $\sim$ defines an equivalence relation on $R \times S$. Of course, $(a, s) \sim (a, s)$. Furthermore, $(a, s) \sim (b, t)$ implies $(b, t) \sim (a, s)$. Finally, to show transitivity, assume that $(a, s) \sim (b, t)$ and $(b, t) \sim (c, r)$. This means, there exist $v, w \in S$ such that

$$(at - bs)v = 0, \quad (br - ct)w = 0.$$

It follows that

$$(at - bs)rvw = 0, \quad (br - ct)svw = 0,$$

and hence $atrvw = bsrvw = ctsvw$, so that

$$(ar - cs)tvw = 0.$$

Since $S$ is multiplicatively closed, $tvw \in S$, hence $(a, s) \sim (c, r)$.
Denote the equivalence class of $(a, s)$ simply by $\frac{a}{s}$. Define

$$S^{-1}R := \{a/s \mid (a, s) \in R \times S\}.$$

Define an addition and a multiplication on $S^{-1}R$ as follows:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st},$$
$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

One can verify that these definitions are independent of the choice of representatives $(a, s)$ and $(b, t)$, and that $S^{-1}R$ becomes a commutative ring with 1.

Definition 1.2.11. For $S \subseteq R$ multiplicativiely closed, the ring $S^{-1}R$ is called the *localization of $R$*, or the *ring of fractions of $R$*.

If $0 \in S$ then $(a, s) \sim (0, 1)$ for all $(a, s) \in R \times S$, so that $S^{-1}R = \{\frac{0}{1}\}$ is the zero ring. Conversely, if $S^{-1}R = 0$, then $0 \in S$. Thus it makes sense to assume that $0 \notin S$.
Note that for all $s \in S$, the elements $\frac{s}{1}$ in $S^{-1}R$ are units: $\frac{1}{s} \cdot \frac{s}{1} = \frac{1}{1} = 1$.

Example 1.2.12. *If $R$ is an integral domain and $S = R \setminus 0$, then $S^{-1}R$ is just the quotient field of $R$. In this case the equivalence relation takes the simpler form*

$$(a, s) \sim (b, t) \iff at - bs = 0.$$

If $R$ is not an integral domain then this does not work, because the verification that $\sim$ is transitive involves cancelling, i.e., it uses that $R$ has no zero-divisor except 0: suppose that $(a, s) \sim (b, t)$ and $(b, t) \sim (c, r)$. Then $at = bs$ and $br = ct$, so that $cat = cbs$ and $abr = act = cat$. This implies $b(ar) = b(cs)$, or $b(ar - cs) = 0$. Since $b \neq 0$ we obtain $ar = cs$, hence $(a, s) \sim (c, r)$.

Example 1.2.13. *Let $S = R \setminus P$, where $P$ is a prime ideal of $R$. Then we obtain the localization of $R$ at $P$:*

$$R_P := S^{-1}R.$$

Definition 1.2.14. A commutative ring $R$ is called a *local ring*, if it has exactly one maximal ideal $M$. Then $R/M$ is called the *residue field* of $R$.

Note that any $x \notin M$ here is a unit, since $(x) \not\subseteq M$, so that $(x) = R$.
We claim that $R_P$ is a local ring, with the maximal ideal given by

$$PR_P := \{a/s \mid a \in P, s \in S\}.$$

Indeed, any element $\frac{b}{s}$ of $R_P$ that is not in $PR_P$ is a unit in $R_P$, because $b \notin P$, so that $b \in S$. It follows that if $I$ is an ideal in $R_P$, and $I$ is not contained in $PR_P$, then there is a unit in $I$, so that $I = R$. Hence $PR_P$ is the only maximal ideal in $R_P$.

Example 1.2.15. *Let $R = \mathbb{Z}$, $P = (p)$ and $S = \mathbb{Z} \setminus p\mathbb{Z}$. Then*

$$R_P = \mathbb{Z}_{(p)} = \{m/n \in \mathbb{Q} \mid (n, p) = 1\},$$

*and the residue field of $\mathbb{Z}_{(p)}$ is given by $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{F}_p$.*

In general, we have the natural ring homomorphism $\varphi\colon R \to S^{-1}R$ defined by $\varphi(a) = a/1$ for $a \in R$. This map is not injective in general. In fact, $a \in \ker(\varphi)$ if and only if $a/1 = 0/1$, i.e., $sa = 0$ for some $s \in S$:

$$\ker(\varphi) = \bigcup_{s\in S}(0 : s) = \{a \in R \mid sa = 0 \text{ for some } s \in S\}.$$

where $(0 : I) := \{a \in R \mid aI = 0\}$ denotes the *annihilator* of the ideal $I$ in $R$. If $I = (s)$ we write $(0 : s)$ instead of $(0 : (s))$. More generally, we have the following definition.

Definition 1.2.16. Let $I, J$ be ideals in $R$. Then then

$$(I : J) = \{a \in R \mid aJ \subseteq I\}$$

is again an ideal in $R$, called the *ideal quotient*.

We have $I \subseteq (I : J)$.

Example 1.2.17. *Let $R = \mathbb{Z}$ and $I = a\mathbb{Z}$, $J = b\mathbb{Z}$. Then*

$$(I : J) = c\mathbb{Z}, \quad c := \frac{a}{(a, b)}.$$

Lemma 1.2.18. *Let $I, J, K$ be ideals of the commutative ring $R$, and let $(I_\alpha)_{\alpha\in\mathcal{A}}$, be a family of ideals of $R$. Then*

(1) $((I : J) : K) = (I : JK) = ((I : K) : J)$,

(2) $(\cap_{\alpha\in\mathcal{A}} I_\alpha : J) = \cap_{\alpha\in\mathcal{A}}(I_\alpha : J)$,

(3) $(K : \sum_{\alpha\in\mathcal{A}} I_\alpha) = \cap_{\alpha\in\mathcal{A}}(K : I_\alpha)$.

Comming back to $\ker(\varphi)$ above, we see that $\varphi$ is injective if and only if $S$ consists of nonzerodivisors; in this case $R$ may be regarded as a subring of $S^{-1}R$. This applies for $R$ being an integral domain, and $S^{-1}R$ being the quotient field of $R$.

The ring of fractions, $S^{-1}R$ has the following universal property:

Proposition 1.2.19. *Let $\varphi\colon R \to S^{-1}R$ be the above ring homomorphism, and $g\colon R \to R'$ be a ring homomorphism such that $g(s)$ is a unit in $R'$ for all $s \in S$. Then there exists a unique ring homomorphism $h\colon S^{-1}R \to R'$ such that $g = h \circ \varphi$.*

Proof. Suppose there is such a homomorphism. Then $h(a/1) = h(\varphi(a)) = g(a)$ for all $a \in R$. Hence, for $s \in S$ we have

$$h(1/s) = h((s/1)^{-1}) = h(s/1)^{-1} = g(s)^{-1},$$

and therefore $h(a/s) = h(a/1)h(1/s) = g(a)g(s)^{-1}$, so that $h$ is uniquely determined by $g$.
To show the existence just put $h(a/s) := g(a)g(s)^{-1}$. This is well-defined: suppose that $a/s = a'/s'$, i.e., $(as' - a's)t = 0$ for some $t \in S$. It follows

$$(g(a)g(s') - g(a')g(s)) \cdot g(t) = 0;$$

but $t \in S$ says that $g(t)$ is a unit in $R'$, so that $g(a)g(s)^{-1} = g(a')g(s')^{-1}$.
Finally, $h$ is a ring homomorphism satisfying $g = h \circ \varphi$. □

The ring $S^{-1}R$ and the ring homomorphism $\varphi\colon R \to S^{-1}R$, $\varphi(s) = \frac{s}{1}$ have the following properties:

(1) For $s \in S$ the images $\varphi(s)$ are units in $S^{-1}R$.
(2) If $\varphi(a) = 0$ then $as = 0$ for some $s \in S$.
(3) Every element of $S^{-1}R$ is of the form $\varphi(a)\varphi(s)^{-1}$ for some $a \in R$ and some $s \in S$.

Conversely, these three conditions determine the ring up to isomorphism, see for example [**1**].
We want to consider ideals in $S^{-1}R$.

DEFINITION 1.2.20. For an ideal $I$ in $R$ the ideal of $S^{-1}R$ generated by $\varphi(I)$ is called the *extension* of $I$, and is denoted by $S^{-1}I$.

We have $S^{-1}I = \{a/s \mid a \in I, s \in S\}$.

DEFINITION 1.2.21. For an ideal $J$ in $S^{-1}R$ the ideal $\varphi^{-1}(J)$ of $R$ is called the *contraction* of $J$ to $R$, and is denoted by $J^c$.

Some properties of extension and contraction of ideals are desribed in the following result.

PROPOSITION 1.2.22. *Let $R$ be a ring and let $S$ be a multiplicatively closed subset of $R$. We have the following:*

(1) *Let $J$ be an ideal in $S^{-1}R$. If $I = J^c$, then $J = S^{-1}I$. In particular, every ideal $J$ in $S^{-1}R$ is the extension of some ideal of $R$.*

(2) *Let $I$ be an ideal in $R$. Then $(S^{-1}I)^c = \bigcup_{s\in S}(I : s)$. In particular, $S^{-1}I = S^{-1}R$ if and only if $I \cap S \neq \emptyset$.*

(3) *An ideal $I \subseteq R$ is a contraction of an ideal of $S^{-1}R$ if and only if every element of $S$ is a nonzerodivisor in $R/I$. In this case we have $I = (S^{-1}I)^c$.*

(4) *The prime ideals of $S^{-1}R$ are in one-to-one correspondence with the prime ideals $P$ of $R$ which do not meet $S$, i.e. with $P \cap S = \emptyset$.*

PROOF. (1): Since $I = \varphi^{-1}(J)$ we have $\varphi(I) \subseteq J$ and hence $S^{-1}I \subseteq J$. Conversely, if $a \in R$ and $s \in S$ such that $a/s \in J$, then $\frac{a}{1} = \frac{s}{1} \cdot \frac{a}{s} \in J$, hence $a \in J^c = I$. This shows that $a/s \in S^{-1}I$. Thus, $J \subseteq S^{-1}I$.

(2): Given any $x \in (S^{-1}I)^c$, we have $x/1 = a/t$ for some $a \in I$ and $t \in S$. Hence, by definition, $u(tx - a) = 0$ for some $u \in S$. Then the element $s := ut$ is in $S$ and $sx = utx = ua \in I$. It follows that $x \in (I : s)$. On the other hand, if $x \in (I : s)$ for some $s \in S$, then $sx \in I$, so that $\frac{x}{1} = \frac{1}{s} \cdot \frac{sx}{1} \in S^{-1}I$. This means $x \in (S^{-1}I)^c$. Altogether this shows that $(S^{-1}I)^c$ is the union of $(I : s)$ as $s$ varies over $S$. In particular, $S^{-1}I = S^{-1}R$ if and only if $1 \in (I : s) = \{x \in R \mid sx \in I\}$ some some $s \in S$, that is, $I \cap S \neq \emptyset$.

(3): We need to show that $s \in S$ is a nonzerodivisor in $R/I$ if and only if $(I : s) = I$. Then the claim follows from (2). We always have $I \subseteq (I : s)$. However, $(I : s) \subseteq I$ for some $s \in S$ means that all $x \in R$ with $sx \in I$ satisfy $x \in I$, i.e., all $x \in R$ with $\overline{sx} = \overline{s} \cdot \overline{x} = \overline{0}$ in $R/I$ satisfy $\overline{x} = \overline{0}$.

Thus $s$ is a nonzerodivisor in $R/I$.

(4): If $Q$ is a prime ideal of $S^{-1}R$, then $Q^c = \varphi^{-1}(Q)$ is a prime ideal of $R$, being the inverse image of a prime ideal under a ring homomorphism (see lemma 1.2.25). Moreover, $Q = S^{-1}P$ by (1), and $S \cap P = \emptyset$, since otherwise, using (2), $Q = S^{-1}P = S^{-1}R$, which is not possible since $Q$ is prime.
Conversely, suppose that $P$ is a prime ideal of $R$ such that $P \cap S = \emptyset$. We claim that $Q := S^{-1}P$ is a prime ideal of $S^{-1}R$. We have $Q \neq S^{-1}R$ because of (2). Further, if $x, y \in R$ and $s, t \in S$ are such that $\frac{x}{s} \cdot \frac{y}{t} \in S^{-1}P$, then $\frac{xy}{1} \in Q$, and hence there is a $p \in P$, and an $s \in S$ such that $\frac{xy}{1} = \frac{p}{s}$. Then there is a $t \in S$ such that $(xys - p)t = 0$. Because of $s \notin P$ we have $xy \in P$. It follows that $x \in P$ or $y \in P$, which implies in turn that $x/s \in Q$ or $y/t \in Q$. Thus $Q$ is a prime ideal as claimed. In view of (1) and (3) it follows that the processes of contraction and extension set up the desired one-to-one correspondence. □

COROLLARY 1.2.23. *If $P$ is a prime ideal of $R$, the prime ideals of the local ring $R_P$ are in one-to-one correspondence with the prime ideals of $R$ contained in $P$.*

PROOF. Take $S = R \setminus P$ in (4). □

REMARK 1.2.24. The result again shows that the localization $R_P$ is a local ring, i.e., has only one maximal ideal, namely $PR_P$. Indeed, prime ideals of $R_P$ correspond to prime ideals of $R$ which are contained in $P$. Hence the only maximal ideal of $R_P$ corresponds to $P$. All other maximal ideals of $R$ disappear in $R_P$.

We have already used the following lemma, which we want to prove now.

LEMMA 1.2.25. *If $f\colon R \to R'$ is a ring homomorphism, and $P$ a prime ideal in $R'$, then $f^{-1}(P)$ is a prime ideal in $R$.*

PROOF. The ring $R'/P$ is an integral domain since $P$ is prime. We have a ring homomorphism $R \to R' \to R'/P$ with kernel $f^{-1}(P)$, hence an embedding

$$R/f^{-1}(P) \hookrightarrow R'/P.$$

Since $R'/P$ is an integral domain, so is the subring $R/f^{-1}(P)$. Hence $f^{-1}(P)$ is a prime ideal. □

REMARK 1.2.26. In general we do not have $I = (S^{-1}I)^c$, not even if $I \cap S = \emptyset$, see (3). For example, take $R = \mathbb{Z}$, $S = \{2^n \mid n \geq 0\}$ and $I = (6)$. Then

$$S^{-1}I = \left\{ \frac{3n}{2^k} \mid n \in \mathbb{Z}, k \geq 1 \right\},$$
$$(S^{-1}I)^c = (3).$$

Indeed, $2 \in S$ is not a nonzerodivisor in $\mathbb{Z}/6\mathbb{Z}$.

COROLLARY 1.2.27. *Let $R$ be a commutative ring and $S$ be a multiplicatively closed subset of $R$. If $R$ is a PID, so is $S^{-1}R$.*

PROOF. Every ideal $J$ of $S^{-1}R$ is of the form $S^{-1}I = \{a/s \mid a \in I, s \in S\}$, where $I = \varphi^{-1}(J)$ is an ideal of $R$. Since $I$ is a principal ideal, so is $J$. □

## 1.3. Noetherian rings

Let $R$ be a commutative ring. An ideal $I \subseteq R$ is called *finitely generated*, if there exist generators $a_1, \ldots, a_n \in R$ such that

$$I = \left\{ \sum_{i=1}^{n} r_i a_i \mid r_i \in R \right\}.$$

We denote this by $I = (a_1, \ldots, a_n)$. For $n = 1$ this coincides with the notion of a principal ideal $I = (a)$.
Now we will define a class of commutative rings named after Emmy Noether (1921).

DEFINITION 1.3.1. The ring $R$ is called *Noetherian*, if every ideal of $R$ is finitely generated.

Obvioulsly every PID is Noetherian, so that we already have a lot of examples. An easy observation is the following:

PROPOSITION 1.3.2. *Let $R$ be a Noetherian ring and $I \subseteq R$ be an ideal. Then $R/I$ is a Noetherian ring.*

PROOF. Denote by $\pi\colon R \to R/I$ the canonical epimorphism and let $J \subseteq R/I$ be an ideal. Then $\pi^{-1}(J)$ is an ideal of $R$. By assumption there exist $a_1, \ldots, a_n \in R$ such that $\pi^{-1}(J) = (a_1, \ldots, a_n)$. But then

$$J = \pi(\pi^{-1}(J)) = (\pi(a_1), \ldots, \pi(a_n))$$

is finitely generated, and $R/I$ is Noetherian. □

The ring $\mathbb{Z}[x]$ not a PID, but it is Noetherian since $\mathbb{Z}$ is (see theorem 1.3.6). It follows, for example, that the ring $\mathbb{Z}[\sqrt{-5}] \simeq \mathbb{Z}[x]/(x^2+5)$ is Noetherian. Note that it is not factorial. Hence a Noetherian ring need not be factorial. Conversely, a factorial ring need not be Noetherian: one can show that polynomial ring $R[X]$ for an infinite set $X$ of variables is factorial and not Noetherian.

PROPOSITION 1.3.3. *The following statements for $R$ are equivalent:*

1. *$R$ is a Noetherian ring.*
2. *In $R$ holds the ascending chain condition: if $I_1, I_2, \ldots$ are ideals of $R$ with $I_1 \subseteq I_2 \subseteq \cdots$, then there exists an $m \geq 1$ such that $I_n = I_m$ for all $n \geq m$.*
3. *In $R$ holds the maximality condition: every nonempty set of ideals of $R$ has a maximal element.*

PROOF. (1) ⇒ (2): Given such a chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$, the union

$$I := \bigcup_{n \geq 1} I_n$$

is an ideal of $R$. By assumption there are $a_1, \ldots, a_r \in I$, such that $I = (a_1, \ldots, a_r)$. Every $a_i$ lies in some ideal $I_{k_i}$, so that all $a_i$ are contained in $I_m$ with $m = \max\{k_1, \ldots, k_r\}$. For $k \geq m$ we have

$$I = (a_1, \ldots, a_r) \subseteq I_m \subseteq I_k \subseteq I,$$

so that $I_k = I_m$ for all $k \geq m$.
(2) ⇒ (3): Let $\mathcal{F}$ be a nonempty set of ideals of $R$ that does not have a maximal element. Since $\mathcal{F}$ is nonempty, there is some ideal $I_1 \in \mathcal{F}$. But $I_1$ is not a maximal element, and so there is $I_2 \in \mathcal{F}$ such that $I_1 \subset I_2$. Further, $I_2$ is not a maximal element, and so there is $I_3 \in \mathcal{F}$ such

that $I_2 \subset I_3$. Continuing this way, or by induction, we obtain an infinite strictly ascending chain of ideals in $\mathcal{F}$. This contradicts (2).

(3) $\Rightarrow$ (1): Let $I$ be an ideal of $R$ and consider the set $\mathcal{F}$ of all finitely generated ideals in $R$ which are contained in $I$. Let $M$ be a maximal element in $\mathcal{F}$. We claim that $I = M$, so that $I$ is finitely generated. Assume that there is some $x \in I \setminus M$. Then $M + (x) \in \mathcal{F}$, which contradicts the maximality of $M$. Thus $I = M \in \mathcal{F}$. □

REMARK 1.3.4. The class of Noetherian rings is closed w.r.t. three fundamental processes: if $R$ is Noetherian, then $R/I$ is again Noetherian for all ideals $I$ if $R$; furthermore $S^{-1}R$ is again Noetherian for every multiplicatively closed subset $S$ of $R$; and finally all polynomial rings $R[x_1, \ldots, x_n]$ are again Noetherian.

PROPOSITION 1.3.5. *Let $S$ be a multiplicatively closed set of $R$. If $R$ is Noetherian, so is $S^{-1}R$.*

PROOF. Every ideal $J$ of $S^{-1}R$ is of the form $S^{-1}I = \{a/s \mid a \in I, s \in S\}$, where $I = \varphi^{-1}(J)$ is an ideal of $R$. Since $I$ is finitely generated, so is $J$. □

THEOREM 1.3.6 (Hilbertscher Basissatz). *If $R$ is Noetherian, so is the polynomial ring $R[x]$.*

PROOF. Suppose that $R[x]$ is not Noetherian, and let $I \subseteq R[x]$ be an ideal, which is not finitely generated. Let $f_1 \in I$ be a polynomial of minimal degree. Choose $f_2 \in I \setminus (f_1)$ with minimal degree, and so on. In other words, if we have chosen $f_1, \ldots f_k$ in this way, choose $f_{k+1}$ of minimal degree in $I \setminus (f_1, \ldots, f_k)$. Let

$$n_k = \deg(f_k),$$
$$a_k = lc(f_k)$$

be the degree and the leading coefficient of $f_k$. Then we have $n_1 \leq n_2 \leq n_3 \leq \cdots$ and

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots$$

is an ascending chain of ideals in $R$. Since $R$ is Noetherian, there is a $k \geq 1$ such that

$$(a_1, \ldots, a_k) = (a_1, \ldots, a_{k+1}).$$

Then there is an equation

$$a_{k+1} = \sum_{i=1}^{k} b_i a_i$$

with $b_i \in R$. Consider the polynomial

$$g := f_{k+1} - \sum_{i=1}^{k} b_i x^{n_{k+1} - n_i} f_i.$$

Then we have $g \in I \setminus (f_1, \ldots, f_k)$ with $\deg(g) < \deg(f_{k+1})$. This is a contradiction to the choice of $f_{k+1}$. □

COROLLARY 1.3.7. *If $R$ is Noetherian, so is $R[x_1, \ldots, x_n]$.*

PROOF. We have $R[x_1, \ldots, x_n] \simeq R[x_1, \ldots, x_{n-1}][x_n]$, so that we can argue inductively. □

THEOREM 1.3.8 (I. S. Cohen). *Let $R$ be a commutative ring where all prime ideals are finitely generated. Then $R$ is Noetherian.*

PROOF. Suppose that $R$ is not Noetherian and consider the set $\mathcal{F}$ of ideals of $R$ which are not finitely generated. Then $\mathcal{F} \neq \emptyset$. We order $\mathcal{F}$ partially by inclusion. Let $\Phi$ be a non-empty totally ordered subset of $\mathcal{F}$. Consider the ideal

$$J := \bigcup_{I \in \Phi} I.$$

We claim that $J$ is not finitely generated. Assume that it is, say $J = (a_1, \ldots, a_t)$. Then for each $i = 1, \ldots, t$, there exists $I_i \in \Phi$ such that $a_i \in I_i$. Since $\Phi$ is totally ordered, there exists $h \in \mathbb{N}$ with $1 \leq h \leq t$ such that $I_i \subseteq I_h$ for all $i = 1, \ldots, t$. Then we have

$$J = Ra_1 + \cdots + Ra_t \subseteq I_h \subseteq J,$$

so that $I_h$ is finitely generated, a contradiction. Hence $J$ is not finitely generated, so that $J \in \mathcal{F}$. Then $J$ is an upper bound for $\Phi$ in $\mathcal{F}$. We apply Zorn's lemma to see that $\mathcal{F}$ has a maximal element. We will show that each maximal element $P$ of $\mathcal{F}$ is prime. This finishes the proof, since then we have found a prime ideal in $R$ which is not finitely generated. First of all, $P \neq R$, since $R = (1)$ is finitely generated, but $P$ is not. Let $a, b \in R \setminus P$ and suppose that $ab \in P$. We will obtain a contradiction, so that $P$ must be prime. Since $P \subseteq P + Ra$, it follows from the maximality of $P$ in $\mathcal{F}$ that $P + Ra$ is finitely generated, say,

$$P + Ra = (p_1 + r_1 a, \ldots, p_n + r_n a),$$

where $p_1, \ldots, p_n \in P$ and $r_1, \ldots, r_n \in R$. Let $K = (P : a)$. Since $K \supseteq P + Rb \supseteq P$, it again follows from maximality of $P$ that $K$ is finitely generated; therefore the ideal $aK$ is also finitely generated. We claim that

$$P = Rp_1 + \cdots + Rp_n + aK.$$

Clearly $P \supseteq Rp_1 + \cdots + Rp_n + aK$. Let $p \in P \subseteq P + aR$. Then there exist $c_1, \ldots, c_n \in R$ such that

$$p = c_1(p_1 + r_1 a) + \cdots + c_n(p_n + r_n a).$$

Then

$$\left( \sum_{i=1}^{n} c_i r_i \right) a = p - \sum_{i=1}^{n} c_i p_i \in P,$$

so that $\sum_{i=1}^{n} c_i r_i \in (P : a) = K$. Hence

$$p = \sum_{i=1}^{n} c_i p_i + \left( \sum_{i=1}^{n} c_i r_i \right) a \in \sum_{i=1}^{n} Rp_i + aK.$$

Thus also $P \subseteq Rp_1 + \cdots + Rp_n + aK$. Together we obtain that $P$ is finitely generated, a contradiction. Hence $P$ is prime. □

REMARK 1.3.9. Cohen's theorem can be used to show that if $R$ is Noetherian, so is the formal power series ring $R[[x]]$, see [**7**], Theorem 8.13.

Next we come to factorizations in Noetherian rings. Not all such rings are factorial. But there is a generalized form of a unique factorization of ideals (not of elements). For example, for $R = \mathbb{Z}$ we have a factorization $n = p_1^{e_1} \cdots p_r^{e_r}$ into prime powers. As ideals we have

$$(n) = (p_1^{e_1}) \cap \cdots \cap (p_r^{e_r}).$$

A prime ideal in $R$ is in some sense a generalization of a prime number in $\mathbb{Z}$. The corresponding generalization of a prime power is a primary ideal:

DEFINITION 1.3.10. An ideal $Q$ in a commutative ring $R$ is a *primary ideal* if $Q \neq R$, and for all elements $x, y \in R$, we have that if $xy \in Q$, then either $x \in Q$ or $y^n \in Q$ for some $n \in \mathbb{N}$.

The condition can be rephrased as follows: $x, y \in R$ and $xy \in Q$ imply $x \in Q$ or $y \in \sqrt{Q}$. Obviously every prime ideal is a primary ideal. The converse need not be true.

EXAMPLE 1.3.11. *Let $R = \mathbb{Z}$ and $Q = 25\mathbb{Z}$. Then $Q$ is primary.*

Indeed, let $xy \in Q$ and $x \notin Q$, i.e. $25 \mid xy$, $25 \nmid x$. Then $5 \mid y$ so that $y^2 \in Q$.

LEMMA 1.3.12. *Let $Q$ be an ideal in $R$. Then $Q$ is primary if and only if $R/Q \neq 0$, and every zero-divisor in $R/Q$ is nilpotent.*

PROOF. Suppose that $Q$ is primary. Since $Q \neq R$ we deduce that $R/Q \neq 0$. Let $b \in R$ be such that the element $b + Q$ in $R/Q$ is a zero-divisor, so that there exists $a \in R$ such that $a + Q$ is not the zero class in $R/Q$ but $(a + Q)(b + Q) = \overline{0}$. These conditions mean that $a \notin Q$ but $ab \in Q$, so that $b^n \in Q$ for some $n \geq 1$, since $Q$ is primary. Hence $(b + Q)^n = b^n + Q = \overline{0}$. The converse can be proved similarly. □

LEMMA 1.3.13. *Let $R$ be an integral domain. If $p \in R$ is a prime element, then $(p^n) = (p)^n$ is a primary ideal for every $n \geq 1$.*

PROOF. Let $a, b \in R$ such that $ab \in (p^n)$ and $a \notin (p^n)$. If $b \in (p)$, then $b^n \in (p^n)$. We will show that the other case $b \notin (p)$ is not possible, so that we are done. Assume that $b \notin (p)$. Then $a \in (p)$ and there exists $1 \leq d < n$ such that $a \in (p^d) \setminus (p^{d+1})$. This means, we have $a = p^d u$ with some $u \in R \setminus (p)$. It follows that $ub \notin (p)$, because $(p)$ is prime. Then $ab = p^d ub \notin (p^{d+1})$, because otherwise $p^d ub = p^{d+1} r$ and $ub = pr \in (p)$ by cancelling. This contradicts $ab \in (p^n) \subset (p^{d+1})$. □

LEMMA 1.3.14. *If $Q$ is a primary ideal, then $P = \sqrt{Q}$ is a prime ideal, in fact, the smallest prime ideal containing $Q$.*

In this case $P$ is called the prime ideal associated to $Q$. Conversely $Q$ is also said to be $P$-primary, or the primary ideal associated to $P$.

PROOF. By proposition 1.2.8, the radical of $Q$ is the intersection of all prime ideals which contain $Q$. Hence it is enough to prove that $P = \sqrt{Q}$ is a prime ideal. Let $a, b \in R$ such that $ab \in \sqrt{Q}$. Then $a^n b^n \in Q$ for some $n \geq 1$. Assume that $a \notin \sqrt{Q}$. Then $a^n \notin Q$, hence $(b^n)^m \in Q$ for some $m \geq 1$. It follows that $b \in \sqrt{Q}$. □

EXAMPLE 1.3.15. *In $R = \mathbb{Z}$ the primary ideals are $(0)$ and $(p^n)$, where $p \in \mathbb{P}$ and $n \geq 1$.*

Indeed, these ideals are primary, and the only ideals in $\mathbb{Z}$ with prime radical. The claim follows from lemma 1.3.14.

On the other hand, if $Q$ is an ideal of $R$ such that $\sqrt{Q}$ is prime, then $Q$ need not be primary.

EXAMPLE 1.3.16. *Let $R = K[x, y]$ and $Q = (x^2, xy)$. Then $\sqrt{Q}$ is a prime ideal, but $Q$ is not primary.*

We have $xy \in Q$, but $x \notin Q$ and no power of $y$ is in $Q$. Hence $Q$ is not primary. Let $Q_1 = (x)$ and $Q_2 = (x^2, y)$. We have a decomposition $Q = Q_1 \cap Q_2$, i.e.,

$$(x^2, xy) = (x) \cap (x^2, y)$$

into primary ideals $Q_1$ and $Q_2$. The associated prime ideals are given by $P_1 = \sqrt{Q_1} = (x)$ and $P_2 = \sqrt{Q_2} = (x, y)$. In the decomposition $Q = Q_1 \cap Q_2$ the ideal $Q_1$ is prime and $Q_2 = (x^2, y)$

is primary, since $R/Q_2 \simeq K[x]/(x^2)$, in which the zero-divisors are all multiples of $x$, hence are nilpotent. We have $\sqrt{Q} = P_1 \cap P_2 = P_1 = (x)$, which is prime.

In contrast to the above example, if $\sqrt{Q}$ is maximal, then $Q$ is primary.

LEMMA 1.3.17. *Let $Q$ be an ideal of $R$ such that $\sqrt{Q} = M$ is maximal. Then $Q$ is $M$-primary, i.e., $Q$ is a primary ideal. Moreover all powers $M^n$ for $n \geq 1$ are $M$-primary.*

PROOF. Let $ab \in Q$. If $a \in \sqrt{Q}$ then $a^n \in Q$. Otherwise $a \notin \sqrt{Q}$, so that $a \notin Q$. Then $\sqrt{Q + Ra} \supseteq M + Ra = R$, and so $1 \in Q + Ra$, which implies $b \in Qb + Rab \subseteq Q$. Since we have $\sqrt{M^n} = M$ for all maximal ideals $M$, for all $n \geq 1$, the last claim follows. □

This lemma shows again that $Q_2 = (x^2, y)$ is a primary ideal in $K[x, y]$, see example 1.3.16, since $\sqrt{Q_2} = (x, y)$ is a maximal ideal in $K[x, y]$.

DEFINITION 1.3.18. A proper ideal $I$ in $R$ is called *irreducible* if it is not a finite intersection of strictly larger ideals, i.e., if $I = J \cap K$ implies $I = J$ or $I = K$, for all ideals $J, K$ of $R$ with $I \subseteq J$ and $I \subseteq K$.

LEMMA 1.3.19. *Every irreducible ideal in a Noetherian ring $R$ is primary.*

PROOF. Let $I$ be an irreducible ideal in $R$. Assume that $ab \in I$, $b \notin I$ and no power of $a$ is in $I$. Consider the chain of ideals

$$(I : a) \subseteq (I : a^2) \subseteq (I : a^3) \subseteq \cdots$$

By a.c.c. (the ascending chain condition) in $R$, $(I : a^n) = (I : a^{n+1})$ for some $n \geq 1$. We will show that this implies

$$I = (I + Ra^n) \cap (I + Rb),$$

which contradicts the irreducibility of $I$, so that some power of $a$ is in $I$, and $I$ is primary. First, it is clear that $I \subseteq (I + Ra^n) \cap (I + Rb)$. To see the converse, let $x = j + sa^n = i + rb \in (I + Ra^n) \cap (I + Rb)$, with $i, j \in I$ and $r, s \in R$. Then $ax = ia + rab \in I$, so that $ja + sa^{n+1} \in I$ and hence $sa^{n+1} \in I$. It follows that $s \in (I : a^{n+1}) = (I : a^n)$, hence $x = j + sa^n \in I$. □

LEMMA 1.3.20. *If $Q_i$ are $P$-primary ideals in $R$ for $1 \leq i \leq n$, then $Q = \cap_{i=1}^n Q_i$ is $P$-primary.*

PROOF. We have

$$\sqrt{Q} = \sqrt{Q_1 \cap \cdots \cap Q_n} = \bigcap_{i=1}^{n} \sqrt{Q_i} = P.$$

Let $xy \in Q$ and $y \notin Q$. Then $xy \in Q_i$ and $y \notin Q_i$ for some $i \geq 1$, hence $x \in P = \sqrt{Q}$, since $Q_i$ is primary. It follows that $Q$ is primary. □

The following theorem, due to E. Lasker and E. Noether, shows that ideals in Noetherian rings admit a nice decomposition into primary ideals.

THEOREM 1.3.21 (Primary Decomposition). *Let $R$ be a Noetherian ring and $I$ be any ideal of $R$ with $I \neq R$. Then we have the following.*

(1) *There exist primary ideals $Q_1, \ldots Q_h$ of $R$ such that*

$$I = Q_1 \cap \cdots \cap Q_h.$$

(2) *The ideals $Q_1, \dots Q_h$ in the above decomposition can be chosen such that*

$$Q_i \not\supseteq \bigcap_{j \neq i} Q_j$$

*for all $1 \leq i \leq h$, and all $P_i = \sqrt{Q_i}$, $i = 1, \dots, h$ are distinct.*

(3) *The ideals $P_1, \dots, P_h$ are unique. Indeed, the set $\{P_1, \dots, P_h\}$ equals the set of prime ideals among the ideals $(I : x)$, where $x$ varies over the elements of $R$.*

(4) *If for a fixed $i$ the ideal $P_i$ is minimal, i.e., if $P_i \not\supseteq P_j$ for all $j \neq i$, then the corresponding primary ideal $Q_i$ is also unique.*

PROOF. (1): The maximality condition in $R$ implies that every ideal $I$ of $R$ is a finite intersection of irreducible ideals. Indeed, let $S$ be the set of ideals of $R$ which are *not* a finite intersection of irreducible ideals. If $S \neq \emptyset$, then $S$ has a maximal element $M$, since $R$ is Noetherian. Clearly $M \neq R$. Moreover $M$ is reducible because of $M \in S$, i.e., $M = I_1 \cap I_2$ with $M \subseteq I_1$ and $M \subseteq I_2$, hence with $I_1, I_2 \notin S$. It follows that $I_1$ and $I_2$ are finite intersections of irreducible ideals, so that the same is true for $M$, a contradiction. It follows $S = \emptyset$, and $I = Q_1 \cap \dots \cap Q_h$ with irreducible ideals $Q_i$. Lemma 1.3.19 says that the $Q_i$ are primary. This proves (1).

(2): If $P_i = P_j = P$ then $Q_i \cap Q_j$ is $P$-primary by lemma 1.3.20. Hence it can replace both $Q_i$ and $Q_j$ in the decomposition. In this way we arrive at a *minimal* or *irredundant* decomposition, where all $\sqrt{Q_i}$ are distinct and $Q_i \not\supseteq \cap_{j \neq i} Q_j$.

(3): Let $i \in \{1, \dots, h\}$ and choose $c_i \in (\cap_{j \neq i} Q_j) \setminus Q_i$. Then we have

$$Q_i \subseteq (I : c_i) \subseteq P_i,$$

and so there is, by lemma 1.3.26, a $k \geq 1$ such that $P_i^k \subseteq (I : c_i)$, but $P_i^{k-1} \not\subseteq (I : c_i)$. Choose $y \in P_i^{k-1} \setminus (I : c_i)$, and let $x_i := yc_i$. We claim that

$$P_i = (I : x_i).$$

Clearly, $P_i \subseteq (I : x_i)$. On the other hand, if there is $x \in (I : x_i) \setminus P_i$, then $xyc_i \in I \subseteq Q_i$. Since $Q_i$ is primary and $x \notin P_i$, we obtain $yc_i \in Q_i$. By the choice of $c_i$ we have $yc_i \in I$, that is, $y \in (I : c_i)$, which contradicts the choice of $y$. Hence we have $(I : x_i) \subseteq P_i$, and the above claim is proved.

Conversely, suppose that $(I : x) = P$ is a prime ideal for some $x \in R$. Then

$$P = (I : x) = (\cap_{i=1}^h Q_i : x) = \bigcap_{i=1}^h (Q_i : x),$$

and thus $(Q_i : x) \subseteq P$ for some $i$. Hence $x \notin Q_i$ and

$$P_i = \sqrt{Q_i} \subseteq \sqrt{(Q_i : x)} \subseteq P.$$

Conversely, if $a \in P$ then $ax \in I \subseteq Q_i$, so that $a \in P_i$. Together we have $P = P_i$.

(4): We leave this as an exercise (localize at $P_i$). □

DEFINITION 1.3.22. The decomposition $I = Q_1 \cap \dots \cap Q_h$ as in (1) above is called a *primary decomposition* of $I$. If the $Q_i$ satisfy the conditions in (2), then this decomposition is called

*minimal*, or *irredundant*. The german word is *unverkürzbar*. The uniquely determined prime ideals $P_i$ are called the *associated primes* of $I$. The set of them is denoted by

$$\mathrm{Ass}_R(I) = \{P_1, \dots, P_h\}.$$

EXAMPLE 1.3.23. *Let $R = K[x, y]$ and $I = (x^2, xy)$. Then*

$$(x^2, xy) = (x) \cap (x^2, y)$$

*is an irredundant primary decomposition of $I$. The associated primes are*

$$\{P_1, P_2\} = \{(x), (x, y)\}.$$

Note that $P_1$ is minimal, see (4), but $P_2$ is not since $P_2 \supseteq P_1$.

REMARK 1.3.24. The primary decomposition is not unique in general. In fact, $(x^2, xy) = (x) \cap (x^2, y) = (x) \cap (x^2, y + cx)$ are irredundant primary decompositions of $I$ for any $c \in K$. Also, $(x^2, xy) = (x) \cap (x^2, xy, y^2)$ is an irredundant primary decomposition of $I$.

Primary decompositions are preserved under localizations w.r.t. multiplicatively closed subsets that are disjoint from all associated primes.

PROPOSITION 1.3.25. *Let $S$ be a multiplicatively closed subset of a Noetherian ring $R$ and $I = Q_1 \cap \cdots \cap Q_h$ be a minimal primary decomposition of $I$. Let $P_i = \sqrt{Q_i}$ for $i = 1, \dots, h$. Then*

$$S^{-1}I = \bigcap_{S \cap P_i = \emptyset} S^{-1}Q_i, \quad (S^{-1}I)^c = \bigcap_{S \cap P_i = \emptyset} Q_i,$$

*and these are minimal primary decompositions.*

PROOF. We only remark that if $S \cap P_i \neq \emptyset$, then $S^{-1}Q_i = R$, whereas if $S \cap P_i = \emptyset$, then $S^{-1}Q_i$ is $S^{-1}P_i$-primary and the contraction equals $Q_i$, i.e., $(S^{-1}Q_i)^c = Q_i$. □

LEMMA 1.3.26. *Let $I$ be an ideal in a Noetherian ring $R$ and $J = \sqrt{I}$. Then $I$ contains a power of its radical, i.e., $J^n \subseteq I$ for some $n \geq 1$.*

PROOF. Since $R$ is Noetherian, $J$ is finitely generated. Let $J = (a_1, \dots, a_k)$. For each $i = 1, \dots, k$ there exists $n_i \in \mathbb{N}$ such that $a_i^{n_i} \in I$. Set

$$n := 1 + \sum_{i=1}^{k} (n_i - 1).$$

Then $J^n = (\sqrt{I})^n$ is the ideal of $R$ generated by

$$L := \{a_1^{r_1} a_2^{r_2} \cdots a_k^{r_k} \mid r_i \geq 0, r_1 + \cdots + r_k = n\}.$$

Given non-negative integers $r_1, \dots, r_k$ which sum to $n$, we must have $r_j \geq n_j$ for at least one integer $j$ with $1 \leq j \leq k$, for otherwise

$$n = \sum_{i=1}^{k} r_i \leq \sum_{i=1}^{k} (n_i - 1) < n,$$

which is a contradiction. Hence $a_1^{r_1} \cdots a_j^{r_j} \cdots a_k^{r_k} \in I$, so that $L \subseteq I$ and $J^n = RL \subseteq I$. □

We can use this lemma together with the primary decomposition to prove the following result:

PROPOSITION 1.3.27. *Let $I$ be an ideal of a Noetherian ring $R$, and let $J = \cap_{n=1}^{\infty} I^n$. Then $J = IJ$.*

PROOF. If $I = R$ then the claim is obvious. Hence assume that $I \neq R$. Since $IJ \subseteq J \subseteq I$, we see that $IJ$ is also a proper ideal of $R$. Look at the minimal primary decomposition of $IJ$, i.e.,

$$IJ = Q_1 \cap \ldots \cap Q_n,$$

with $\sqrt{Q_i} = P_i$ for $i = 1, \ldots, n$. We want to show that $J \subseteq IJ$ by showing that $J \subseteq Q_i$ for each $i = 1, \ldots, n$. Suppose that, for some $1 \leq i \leq n$ we have $J \nsubseteq Q_i$, so that there exists $a \in J \setminus Q_i$. Since

$$aI \subseteq IJ = Q_1 \cap \ldots \cap Q_n \subseteq Q_i,$$

and $Q_i$ is $P_i$-primary, it follows form $a \notin Q_i$ that $I \subseteq P_i$. But $P_i = \sqrt{Q_i}$, and so, by lemma 1.3.26, there exists $t \in \mathbb{N}$ such that $P_i^t \subseteq Q_i$. Hence

$$J = \bigcap_{n=1}^{\infty} I^n \subseteq I^t \subseteq P_i^t \subseteq Q_i.$$

This is a contradiction. Hence $J \subseteq Q_i$ for all $i$ and $J \subseteq IJ \subseteq J$. □

REMARK 1.3.28. By Nakayama's lemma for Noetherian modules it follows from the above proposition that $(1 - a) \cap_{n=1}^{\infty} I^n = 0$ for some $a \in I$. If in addition $I \in \mathcal{J}(R)$, then $1 - a$ is a unit of $R$ so that $\cap_{n=1}^{\infty} I^n = 0$. This statement is called *Krull's intersection theorem*. If $(R, M)$ is a local ring with maximal ideal $M$, then $\mathcal{J}(R) = M$ and $\cap_{n=1}^{\infty} M^n = 0$.

## 1.4. Affine algebraic sets

Let $K$ be a field and $n \geq 1$ be an integer. The set of $n$-tuples

$$\mathbb{A}_K^n = \{(a_1, \dots a_n) \mid a_1, \dots, a_n \in K\}$$

is called the *n-dimensional affine space*. An element $(a_1, \dots a_n) \in \mathbb{A}_K^n$ is called a *point*, and the $a_i$ are called the *coordinates* of the point. $\mathbb{A}_K^1$ is often called the *affine line*, and $\mathbb{A}_K^2$ the *affine plane*. A point $(a_1, \dots a_n) \in \mathbb{A}_K^n$ is called a *zero* of a polynomial $f \in K[x_1, \dots, x_n]$, if $f(a_1, \dots, a_n) = 0$.

Definition 1.4.1. A set $V \subseteq \mathbb{A}_K^n$ is called an *affine algebraic set*, if there exists a subset $T \subseteq K[x_1, \dots, x_n]$ such that $V = V(T)$, where

$$V(T) = \{(a_1, \dots, a_n) \in \mathbb{A}_K^n \mid f(a_1, \dots, a_n) = 0 \ \ \forall\, f \in T\}.$$

In linear algebra we study the solution sets of linear equations

$$\begin{aligned} c_{11}x_1 + \cdots + c_{1n}x_n &= b_1 \\ \vdots \qquad\qquad\quad &= \vdots \\ c_{m1}x_1 + \cdots + c_{mn}x_n &= b_m \end{aligned}$$

Denote by $V$ the solution set, then $V = V(T)$ is an affine algebraic set with

$$T = \{f_i = \sum_{i=1}^{n} c_{ij}x_j - b_j\},\ i = 1, \dots, m.$$

$V(T)$ is a linear algebraic variety of dimension $n - r$, where $r$ is the rank of the matrix $(c_{ij})$. The zeroset of a single polynomial is called an *affine hyperplane*. If $n = 2$, we have an affine plane curve. For example $V(x^2+y^2-1) \subset \mathbb{A}_{\mathbb{R}}^2$ is the circle, with $f \in \mathbb{R}[x, y]$. Or $V(y^2 - x^3 + x)$ is an elliptic curve. In general, this depends on the field. For example, $V(x^2 + 1)$ is empty for $K = \mathbb{R}$, but equals $\{i, -i\}$ for $K = \mathbb{C}$.

Proposition 1.4.2. *Let $V(T) \subseteq \mathbb{A}_K^n$ be an affine algebraic set with $T \subseteq K[x_1, \dots, x_n]$. Let $I$ be the ideal of $K[x_1, \dots, x_n]$ generated by $T$. Then $V(T) = V(I)$, where*

$$V(I) = \{(a_1, \dots, a_n) \in \mathbb{A}_K^n \mid f(a_1, \dots, a_n) = 0 \ \ \forall\, f \in I\}.$$

*In other words, algebraic sets are zerosets of ideals $I$ of $K[x_1, \dots, x_n]$.*

Proof. We have $V(I) \subseteq V(T)$ since $I \supseteq T$. Let $(a_1, \dots, a_n) \in V(T)$ and $f \in I$. Then $f = \sum_{i=1}^m g_i h_i$ with $h_i \in T$ and $g_i \in K[x_1, \dots, x_n]$. Hence

$$\begin{aligned} f(a_1, \dots, a_n) &= \sum_{i=1}^{m} g_i(a_1, \dots, a_n)h_i(a_1, \dots, a_n) \\ &= 0, \end{aligned}$$

since $h_i(a_1, \dots, a_n) = 0$. It follows $(a_1, \dots, a_n) \in V(I)$. □

Since the ring $K[x_1, \dots, x_n]$ is Noetherian we have the following result.

Proposition 1.4.3. *Let $V(I) \subseteq \mathbb{A}_K^n$ be an algebraic set with defining ideal $I \subseteq K[x_1, \dots, x_n]$. Then there are finitely many polynomials $f_1, \dots, f_m$ with $I = (f_1, \dots, f_m)$ and $V(I) = V(f_1, \dots, f_m)$.*

The map $V\colon I \to V(I)$ of ideals of $K[x_1,\dots,x_n]$ to algebraic sets $V(I)$ of $\mathbb{A}^n_K$ is surjective, but not injective. Indeed, $V(x_1) = V(x_1^k)$ for all $k \geq 1$. We have $V(0) = \mathbb{A}^n_K$ and $V(K[x_1,\dots,x_n]) = \emptyset$. If $I \subseteq J$ are ideals of $K[x_1,\dots,x_n]$, then $V(I) \supseteq V(J)$.

PROPOSITION 1.4.4. *If $I, J$ are ideals of $K[x_1,\dots,x_n]$, then $V(I)\cup V(J) = V(I\cap J)$. If $I_\alpha$ is a family of ideals for $\alpha \in \mathcal{A}$ then*

$$\bigcap_{\alpha\in\mathcal{A}} V(I_\alpha) = V\left(\sum_{\alpha\in\mathcal{A}} I_\alpha\right).$$

PROOF. Let $a \in V(I)\cup V(J)$. We may assume that $a \in V(I)$. Let $g \in I\cap J$. Then $g(a) = 0$ and hence $a \in V(I\cap J)$. Conversely, assume that $a \in V(I\cap J)$. If $a \in V(I)$ then certainly $a \in V(I)\cup V(J)$. Otherwise $a \notin V(I)$. Then there exists $f \in I$ with $f(a) \neq 0$. For any $g \in J$ we have $fg \in I\cap J$, so that $f(a)g(a) = 0$. It follows $g(a) = 0$ and $a \in V(J)$. The second claim can be proved similarly. □

In other words, finite unions of algebraic sets are algebraic, and arbitrary intersections of algebraic sets are algebraic.

DEFINITION 1.4.5. The *Zariski topology* on $\mathbb{A}^n_K$ is defined to be the topology whose closed sets are the sets $V(I)$ for all $f \in I \subseteq \mathbb{A}^n_K$, where $I \subseteq K[x_1,\dots,x_n]$ is any ideal in the polynomial ring $K[x_1,\dots,x_n]$.

The family $\{V(I)\}$ indeed satisfies all the axioms of closed sets for a topology on $\mathbb{A}^n_K$. The open sets are the complements of the closed sets. The Zariski topology is quite different from the Euclidean topology on $K^n$. It is not Hausdorff in general.

EXAMPLE 1.4.6. *Consider the affine line $\mathbb{A}^1_{\mathbb{C}}$. Then $\emptyset$ and $\mathbb{A}^1_{\mathbb{C}}$ are Zariski-open and closed, and all other closed sets are just finite sets of points. Hence every non-empty open set is dense in $\mathbb{A}^1_{\mathbb{C}}$, and the topology on $\mathbb{A}^1_{\mathbb{C}}$ is not Hausdorff.*

Note that each proper ideal $I \in K[x]$ is a principal ideal, i.e., is of the form $I = ((x - a_1)\cdots(x - a_n))$ for $a_i \in K$. Hence each closed set of $\mathbb{A}^1_{\mathbb{C}}$, different from $\emptyset$ and $\mathbb{A}^1_{\mathbb{C}}$ is a finite set of points. Given two points we cannot find two disjoint open sets which seperate the points.

DEFINITION 1.4.7. Let $W \subseteq \mathbb{A}^n_K$ be a subset. Then the ideal

$$I(W) = \{f \in K[x_1,\dots,x_n] \mid f(a_1,\dots,a_n) = 0 \ \ \forall\, (a_1,\dots,a_n) \in W\}$$

is called the *vanishing ideal* (Verschwindungsideal) of $W$.

The map $I\colon W \mapsto I(W)$ is neither injective nor surjective. For example, $I(\mathbb{A}^1_{\mathbb{C}}) = I(\mathbb{Z}) = (0)$, and the ideal $(x_1^2) \subseteq K[x_1]$ lies not in the image of the map $I$.

We have $I(W) \supseteq I(V)$ for $W \subseteq V$. If $J \subseteq K[x_1,\dots,x_n]$ is an ideal then $J \subseteq I(V(J))$. For every subset $W \subseteq \mathbb{A}^n_K$ we have $W \subseteq V(I(W))$.

PROPOSITION 1.4.8. *Let $W \subseteq \mathbb{A}^n_K$. We have $W = V(I(W))$ if and only if $W$ is an algebraic set.*

PROOF. If $W = V(I(W))$ then $W$ is algebraic by definition. Conversely, let $W = V(J)$ be an algebraic set for an ideal $J \subseteq K[x_1,\dots,x_n]$. Then $J \subseteq I(W)$, so that $W = V(J) \supseteq V(I(W)) \supseteq W$. □

LEMMA 1.4.9. *Let $W \subseteq \mathbb{A}^n_K$ be a subset and $I(W)$ the corresponding ideal in $K[x_1,\dots,x_n]$. Then $I(W)$ is a radical ideal, i.e., $\sqrt{I(W)} = I(W)$.*

PROOF. We always have $I(W) \subseteq \sqrt{I(W)}$. Conversely, let $f \in \sqrt{I(W)}$. Then $f^m \in I(W)$ for some $m \geq 1$. Let $a = (a_1, \ldots, a_n) \in \mathbb{A}^n_K$. Then $f^m(a) = 0$ for all $a \in W$. This means $f(a)^m = 0$ and $f(a) = 0$ since $K$ is a field. Thus $f \in I(W)$. □

We have now an inclusion reversing map $I$ from algebraic subsets of $\mathbb{A}^n_K$ to radical ideals of $K[x_1, \ldots, x_n]$, given by $W \mapsto I(W)$. The question is, whether this map is a bijection. This is not the case in general.

EXAMPLE 1.4.10. *The radical ideal $J = (x^2+1) \subseteq \mathbb{R}[x]$ does not correspond to any algebraic subset of $\mathbb{A}^1_{\mathbb{R}}$ under the map $I$.*

First, the polynomial $x^2 + 1$ is irreducible in $\mathbb{R}[x]$, so that $J$ is a prime ideal, and hence $\sqrt{J} = J$. Assume that $J = I(W)$ for some algebraic subset $W$. By proposition 1.4.8 we have $W = V(I(W)) = V(J) = V(x^2 + 1) = \emptyset$, so that $J = I(W) = I(\emptyset) = \mathbb{R}[x]$, which is a contradiction.

If $K$ is algebraically closed, however, then the map $I$ will be a bijection:

THEOREM 1.4.11 (Hilbert's Nullstellensatz). *Let $K$ be an algebraically closed field. Then the following holds:*

(1) *Every maximal ideal $M \subseteq K[x_1, \ldots, x_n]$ is of the form*
$$M = (x_1 - a_1, \ldots, x_n - a_n) = I(a_1, \ldots, a_n)$$
*for some point $a = (a_1, \ldots, a_n) \in \mathbb{A}^n_K$.*

(2) *Let $J \subseteq K[x_1, \ldots, x_n]$ be an ideal. Then $V(J) \neq \emptyset$ if and only if $J \neq K[x_1, \ldots, x_n]$.*

(3) *For every ideal $J \subseteq K[x_1, \ldots, x_n]$ we have $I(V(J)) = \sqrt{J}$.*

PROOF. We will first show that all three statements are equivalent. Then we will indicate how to prove the statement (1), but without the details. There are some recent articles on how to give an elementary proof, i.e., "aimed at undergraduates", and we will refer the reader to these references. For a proof with more theory one may take a standard book on algebraic geometry. Write $S = K[x_1, \ldots, x_n]$ as a shorthand.

(1) ⇒ (2): Suppose that $J \subset S$ is a proper ideal of $S$. Since $S$ is Noetherian, there exists a maximal ideal $M$ of $S$ such that $J \subseteq M$. By (1) we know that $M = (x_1 - a_1, \ldots, x_n - a_n) = I(a_1, \ldots, a_n)$, so that $(a_1, \ldots, a_n) \in V(M) \subseteq V(J)$. This shows $V(J) \neq \emptyset$. Conversely, if $(a_1, \ldots, a_n) \in V(J)$ for some point $(a_1, \ldots, a_n) \in \mathbb{A}^n_K$, then we have $J \neq S$, because otherwise $V(J) = V(S) = \emptyset$.

(2) ⇒ (3): Let $f \in \sqrt{J}$. Then $f^m \in J \subseteq I(V(J))$ for some $m \geq 1$. This means $f \in \sqrt{I(V(J))}$ which equals $I(V(J))$ by lemma 1.4.9. It follows $\sqrt{J} \subseteq I(V(J))$. Conversely, let $f \in I(V(J))$. We show using the trick of Rabinowitsch that $f \in \sqrt{J}$. Consider the polynomial ring $S_t = K[x_1, \ldots, x_n, t]$ and the ideal $J_f = J + (ft - 1) \subseteq S_t$. We have
$$V(J_f) = \{(a_1, \ldots, a_n, b) \in \mathbb{A}^{n+1}_K \mid bf(a_1, \ldots, a_n) = 1, (a_1, \ldots, a_n) \in V(J)\}.$$
Suppose that there exists a point $(a_1, \ldots, a_n, b) \in V(J_f)$. Then $f(a_1, \ldots, a_n) = 0$ because of $f \in I(V(J))$. But we have also $1 = f(a_1, \ldots, a_n)b = 0$, which is impossible. It follows that

$V(J_f) = \emptyset$. By (2) it follows $J_f = S_t$, in particular $1 \in J_f$. Hence there exist $f_i \in J$, $g_0, g_i \in S_t$ such that

$$1 = \sum_i g_i f_i + g_0(ft - 1).$$

Consider the ring homomorphism $\varphi\colon S_t \to K(x_1, \ldots, x_n)$, working in the field of fractions of $S$, given by $\varphi(x_i) = x_i$ and $\varphi(t) = 1/f$. Then

$$\begin{aligned} 1 = \varphi(1) &= \sum_i \varphi(g_i) f_i + \varphi(g_0)(f\frac{1}{f} - 1) \\ &= \sum_i \varphi(g_i) f_i. \end{aligned}$$

Writing $g_i = \sum_j g_{ij} t^j$ with $g_{ij} \in S$ we obtain $\varphi(g_i) = \sum_j g_{ij}(1/f)^j$, which is of the form $h_i/f^{c_i} \in K(x_1, \ldots, x_n)$ for some $h_i \in S$ and $c_i \in \mathbb{N}$. Substitute this in the above equation:

$$1 = \sum_i \varphi(g_i) f_i = \sum_i \frac{h_i}{f^{c_i}}.$$

Now multiply this with $f^m$ and $m \geq 1$ large enough to clear denominators, i.e., for $m = \max_i\{c_i\}$. Then we obtain

$$f^m = \sum_i h_i f^{m-c_i} f_i \in J.$$

This implies $f \in \sqrt{J}$.

(3) $\Rightarrow$ (1): First, the ideal $M = (x_1 - a_1, \ldots, x_n - a_n)$ is maximal, since it is the kernel of the evaluation map

$$\varphi\colon S = K[x_1, \ldots, x_n] \twoheadrightarrow K, \quad f \mapsto f(a_1, \ldots, a_n).$$

Then $S/M \simeq K$ is field, so that $M$ is maximal.
Now let $M$ be an arbitrary maximal ideal of $S$. By assumption $M = \sqrt{M} = I(V(M))$, hence $V(M) \neq \emptyset$. Let $(a_1, \ldots, a_n) \in V(M)$. Then

$$M = I(V(M)) \subseteq I(a_1, \ldots, a_n) = (x_1 - a_1, \ldots, x_n - a_n),$$

and (3) is proved. Because $M$ is maximal, it follows $M = (x_1 - a_1, \ldots, x_n - a_n)$.

For an elementary proof of (1) see [**6**] and the references therein. The idea is as follows. Let $M$ be a maximal ideal in $K[x_1, \ldots, x_n]$, where we can assume $n \geq 2$. The case $n = 1$ is the fundamental theorem of algebra, i.e., every polynomial $f \in K[x]$ has a root, for $K$ being algebraically closed. Hence every monic $f \in K[x]$ splits completely as a product of linear polynomials $x - a_i$, so that the only maximal ideals in $K[x]$ are principal ideals $(x - a)$. Now regard $K[x_1, \ldots, x_n]$ as $K[x_1][x_2, \ldots, x_n]$. By Kaplansky's lemma below, the integral domain $R = K[x_1]$ satisfies the hypothesis in Munshi's lemma below. Therefore there is a nonzero element $f \in M \cap K[x_1]$. Since $K$ is algebraically closed, $f$ splits into a product of linear factors. Because $f \in M$ and $M$ is maximal, hence prime, at least one of those factors, say $x_1 - a_1$, is in $M$. The same argument gives an element $x_i - a_i$ in $M$ for each $1 \leq i \leq n$. Then $(x_1 - a_1, \ldots, x_n - a_n) \subseteq M$, which implies equality, since both ideals are maximal. □

Corollary 1.4.12. *Let $K$ be an algebraically closed field. Then the map $I$ from algebraic subsets of $\mathbb{A}^n_K$ to radical ideals in $K[x_1, \ldots, x_n]$ is a bijection, with inverse map $V$.*

REMARK 1.4.13. The name "Nullstellensatz" comes from the statement (2): if $J$ is a proper ideal of $K[x_1, \ldots, x_n]$, then there is an element $a = (a_1, \ldots, a_n) \in \mathbb{A}^n_K$ such that $f(a) = 0$ for all $f \in J$.

In [**6**] we find the proof of the following two lemmas.

LEMMA 1.4.14 (Munshi). *Assume that the intersection of the nonzero prime ideals of a commutative ring $R$ is zero. If $M$ is a maximal ideal in $R[x_1, \ldots, x_n]$, then $M \cap R \neq 0$.*

LEMMA 1.4.15 (Kaplansky). *Let $R$ be a commutative ring. The intersection of the nonzero prime ideals of $R[x]$ is zero.*

CHAPTER 2

# Gröbner Bases

In this chapter let $K$ be a field and $S = K[x_1, \ldots, x_n]$. Let $I$ be an ideal of $S$. Then there are some computational problems:

(1) Is $V(I) \neq \emptyset$ ?
(2) The *ideal membership problem*: let $f \in S$ be a given polynomial. Determine if $f \in I$.
(3) The problem of *solving polynomial equations*: find all common solutions in $\mathbb{A}_K^n$ of a system of polynomial equations

$$f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0.$$

Of course, this is the same as asking for the points of $V(I)$, where $I = (f_1, \ldots, f_s)$.

A *Gröbner basis* is a particular basis for $I$, for which, among other things, we can answer the three problems from above.

For $n = 1$ the situation is a lot easier than in general. Then $S = K[x]$ is a Euclidean ring, hence $I = (f_1, \ldots, f_s) = (g)$ is a principal ideal. The solution of the ideal membership problem follows easily from the division algorithm in $K[x]$: given $f \in K[x]$, to check whether $f \in I = (g)$, just divide to obtain $f = qg + r$, where $q, r \in K[x]$ and $r = 0$ or $\deg(r) < \deg(g)$. Then it follows $f \in (g)$ if and only if $r = 0$. Thus, we have an algorithmic test for the ideal membership problem, if $n = 1$. If $g$ splits into the linear factors $(x - a_i)$, then $V(I) = \{a_1, \ldots, a_r\}$.

For $n \geq 2$ the situation is much more complicated. The ring $K[x_1, \ldots, x_n]$ is not Euclidean, and not a PID. We do not have a division algorithm. We can, however, try to restore some of the properties of a division algorithm, and this will lead us to Gröbner bases.

## 2.1. Monomial orderings

Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ be a tuple of non-negative integers. We write

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

for a monomial in $S = K[x_1, \ldots, x_n]$. We want to order the monomials (terms) in a polynomial unambiguously, in descending or ascending order. Recall the following definition:

DEFINITION 2.1.1. A relation $\leq$ is a *partial order* on a set $S$ if it satisfies:

(1) Reflexivity: $a \leq a$ for all $a \in S$.
(2) Antisymmetry: $a \leq b$ and $b \leq a$ imply $a = b$ for all $a, b \in S$.
(3) Transitivity: $a \leq b$ and $b \leq c$ imply $a \leq c$ for all $a, b, c \in S$.

A partial order on $S$ is called a *total order*, if $a \leq b$ or $b \leq a$ for any two elements $a, b \in S$. This property implies reflexivity.

EXAMPLE 2.1.2. *The set $2^{\mathbb{N}}$ of all subsets of $\mathbb{N}$ is a partial ordered set with the inclusion $\subseteq$, but not a total order.*

For polynomial rings however the following orderings are relevant:

DEFINITION 2.1.3. A *well-ordering* on a set $S$ is a total order on S with the property that every non-empty subset of $S$ has a least element in this ordering.

EXAMPLE 2.1.4. *The standard ordering $\leq$ on $\mathbb{N}$ is a well-ordering. However, on $\mathbb{Z}$ it is not a well-ordering, since, for example, the set of negative integers does not contain a least element.*

DEFINITION 2.1.5. A *monomial ordering* on $S = K[x_1, \ldots, x_n]$ is any relation $\prec$ on $\mathbb{N}^n$ satisfying

(1) $\prec$ is a well-ordering on $\mathbb{N}^n$.
(2) $\alpha \prec \beta$ implies $(\alpha + \gamma) \prec (\beta + \gamma)$ for all $\alpha, \beta, \gamma \in \mathbb{N}^n$.

The following lemma is easy, see for example [**2**].

LEMMA 2.1.6. *A total order $\prec$ on $\mathbb{N}^n$ is a well-ordering if and only if every strictly decreasing sequence in $\mathbb{N}^n$*

$$\alpha(1) \succ \alpha(2) \succ \alpha(3) \succ \cdots$$

*eventually terminates.*

DEFINITION 2.1.7 (Lexicographic Order). Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ in $\mathbb{N}^n$. We say that $\alpha \prec_{lex} \beta$, if in the vector difference $\alpha - \beta \in \mathbb{Z}^n$ the left-most nonzero entry is negative.

EXAMPLE 2.1.8. *Let $n = 3$, $S = K[x, y, z]$ and*

$$\alpha = (0, 4, 0) \leftrightarrow y^4$$
$$\beta = (1, 1, 2) \leftrightarrow xyz^2$$
$$\gamma = (1, 2, 1) \leftrightarrow xy^2z$$
$$\delta = (3, 0, 0) \leftrightarrow x^3$$

*Then $\alpha \prec_{lex} \beta \prec_{lex} \gamma \prec_{lex} \delta$.*

DEFINITION 2.1.9 (Graded Lex Order). Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ in $\mathbb{N}^n$. Let $|\alpha| = \sum_{i=1}^n \alpha_i$. We say that $\alpha \prec_{grlex} \beta$, if

$$|\alpha| < |\beta|, \text{ or if } |\alpha| = |\beta| \text{ and } \alpha \prec_{lex} \beta.$$

This means, *grlex* orders by total degree first, and then does a "tie-break" by using *lex*. For the above example we obtain

$$\delta \prec_{grlex} \alpha \prec_{grlex} \beta \prec_{grlex} \gamma.$$

Indeed, the decision $\alpha \prec_{grlex} \beta \prec_{grlex} \gamma$ is by tie-break. We have $|\alpha| = |\beta| = |\gamma| = 4$.

DEFINITION 2.1.10 (Graded Reverse Lex Order). Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ in $\mathbb{N}^n$. We say that $\alpha \prec_{grevlex} \beta$, if $|\alpha| < |\beta|$, or if $|\alpha| = |\beta|$ and, in $\alpha - \beta \in \mathbb{Z}^n$, the right-most nonzero entry is positive.

To take our previous example, we have

$$\delta \prec_{grevlex} \beta \prec_{grevlex} \gamma \prec_{grevlex} \alpha.$$

Here also $\beta \prec_{grevlex} \gamma$, because $\beta - \gamma = (0, -1, 1)$. Note that *grevlex* cannot be derived from *grlex* by rearranging variables, as the name might suggest.

PROPOSITION 2.1.11. *The lex ordering, graded lex ordering and the graded reverse lex ordering on $\mathbb{N}^n$ are monomial orderings.*

Once we have fixed a monomial ordering $\prec$ on $\mathbb{N}^n$, we can order the monomials of a polynomial $f \in S$ in an unambiguous way with respect to $\prec$.

EXAMPLE 2.1.12. *Consider the polynomial* $f = 4xyz^2 + 4x^3 - 5y^4 + 7xy^2z$ *in* $\mathbb{Q}[x, y, z]$.

With respect to the lex order we would reorder the terms of $f$ in decreasing order as

$$f = 4x^3 + 7xy^2z + 4xyz^2 - 5y^4,$$

whereas with respect to the graded lex order we would have

$$f = 7xy^2z + 4xyz^2 - 5y^4 + 4x^3,$$

and with respect to the graded reverse lex order we would have

$$f = -5y^4 + 7xy^2z + 4xyz^2 + 4x^3.$$

REMARK 2.1.13. There is another ordering *alex*, defined by

$$\alpha \prec_{alex} \beta \Leftrightarrow \beta \prec_{lex} \alpha.$$

However this is not a monomial ordering on $\mathbb{N}^n$, since it is not a well-ordering: Take the set $\mathbb{N} \times \{0\} \subset \mathbb{N}^2$. Then the strictly decreasing sequence in $\mathbb{N}^2$

$$(0,0) \succ_{alex} (1,0) \succ_{alex} (2,0) \succ_{alex} \cdots$$

does not terminate.

DEFINITION 2.1.14. Let $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha$ be a nonzero polynomial in $S$, and $\prec$ be a monomial order.

(1) The *multidegree* of $f$ is $\operatorname{mdeg}(f) = \max_\prec\{\alpha \in \mathbb{N}^n \mid c_\alpha \neq 0\}$.

(2) The *leading coefficient* of $f$ is $\operatorname{lc}(f) = c_{\operatorname{mdeg}(f)}$.

(3) The *leading monomial* of $f$ is $\operatorname{lm}(f) = x^{\operatorname{mdeg}(f)}$.

(4) The *leading term* of $f$ is $\operatorname{lt}(f) = \operatorname{lc}(f) \cdot \operatorname{lm}(f)$.

EXAMPLE 2.1.15. *Consider again* $f = 4xyz^2 + 4x^3 - 5y^4 + 7xy^2z$ *in* $\mathbb{Q}[x, y, z]$.

| *ordering* | $\prec_{lex}$ | $\prec_{grlex}$ | $\prec_{grevlex}$ |
|---|---|---|---|
| $\operatorname{mdeg}(f)$ | $(3,0,0)$ | $(1,2,1)$ | $(0,4,0)$ |
| $\operatorname{lc}(f)$ | $4$ | $7$ | $-5$ |
| $\operatorname{lm}(f)$ | $x^3$ | $xy^2z$ | $y^4$ |
| $\operatorname{lt}(f)$ | $4x^3$ | $7xy^2z$ | $-5y^4$ |

For the zero polynomial one could define $\operatorname{mdeg}(0) = -\infty \in \overline{\mathbb{N}^n}$.

LEMMA 2.1.16. *Let* $\prec$ *be a monomial order on* $\mathbb{N}^n$ *and* $f, g \in S$. *Then:*

(1) $\operatorname{mdeg}(fg) = \operatorname{mdeg}(f) + \operatorname{mdeg}(g)$.
(2) $\operatorname{mdeg}(f + g) \prec \max_\prec\{\operatorname{mdeg}(f), \operatorname{mdeg}(g)\}$. *If, in addition,* $\operatorname{mdeg}(f) \neq \operatorname{mdeg}(g)$ *then* $\operatorname{mdeg}(f + g) = \max_\prec\{\operatorname{mdeg}(f), \operatorname{mdeg}(g)\}$.

## 2.2. Multivariate division

We would like to have a division algorithm in $S$ for several variables. Our goal is to divide $f \in S$ by $f_1, \dots, f_s \in S$, i.e., expressing $f$ in the form

$$f = q_1 f_1 \cdots + q_s f_s + r.$$

The algorithm goes as follows:

*Input*: Nonzero polynomials $f, f_1, \dots, f_s \in S$, and a monomial order $\prec$ on $\mathbb{N}^n$.

*Output*: Polynomials $q_1, \dots, q_s, r \in S$ such that $f = q_1 f_1 \cdots + q_s f_s + r$ and no monomial in $r$ is divisible by any of $\mathrm{lt}(f_1), \dots, \mathrm{lt}(f_s)$.

1. $r \leftarrow 0$, $p \leftarrow f$.
   for $i = 1, \dots, s$ do $q_i \leftarrow 0$.

2. while $p \neq 0$ do
   if $\mathrm{lt}(f_i) \mid \mathrm{lt}(p)$ for some $1 \leq i \leq s$, then choose some such $i$,
   $$q_i \leftarrow q_i + \frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)}, \quad p \leftarrow p - \frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)} f_i$$
   else $r \leftarrow r + \mathrm{lt}(p)$, $p \leftarrow p - \mathrm{lt}(p)$.

3. return $q_1, \dots, q_s, r$.

Note that the result of the algorithm is not yet unique - we have a choice of possible indices $i$ where $\mathrm{lt}(f_i)$ divides $\mathrm{lt}(p)$. We can restore uniqueness by always taking the *smallest* index $i$.

EXAMPLE 2.2.1. *Let $S = K[x, y]$ with the lex order $\prec$, and $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$, $f_2 = y^2 - 1$. Then the algorithm gives $q_1 = x + y$, $q_2 = 1$ and $r = x + y + 1$, i.e.,*

$$f = (x + y)(xy - 1) + (y^2 - 1) + (x + y + 1).$$

Note that $x^2y \succ xy^2 \succ y^2$, and $\mathrm{lt}(f_1) = xy$, $\mathrm{lt}(f_2) = y^2$. Now the steps in the algorithm are:

1. $r = 0$, $p = x^2y + xy^2 + y^2$, $q_1 = q_2 = 0$.

2. $\mathrm{lt}(f_1) \mid \mathrm{lt}(p)$, i.e., for $i = 1$. Then
$$q_1 = 0 + \frac{x^2y}{xy} = x,$$
$$p = (x^2y + xy^2 + y^2) - \frac{x^2y}{xy}(xy - 1) = xy^2 + x + y^2.$$

Then $\mathrm{lt}(f_1) \mid \mathrm{lt}(p)$, but also $\mathrm{lt}(f_2) \mid \mathrm{lt}(p)$. Hence we may take $i = 1$ or $i = 2$. Let us take $i = 1$ and

$$q_1 = x + \frac{xy^2}{xy} = x + y,$$
$$p = (xy^2 + x + y^2) - \frac{xy^2}{xy}(xy - 1) = x + y^2 + y.$$

Next there is no $i$ such that $\mathrm{lt}(f_i) \mid \mathrm{lt}(p)$. The algorithm then gives

$$r = 0 + \mathrm{lt}(p) = x,$$
$$p = (x + y^2 + y) - \mathrm{lt}(p) = y^2 + y.$$

Then $\mathrm{lt}(f_2) \mid \mathrm{lt}(p) = y^2$, so that

$$q_2 = 0 + \frac{y^2}{y^2} = 1,$$
$$p = (y^2 + y) - \frac{y^2}{y^2}(y^2 - 1) = y + 1.$$

Here we have $\mathrm{lt}(f_i) \nmid \mathrm{lt}(p)$ for all $i$, so that

$$r = x + \mathrm{lt}(p) = x + y,$$
$$p = (y + 1) - \mathrm{lt}(p) = 1.$$

Again $\mathrm{lt}(f_i) \nmid \mathrm{lt}(p)$ for all $i$, so that

$$r = x + y + 1,$$
$$p = 0,$$

so that the algorithm terminates and gives back $q_1 = x + y$, $q_2 = 1$ and $r = x + y + 1$.

REMARK 2.2.2. It is easy to see that the other choice above, i.e., with $i = 2$ gives $q_1 = x$, $q_2 = x + 1$ and $r = 2x + 1$, i.e.,

$$f = x(xy - 1) + (x + 1)(y^2 - 1) + (2x + 1).$$

DEFINITION 2.2.3. We will call the polynomial $r$ the *remainder* of $f$ on division by the *ordered* tuple of polynomials $(f_1, \ldots, f_s)$. The polynomials $q_1, \ldots, q_s$ are called *quotients*. We write $r = f \mod (f_1, \ldots, f_s)$.

Is it true that this division algorithm always solves the ideal membership problem ? In any case, *if* we obtain $r = 0$ after the division, we know that $f = q_1 f_1 + \ldots + q_s f_s$, so that $f$ is a member of the ideal $I = (f_1, \ldots, f_s)$. Hence $r = 0$ is a sufficient condition for the membership. Unfortunately $r = 0$ is not a necessary condition, as the following example shows.

EXAMPLE 2.2.4. *Let $f = xy^2 - x$ and $f_1 = xy + 1$, $f_2 = y^2 - 1$ in $K[x, y]$. Then $f$ is contained in the ideal $I = (f_1, f_2)$, but $r = f \mod (f_1, f_2) = -(x + y) \neq 0$.*

Indeed, the result of the multivariate division algorithm is

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) - (x + y),$$

but clearly $f = 0 \cdot f_1 + x \cdot f_2 + 0$, so that $f \in (f_1, f_2)$.

It is possible to remedy this situation. Just find another "good" generating set for the ideal $I = (f_1, \ldots, f_s)$, such that $r = 0$ is equivalent membership in the ideal. It is by no means clear that such a "good" set will exist, but we will see that a *Gröbner basis* is exactly such a good set.

## 2.3. Monomial ideals and Dickson's lemma

The following definition of monomial ideals in $S$ turns out to be important.

DEFINITION 2.3.1. An ideal $I \subseteq S$ is a *monomial ideal* if there is a subset $A \subseteq \mathbb{N}^n$, such that $I = \langle x^A \rangle = \langle \{x^\alpha \mid \alpha \in A\} \rangle$.

In other words, $I$ is generated by monomials with exponents from $A$. For example, take $A = \{(4,2),(3,4),(2,5)\} \subset \mathbb{N}^2$. Then $I = (x^4y^2, x^3y^4, x^2y^5) \subset K[x,y]$ is the monomial ideal corresponding to $A$.

EXAMPLE 2.3.2. *Let $n = 2$ and $S = K[x,y]$. Then $I = (x^2 - y, x^2 + y)$ is a monomial ideal, but $I = (x + y, y^2 - 1)$ is not.*

Indeed, $I = (x^2 - y, x^2 + y) = (x^2, y)$.

LEMMA 2.3.3. *Let $I = \langle x^A \rangle$ be a monomial ideal of $S$ and $\beta \in \mathbb{N}^n$. Then $x^\beta \in I$ if and only if there is an $\alpha \in A$ such that $x^\alpha \mid x^\beta$.*

PROOF. From $x^\alpha \mid x^\beta$ it follows $\langle x^\beta \rangle \subseteq \langle x^\alpha \rangle \subseteq I$. Conversely, if $x^\beta \in I$, then

$$x^\beta = \sum_{i=1}^{s} q_i x^{\alpha_i}$$

for $q_i \in S$ and $\alpha_i \in A$. Expanding each $q_i$ as a linear combination of monomials we obtain a sum where each term is divisible by some $x^{\alpha_i}$. But then $x^\beta$ must be one of these terms, i.e., divisibly by some $x^{\alpha_i}$. □

REMARK 2.3.4. Note that $x^\alpha \mid x^\beta$ exactly when $x^\beta = x^\alpha x^\gamma$ for some $\gamma \in \mathbb{N}^n$. This is equivalent to $\beta = \alpha + \gamma$. In other words, the exponents of all monomials divisible by $x^\alpha$ is given by the set $\alpha + \mathbb{N}^n = \{\alpha + \gamma \mid \gamma \in \mathbb{N}^n\}$. For example, let $I = (y^3, xy^2, x^3y)$ in $K[x,y]$. The exponents of the monomials in $I$ form the set

$$\left((0,3) + \mathbb{N}^2\right) \cup \left((1,2) + \mathbb{N}^2\right) \cup \left((3,1) + \mathbb{N}^2\right),$$

which can be visualized in the plane as a set of integer points "lying above" and "lying right" from the three given points.

LEMMA 2.3.5. *Let $I$ be a monomial ideal, and let $f \in S$. Then the following are equivalent.*

1. *We have $f \in I$.*
2. *Every term of $f$ lies in $I$.*
3. *$f$ is a $K$-linear combination of the monomials in $I$.*

PROOF. The implications (2) ⇒ (3) ⇒ (1) are clear and hold for any ideal of $S$. The implication (1) ⇒ (2) however is not true in general. Here it holds since $I$ is a monomial ideal. Let $f = \sum_{i=1}^{s} q_i x^{\alpha_i}$, then each monomial here, as above, is divisibe by some $x^\gamma$ with $\gamma \in A$. Hence $I = \langle x^A \rangle$. □

REMARK 2.3.6. In fact, $I$ is a monomial ideal if and only if for all $f \in I$ each term of $f$ lies in $I$.

EXAMPLE 2.3.7. *Let $I = (x + y, y^2 - 1)$ as above, in $K[x,y]$. Then $x + y \in I$ but $x \notin I$, $y \notin I$.*

Since, by (3), a monomial ideal is uniquely determined by its monomials, we obtain the following corollary.

COROLLARY 2.3.8. *Two monomial ideals are the same if and only if they contain the same monomials.*

THEOREM 2.3.9 (Dickson's Lemma). *Every monomial ideal $I = \langle x^A \rangle$ is generated by a finite set of monomials, i.e., for all $A \subseteq \mathbb{N}^n$ there exists a finite subset $B \subseteq A$ with $I = \langle x^A \rangle = \langle x^B \rangle$.*

PROOF. Note that we do not assume Hilbert's Basissatz. Rather we will prove it again. We may assume that $A \neq \emptyset$. For $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ define $\alpha \leq \beta \Leftrightarrow \alpha_i \leq \beta_i$ for $i = 1, \ldots, n$. This defines a partial order on $\mathbb{N}^n$, with

$$\alpha \leq \beta \Leftrightarrow x^\alpha \mid x^\beta \Leftrightarrow x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid x_1^{\beta_1} \cdots x_n^{\beta_n}$$

We write $\alpha < \beta$ for $\alpha \leq \beta$ with $\alpha \neq \beta$. This partial order is not a total order, if $n \geq 2$. We have neither $(1,0) < (0,1)$ nor $(0,1) < (1,0)$. Let $B$ be the set of minimal elements of $A$ with respect to $\leq$, i.e.,

$$B = \{\alpha \in A \mid \beta \not< \alpha \text{ for all } \beta \in A\}.$$

*Claim*: $B$ is a finite subset of $A$, and for every $\alpha \in A$ there is a $\beta \in B$ such that $\beta \leq \alpha$.

First, for every $\alpha \in A$ there are only *finitely many* $\beta \in \mathbb{N}^n$ with $\beta \leq \alpha$. Hence there is no strictly decreasing sequence

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots$$

in $\mathbb{N}^n$. It follows that for every $\alpha \in A$ there exists a *minimal* element $\beta \in B$ with $\beta \leq \alpha$. We use induction on $n \geq 1$ to show that $B$ is finite.

$n = 1$: then $\leq$ is a total order on $\mathbb{N}$, and $B$ consists of the unique smallest element of $A$.

$n \geq 2$: Define $A^\times = \{(\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{N}^{n-1} \mid \exists\, \alpha_n \text{ with } (\alpha_1, \ldots, \alpha_n) \in A\}$.
By induction assumption, the set $B^\times$ of minimal elements of $A^\times$ is finite. For each $\beta = (\beta_1, \ldots, \beta_{n-1}) \in B^\times$ we choose an element $b_\beta \in \mathbb{N}$ such that

$$(\beta_1, \ldots, \beta_{n-1}, b_\beta) \in A.$$

We set

$$b := \max\{b_\beta \mid \beta \in B^\times\}.$$

Then we have $\alpha_n \leq b$ for every $(\alpha_1, \ldots, \alpha_n) \in B$: in fact, let $\alpha = (\alpha_1, \ldots, \alpha_n) \in B$. Then there exists a minimal element $\beta = (\beta_1, \ldots, \beta_{n-1}) \in B^\times$ such that $\beta \leq (\alpha_1, \ldots, \alpha_{n-1})$. If $\alpha_n > b$, then

$$(\beta_1, \ldots, \beta_{n-1}, b_\beta) \leq (\beta_1, \ldots, \beta_{n-1}, b) < \alpha,$$

which is a contradiction to the minimality of $\alpha \in B$. Hence it follows $\alpha_n \leq b$. Similarly it can be shown that all other coordinates $\alpha_i$ of minimal elements are bounded. Hence there are only finitely many coordinates of such elements, i.e. $\#B < \infty$.
By the above claim with $\beta \leq \alpha$ we have $x^\beta \mid x^\alpha$, i.e., $x^A \subseteq \langle x^B \rangle$ and $\langle x^A \rangle \subseteq \langle x^B \rangle$. Because of $B \subseteq A$ we also have $\langle x^B \rangle \subseteq \langle x^A \rangle$. □

EXAMPLE 2.3.10. *Let $A = \{(\alpha_1, \alpha_2) \in \mathbb{N}^2 \mid 6\alpha_2 = \alpha_1^2 - 7\alpha_1 + 18\}$ and $I = \langle x^A \rangle$. Then the set $B$ of minimal elements of $A$ is*

$$B = \{(0,3), (1,2), (3,1)\}.$$

Hence $I = \langle x^A \rangle = \langle y^3, xy^2, x^3y \rangle$.

## 2.4. Gröbner Bases and their properties

Suppose we have fixed a monomial order on $\mathbb{N}^n$. Then each $f \in S$ has a unique leading term $\mathrm{lt}(f)$. For any set $P \subseteq S = K[x_1, \ldots, x_n]$ we define its set of leading terms as follows:

DEFINITION 2.4.1. For $P \subseteq S$ let $\mathrm{lt}(P) = \{\mathrm{lt}(f) \mid f \in P\}$. We denote by $\langle \mathrm{lt}(P) \rangle$ the ideal generated by the elements of $\mathrm{lt}(P)$.

By Dickson's lemma, for every ideal $I$ of $S$ there exists a finite set $P \subseteq I$ such that $\langle \mathrm{lt}(P) \rangle \subseteq \langle \mathrm{lt}(I) \rangle$: let $P = \{f_1, \ldots, f_s\}$ and $I = \langle f_1, \ldots, f_s \rangle$ (we have also used the notation $I = (f_1, \ldots, f_s)$ before). Then, as we said,

$$\langle \mathrm{lt}(P) \rangle = \langle \mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s) \rangle \subseteq \langle \mathrm{lt}(I) \rangle$$

However, there need not be equality in general, $\langle \mathrm{lt}(I) \rangle$ can be strictly larger than $\langle \mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s) \rangle$, although $I = \langle f_1, \ldots, f_s \rangle$.

EXAMPLE 2.4.2. *Let $I = \langle f_1, f_2 \rangle$, where $f_1 = x^3 - 2xy$ and $f_2 = x^2y + x - 2y^2$ in $K[x, y]$, with the grlex order. Then $x^2 \in \langle \mathrm{lt}(I) \rangle$, but $x^2 \notin \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2) \rangle = \langle x^3, x^2y \rangle$.*

Indeed, we have

$$x^2 = x(x^2y + x - 2y^2) - y(x^3 - 2xy) = -y \cdot f_1 + x \cdot f_2 \in I.$$

However, $x^2$ is not divisible by $\mathrm{lt}(f_1) = x^3$ or $\mathrm{lt}(f_2) = x^2y$, so that $x^2 \notin \langle x^3, x^2y \rangle$ by lemma 2.3.3.
On the other hand, the following is true:

LEMMA 2.4.3. *Let $I \subseteq S$ be an ideal. If $P \subseteq I$ is a finite set with $\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(P) \rangle$ then $\langle P \rangle = I$.*

PROOF. Let $P = \{f_1, \ldots, f_s\}$ and $f \in I$. Then by the multivariate division algorithm,

$$f = q_1 f_1 + \cdots + q_s f_s + r$$

with $q_1, \ldots, q_s, r \in S$, where either $r = 0$, or no term of $r$ is divisible by some $\mathrm{lt}(f_i)$. But since $r = f - q_1 f_1 - \cdots - q_s f_s \in I$ we have

$$\mathrm{lt}(r) \in \mathrm{lt}(I) \subseteq \langle \mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s) \rangle.$$

This contradicts the divisibility by lemma 2.3.3, and we obtain $r = 0$ and $f \in \langle f_1, \ldots, f_s \rangle = \langle P \rangle$. □

Now we will show that $\langle \mathrm{lt}(I) \rangle$ is a monomial ideal, so that we can apply Dickson's lemma.

PROPOSITION 2.4.4. *Let $I \subseteq S$ be an ideal. Then $\langle \mathrm{lt}(I) \rangle$ is a monomial ideal, and there are $g_1, \ldots, g_s \in I$ such that $\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s) \rangle$.*

PROOF. The leading monomials $\mathrm{lm}(g)$ of elements $g \in I$, $g \neq 0$ generate the monomial ideal $\langle \mathrm{lm}(g) \mid g \in I, g \neq 0 \rangle$. Since $\mathrm{lm}(g)$ and $\mathrm{lt}(g)$ differ only by a nonzero constant, this ideal equals $\langle \mathrm{lt}(g) \mid g \in I, g \neq 0 \rangle = \langle \mathrm{lt}(I) \rangle$.
Since $\langle \mathrm{lt}(I) \rangle$ is generated by the monomials $\mathrm{lm}(g)$ for $g \in I, g \neq 0$, Dickson's lemma says that finitely many of them will already generate it, i.e.,

$$\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s) \rangle.$$

□

This implies again Hilbert's Basissatz:

THEOREM 2.4.5. *Every ideal $I \subseteq S$ is finitely generated: there exists a finite set $P \subseteq I$ with $\langle P \rangle = I$ and $\langle \mathrm{lt}(P) \rangle = \langle \mathrm{lt}(I) \rangle$.*

Here the zero ideal is generated by $f = 0$. The finite set $P = \{g_1, \ldots, g_s\}$ is also called *basis* of $I$, since it generates $I$ as an ideal by lemma 2.4.3. It has the nice property that $\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s) \rangle$. As we saw in example 2.4.2, not all bases behave this way. Therefore we will give this special bases the following name.

DEFINITION 2.4.6. Fix a monomial order on $\mathbb{N}^n$ and let $I \subseteq S$ be an ideal. A finite set $G \subseteq I$ is called *Gröbner basis* for $I$, if $\langle \mathrm{lt}(G) \rangle = \langle \mathrm{lt}(I) \rangle$.

COROLLARY 2.4.7. *Fix a monomial order on $\mathbb{N}^n$. Then every ideal $I \subseteq S$ has a Gröbner basis.*

Let us continue our example 2.4.2:

EXAMPLE 2.4.8. *Let $I = \langle f_1, f_2 \rangle$, where $f_1 = x^3 - 2xy$ and $f_2 = x^2y + x - 2y^2$ in $K[x, y]$, with the grlex order. Then $G = \{f_1, f_2\}$ is not a Gröbner basis. A possible Gröbner basis is given by*

$$G = \{f_1, f_2, x^2, 2xy, x - 2y^2\}.$$

We have already seen that $\langle \mathrm{lt}(G) \rangle = \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2) \rangle \neq \langle \mathrm{lt}(I) \rangle$, because

$$x^2 \in \langle \mathrm{lt}(I) \rangle \setminus \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2) \rangle.$$

Therefore $G = \{f_1, f_2\}$ is not a Gröbner basis. We will see later how to compute a Gröbner basis.

EXAMPLE 2.4.9. *Let $I = \langle g_1, g_2 \rangle$ in $K[x, y, z]$ with the lex order, where $g_1 = x + z$ and $g_2 = y - z$. Then $G = \{g_1, g_2\}$ is a Gröbner basis of $I$.*

In this case we can just check the definition. We have to show that

$$\langle \mathrm{lt}(I) \rangle \subseteq \langle \mathrm{lt}(G) \rangle = \langle \mathrm{lt}(g_1), \mathrm{lt}(g_2) \rangle = \langle x, y \rangle,$$

i.e., that the leading term of every nonzero element $f \in I$ lies in $\langle x, y \rangle$. By lemma 2.3.3 this is equivalent to showing that the leading term of any nonzero $f \in I$ is divisible by either $x$ or $y$. Suppose there is a nonzero $f \in I$ with $\mathrm{lt}(f)$ not divisible by either $x$ or $y$. Then $f$ must be a polynomial in $z$ alone. It must vanish on all points of $V(I)$, because $f \in I$. Now $(-t, t, t)$ is a point of $V(I)$ for all $t \in K$ since $g_i(-t, t, t) = 0$. In particular $f$ vanishes on all points $(-t, t, t) \in V(I)$, i.e., $f(t) = 0$ for all $t \in K$. This means $f = 0$ which is a contradiction.

REMARK 2.4.10. Gröbner bases were introduced 1965 by B. Buchberger and named by him in honor of his advisor W. Gröbner (1899-1980).

PROPOSITION 2.4.11. *Let $I \subseteq S$ be an ideal, $f \in S$ and $G = \{g_1, \ldots, g_s\}$ be a Gröbner basis of $I$. Then there exists a unique $r \in S$ such that $f - r \in I$ and no term of $r$ is divisible by any of $\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s)$.*

PROOF. The multivariate division algorithm gives $f = q_1 g_1 + \ldots + q_s g_s + r$ with the required properties for $r$. Recall that the remainder

$$r = f \mod (g_1, \ldots, g_s)$$

is only unique with respect to the given order of the polynomials $g_i$. It does depend on the order of the polynomials in general. But if these form a Gröbner basis for $I$ then $r$ is unique,

no matter how the elements of $G$ are listed when using the division algorithm. To prove the uniqueness of $r$ in this sense, suppose that $f = g + r = g' + r'$ both satisfy the requirements. Then $r - r' = g' - g \in I$. Assume that $r \neq r'$. Then

$$\mathrm{lt}(r - r') \in \langle \mathrm{lt}(I) \rangle = \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s) \rangle$$

By lemma 2.3.3 it follows that $\mathrm{lt}(r' - r)$ is divisible by some $\mathrm{lt}(g_i)$. This is impossible, since no term of $r$ and $r'$ is divisible by one of $\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s)$. Thus $r - r'$ must be zero, and the claim follows. □

COROLLARY 2.4.12. *The remainder $r$ of the multivariate division of $f$ by $G$ does not depend on the order of the elements of $G$. We will write*

$$r = f \mod G.$$

Now this property solves the ideal membership problem, provided we have a Gröbner basis of the ideal.

COROLLARY 2.4.13. *Let $I \subseteq S$ be an ideal and $G = \{g_1, \ldots, g_s\}$ be a Gröbner basis of $I$. Then for every polynomial $f \in S$ we have $f \in I$ if and only if $r = f \mod G$ equals zero:*

$$f \in I \Leftrightarrow r = 0.$$

PROOF. If $r = 0$ then clearly $f \in I$. Conversely, if $f \in I$, then $f = f + 0$ satisfies the conditions in proposition 2.4.11. Hence $r = 0$ is the unique remainder of $f$ on division by $G$. □

REMARK 2.4.14. It is not difficult to show that a set $G = \{g_1, \ldots, g_s\}$ is a Gröbner basis for $I$, if we have for all $f \in S$ the property

$$f \in I \Leftrightarrow f \mod G = 0.$$

Indeed, this is equivalent to $\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s) \rangle$.

We know that every ideal $I \subseteq S$ has a Gröbner basis, but we do not have an algorithm yet to such a basis - this will be provided by the *Buchberger algorithm*. If we take any generating set $\{f_1, \ldots, f_s\}$ of $I$, then the obstruction to being a Gröbner basis is the possible occurence of polynomial combinations of the $f_i$ whose leading terms are not in the ideal generated by the $\mathrm{lt}(f_i)$. One way this can occur is if the leading terms in a suitable combination $\lambda x^\alpha f_i - \mu x^\beta f_j$ cancel, leaving only smaller terms, such that the new leading term will not be divisible by any $\mathrm{lt}(f_i)$. On the other hand, $\lambda x^\alpha f_i - \mu x^\beta f_j \in I$, so that its leading term will be in $\langle \mathrm{lt}(I) \rangle$. Hence $\{f_1, \ldots, f_s\}$ is not a Gröbner basis.

EXAMPLE 2.4.15. *Let $I = \langle f_1, f_2 \rangle$ as in example 2.4.2, i.e.,*

$$f_1 = x^3 - 2xy$$
$$f_2 = x^2 y + x - 2y^2$$

*Then a suitable combination is $-yf_1 + xf_2 = x^2$, where $\mathrm{lt}(x^2) = x^2$ is not divisible by $\mathrm{lt}(f_1)$ or $\mathrm{lt}(f_2)$.*

To study this cancellation phenomenon, the following polynomials are introduced.

DEFINITION 2.4.16. Let $f, g \in S$ be nonzero polynomials with

$$\alpha = (\alpha_1, \ldots, \alpha_n) = \mathrm{mdeg}(f),$$
$$\beta = (\beta_1, \ldots, \beta_n) = \mathrm{mdeg}(g),$$
$$\gamma = (\max\{\alpha_1, \beta_1\}, \ldots, \max\{\alpha_n, \beta_n\}).$$

Then $x^\gamma$ is called the *least common multiple* of $\mathrm{lm}(f)$ and $\mathrm{lm}(g)$. The *S-polynomial* of $f$ and $g$ is defined by

$$S(f,g) = \frac{x^\gamma}{\mathrm{lt}(f)} \cdot f - \frac{x^\gamma}{\mathrm{lt}(g)} \cdot g.$$

An $S$-polynomial is designed to produce cancellation of leading terms. We have $S(f,g) = -S(g,f)$ and $S(f,g) \in \langle f, g\rangle$.

EXAMPLE 2.4.17. *Let $f_1, f_2 \in K[x,y]$ as above with the grlex order. Then $S(f_1,f_2) = -x^2$.*

We have $\alpha = \mathrm{mdeg}(f_1) = (3,0)$, $\beta = \mathrm{mdeg}(f_2) = (2,1)$, so that $\gamma = (3,1)$, and the least common multiple of $x^3$ and $x^2y$ is $x^\gamma = x^3y$. It follows that

$$S(f_1,f_2) = \frac{x^3y}{x^3} \cdot f_1 - \frac{x^3y}{x^2y} \cdot f_2 = yf_1 - xf_2 = -x^2.$$

EXAMPLE 2.4.18. *Let $f, g \in K[x,y]$ be given, with the grlex order by*

$$f = x^3y^2 - x^2y^3 + x,$$
$$g = 3x^4y + y^2.$$

*Then $S(f,g) = -x^3y^3 + x^2 - \frac{1}{3}y^3$.*

We have $\gamma = (4,2)$ and

$$\begin{aligned} S(f,g) &= \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g \\ &= x \cdot f - \frac{1}{3}y \cdot g \\ &= -x^3y^3 + x^2 - \frac{1}{3}y^3. \end{aligned}$$

The next lemma shows that all cancellation can be accounted for in principle by $S$-polynomials. As always, fix a monomial order $\prec$ on $S$, i.e., on $\mathbb{N}^n$.

LEMMA 2.4.19. *Let $f = \sum_{i=1}^s c_i f_i \in S$ with $f_i \in S$, $c_i \in K$ and $\mathrm{mdeg}(f_i) = \delta$ for all $i$. If $\mathrm{mdeg}(f) \prec \delta$, then we can write $f$ as a $K$-linear combination of $S$-polynomials $S(f_j, f_k)$ for $1 \le j, k \le s$,*

$$f = \sum_{1 \le j < k \le s} c_{jk} S(f_j, f_k),$$

*such that $\mathrm{mdeg}(S(f_j,f_k)) \prec \delta$ for all $1 \le j < k \le s$.*

PROOF. Let $d_i = \mathrm{lc}(f_i)$ so that $c_i d_i = \mathrm{lc}(c_i f_i)$. Since the $c_i f_i$ have multidegree $\delta$, but their sum has strictly smaller multidegree, it follows that

$$\sum_{i=1}^s c_i d_i = 0.$$

Let $p_i = f_i/d_i$. Then $p_i$ has leading coefficient $\mathrm{lc}(p_i) = 1$. Consider the telescoping sum

$$\begin{aligned} f &= \sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i d_i p_i \\ &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots + (\sum_{i=1}^{s-1} c_i d_i)(p_{s-1} - p_s) \\ &\quad + (c_1 d_1 + \cdots + c_s d_s) p_s. \end{aligned}$$

We have $\mathrm{lt}(f_i) = \mathrm{lc}(f_i)\,\mathrm{lm}(f_i) = d_i x^\delta$, so that the least common multiple of $\mathrm{lm}(f_j)$ and $\mathrm{lm}(f_k)$ equals $x^\delta$. It follows that

$$\begin{aligned} S(f_j, f_k) &= \frac{x^\delta}{\mathrm{lt}(f_j)} f_j - \frac{x^\delta}{\mathrm{lt}(f_k)} f_k \\ &= \frac{x^\delta}{d_j x^\delta} f_j - \frac{x^\delta}{d_k x^\delta} f_k \\ &= p_j - p_k. \end{aligned}$$

Using this equation and $\sum_{i=1}^{s} c_i d_i = 0$ the above telescoping sum becomes

$$\begin{aligned} f &= \sum_{i=1}^{s} c_i f_i \\ &= c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) + \cdots + (\sum_{i=1}^{s-1} c_i d_i) S(f_{s-1}, f_s). \end{aligned}$$

This is a sum of the desired form, since $c_i, d_i \in K$. Since $p_j$ and $p_k$ have multidegree $\delta$ and leading coefficient 1, the difference $p_j - p_k = S(f_j, f_k)$ has multidegree $\prec \delta$. □

Using the above lemma one can prove the following criterion of Buchberger for when a basis of an ideal in $S$ is a Gröbner basis.

THEOREM 2.4.20. *A finite set $G = \{g_1, \ldots, g_s\}$ of polynomials in $S$ is a Gröbner basis for the ideal $I = \langle G \rangle$, if and only if*

$$S(g_i, g_j) \mod G = 0 \quad \textit{for all } 1 \le i < j \le s.$$

PROOF. We will only give the idea of the proof. For the details see for example [**2**]. If $G$ is a Gröbner basis, then by corollary 2.4.13 the remainder of $S(g_i, g_j) \mod G$ is zero, since $S(g_i, g_j) \in I$. The converse direction is more difficult. Given $f \in I = \langle g_1, \ldots, g_s \rangle$ we can write $f = \sum_{i=1}^{s} h_i g_i$ with $h_i \in S$. Then

$$\mathrm{mdeg}(f) \le \max\{\mathrm{mdeg}(h_i g_i)\}.$$

Assume first that equality does not occur here. Then some cancellation must occur among the leading terms of $f = \sum_{i=1}^{s} h_i g_i$, and we can use lemma 2.4.19 to rewrite this in terms of $S$-polynomials. Our assumption that $S$-polynomials have zero remainders will allow us to replace the $S$-polynomials by expressions that involve less cancellation. In other words, we can write $f = \sum_{i=1}^{s} h_i' g_i$ with less cancellation of leading terms as before. Continuing in this way we will eventually find an expression $f = \sum_{i=1}^{s} h_i g_i$ with

$$\mathrm{mdeg}(f) = \max\{\mathrm{mdeg}(h_i g_i)\}.$$

The reason is that a monomial order is a well-ordering, so that we can select an expression $f = \sum_{i=1}^{s} h_i g_i$ such that $\delta = \max\{\text{mdeg}(h_1 g_1, \ldots, h_s g_s\}$ is minimal. Once this minimal $\delta$ is chosen one can show $\text{mdeg}(f) = \delta$. But then $\text{mdeg}(f) = \text{mdeg}(h_i g_i)$ for some $i$, so that $\text{lt}(f)$ is divisible by $\text{lt}(g_i)$. This will show that $\text{lt}(f) \in \langle \text{lt}(g_1), \ldots, \text{lt}(g_s) \rangle$, and hence that $G$ is a Gröbner basis for $I$. □

EXAMPLE 2.4.21. *Fix the lex order on $K[x, y, z]$ with $y \succ z \succ x$ and let $g_1 = y - x^2$, $g_2 = z - x^3$ in $K[x, y, z]$. Then $G = \{g_1, g_2\}$ is a Gröbner basis for $I = \langle g_1, g_2 \rangle$.*

We have $\text{mdeg}(g_1) = (1, 0, 0)$, $\text{mdeg}(g_2) = (0, 1, 0)$, so that the least common multiple is $x^\gamma = yz$, with $\gamma = (1, 1, 0)$. Then, using multivariate division, we have

$$\begin{aligned} S(g_1, g_2) &= \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) \\ &= -zx^2 + yx^3 \\ &= x^3 \cdot g_1 - x^2 \cdot g_2 + 0. \end{aligned}$$

This means $S(g_1, g_2) \mod G = 0$, so that $G$ is a Gröbner basis by theorem 2.4.20.

REMARK 2.4.22. It can be checked that $G$ is not a Gröbner basis for $I$ with repect to the lex order with $x \succ y \succ z$.

## 2.5. Buchberger's algorithm

Here comes now the algorithm due to Buchberger for computing a Gröbner basis. It is based on the criterion of theorem 2.4.20. We start with a generating set $\{f_1, \ldots, f_s\}$ for the ideal $I$ and then add each $S$-polynomial which does not satisfy the criterion. Since $S = K[x_1, \ldots, x_n]$ is Noetherian, this will terminate after a finite number of steps. The result is a Gröbner basis for $I$, which need not be minimal or unique yet.

*Input*: Nonzero polynomials $f_1, \ldots, f_s \in S$, and a monomial order $\prec$ on $\mathbb{N}^n$.

*Output*: A Gröbner basis $G$ for the ideal $I = \langle f_1, \ldots, f_s \rangle$ w.r.t. $\prec$ such that $f_i \in G$ for all $i$.

1. $G \leftarrow \{f_1, \ldots, f_s\}$.
2. repeat
3. $H \leftarrow \emptyset$
   order the elements of $G$ as $g_1, \ldots, g_t$.
   for $1 \leq i < j \leq t$ do
4. $r \leftarrow S(g_i, g_j) \mod (g_1, \ldots, g_t)$
   if $r \neq 0$ then $H \leftarrow H \cup \{r\}$.
5. if $H = \emptyset$ then return $G$
   else $G \leftarrow G \cup H$.

EXAMPLE 2.5.1. *Let $\{f_1, f_2\} = \{x^3 - 2xy, x^2y - 2y^2 + x\}$ in $K[x, y]$ with the grlex order, $y \prec x$. Then the algorithm gives the following Gröbner basis for the ideal $I = \langle f_1, f_2 \rangle$:*

$$G = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}.$$

As we have already seen, $S(f_1, f_2) = -x^2$ and $S(f_1, f_2) = 0 \cdot f_1 + 0 \cdot f_2 + (-x^2)$ by multivariate division. Hence $r = S(f_1, f_2) \mod (f_1, f_2) \neq 0$ and we set $H = \{-x^2\} = \{f_3\}$ and $G = \{f_1, f_2, f_3\}$. Then, by construction, $S(f_1, f_2) \mod (f_1, f_2, f_3) = 0$, but unfortunately $S(f_1, f_3) \mod (f_1, f_2, f_3) = -2xy \neq 0$:

$$\begin{aligned} S(f_1, f_3) &= \frac{x^3}{x^3} f_1 - \frac{x^3}{-x^2} f_3 \\ &= -2xy \end{aligned}$$

We put $f_4 = -2xy$ and $G = \{f_1, f_2, f_3, f_4\}$. Then

$$\begin{aligned} S(f_1, f_3) &\mod (f_1, \ldots, f_4) = 0, \\ S(f_1, f_4) &\mod (f_1, \ldots, f_4) = 0, \\ S(f_2, f_3) &\mod (f_1, \ldots, f_4) = -2y^2 + x \neq 0. \end{aligned}$$

Let $f_5 = -2y^2 + x$ and $G = \{f_1, f_2, f_3, f_4, f_5\}$. Then finally

$$S(f_i, f_j) \mod (f_1, \ldots, f_5) = 0 \quad \text{for all } 1 \leq i < j \leq 5.$$

PROPOSITION 2.5.2. *Buchberger's algorithm yields a Gröbner basis for $I$ after finitely many steps.*

PROOF. First it holds $G \subset I$ at every stage of the algorithm. Hence all $G$ are bases for the ideal $I$, as the first $G$ is already.

If $G$ and $G'$ correspond to successive stages in the algorithm, then $G' \supseteq G$ and $\langle \mathrm{lt}(G')\rangle \supseteq \langle \mathrm{lt}(G)\rangle$. Hence the ideals $\langle \mathrm{lt}(G)\rangle$ form an ascending chain for successive steps in the algorithm. Since $S$ is Noetherian, this terminates after finitely many steps with

$$\langle \mathrm{lt}(G')\rangle = \langle \mathrm{lt}(G)\rangle$$

for some $G'$. We claim that then $G' = G$, and this is a Gröbner basis for $I$. Let $g, h \in G$ and $r = S(g,h) \mod G$. Then $r \in G'$ and either $r = 0$ or $\mathrm{lt}(r) \in \langle \mathrm{lt}(G')\rangle = \langle \mathrm{lt}(G)\rangle$. Since no term of $r$ is divisible by some $\mathrm{lt}(g_i)$ we must have $r = 0$. By the criterion of theorem 2.4.20 we have obtained a Gröbner basis. □

The next question is about minimality and uniqueness of Gröbner bases.

LEMMA 2.5.3. *Let $G$ be a Gröbner basis for the ideal $I \subseteq S$. Let $p \in G$ be a polynomial such that $\mathrm{lt}(p) \in \langle \mathrm{lt}(G \setminus \{p\})\rangle$. Then $G \setminus \{p\}$ is also a Gröbner basis for $I$.*

PROOF. By assumption $\langle \mathrm{lt}(G)\rangle = \langle \mathrm{lt}(I)\rangle$. So we have

$$\langle \mathrm{lt}(G \setminus \{p\})\rangle = \langle \mathrm{lt}(G)\rangle = \langle \mathrm{lt}(I)\rangle$$

if $\mathrm{lt}(p) \in \langle \mathrm{lt}(G \setminus \{p\})\rangle$. Hence $G \setminus \{p\}$ is a Gröbner basis for $I$. □

By adjusting constants to make all leading coefficients 1 and removing any $p$ with $\mathrm{lt}(p) \in \langle \mathrm{lt}(G \setminus \{p\})\rangle$ from $G$, we arrive at a Gröbner basis which we call *minimal*.

DEFINITION 2.5.4. A Gröbner basis for an ideal $I \subseteq S$ is called *minimal*, if

(1) $\mathrm{lc}(p) = 1$ for all $p \in G$.
(2) We have $\mathrm{lt}(p) \notin \langle \mathrm{lt}(G \setminus \{p\})\rangle$ for all $p \in G$.

EXAMPLE 2.5.5. *Let $I = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$ in $K[x,y]$ with the grlex order, $y \prec x$, and Gröbner basis*

$$G = \{f_1, \ldots, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}.$$

*Then*

$$G' = \{g_3, g_4, g_5\} = \{x^2, xy, y^2 - \frac{1}{2}x\}$$

*is a minimal Gröbner basis of $I$.*

First we normalize the leading coefficients to 1, i.e., consider

$$G = \{g_1, \ldots, g_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, x^2, xy, y^2 - \frac{1}{2}x\}$$

Then we apply lemma 2.5.3. For $p = g_1$ we have $\mathrm{lt}(p) = x^3$ and $\mathrm{lt}(p) \in \langle \mathrm{lt}(G \setminus \{p\})\rangle = \langle \mathrm{lt}(g_2), \ldots, \mathrm{lt}(g_5)\rangle$, since $x\,\mathrm{lt}(g_3) = x^3 = \mathrm{lt}(p)$. Hence $\{g_2, \ldots, g_5\}$ is again a Gröbner basis. For $p = g_2$ we have $\mathrm{lt}(p) = x^2y = x\,\mathrm{lt}(g_4)$, so that $G' = \{g_3, g_4, g_5\}$ is a Gröbner basis of $I$. It is minimal, since now there are no further cases where some $\mathrm{lt}(g_i)$ divides some other $\mathrm{lt}(g_j)$.

REMARK 2.5.6. A given ideal may have many minimal Gröbner bases. For example, for the ideal $I$ considered above, for every $\lambda \in K$,

$$G' = \{g_3 + \lambda g_4, g_4, g_5\} = \{x^2 + \lambda xy, xy, y^2 - \frac{1}{2}x\}$$

is a minimal Gröbner basis of $I$.

We can achieve uniqueness of minimal Gröbner bases as follows:

DEFINITION 2.5.7. A Gröbner basis $G$ for an ideal $I \subseteq S$ is called *reduced*, if

(1) $\mathrm{lc}(p) = 1$ for all $p \in G$.
(2) For all $p \in G$, no monomial of $p$ lies in $\langle \mathrm{lt}(G \setminus \{p\})\rangle$.

Obviously a reduced Gröbner basis is minimal. Note that in the above remark for $p = x^2 + \lambda xy$ the monomial $\lambda xy$ does lie in $\langle \mathrm{lt}(G \setminus \{p\})\rangle$ for all $\lambda \neq 0$. Hence the only minimal Gröbner basis there which is reduced is the one with $\lambda = 0$.

It is not difficult to prove the following result, see for example [**2**].

PROPOSITION 2.5.8. *Let $I \subseteq S$ be an ideal, other than 0, and fix a monomial order. Then $I$ has a unique reduced Gröbner basis.*

If $I = S$, then $G = \{1\}$ is a reduced Gröbner basis for $I$.

As a consequence of the unique reduced Gröbner basis we have an algorithm for deciding the following problems:

1. *The ideal equality problem*: when generate two sets of polynomials the same ideal ? Let $I = \langle f_1, \ldots, f_s\rangle$ and $J = \langle g_1, \ldots, g_t\rangle$. Fix a monomial order and compute a reduced Gröbner basis $G_I$ for $I$, and $G_J$ for $J$. Then $I = J$ if and only if $G_I = G_J$.

EXERCISE 2.5.9. *Consider the following ideals in $K[x, y]$,*

$$I = \langle x^2 + y - 1, xy - x\rangle,$$
$$J = \langle x^2 + y^2 - 1, xy - 1, x + x^3 - y\rangle$$

*Is $I = J$ ? As a hint, $J = K[x, y]$.*

2. *The ideal membership problem*: for a given ideal $I = \langle f_1, \ldots, f_s\rangle$, is the polynomial $f \in S$ contained in $I$ ? Let $G$ be a Gröbner basis of $I$ (not necessarily reduced). Then we know that $f \in I$ if and only if $f \mod G = 0$.

EXAMPLE 2.5.10. *Let $I = \langle xz - y^2, x^3 - z^2\rangle$ in $K[x, y, z]$ with the grlex order, and*

$$f = -4x^2y^2z^2 + y^6 + 3z^5,$$
$$g = xy - 5z^2 + x.$$

*Then $f \in I$ but $g \notin I$.*

A reduced Gröbner basis of $I$ is given by

$$G = \{f_1, \ldots, f_5\} = \{xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5\}.$$

The division algorithm yields

$$f = 0 \cdot f_1 + 0 \cdot f_2 + (-4z^2) \cdot f_3 + 0 \cdot f_4 + 1 \cdot f_5 + 0.$$

This shows $f \in I$. On the other hand, $g \mod G = g \neq 0$, so that $g \notin I$. Here $\mathrm{lt}(g) = xy$ is not contained in $\langle \mathrm{lt}(G)\rangle = \langle xz, x^3, x^2y^2, xy^4, y^6\rangle$.

3. *The Problem of solving polynomial equations*: given a finite set of polynomials $\{f_1, \ldots, f_s\}$ we want so solve the system of polynomial equations

$$f_i = 0, \quad i = 1, \ldots, s.$$

If $I = \langle f_1, \ldots, f_s\rangle$, then we want to find all points in $V(I)$. We can compute $V(I)$ using *any* basis of $I$, in particular a reduced Gröbner basis.

EXAMPLE 2.5.11. *Consider the system of polynomial equations over the complex numbers given by $f_1 = f_2 = f_3 = 0$ with*

$$\begin{aligned} f_1 &= x^2 + y + z - 1, \\ f_2 &= x + y^2 + z - 1, \\ f_3 &= x + y + z^2 - 1. \end{aligned}$$

*Then there are exactly five solutions for $(x, y, z)$, namely*

$$\begin{aligned} (x, y, z) &= (1, 0, 0), \\ &= (0, 1, 0), \\ &= (0, 0, 1), \\ &= (\sqrt{2} - 1, \sqrt{2} - 1, \sqrt{2} - 1), \\ &= (-\sqrt{2} - 1, -\sqrt{2} - 1, -\sqrt{2} - 1). \end{aligned}$$

Indeed, the reduced Gröbner basis with respect to the lex order $x \succ y \succ z$ is given by

$$\begin{aligned} g_1 &= x + y + z^2 - 1, \\ g_2 &= y^2 - y - z^2 + z, \\ g_3 &= 2yz^2 + z^4 - z^2, \\ g_4 &= z^6 - 4z^4 + 4z^3 - z^2 \\ &= z^2(z - 1)^2(z^2 + 2z - 1). \end{aligned}$$

To solve $f_i = 0$ is equivalent to solving $g_j = 0$. In particular, $g_4 = 0$ implies that $z$ is one of the following: $\{0, 1, -1 \pm \sqrt{2}\}$. Now we solve the system recursively by substituting $z$ into the other equations. For example, if $z = 0$ then $y = 0, x = 1$ or $y = 1, x = 0$. Note that we take $x = y = z$ in the original equations, then we obtain exactly the equation $z^2 + 2z - 1 = 0$, which has the solutions $z = \pm\sqrt{2} - 1$.

It is very easy however, to come up with similar examples which are much harder to treat. Here is one, again in $K[x, y, z]$ which is less trivial but still not too difficult:

EXAMPLE 2.5.12. *Consider the system of polynomial equations over the complex numbers given by $f_1 = f_2 = f_3 = 0$ with*

$$\begin{aligned} f_1 &= x^2 + yz + y^3, \\ f_2 &= y^2 + xz + z^3, \\ f_3 &= z^2 + xy + x^3. \end{aligned}$$

The reduced Gröbner basis with respect to the lex order is given by

$$
\begin{aligned}
g_1 = {} & 266651036x^2 + 266651036yz + 197658338z^{22} - 117772397z^{21} \\
& - 1086272125z^{20} + 1400326574z^{19} + 1418506608z^{18} - 4458555302z^{17} \\
& + 2165256016z^{16} + 6216650326z^{15} - 8114466480z^{14} + 2035628240z^{13} \\
& + 6194533388z^{12} - 14268851402z^{11} + 6689390272z^{10} + 11950174712z^9 \\
& - 13259733192z^8 - 126800716z^7 + 5778117836z^6 - 1805173560z^5 \\
& - 320960896z^4 + 266651036z^3,
\end{aligned}
$$

$$
\begin{aligned}
g_2 = {} & 266651036xy + 90898956z^{22} + 171270038z^{21} - 625218259z^{20} \\
& - 612698984z^{19} + 2173709956z^{18} - 341132318z^{17} - 3933066550z^{16} \\
& + 5106508968z^{15} + 3317575086z^{14} - 7922158412z^{13} + 4875953022z^{12} \\
& + 30874218z^{11} - 13278867924z^{10} + 12624023320z^9 + 7606158440z^8 \\
& - 13975832532z^7 + 2781942668z^6 + 4562650032z^5 - 2500340976z^4 \\
& + 266651036z^3 + 266651036z^2,
\end{aligned}
$$

$$
g_3 = xz + y^2 + z^3,
$$

$$
\begin{aligned}
g_4 = {} & 266651036y^3 - 197658338z^{22} + 117772397z^{21} + 1086272125z^{20} \\
& - 1400326574z^{19} - 1418506608z^{18} + 4458555302z^{17} - 2165256016z^{16} \\
& - 6216650326z^{15} + 8114466480z^{14} - 2035628240z^{13} - 6194533388z^{12} \\
& + 14268851402z^{11} - 6689390272z^{10} - 11950174712z^9 + 13259733192z^8 \\
& + 126800716z^7 - 5778117836z^6 + 1805173560z^5 + 320960896z^4 \\
& - 266651036z^3,
\end{aligned}
$$

$$
\begin{aligned}
g_5 = {} & 533302072y^2z - 32095249z^{22} + 160583612z^{21} + 74662950z^{20} \\
& - 1041538486z^{19} + 803109772z^{18} + 1846032136z^{17} - 3520673110z^{16} \\
& + 411935250z^{15} + 5803156092z^{14} - 6045137960z^{13} - 96651104z^{12} \\
& + 5917877460z^{11} - 11339845416z^{10} + 2931161224z^9 + 11342387608z^8 \\
& - 7995131872z^7 - 1478749104z^6 + 3126060360z^5 - 556549268z^4, \\
g_6 = {} & 533302072yz^2 - 34894929z^{22} + 52776600z^{21} + 133473826z^{20} \\
& - 359534350z^{19} + 216069032z^{18} + 581218192z^{17} - 1344783470z^{16} \\
& + 287419382z^{15} + 1684866956z^{14} - 2735063864z^{13} + 1370693620z^{12} \\
& + 2925527428z^{11} - 3742802752z^{10} + 2233420272z^9 + 1636689360z^8 \\
& - 4443920640z^7 + 1233856416z^6 + 1255711744z^5 - 372500964z^4, \\
g_7 = {} & z^{23} - 6z^{21} + 4z^{20} + 12z^{19} - 20z^{18} - 2z^{17} + 42z^{16} - 28z^{15} \\
& - 16z^{14} + 48z^{13} - 64z^{12} - 12z^{11} + 96z^{10} - 48z^9 - 40z^8 + 48z^7 \\
& - 8z^6 - 12z^5 + 8z^4.
\end{aligned}
$$

Here $g_7$ factors as

$$
\begin{aligned}
g_7 = {} & (z^{18} - 2z^{17} - 2z^{16} + 8z^{15} - 4z^{14} - 12z^{13} + 22z^{12} - 2z^{11} - 24z^{10} \\
& + 32z^9 - 16z^8 - 32z^7 + 52z^6 - 8z^5 - 32z^4 + 24z^3 - 8z + 4)(z + 2)z^4
\end{aligned}
$$

If $z = 0$ then $(x, y, z) = (0, 0, 0)$, which is a solution. For $z = -2$ we obtain $(x, y, z) = (-2, -2, -2)$. Finally, if $z$ is a root of the polynomial of degree 18, then $x$ and $y$ are uniquely determined by $z$. In fact, $y$ can be eliminated using the polynomial $g_6$, and then $x$ can be eliminated using $g_3$, i.e.,

$$x = \frac{-y^2 + z^3}{z}.$$

Then the remaining equations are consistent, so that we obtain exactly 20 solutions over $\mathbb{C}$. A numerical computation shows what the 20 values for $z$ are (the zeros of $g_7$):

$$
\begin{aligned}
z &= 0,\\
z &= -2,\\
z &= 1.54015732321 + 0.463262016331i,\\
z &= 1.54015732321 - 0.463262016331i,\\
z &= 0.997047698794 + 0.166159838803i,\\
z &= 0.997047698794 - 0.166159838803i,\\
z &= 0.70789851038 + 0.432159362393i,\\
z &= 0.70789851038 - 0.432159362393i,\\
z &= 0.692142876572 + 1.22976808183i,\\
z &= 0.692142876572 - 1.22976808183i,\\
z &= 0.316537971626 + 0.583040691616i,\\
z &= 0.316537971626 - 0.583040691616i,\\
z &= -0.016429162242 + 1.14949458231i,\\
z &= -0.016429162242 - 1.14949458231i,\\
z &= -0.865681713034 + 0.0468836084754i,\\
z &= -0.865681713034 - 0.0468836084754i,\\
z &= -1.13430447898 + 0.225954608016i,\\
z &= -1.13430447898 - 0.225954608016i,\\
z &= -1.23736902632 + 0.59844023101i,\\
z &= -1.23736902632 - 0.59844023101i.
\end{aligned}
$$

In particular, the only solutions over $\mathbb{R}$ (and over $\mathbb{Q}$) are given by $(x, y, z) = (0, 0, 0)$ and $(x, y, z) = (-2, -2, -2)$.

CHAPTER 3

# Module Theory

## 3.1. Modules

Modules are like vector spaces except that the scalars come from a commutative ring instead from a field. It turns out, however, that this difference is an important one. The theory of modules is much more difficult than the theory of vector spaces.

DEFINITION 3.1.1. Let $R$ be a commutative ring (always with 1). A *module over* $R$, or an $R$-module is an abelian group $M$, written additively, together with an operation $R \times M \to M$, $(r, m) \mapsto rm$ satisfying

(1) $r(m+n) = rm + rn$
(2) $(r+s)m = rm + sm$
(3) $(rs)m = r(sm)$
(4) $1m = m$

for all $r, s \in R$ and $n, m \in M$.

Obviously, for $R$ being a field, these are the axioms of a vector space. Thus every vector space over a field $K$ is a $K$-module.

EXAMPLE 3.1.2. *The ring $R$ itself is an $R$-module. More generally, every ideal $I$ of $R$ is an $R$-module, and also the residue class ring $R/I$.*

For $M = R$ the operation $(r, m) \mapsto rm$ is just the ring multiplication. Since $RI \subseteq I$, also $I$ is an $R$-module. It is easy to check that the mapping $R \times R/I \to R/I$, $(r, s+I) \mapsto rs+I$ is well-defined and that $R/I$ becomes an $R$-module with respect to this operation.

EXAMPLE 3.1.3. *The $\mathbb{Z}$-modules are exactly the abelian groups.*

Every $\mathbb{Z}$-module is an abelian group by forgetting the multiplication. Every abelian group $(G, +)$ becomes a $\mathbb{Z}$-module by $kg = g + \cdots + g$ for $k \geq 0$ and $-kg = -g - \cdots - g$.

EXAMPLE 3.1.4. *Let $V$ be a vector space over a field $K$ and $\varphi \in \mathrm{End}(V)$. Then $V$ becomes a $K[x]$-module by $f(x)v = f(\varphi)(v)$ for $f \in K[x]$, $v \in V$.*

DEFINITION 3.1.5. Let $M, N$ be two $R$-modules. A map $\varphi\colon M \to N$ is called a *hohomorphism of $R$-modules* if

(1) $\varphi(m+n) = \varphi(m) + \varphi(n)$,
(2) $\varphi(rm) = r\varphi(m)$

for all $r \in R$ and $n, m \in M$. We denote the module homomorphisms by $\mathrm{Hom}_R(M, N)$.

Note that $\mathrm{Hom}_R(M, N)$ itself becomes an $R$-module by

$$(rf)(m) = rf(m),$$
$$(f+g)(m) = f(m) + g(m).$$

for $r \in R$, $m \in M$ and $f, g \in \mathrm{Hom}_R(M, N)$. We have $\mathrm{Hom}_R(R, N) \simeq N$.

DEFINITION 3.1.6. A subgroup $N$ of an $R$-module $M$ is called an *$R$-submodule* of $M$, if $rn \in N$ for all $r \in R$, $n \in N$.

The submodules of the $R$-module $R$ are just the ideals of $R$. If $\varphi\colon M \to N$ is an $R$-module homomorphism, then $\ker(\varphi) = \{m \in M \mid \varphi(m) = 0\}$ is a submodule of $M$, and

$$M/\ker(\varphi) \simeq \operatorname{im}(\varphi).$$

PROPOSITION 3.1.7. *For $R$-modules $L \subseteq M \subseteq N$ we have*

$$N/M \simeq (N/L)/(M/L).$$

*If $M, N$ are submodules of $L$ then*

$$N/(M \cap N) \simeq (M + N)/M.$$

Let $M$ be an $R$-module and $T \subseteq M$ be a subset. Then there exists a minimal submodule $\langle T\rangle$ of $M$ which contains $T$. We have

$$\langle T\rangle = \{\sum_{t\in T} r_t t \mid r_t \in R\},$$

where $r_t = 0$ for almost all $t$.

DEFINITION 3.1.8. Let $M$ be an $R$-module. A subset $T \subseteq M$ is called a *generating set* of $M$ if $M = \langle T\rangle$. The minimal number of *generators*, if it exists, $x_i \in T$ is called the *rank* of $M$. The $R$-module $M$ is called *free*, if $M$ has generators $x_i$ such that every representation $\sum r_i x_i = 0$ implies $r_i = 0$ for all $i$. Such a set of free generators is called *basis* of $M$.

Every module of rank $n$ over a field $K$ is free and has a basis.

EXAMPLE 3.1.9. *The $\mathbb{Z}$-module $M = \mathbb{Z}/n\mathbb{Z}$ for $n \geq 2$ has rank 1 and is not free.*

This follows from the fact that every free $R$-module of rank $n$ is isomorphic to $R^n = R \oplus \cdots \oplus R$. But $M \simeq \mathbb{Z}$ here is impossible, since $|M| = n$.

PROPOSITION 3.1.10. *The $R$-module $R^n$ is free of rank $n$, and every free module of rank $n$ is isomorphic to $R^n$.*

PROOF. The first statement follows from the definitions. If $M$ is a free module of rank $n$, with generating set $T = \{x_1, \ldots, x_n\}$, then the homomorphism $f\colon R^n \to M$, $(r_1, \ldots, r_n) \mapsto \sum_i r_i x_i$ is surjective and injective. □

Denote by $M_n(R)$ the ring of $n \times n$-matrices over a commutative ring $R$. Then $\det(A)$ is defined for $A \in M_n(R)$, and $AB = \det(A)E$, where $B$ is the adjoint matrix of $A$.

LEMMA 3.1.11. *Let $M$ be a finitely generated $R$-module, $I \subseteq R$ and ideal and $f \in \operatorname{End}_R(M)$ with $f(M) \subseteq IM$. Then $f$ satisfies an operator equality*

$$f^n + a_1 f^{n-1} + \cdots + a_n = 0.$$

*with $a_i \in I$.*

PROOF. Let $T = \{x_1, \ldots, x_n\}$ be a generating set of $M$. Then $f(x_i) \in IM$, hence there are $a_{ij} \in I$ such that

$$f(x_i) = \sum_j a_{ij} x_j.$$

Consider now the matrix $A = (f\delta_{ij} - a_{ij})$ in $M_n(R[f])$. Then $Ax = 0$, where $x$ denotes the column vector formed by the $x_i$. Multiplying with the adjoint matrix of $A$ we obtain $\det(A)x_i = 0$ for all $i$, so that $\det(A) = 0$ in $\mathrm{End}_R(M)$. But $\det(A)$ is a polynomial in $f$. □

COROLLARY 3.1.12 (Nakayama's Lemma). *Let $M$ be a finitely generated $R$-module and $I$ be an ideal of $R$ such that $IM = M$. Then $(1 - a)M = 0$ for some $a \in I$. In particular, if $I \neq R$ and if $R$ is a local ring, then $M = 0$.*

PROOF. Choose $f = \mathrm{id}$ in the above lemma. Then there are $a_i \in I$ such that $E + a_1E + \cdots + a_nE = 0$ in $\mathrm{End}_R(M)$. Let $a = -\sum_{i=1}^{n} a_i$. Then $(1 - a)M = 0$. If $R$ is a local ring, $1 - a$ is a unit, since $1 - a$ is not contained in the maximal ideal of $R$ and hence $(1 - a) = R$. Then $M = 0$. □

## 3.2. Tensor products of modules

Let $M, N, P$ be three $R$-modules. A map $f\colon M \times N \to P$ is called $R$-bilinear, if the map $N \to P$, $n \mapsto f(m,n)$ is a homomorphism of $R$-modules for every $m \in M$, and if the map $M \to P$, $m \mapsto f(m,n)$ is a homomorphism of $R$-modules for every $n \in N$. Explicitly this means:

DEFINITION 3.2.1. A map $f\colon M \times N \to P$ is called *$R$-bilinear*, if for all $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ and all $r \in R$

$$\begin{aligned} f(m, n_1 + n_2) &= f(m, n_1) + f(m, n_2), \quad & f(m, rn) &= rf(m, n), \\ f(m_1 + m_2, n) &= f(m_1, n) + f(m_2, n), \quad & f(rm, n) &= rf(m, n). \end{aligned}$$

Denote the set of all $R$-bilinear maps $f\colon M \times N \to P$ by $\mathrm{Bil}_R(M, N, P)$.

REMARK 3.2.2. Note that an $R$-bilinear map $f\colon M \times N \to P$ does not induce a homomorphism of $R$-modules $M \oplus N \to P$, since

$$f(r(m,n)) = f(rm, rn) = r^2 f(m,n)$$

need not be equal to $rf(m,n)$ in general.

We will define an $R$-module $T$ and an $R$-module isomorphism

$$\mathrm{Bil}_R(M, N, P) \simeq \mathrm{Hom}_R(T, P),$$

$T$ being the same for all $P$, as follows: let $L$ be the free $R$-module with a basis consisting of elements $l_{m,n}$, indexed by the elements of $M \times N$. An arbitrary element of $L$ is a finite sum $\sum_i r_i l_{m_i,n_i}$ with $r_i \in R$, $m_i \in M$ and $n_i \in N$. Define $K$ to be the $R$-submodule of $L$ generated by the elements

$$\begin{gathered} l_{m_1+m_2,n} - l_{m_1,n} - l_{m_2,n}, \\ l_{m,n_1+n_2} - l_{m,n_1} - l_{m,n_2}, \\ l_{rm,n} - r l_{m,n}, \\ l_{m,rn} - r l_{m,n} \end{gathered}$$

for all $r \in R$, $m \in M$ and $n \in N$. Let $T = L/K$ and denote the image of $l_{m,n}$ in $T$ (i.e., the coset $l_{m,n} + K$) by $m \otimes n$. Since $L$ is generated by all $l_{m,n}$, the $R$-module $T$ is generated by all $m \otimes n$, i.e.,

$$T = \{\sum_i r_i m_i \otimes n_i \mid r_i \in R, m_i \in M, n_i \in N\}.$$

By definition the generators satisfy the following relations:

$$\begin{aligned} m \otimes (n_1 + n_2) &= m \otimes n_1 + m \otimes n_2, \quad & m \otimes (rn) &= r(m \otimes n), \\ (m_1 + m_2) \otimes n &= m_1 \otimes n + m_2 \otimes n, \quad & rm \otimes n &= r(m \otimes n). \end{aligned}$$

In particular we have $n \otimes 0 = 0(n \otimes 1) = 0$.

DEFINITION 3.2.3. The module $T$ is denoted by $M \otimes_R N$ and is called the *tensor product* of $M$ and $N$ over $R$.

Define the map $g\colon M \times N \to M \otimes_R N$ by $g(m,n) = m \otimes n$. It is an $R$-bilinear map.

PROPOSITION 3.2.4. *For any $R$-bilinear map $f\colon M\times N\to P$ define the map $\hat{f}\colon M\otimes_R N\to P$ by $\hat{f}(\sum_i r_i m_i\otimes n_i)=\sum_i r_i f(m_i,n_i)$. This is a well-defined map and a homomorphism of $R$-modules. The correspondence $f\mapsto\hat{f}$ gives an isomorphism of the $R$-modules $\mathrm{Bil}_R(M,N,P)$ and $\mathrm{Hom}_R(M\otimes_R N,P)$.*

PROOF. Extend $f$ to a module homomorphism $L\to P$ by $l_{m,n}\mapsto f(m,n)$. Since $f$ is $R$-bilinear, all generators of $K$ are mapped to zero. We obtain a map $\hat{f}=\alpha(f)$ as above. Then $\alpha$ is a homomorphism of $R$-modules. Conversely, for a given $\hat{f}\in\mathrm{Hom}_R(M\otimes_R N,P)$ define $f=\beta(\hat{f})\colon M\times N\to P$ by $f(m,n)=(\hat{f}\circ g)(m,n)$. Then $\beta$ is an $R$-module homomorphism.

$$\begin{array}{ccc} M\times N & \xrightarrow{f} & P \\ {\scriptstyle g}\downarrow & \nearrow_{\hat{f}} & \\ M\otimes_R N & & \end{array}$$

It remains to show that $\alpha\circ\beta=\mathrm{id}$ and $\beta\circ\alpha=\mathrm{id}$, so that $\alpha$ and $\beta$ are isomorphisms of $R$-modules. We have

$$\begin{aligned}(\alpha\circ\beta)(\hat{f})\left(\sum_i r_i m_i\otimes n_i\right)&=\alpha(\hat{f}\circ g)\left(\sum_i r_i m_i\otimes n_i\right)\\&=\sum_i r_i(\hat{f}\circ g)(m_i,n_i)\\&=\hat{f}\left(\sum_i r_i m_i\otimes n_i\right)\end{aligned}$$

and

$$\begin{aligned}(\beta\circ\alpha)(f)(m,n)&=(\alpha(f)\circ g)(m,n)\\&=\alpha(f)(m\otimes n)\\&=f(m,n).\end{aligned}$$

□

REMARK 3.2.5. We can also define the tensor product of two $R$-modules $M$ and $N$ by a universal property. The tensor product of $M$ and $N$ is an $R$-module $T$ together with an $R$-bilinear map $g\colon M\times N\to T$, which satisfies the following universal property. For every $R$-module $P$ and every bilinear map $f\colon M\times N\to P$ there exists a unique linear map $\hat{f}\colon T\to P$ with $\hat{f}\circ g=f$. See the commuting diagram above.
As usual the tensor product is uniquely determined by this universal property, and the existence is just the construction we have given above.

PROPOSITION 3.2.6. *We list some first properties of the tensor product:*

(1) $M\otimes_R R\simeq M$.
(2) $M\otimes_R N\simeq N\otimes_R M$.
(3) $(M\otimes_R N)\otimes_R P\simeq M\otimes_R(N\otimes_R P)$.
(4) $M\otimes_R(N\oplus P)\simeq(M\otimes_R N)\oplus(M\otimes_R P)$.

PROOF. (1): Define an $R$-module homomorphism $f\colon L \to M$ by $l_{m,r} \to rm$, where $L$ is a free $R$-module with basis $l_{m,r}$ for $m \in M$ and $r \in R$. Then $K \subseteq \ker(f)$ (for the definition of $K$ see above). Hence $f$ induces an $R$-module homomorphism $g\colon M \otimes_R R = L/K \to M$, $m \otimes r \to rm$. Let $h\colon M \to M \otimes_R R$, $m \mapsto m \otimes 1$. Then $g \circ h = \mathrm{id}, h \circ g = id$.

(2): We have $R$-module homomorphisms $f\colon M \otimes N \to N \otimes M$, $m \otimes n \mapsto n \otimes m$ and $g\colon N \otimes M \to M \otimes N$, $n \otimes m \mapsto m \otimes n$, which are inverse to each other.

(3): Use the obvious homomorphisms $m \otimes (n \otimes p) \mapsto (m \otimes n) \otimes p$ and $(m \otimes n) \otimes p \mapsto m \otimes (n \otimes p)$.

(4): Use $m \otimes (n, p) \mapsto (m \otimes n, m \otimes p)$ and $(m_1 \otimes n, m_2 \otimes p) \mapsto m_1 \otimes (n, 0) + m_2 \otimes (0, p)$. □

EXAMPLE 3.2.7. *For $n, m \in \mathbb{Z}$ and any $\mathbb{Z}$-module $M$ we have*

(1) $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} = 0$.
(2) $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}$.
(3) $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z}$, *where $d$ is the gcd of $m$ and $n$.*
(4) $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} M \simeq M/mM$.

We have

$$\begin{aligned}\frac{p}{q} \otimes (k + m\mathbb{Z}) &= m\frac{p}{qm} \otimes (k + m\mathbb{Z}) \\ &= \frac{p}{qm} \otimes (mk + m\mathbb{Z}) \\ &= \frac{p}{qm} \otimes 0 = 0.\end{aligned}$$

This implies (1). Recall that $\mathbb{Z}/m\mathbb{Z}$ is not a free $\mathbb{Z}$-module. For (2) define $f\colon \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathbb{Q}$, $m \otimes n \mapsto mn$. It is clear that $f$ is surjective. Suppose that $\sum_i m_i \otimes n_i \in \ker(f)$. Then $\sum_i m_i n_i = 0$. Let $q$ be the least common multiple of denominators of $n_i$. Then $n_i = r_i/q$ for integers $r_i$. We obtain

$$\sum_i m_i \otimes n_i = \sum_i m_i r_i \otimes \frac{1}{q} = 0.$$

Thus $f$ is an isomorphism.
Property (3) will follow from (4), which is a special case of the following lemma.

LEMMA 3.2.8. *Let $M$ be an $R$-module and $I$ be an ideal in $R$. Then we have*

$$R/I \otimes_R M \simeq M/IM.$$

PROOF. The map $f\colon R/I \times M \to M/IM$, $(\overline{r}, m) \mapsto rm$ is well-defined and bilinear. By the universal property of the tensor product there is a homomorphism $\hat{f}\colon R/I \otimes_R M \to M/IM$ with $\hat{f}(\overline{r} \otimes m) = \overline{rm}$. It is clear that $\hat{f}$ is surjective. It remains to show that $\hat{f}$ is also injective. Let $x = \sum_i \overline{r_i} \otimes m_i \in \ker(\hat{f})$. Since

$$x = \sum_i \overline{1} \otimes r_i m_i = \overline{1} \otimes \left( \sum_i r_i m_i \right)$$

we can write $x = \overline{1} \otimes m$. By assumption $\hat{f}(x) = 0$, so that $m \in IM$, i.e., $m = \sum_j a_j n_j$, with $a_j \in I$ and $n_j \in M$. This means

$$x = \sum_j \overline{a_j} \otimes n_j = \sum_j 0 \otimes n_j = 0.$$

□

COROLLARY 3.2.9. *The $R$-modules $R^m$ and $R^n$ are isomorphic if and only if $m = n$.*

PROOF. Assume that $R^m \simeq R^n$. Choose a maximal ideal $M$ in $R$. Then

$$\begin{aligned}(R/M)^m &\simeq R^m/MR^m \\ &\simeq R/M \otimes_R R^m \\ &\simeq R/M \otimes_R R^n \\ &\simeq (R/M)^n.\end{aligned}$$

Both are vector spaces over the field $R/M$, hence it follows $m = n$. □

DEFINITION 3.2.10. Let $M$ be an $R$-module. The $R$-module

$$M^* := \mathrm{Hom}_R(M, R)$$

is called the *dual module* to $M$.

For example, if $R = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$, then $M^* = 0$. We have a bilinear pairing $M \times M^* \to R$ given by $(m, f) \mapsto f(m)$, which induces a homomorphism $M \otimes_R M^* \to R$ and a homomorphism $M \to (M^*)^*$.

If $M, N$ are $R$-modules and $L$ is a submodule of $M$ then, then $L \otimes N$ in general cannot be considered as a submodule of $M \otimes N$, i.e., the canonical map $L \otimes N \to M \otimes N$ need not be injective.

EXAMPLE 3.2.11. *For $R = \mathbb{Z}$, $M = R = \mathbb{Z}$, $L = 2\mathbb{Z}$ and $N = \mathbb{Z}/2\mathbb{Z}$ the canonical map $L \to M$ is injective, but $L \otimes N \to M \otimes N$ is not.*

First we have $2 \otimes 1 = 1 \otimes 2 = 1 \otimes 0 = 0$ in $\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$. On the other hand, $2 \otimes 1$ is non-zero in $2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$: let $f\colon 2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ be the $R$-linear map given by

$$f(x, y) = \frac{\overline{x}}{2} \cdot y.$$

Then there exists an $R$-linear map $\hat{f}\colon 2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ with $\hat{f}(2 \otimes 1) = f(2, 1) = 1 \cdot 1 = 1$, hence $2 \otimes 1 \neq 0$, since otherwise $\hat{f}(0) = 0$. It follows that $2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$ cannot be considered as a submodule of $\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$.

## 3.3. Localization

The localization of $R$-modules is defined in a similar way as for rings. Let $R$ be a ring, $S \subset R$ be a multiplicatively closed subset and $M$ be an $R$-module. Define an equivalence relation on the set of all ordered pairs of $M \times S$ as follows: given any $(m, s), (n, t) \in M \times S$,

$$(m, s) \sim (n, t) \iff u(mt - ns) = 0 \text{ for some } u \in S.$$

By $S^{-1}M$ we denote the set of equivalence classes $m/s$. This set has the structure of an $S^{-1}R$-module with respect to

$$\frac{m}{s} + \frac{n}{t} = \frac{mt + ns}{st},$$
$$\frac{r}{s} \cdot \frac{n}{t} = \frac{rn}{st}$$

for $m, n \in M$, $s, t \in S$ and $r \in R$. This $S^{-1}R$-module is called the localization (or quotient module) of $M$ with respect to $S$. For $m \in M$ and $s \in S$ we have $m/s = 0$ in $S^{-1}M$ if and only if there exists a $t \in S$ such that $tm = 0$. The map

$$g \colon M \to S^{-1}M, \quad m \mapsto \frac{m}{1}$$

for all $m \in M$ is a homomorphism of $R$-modules when we regard $S^{-1}M$ as an $R$-module by restriction of scalars via the natural ring homomorphism $R \to S^{-1}R$. The kernel of $g$, also denotes as $S$-torsion of $M$, is given by

$$Tor_S(M) = \ker(g) = \{m \in M \mid am = 0 \text{ for some } a \in S\}.$$

Example 3.3.1. *For a prime ideal $P$ and $S = R \setminus P$ we obtain the $R_P$-module $M_P = S^{-1}M$.*

Recall that $R_P = S^{-1}R$ is a local ring, see example 1.2.13.

Proposition 3.3.2. *Suppose that $f \colon N \to M$ is a homomorphism of $R$-modules and let $S$ be a multiplicatively closed subset of $R$. Then $f$ induces an homomorphism $S^{-1}f \colon S^{-1}N \to S^{-1}M$ for which*

$$(S^{-1}f)(\frac{a}{s}) = \frac{f(a)}{s}.$$

*for all $a \in N$, $s \in S$.*

Proof. Suppose that $a, b \in N$ and $s, t \in S$ are given such that $a/s = b/t$ in $S^{-1}N$. Then there exists $u \in S$ such that $u(ta - sb) = 0$. It follows

$$\begin{aligned} 0 &= uf(ta - sb) \\ &= u(tf(a) - sf(b)) \end{aligned}$$

in $M$, so that $f(a)/s = f(b)/t$ in $S^{-1}M$. This shows that the map given above is well-defined. It is easy to see that it is a homomorphism of $S^{-1}R$-modules. □

Remark 3.3.3. In the language of homological algebra $F = S^{-1}$ can be thought of as an additive, covariant functor from the category of $R$-modules to the category of $S^{-1}R$-modules.

Proposition 3.3.4. *Let $S$ be a multiplicatively closed subset of $R$ and $M$ be an $R$-module. Then there is an isomorphism of $S^{-1}R$-modules*

$$S^{-1}R \otimes_R M \simeq S^{-1}M.$$

PROOF. Consider the $R$-bilinear map $f\colon S^{-1}R \times M \to S^{-1}M$ given by

$$f(\frac{a}{s}, m) = \frac{am}{s}.$$

By the universal property of the tensor product there exists an $S^{-1}R$-module homomorphism $g\colon S^{-1}R \otimes_R M \to S^{-1}M$ satisfying

$$g(\frac{a}{s} \otimes m) = \frac{am}{s}.$$

We will show that $g$ is bijective. Clearly $g$ is surjective. To show injectivity, pick an element of the kernel of $g$,

$$x = \sum_{i=1}^{n} \frac{a_i}{s_i} \otimes m_i \in \ker(g).$$

With $s = s_1 s_2 \cdots s_n$ we can write $x = (1/s) \otimes m$ for some $m \in M$. By assumption we have $m/s = g(x) = 0$ in $S^{-1}M$. This means that there exists a $t \in S$ such that $mt = 0$. It follows that

$$\begin{aligned} x &= \frac{1}{s} \otimes m \\ &= \frac{t}{st} \otimes m \\ &= \frac{1}{st} \otimes tm = 0. \end{aligned}$$

□

DEFINITION 3.3.5. A sequence of $R$-modules and $R$-module homomorphisms

$$\cdots \to M_{n-1} \xrightarrow{f_n} M_n \xrightarrow{f_{n+1}} M_{n+1} \to \cdots$$

is called exact at $M_n$ if $\operatorname{im} f_n = \ker f_{n+1}$. The sequence is called *exact* if it is exact at each module.

EXAMPLE 3.3.6. *The sequence $0 \to M \xrightarrow{f} N$ is exact if and only if $f$ is a monomorphism. The sequence $M \xrightarrow{f} N \xrightarrow{g} 0$ is exact if and only if $f$ is an epimorphism.*

In the first case the image of the map $0 \to M$ is zero, so that $\ker(f) = 0$. Similarly, $\operatorname{im}(f) = \ker(g) = N$ in the second case.

EXAMPLE 3.3.7. *A short exact sequence is given by*

$$0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$$

From the exactness we conclude that $f$ is injective, $g$ is surjective and

$$L \simeq \operatorname{im}(f) = \ker(g)$$

is a submodule of $M$. Sometimes we will identify $L$ with its image $f(L)$. Furthermore we have $M/\ker(g) \simeq g(M) = N$, hence

$$N \simeq M/L.$$

LEMMA 3.3.8. *Let $L \xrightarrow{f} M \xrightarrow{g} N$ be an exact sequence of $R$-modules, and let $S$ be a multiplicatively closed subset of $R$. Then*

$$S^{-1}L \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}N$$

*is exact too.*

PROOF. Since $\ker(g) = \mathrm{im}(f)$ we have $g \circ f = 0$. It follows that

$$S^{-1}g \circ S^{-1}f = S^{-1}(g \circ f) = S^{-1}(0) = 0,$$

so that $\mathrm{im}(S^{-1}f) \subseteq \ker(S^{-1}g)$. Conversely, let $x \in \ker(S^{-1}g)$. Then there exists $m \in M$ and $s \in S$ such that $x = m/s$ and $g(m)/s = (S^{-1}g)(m/s) = 0$. This means $tg(m) = 0$ for some $t \in S$, i.e., $g(tm) = 0$ and $tm \in \ker(g) = \mathrm{im}(f)$. Then $tm = f(a)$ for some $a \in L$. Thus

$$\begin{aligned} x = \frac{m}{s} &= \frac{tm}{ts} \\ &= \frac{f(a)}{ts} \\ &= (S^{-1}f)(\frac{a}{ts}) \end{aligned}$$

which is in $\mathrm{im}(S^{-1}f)$. □

REMARK 3.3.9. The functor $F = S^{-1}$ is *exact*, i.e., it takes short exact sequences to short exact sequences. To see this apply lemma 3.3.8 also to $0 \to M \to N$ and $M \to N \to 0$.

As we have seen in example 3.2.11, an exact sequence $0 \to L \to M$ does not imply in general that the sequence $0 \to L \otimes N \to M \otimes N$ is exact. The tensor product functor is not left exact. However, it is right exact.

PROPOSITION 3.3.10. *If $L \to M \to N \to 0$ is an exact sequence of $R$-modules, so is $L \otimes F \to M \otimes F \to N \otimes F \to 0$ for any $R$-module $F$.*

We leave the proof as an exercise.

REMARK 3.3.11. An $R$-module $F$ is called *flat* if the above tensor product functor is also left exact, i.e., is exact. This means, that for a flat module $F$ and any exact sequence $L \to M \to N$, the sequence $L \otimes F \to M \otimes F \to N \otimes F$ is again exact. For example, $R$ is a flat $R$-module.

(1) Every projective (hence every free) $R$-module is flat. Recall that a free module is projective, hence flat.

(2) If $R$ is a PID, then an $R$-module $F$ is flat if and only it is $R$-torsionfree, i.e., if $rm = 0$ for $r \in R$, $m \in M$ always implies $r = 0$ or $m = 0$.

(3) For any multiplicatively closed subset $S \subset R$, the localization ring $S^{-1}R$ is flat as an $R$-module.

## 3.4. Noetherian Modules

The concept of a Noetherian ring is generalized as follows:

DEFINITION 3.4.1. An $R$-module $M$ is called *Noetherian*, if every every submodule of $M$ is finitely generated.

Recall that an $R$-module is finitely generated if and only if there exists a surjective $R$-module homomorphism $R^n \to M$. If $R$ is regarded as a module over itself then $R$ is a Noetherian $R$-module if and only if $R$ is a Noetherian ring. For example, the $\mathbb{Z}$-module $\mathbb{Z}$ is Noetherian, as $\mathbb{Z}$ is a PID, hence a Noetherian ring (every submodule is generated by a single element).

EXAMPLE 3.4.2. *The $\mathbb{Z}$-module $\mathbb{Q}$ is not Noetherian, as it is not finitely generated.*

EXAMPLE 3.4.3. *A finite-dimensional vector space over a field $K$ is a Noetherian $K$-module.*

PROPOSITION 3.4.4. *Let $M$ be an $R$-module. The following statements are equivalent:*

1. *$M$ is a Noetherian $R$-module.*
2. *In $M$ holds the ascending chain condition: if $M_1, M_2, \ldots$ are submodules of $M$ with $M_1 \subseteq M_2 \subseteq \cdots$, then there exists an $m \geq 1$ such that $M_n = M_m$ for all $n \geq m$.*
3. *In $M$ holds the maximality condition: every nonempty set of submodules of $M$ has a maximal element.*

The proof is more or less the same as the proof of proposition 1.3.3 for Noetherian rings.

LEMMA 3.4.5. *Let $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ be a short exact sequence of $R$-modules. If $M$ is finitely generated so is $N$. If $L$ and $N$ are finitely generated, so is $M$.*

PROOF. If $(v_1, \ldots, v_n)$ is a generating set for $M$ then $(g(v_1), \ldots, g(v_n))$ is a generating set for $N$. This shows the first claim. If $(x_1, \ldots, x_r)$ is a generating set of $L$, and $(y_1, \ldots, y_s)$ is one for $N$, then one chooses $z_i \in M$ such that $g(z_i) = y_i$. Then $(x_1, \ldots, x_r, z_1, \ldots, z_s)$ is a generating set for $M$. □

REMARK 3.4.6. If $M$ is finitely generated then $L$ need not be finitely generated in general. For example, let $R = K[x_1, x_2, \ldots]$ be the polynomial ring in infinitely many variables $x_i, i \in \mathbb{N}$. Then $M = R$ is clearly finitely generated, but the submodule $L = (x_1, x_2, \ldots)$ of $M$ is not finitely generated. Of course, $M$ is not Noetherian.

LEMMA 3.4.7. *Let $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ be a short exact sequence of $R$-modules. Then $M$ is Noetherian if and only if $L$ and $N$ are Noetherian.*

PROOF. Suppose that $M$ is Noetherian. Then $L$ is Noetherian, since every submodule of $L$ is, under $f$, isomorphic to a submodule of $M$, hence finitely generated. Furthermore $N$ is Noetherian, since every submodule of $N$ is a homomorphic image of a submodule of $M$, hence finitely generated. Conversely assume that $L$ and $N$ are Noetherian, and let $F$ be a submodule of $M$. Then we have an exact sequence

$$0 \to f^{-1}(F) \to F \to g(F) \to 0$$

where the maps are the restrictions of $f$ and $g$. Now lemma 3.4.5 implies that $F$ is finitely generated, since $f^{-1}(F)$ and $g(F)$ are finitely generated. □

LEMMA 3.4.8. *Let $M_1, \ldots, M_n$ be Noetherian $R$-modules. Then $M_1 \oplus \cdots \oplus M_n$ is a Noetherian $R$-module.*

PROOF. We may assume that $n = 2$. Consider the exact sequence

$$0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$$

and apply lemma 3.4.7. It follows that $M_1 \oplus M_2$ is Noetherian. □

PROPOSITION 3.4.9. *Every finitely generated $R$-module $M$ over a Noetherian ring $R$ is Noetherian.*

PROOF. By assumption there is a surjective module homomorphism $R^n \to M$ for some $n \geq 1$. Since $R$ is a Noetherian $R$-module, so is $R^n$ by lemma 3.4.8. Then $M$ is Noetherian by lemma 3.4.7. □

PROPOSITION 3.4.10. *Let $S$ be a multiplicatively closed subset of $R$. If $M$ is a Noetherian $R$-module, the its localization $S^{-1}M$ is a Noetherian $S^{-1}R$-module.*

PROOF. First, every submodule of $S^{-1}M$ is of the form $S^{-1}N$ for a submodule $N$ of $M$. By assumtion $N$ is finitely generated, say, by $(n_1, \ldots, n_s)$. It follows that $S^{-1}N$ is generated by $(n_1/1, \ldots, n_s/1)$. □

CHAPTER 4

# Integral Extensions

All rings here (frequently denoted by $A, B, C$) are assumed to be commutative and with unity, if not said otherwise. We will study *integral ring extensions*, which are certain ring extensions, as an analogue to algebraic field extensions. They play an important role for many applications in algebraic geometry and algebraic number theory.

## 4.1. Integral elements

Let $A$ be a subring of a ring $B$. An element $x \in B$ is called *integral over* $A$, if there exists a monic polynomial $f \in A[t]$ with $f(x) = 0$, i.e., if $x$ satisfies a polynomial equation

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0$$

with $a_i \in A$. For example, every $x \in A$ is integral over $A$. If $A$ and $B$ are fields, then $x \in B$ is integral over $A$ if and only if $x$ is algebraic over $A$.

EXAMPLE 4.1.1. *Let $A = \mathbb{Z}$ and $B = \mathbb{C}$. Then $\sqrt{2}$ is integral over $\mathbb{Z}$, but $\frac{1}{2}$ is not.*

The polynomial for $\sqrt{2}$ is $f(t) = t^2 - 2$ in $\mathbb{Z}[t]$. Assume that there is a monic polynomial $f \in \mathbb{Z}[t]$ with coefficients $a_i$ as above, and $f(\frac{1}{2}) = 0$. Multiplying with $2^n$ we obtain

$$1 + 2a_1 + \cdots + 2^n a_n = 0,$$

which is a contradiction modulo 2.

DEFINITION 4.1.2. The ring $B$ is called an *integral extension* of $A$, if every element of $B$ is integral over $A$. We also say that $B/A$ is an integral ring extension.

PROPOSITION 4.1.3. *Let $A$ be a subring of a ring $B$, and $x \in B$. Then the following statements are equivalent:*

(1) *The element $x$ is integral over $A$.*
(2) *The ring $A[x]$ is a finitely generated $A$-module.*
(3) *The ring $A[x]$ is contained in a subring $C \subseteq B$, such that $C$ is a finitely generated $A$-module.*

PROOF. (1) $\Rightarrow$ (2): by assumption there is an $f \in A[x]$, $f = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$ with $f(x) = 0$. For all $j \geq 0$ it follows that

$$x^{n+j} = -(a_1 x^{n+j-1} + a_2 x^{n+j-2} + \cdots + a_{n-1} x^{j+1} + a_n x^j).$$

By induction we see that this implies $x^k \in A[1, x, x^2, \ldots, x^{n-1}]$ for all $k \geq 0$, considered as an $A$-module. This means that the ring $A[x]$ is generated as an $A$-module by the finitely many elements $1, x, x^2, \ldots, x^{n-1}$.
(2) $\Rightarrow$ (3): Put $C = A[x]$. Of course, $A[x] \subseteq B$.

(3) $\Rightarrow$ (1): Let $C$ be generated as an $A$-module by the finitely many elements $c_1, c_2, \ldots, c_n$. We have $A \subseteq A[x] \subseteq C \subseteq B$. Hence all $xc_i$ are contained in $C$, so that there exist $a_{ij} \in A$ with

$$xc_i = \sum_{j=1}^{n} a_{ij} c_j.$$

Let $M = (m_{ij}) \in M_n(A[x])$ be the matrix with $m_{ij} = \delta_{ij}x - a_{ij}$. Denote by $M'$ the adjoint matrix of $M$. We have $M'M = \det(M)I_n$. Let $u = (c_1, \ldots, c_n)^t$, then $M'Mu = 0$ and $\det(M)c_i = 0$ for all $i = 1, \ldots, n$. It follows $\det(M)c = 0$ for all $c \in C = \sum_{i=1}^{n} Ac_i$. Since $C$ contains the unit element 1 as a subring of $B$, we obtain $\det(M) = 0$. This yields the polynomial for $x$ we are looking for: $\det(M) = \det(\delta_{ij}x - a_{ij})$ has degree $n$ in $x$ with coefficients in $A$. □

COROLLARY 4.1.4. *Let $C$ be a finitely generated $A$-module. Then $C/A$ is an integral ring extension.*

COROLLARY 4.1.5. *Let $A$ be a subring of a ring $B$. Then we have*

(1) *If $x_1, \ldots, x_n$ are elements in $B$ which are integral over $A$, then the ring $A[x_1, \ldots, x_n]$ is a finitely generated $A$-module.*
*In particular, $A[x_1, \ldots, x_n]/A$ is an integral ring extension.*

(2) *Let $C$ be a ring containing $B$. If $B$ is a finitely generated $A$-module, and $y \in C$ is integral over $B$, then $y$ is also integral over $A$.*

PROOF. (1): We prove this by induction on $n \geq 1$. The case $n = 1$ has been proved above as the implication (1) $\Rightarrow$ (2). Let $n \geq 2$. By assumption $A[x_1, \ldots, x_{n-1}]$ is finitely generated as an $A$-module. Furthermore $A[x_1, \ldots, x_n]$ is finitely generated as an $A[x_1, \ldots, x_{n-1}]$-module, since $x_n$ is also integral over $A[x_1, \ldots, x_{n-1}]$. Like before this implies the claim.
(2): The ring $B[y]$ is a finitely generated $B$-module. By assumption $B$ is finitely generated as an $A$-module, so that $B[y]$ is finitely generated as an $A$-module, too. Because of $A[y] \subseteq B[y]$ the claim follows from proposition 4.1.3. □

Now we show that integral ring extensions are transitive.

PROPOSITION 4.1.6. *Let $B/A$ and $C/B$ be integral ring extensions. Then $C/A$ is an integral ring extension.*

PROOF. Let $c \in C$. Since $C$ is integral over $B$ there exist $n \geq 1$ and $b_i \in B$ such that

$$c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0.$$

Since the $b_i$ are integral over $A$ we know that $A[b_0, \ldots, b_{n-1}]$ is a finitely generated $A$-module. Because of the above equation $c$ is integral over $A[b_0, \ldots, b_{n-1}]$. Hence $A[b_0, \ldots, b_{n-1}, c]$ is a finitely generated $A[b_0, \ldots, b_{n-1}]$-module. In particular $A[b_0, \ldots, b_{n-1}, c]$ is a finitely generated $A$-module so that $c$ is integral over $A$. □

The following definition is a proposition as well.

DEFINITION 4.1.7. Let $A$ be a subring of a ring $B$. Then the elements $b \in B$, which are integral over $A$ form a subring of $B$. This ring, denoted by $\overline{A}$ is called the *integral closure* of $A$ in $B$. If $A = \overline{A}$ then $A$ is called *integrally closed* in $B$.

Note that $A \subseteq \overline{A}$, because each $a \in A$ is a root of the polynomial $x - a$. If $x, y \in B$ are integral over $A$, then $A[x, y]$ is a finitely generated $A$-module containing $x + y, x - y$ and $xy$. Hence all these elements are again integral over $A$. This shows that $\overline{A}$ is a subring of $B$.

DEFINITION 4.1.8. A domain (Integritätsbereich) is called *integrally closed* (ganz abgeschlossen), or *normal*, if it is integrally closed in its quotient field.

EXAMPLE 4.1.9. *The domain $\mathbb{Z}$ is integrally closed.*

We have $\overline{\mathbb{Z}} = \mathbb{Z}$ in $\mathbb{Q}$, because every $x \in \mathbb{Q}$ satisfying a polynomial equation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ with $a_i \in \mathbb{Z}$ must be an integer (see the proof of the next result).

PROPOSITION 4.1.10. *Every factorial ring is integrally closed.*

PROOF. Let $A$ be a factorial ring with quotient field $K$ (for example, $A = \mathbb{Z}$ and $K = \mathbb{Q}$). Let $a/s \in K$, with $a, s \in A$ and $s \neq 0$, be integral over $A$. We may assume that $a$ and $s$ have no common divisors. We want to show that $a/s \in A$. There exist $n \geq 1$ and $a_0, \ldots, a_{n-1} \in A$ such that

$$(a/s)^n + a_{n-1}(a/s)^{n-1} + \cdots + a_1(a/s) + a_0 = 0.$$

Multiplying with $s^n$ we obtain

$$a^n + sa_{n-1}a^{n-1} + \cdots + s^{n-1}a_1a + s^n a_0 = 0,$$

which implies $s \mid a^n$. Since $A$ is factorial and $a$ and $s$ have no common prime divisors, it follows that $s$ is a unit in $A$, i.e., $a/s \in A$. □

If we take the integral closure of the integral closure, we get nothing new.

PROPOSITION 4.1.11. *The integral closure $\overline{A}$ of $A$ in $B$ is integrally closed in $B$, i.e., $\overline{\overline{A}} = \overline{A}$.*

PROOF. We have $\overline{A} \subseteq \overline{\overline{A}}$. Conversely, let $x \in \overline{\overline{A}}$. Then $x$ is integral over $\overline{A}$. As in the proof of proposition 4.1.6 we conclude that $x$ is integral over $A$. It follows that $x \in \overline{A}$. □

PROPOSITION 4.1.12. *Let $A$ be a domain with quotient field $K$, and let $L/K$ be an algebraic field extension. If $A$ is integrally closed, then an element $\alpha \in L$ is integral over $A$ if and only if the minimal polynomial $m_{\alpha,K}(x)$ of $\alpha$ over $K$ lies in $A[x]$.*

PROOF. Suppose that $m_{\alpha,K} \in A[x]$. Since $m_{\alpha,K}(x)$ is a monic polynomial, $\alpha$ is integral over $A$. Conversely, suppose that $\alpha$ is integral over $A$. Then there is a $f \in A[x]$, $f \neq 0$ with $f(\alpha) = 0$. Then $m_{\alpha,K} \mid f$ in $K[x]$. Over an algebraic closure $\overline{L}$ of $L$ the polynomial splits as

$$m_{\alpha,K}(x) = \prod_{i=1}^{n}(x - \alpha_i)$$

with suitable $\alpha_i \in \overline{L}$. Here $m_{\alpha,K} \mid f$ implies $f(\alpha_i) = 0$ for all $i \geq 1$. Hence every $\alpha_i$ is integral over $A$, and so are all coefficients of $m_{\alpha,K}$. But these coefficients by definition lie in $K$. Since $A$ is integrally closed we have $m_{\alpha,K} \in A[x]$. □

EXAMPLE 4.1.13. *With $A = \mathbb{Z}$, $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{d})$, $d \neq 1$ squarefree it follows that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\sqrt{d}]$ for $d \equiv 2, 3 \mod 4$ and $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ for $d \equiv 1 \mod 4$.*

Clearly $\sqrt{d} \in L$ is integral over $\mathbb{Z}$, because its minimal polynomial $x^2 - d$ lies in $\mathbb{Z}[x]$. For $d \equiv 1 \mod 4$ also $(1+\sqrt{d})/2$ is integral over $\mathbb{Z}$, being a zero of $x^2 - x + \frac{1-d}{4}$. Hence every element of the ring

$$\mathcal{O}_d = \mathbb{Z} \oplus \mathbb{Z}\omega_d$$

is integral over $\mathbb{Z}$, where $\omega_d = (1+\sqrt{d})/2$ for $d \equiv 1 \mod 4$ and $\omega_d = \sqrt{d}$ otherwise. We even have $\overline{\mathbb{Z}}^L = \mathcal{O}_d$, i.e., $\mathcal{O}_d$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{d}]$: every element $\alpha \in \mathbb{Q}[\sqrt{d}]$ can be written uniquely as $\alpha = a + b\sqrt{d}$, with $a, b \in \mathbb{Q}$. If $\alpha$ is integral over $\mathbb{Z}$ then the minimal polynomial $m_\alpha = x^2 - 2ax + a^2 - db^2$ has integer coefficients by proposition 4.1.12 (also called the trace and the norm of $\alpha$), i.e., $2a \in \mathbb{Z}$ and $a^2 - db^2 \in \mathbb{Z}$. Then either $a, b \in \mathbb{Z}$, or $a, b \in \frac{1}{2} + \mathbb{Z}$. The second alternative can only appear if $d \equiv 1 \mod 4$.

PROPOSITION 4.1.14. *Let $A$ be a subring of the integral domain $B$, and let $B$ be integral over $A$. Then $A$ is a field if and only if $B$ is a field.*

PROOF. Assume first that $B$ is a field, and let $a \in A$ be a nonzero element. Since $a^{-1} \in B$, there is by assumption an equation of the form

$$(a^{-1})^n + c_{n-1}(a^{-1})^{n-1} + \cdots + c_1 a^{-1} + c_0 = 0$$

with $c_i \in A$. By multiplying the equation with $a^{n-1}$ we get

$$a^{-1} = -(c_{n-1} + \cdots + c_1 a^{n-2} + c_0 a^{n-1}) \in A.$$

Hence $A$ is a field. Conversely, assume that $A$ is a field, and let $b$ be a nonzero element of $B$. Since $b$ is integral over $A$, $A[b]$ is a finitely generated $A$-module, i.e., a finite-dimensional vector space over the field $A$. Let $f$ be the $A$-linear transformation on this vector space given by left multiplication with $b$, i.e., $f(z) = bz$ for $z \in A[b]$. Since $A[b]$ is a subring of $B$, it is an integral domain. Thus if $bz = 0$ (recall that $b \neq 0$), we have $z = 0$ and $f$ is injective. Any injective linear transformation on a finite-dimensional vector space is also surjective. Therefore, if $b \in B$ with $b \neq 0$, there is an element $c \in A[b] \subseteq B$ such that $bc = 1$. Consequently, $B$ is a field. □

DEFINITION 4.1.15. Let $B/A$ be an integral ring extension. Suppose that $Q$ is a prime ideal of $B$ and let $P = Q \cap A$. Then $P$ is a prime ideal of $A$ and we say that $Q$ *lies over* $P$.

Indeed, $P$ is the preimage of $Q$ under the inclusion map $A \hookrightarrow B$. Hence it is prime by lemma 1.2.25. The map $a + P \mapsto a + Q$ is a well-defined injection $A/P \hookrightarrow B/Q$, because $P = Q \cap A$. Thus we can regard $A/P$ as a subring of $B/Q$.

LEMMA 4.1.16. *Let $B$ be integral over $A$, $Q$ be a prime ideal of $B$ and $P$ the prime ideal $Q \cap A$ as above. Then $B/Q$ is integral over $A/P$.*

PROOF. Let $b + Q \in B/Q$. Then $b \in B$ satisfies an equation of the form

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

with $a_i \in A$. Apply the canonical homomorphism $\pi\colon B \to B/Q$ to this equation. This shows that $b + Q$ is integral over $A/P$, since the $a_i$ are mapped to $a_i + P$. □

PROPOSITION 4.1.17. *Let $B$ integral over the subring $A$, and let $Q$ be a prime ideal of $B$, lying over the prime ideal $P = Q \cap A$ of $A$. Then $P$ is a maximal ideal of $A$ if and only if $Q$ is a maximal ideal of $B$.*

PROOF. By the above lemma, $B/Q$ is integral over $A/P$. Then, by proposition 4.1.14, $B/Q$ is a field if and only $A/P$ is a field. But this is just the claim. □

## 4.2. Integrality and Localization

For a multiplicatively closed set $S$ we always want to have $0 \notin S$. We start with the following lemma.

LEMMA 4.2.1. *Let $B/A$ be an integral ring extension and $S$ be a multiplicatively closed subset of $A$. Then $S^{-1}B$ is integral over $S^{-1}A$.*

PROOF. Let $b/s \in S^{-1}B$ with $b \in B$ and $s \in S$. Then there is an equation of the form

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

with $a_i \in A$. Thus

$$\left(\frac{b}{s}\right)^n + \left(\frac{a_{n-1}}{s}\right)\left(\frac{b}{s}\right)^{n-1} + \cdots + \left(\frac{a_1}{s^{n-1}}\right)\left(\frac{b}{s}\right) + \frac{a_0}{s^n} = 0$$

with $a_{n-j}/s^j \in S^{-1}A$. □

PROPOSITION 4.2.2. *Let $B/A$ be an integral ring extension, and let $Q_1, Q_2$ be prime ideals of $B$ that lie over the prime ideal $P$ of $A$, that is, $Q_1 \cap A = Q_2 \cap A = P$. If $Q_1 \subseteq Q_2$, then $Q_1 = Q_2$.*

PROOF. We use the technique of localization. The result is clear, if $P$ is a maximal ideal, because then also $Q_1$ and $Q_2$ are maximal by proposition 4.1.17. In the general case we localize with respect to $P$. Then $S = A \setminus P$ is a multiplicatively closed subset of $A \subseteq B$. The prime ideals $Q_1, Q_2$ do not meet $S$, because if $x \in S \cap Q_i$, then $x \in A \cap Q_i = P$, contradicting $S = A \setminus P$. By (4) of proposition 1.2.22 the prime ideals in $B$ which do not meet $S$ are in one-to-one correspondence with the prime ideals in $S^{-1}B = B_P$. We also write $S^{-1}A = A_P$ for the localization. To show that $Q_1 = Q_2$ it hence suffices to show that $Q_1 B_P = Q_2 B_P$. We claim that

$$PA_P \subseteq (Q_1 B_P) \cap A_P \subsetneq A_P.$$

The first inclusion holds because $P \subseteq Q_1$ and $A_P \subseteq B_P$. The second inclusion is clear, but it is even proper, for otherwise $A_P \subseteq Q_1 B_P$ and therefore $1 \in Q_1 B_P$, contradicting the fact that $Q_1 B_P$ is a prime ideal. But $PA_P$ is a maximal ideal of $A_P$, as we know. So, by the above claim we obtain

$$PA_P = (Q_1 B_P) \cap A_P$$

We argue the same way for $Q_2$ and obtain

$$PA_P = (Q_2 B_P) \cap A_P$$

Thus $Q_1 B_P$ and $Q_2 B_P$ lie over $PA_P$. By lemma 4.2.1, $B_P$ is integral over $A_P$. Again by proposition 4.1.17, $Q_1 B_P$ and $Q_2 B_P$ are maximal ideals, since $PA_P$ is maximal. If $Q_1 \subseteq Q_2$, then $Q_1 B_P \subseteq Q_2 B_P$. Maximality then implies $Q_1 B_P = Q_2 B_P$. □

REMARK 4.2.3. The result is also called the *incomparability theorem*. This becomes understandable if we rephrase the result as follows: If $Q_1, Q_2$ are two different prime ideals of $B$ which lie over the same prime ideal $P$ in $A$, then $Q_1$ and $Q_2$ are *incomparable* in the sense that neither is contained in the other, i.e., neither $Q_1 \subset Q_2$ nor $Q_2 \subset Q_1$.

REMARK 4.2.4. The proof shows that the technique of localization sometimes can be applied to extend results, which hold for maximal ideals, also to prime ideals.

THEOREM 4.2.5 (Lying Over Theorem). *If $B$ is integral over $A$ and $P$ is a prime ideal of $A$, then there exists a prime ideal $Q$ of $B$ which lies over $P$, that is, with $Q \cap A = P$.*

PROOF. First assume that $A$ is a local ring with unique maximal ideal $P$. If $Q$ is any maximal ideal of $B$, then $Q \cap A$ is maximal by proposition 4.1.17, so that we must have $Q \cap A = P$. In general, let $S = A \setminus P$ and localize. We have the following commutative diagram:

$$\begin{array}{ccc} A & \longrightarrow & B \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ A_P & \longrightarrow & B_P \end{array}$$

In fact, the horizontal maps are inclusions, and the vertical maps are $f(a) = a/1$ and $g(b) = b/1$. We know that $B_P$ is integral over $A_P$ by lemma 4.2.1. If $Q'$ is any maximal ideal of $B_P$, then as at the beginning of the proof, $Q' \cap A_P$ must be the unique maximal ideal of $A_P$, namely $PA_P$. By commutativity of the diagram,

$$f^{-1}(Q' \cap A_P) = g^{-1}(Q') \cap A.$$

Note here that for $a \in A$ we have $f(a) \in Q' \cap A_P$ if and only if $g(a) \in Q'$. Now we choose $Q$ as $g^{-1}(Q')$. This means $f^{-1}(PA_P) = Q \cap A$. By the correspondence of prime ideals of the localization and the base ring we must have $f^{-1}(PA_P) = P$. It follows that $Q \cap A = P$. □

THEOREM 4.2.6 (Going up Theorem). *Let $B$ be integral over $A$, and suppose that we have a chain of prime ideals $P_1 \subseteq \cdots \subseteq P_n$ of $A$, and a chain of prime ideals $Q_1 \subseteq \cdots \subseteq Q_m$ of $B$ with $m < n$. If $Q_i$ lies over $P_i$ for all $i = 1, \ldots, m$, then there are $n - m$ prime ideals $Q_{m+1}, \ldots, Q_n$ of $B$ such that*

$$Q_1 \subseteq \cdots \subseteq Q_m \subseteq Q_{m+1} \subseteq \cdots \subseteq Q_n$$

*and $Q_i$ lies over $P_i$ for every $i = 1, \ldots, n$.*

PROOF. By induction, it suffices to consider the case $n = 2$ and $m = 1$. Thus we have prime ideals $P_1 \subseteq P_2$ of $A$ and a prime ideal $Q_1$ of $B$ with $Q_1 \cap A = P_1$. By lemma 4.1.16, $B/Q_1$ is integral over $A/P_1$. Since $P_2/P_1$ is a prime ideal of $A/P_1$, we may apply the lying over theorem 4.2.5 to produce a prime ideal $Q_2/Q_1$ of $B/Q_1$ such that

$$(Q_2/Q_1) \cap (A/P_1) = P_2/P_1,$$

where $Q_2$ is a prime ideal of $B$ with $Q_2 \supseteq Q_1$. We claim that $Q_2 \cap A = P_2$ which gives the desired extension of the chain of the $Q_i$. To verify this, let $x \in Q_2 \cap A$. Since we have an embedding of $A/P_1$ into $B/Q_1$ (see the discussion after definition 4.1.15), we have

$$x + P_1 = x + Q_1 \in (Q_2/Q_1) \cap (A/P_1) = P_2/P_1.$$

Thus $x + P_1 = y + P_1$ for some $y \in P_2$, so $x - y \in P_1 \subseteq P_2$. Consequently, $x \in P_2$. This shows $Q_2 \cap A \subseteq P_2$. Conversely, if $x \in P_2$ then $x + P_1 \in Q_2/Q_1$, hence $x + P_1 = y + Q_1$ for some $y \in Q_2$. But as above, $x + P_1 = x + Q_1$, so $x - y \in Q_1$, and therefore $x \in Q_2$. Finally, $x \in P_2 \subseteq A$. This finishes the proof. □

It is well known that an embedding of a field $K$ in an algebraically closed field can be extended to an algebraic extension of $K$. There is an analogous result for ring extensions.

PROPOSITION 4.2.7. *Let $B$ be integral over $A$, and let $f\colon A \to C$ be a ring homomorphism from $A$ into an algebraically closed field $C$. Then $f$ can be extended to a ring homomorphism $g\colon B \to C$.*

PROOF. Let $P$ be the kernel of $f$. Since $f$ maps into a field, $P$ is a prime ideal of $A$. By theorem 4.2.5 there is a prime ideal $Q$ of $B$ such that $Q \cap A = P$. By the factor theorem, $f$ induces an injective ring homomorphism $\overline{f}\colon A/P \to C$. It can be extended in a natural way to the fraction field $K$ of $A/P$. Let $L$ be the fraction field of $B/Q$. By lemma 4.1.16, $B/Q$ is integral over $A/P$, hence $L$ is an algebraic extension of $K$. Since $C$ is algebraically closed, $\overline{f}$ extends to a monomorphism $\overline{g}\colon L \to C$, as we have noted above. Let $\pi\colon B \to B/Q$ be the canonical epimorphism and $g = \overline{g} \circ \pi$, then $g$ is the desired extension of $f$, because $\overline{g}$ extends $\overline{f}$ and $(\overline{f} \circ \pi)_{|A} = f$. □

There is a companion theorem to theorem 4.2.6, the so called *going down theorem*, which we want to prove here, too. There will be extra hypotheses, including the assumption that $A$ is integrally closed. For this reason we need some more lemma's.

LEMMA 4.2.8. *Let $A$ be a subring of $B$, and denote by $\overline{A}$ the integral closure of $A$ in $B$. If $S$ is a multiplicatively closed subset of $A$, then $S^{-1}\overline{A}$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

PROOF. We already know from lemma 4.2.1 that $S^{-1}\overline{A}$ is integral over $S^{-1}A$, since $\overline{A}$ is integral over $A$ by definition. If $\alpha/s \in S^{-1}B$, for $\alpha \in B$ and $s \in S$, and $\alpha/s$ is integral over $S^{-1}A$, we must show that $\alpha/s \in S^{-1}\overline{A}$. There is an equation of the form

$$\left(\frac{\alpha}{s}\right)^n + \left(\frac{a_1}{s_1}\right)\left(\frac{\alpha}{s}\right)^{n-1} + \cdots + \frac{a_n}{s_n} = 0$$

with $a_i \in A$ and $s_i \in S$. Let $s' = \prod_{i=1}^n s_i$, and multiply the equation by $(s \cdot s')^n$ to conclude that $s'\alpha$ is integral over $A$. Therefore $s'\alpha \in \overline{A}$, so that $\frac{\alpha}{s} = \frac{s'\alpha}{s's} \in S^{-1}\overline{A}$. □

COROLLARY 4.2.9. *If $S$ is a multiplicatively closed subset of the integrally closed domain $A$, then $S^{-1}A$ is integrally closed.*

PROOF. Apply lemma 4.2.8 with $\overline{A} = A$ and $B = K$, the fraction field of $A$ and $S^{-1}A$. Then $S^{-1}A$ is the integral closure of $S^{-1}A$ in $S^{-1}B = S^{-1}K = K$. This just says that $S^{-1}A$ is integrally closed. □

LEMMA 4.2.10. *Let $M$ be an $A$-module and denote the localization with respect to a prime ideal $P$ of $A$ by $M_P$. The following conditions are equivalent.*

1. *$M = 0$.*
2. *$M_P = 0$ for all prime ideals $P$ of $A$.*
3. *$M_P = 0$ for all maximal ideals $P$ of $A$.*

PROOF. Of course we have (1) ⇒ (2) ⇒ (3). It remains to show that (3) ⇒ (1). Let $m \in M$. If $P$ is a maximal ideal of $A$, then $m/1 \in M_P = 0$ is zero, so there exists $a_P \in A \setminus P$ such that $a_P m = 0$ in $M$. Let $I_m$ be the ideal generated by $a_p$. Then $I_m$ cannot be contained in any maximal ideal $\mathcal{M}$, because $a_{\mathcal{M}} \notin \mathcal{M}$ by construction. Thus $I_m = A$, and in particular, $1 \in I_m$. Thus 1 can be written as a finite sum

$$1 = \sum_P b_P a_P$$

where $P$ is a maximal ideal of $A$ and $b_P \in A$. Consequently

$$m = 1m = \sum_P b_P a_P m = 0.$$

It follows that $M = 0$. □

We say that an $A$-module $M$ is *faithful*, if $(0 : M) = 0$, that is, if and only if $M$ has zero annihilator. The following lemma is a slightly different version of lemma 3.1.11, but has the same proof:

LEMMA 4.2.11. *Let $A$ be a subring of $B$ and $\alpha \in B$ be integral over $A$. Let $M$ be a finitely generated $A$-module that is faithful as an $A[\alpha]$-module, and let $I$ be an ideal of $A$ such that $\alpha M \subseteq IM$. Then $\alpha$ satisfies an equation of integral dependence*

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$$

*with coefficients $a_i \in I$.*

LEMMA 4.2.12. *Let $B$ be integral over the subring $A$, and let $I$ be an ideal of $A$. Then $\sqrt{IB}$ is the set of all $b \in B$ satisfying an equation of integral dependence*

$$b^m + r_{m-1}b^{m-1} + \cdots + r_1 b + r_0 = 0$$

*with $r_i \in I$.*

PROOF. If $b \in B$ satisfies such an equation, then $b^m \in IB$. Hence $b \in \sqrt{IB}$. Conversely, let $b^n \in IB$ for $n \geq 1$, such that $b^n = \sum_{i=1}^k r_i b_i$ for some $r_i \in I$ and $b_i \in B$. Then $B_1 = A[b_1, \ldots, b_k]$ is a subring of $B$, which is a finitely generated $A$-module by corollary 4.1.5. We have

$$b^n B_1 = \sum_{i=1}^k r_i b_i B_1 \subseteq \sum_{i=1}^k r_i B_1 \subseteq IB_1.$$

Now we apply lemma 4.2.11 as follows. $M = B_1$ is a finitely generated $A$-module, which is a faithful $A[b^n]$-module, because an element that annihilates $B_1$ annihilates 1 and is therefore 0. Now, with $\alpha = b^n$ we have $\alpha B_1 \subseteq IB_1$. Then $\alpha = b^n$ satisfies an equation of integral dependence with coefficients in $I$, as given above. □

LEMMA 4.2.13. *Let $A$ be an integral domain with fraction field $K$. Assume that $A$ is integrally closed, and let $f, g$ be monic polynomials in $K[x]$. If $fg \in A[x]$, then both $f$ and $g$ are in $A[x]$.*

PROOF. In a splitting field $C \supseteq K$ we have $f(x) = \prod_i (x - a_i)$ and $g(x) = \prod_j (x - b_j)$ with $a_i, b_j \in C$. Since the $a_i$ and $b_j$ are roots of the monic polynomial $fg \in A[x]$, they are integral over $A$. The coefficients of $f$ and $g$ are in $K$ and are symmetric polynomials in the roots, hence are integral over $A$ as well. But $A$ is integrally closed, and the results follows. □

PROPOSITION 4.2.14. *Let $A$ be an integrally closed domain and $B$ be an overring of $A$ which is integral over $A$. Assume that no nonzero element of $A$ is a zero-divisor of $B$. For $b \in B$, define a ring homomorphism $h_b \colon A[x] \to B$ by $h_b(f) = f(b)$. Then $I = \ker(h_b)$ is a principal ideal in $A[x]$ generated by a monic polynomial.*

PROOF. Note that the assumption on zero-divisors of $B$ is automatic if $B$ is itself an integral domain. Let $K$ be the fraction field of $A$. Then $I \cdot K[x]$ is an ideal of the PID $K[x]$, which is nonzero, because $b$ is integral over $A$ (see the argument in step 1). Thus $I \cdot K[x]$ is generated by a monic polynomial $f$.

*Step* 1: We will show that $f \in A[x]$. Since $b$ is integral over $A$, there is a monic polynomial $h \in A[x]$ such that $h(b) = 0$. Then $h \in I \subseteq I \cdot K[x]$, hence $h$ is a multiple of $f$, say

$$h = fg$$

with a monic polynomial $g \in K[x]$. Since $A$ is integrally closed we may apply lemma 4.2.13 to conclude that both $f$ and $g$ belong to $A[x]$.

*Step* 2: We claim that $f \in I$. Since $f \in I \cdot K[x]$, we may clear denominators to produce a nonzero element $a \in A$ such that $af \in I \cdot A[x] = I$. By definition of $I$ we have $af(b) = 0$, and by hypothesis, $a$ is not a zero-divisor of $B$. Therefore $f(b) = 0$, so that $f \in I$.

*Step* 3: We claim that $f$ generates $I$. This will finish the proof. Let $q \in I \subseteq I \cdot K[x]$ arbitrary. Since $f$ generates $I \cdot K[x]$, we can take a common denominator and write

$$q = \frac{q_1 f}{a_1}$$

with $a_1 \in A^\times$ and $q_1 \in A[x]$. Thus $a_1 q = q_1 f$. If we pass to residue classes in the polynomial ring $(A/a_1A)[x]$, we have $\overline{q_1}\overline{f} = 0$. Since $\overline{f}$ is monic, the leading coefficient of $\overline{q_1}$ must be 0, which means that $\overline{q_1}$ itself must be zero. Consequently, $a_1$ divides every coefficient of $q_1$, so $q_1/a_1 \in A[x]$ and $q = \frac{q_1}{a_1} f$. Thus $I$ is generated by $f$. □

Finally we come to the promised *Going Down Theorem*.

THEOREM 4.2.15 (Going Down). *Let the integral domain $B$ be integral over the integrally closed domain $A$. Suppose we have a chain of prime ideals*

$$P_1 \subseteq \cdots \subseteq P_n$$

*of $A$ and a chain of prime ideals $Q_m \subseteq \cdots \subseteq Q_n$ of $B$, with $1 < m \leq n$. If $Q_i$ lies over $P_i$ for $i = m, \ldots, n$, then there are prime ideals $Q_1, \ldots, Q_{m-1}$ such that $Q_1 \subseteq \cdots \subseteq Q_m$ and $Q_i$ lies over $P_i$ for every $i = 1, \ldots, n$.*

PROOF. By induction, it suffices to consider the case $n = m = 2$. Hence we have prime ideals $P_1 \subseteq P_2$ of $A$ and a prime ideal $Q_2$ of $B$ lying over $P_2$. Let $T$ be a subset of $B$ consisting of all products $at$ with $a \in A \setminus P_1$ and $t \in B \setminus Q_2$,

$$T = \{at \mid a \in A \setminus P_1,\ t \in B \setminus Q_2\}.$$

We want to check that $T$ is a multiplicatively closed set. This is clear except for the property that $0 \notin T$, which we want to have, too. Hence assume that $at = 0$ for some $a \notin P_1$ and $t \notin Q_2$. Because $0 \in P_1$ and $0 \in Q_2$ this means $a \neq 0$ and $t \neq 0$, contradicting the assumption that $B$ is an integral domain. Hence $0 \notin T$. Note that $A \setminus P_1$ is contained in $T$ (take $t = 1$), as well as $B \setminus Q_2$ (take $a = 1$).

*Step* 1: We prove the theorem under the assumption that $T \cap P_1 B = \emptyset$. Then $P_1(T^{-1}B)$ is a proper ideal of $T^{-1}B$, because otherwise 1 would belong to $T \cap P_1 B$. Therefore $P_1(T^{-1}B)$ is contained in a maximal ideal $M$. By the correspondence theorem of localization this $M$ corresponds to a prime ideal $Q_1$ of $B$ with $Q_1 \cap T = \emptyset$. Explicitly, $b \in Q_1$ if and only if $b/1 \in M$. We refer to $Q_1$ as the contraction of $M$ to $B$. It is the preimage of $M$ under the canonical map $b \mapsto b/1$. We have

$$(A \setminus P_1) \cap Q_1 = (B \setminus Q_2) \cap Q_1 = \emptyset.$$

Thus $Q_1 \cap A \subseteq P_1$ and $Q_1 = Q_1 \cap B \subseteq Q_2$. It remains to show that $P_1 \subseteq Q_1 \cap A$. Then $Q_1$ lies over $P_1$ and we are done. We do this by taking the contraction of both sides of the inclusion $P_1(T^{-1}B) \subseteq M$. Since the contraction of $P_1(T^{-1}B)$ to $B$ is $P_1 B$, we have $P_1 B \subseteq Q_1$, so that

$$P_1 \subseteq (P_1 B) \cap A \subseteq Q_1 \cap A.$$

*Step* 2: We show that the above assumption $T \cap P_1 B = \emptyset$ is always true. Suppose that $T \cap P_1 B$ is not empty. Then, by definition of $T$, the set $T \cap P_1 B$ contains an element $at$ with $a \in A \setminus P_1$ and $t \in B \setminus Q_2$. We apply lemma 4.2.12 with $I = P_1$ and $b$ replaced by $at$, to produce a monic polynomial

$$f(x) = x^m + r_{m-1}x^{m-1} + \cdots + r_1 x + r_0$$

with coefficients $r_i \in P_1$ such that $f(at) = 0$. Then define

$$v(x) = a^m x^m + r_{m-1}a^{m-1}x^{m-1} + \cdots + r_1 a x + r_0.$$

It satisfies $v(x) \in A[x]$ and $v(t) = 0$. By proposition 4.2.14, there is a monic polynomial $g \in A[x]$ that generates the kernel of the evaluation map $h_t \colon A[x] \to B$. Therefore $v = ug$ for some $u \in A[x]$. Passing to residue classes in the polynomial ring $(A/P_1)[x]$, we have $\overline{v} = \overline{u}\overline{g}$. Since $r_i \in P_1$ for all $0 \leq i \leq m-1$, we have $\overline{v} = (\overline{a}^m)x^m$. Since $A/P_1$ is an integral domain and $g$ is monic, hence $\overline{g}$ is monic too, we must have $\overline{g} = x^j$ for some $j$ with $0 \leq j \leq m$. Note that $a \notin P_1$, so $\overline{v}$ is not the zero polynomial. Consequently,

$$g(x) = x^j + a_{j-1}x^{j-1} + \cdots + a_1 x + a_0$$

with $a_i \in P_1$ for all $0 \leq i \leq j-1$. Since $g \in \ker(h_t)$ we have $g(t) = 0$. By lemma 4.2.12, $t \in \sqrt{P_1 B}$, so for some positive integer $k$, we have

$$t^k \in P_1 B \subseteq P_2 B \subseteq Q_2 B = Q_2,$$

hence $t \in Q_2$. However, this contradicts our choice of $t$, which was $t \in B \setminus Q_2$. □

CHAPTER 5

# Dedekind Rings and Discrete Valuation Rings

Before we start explaining Dedekind rings and DVRs (discrete valuation rings), we will give a short introduction to dimension theory. We will not need this here really, but it is of course useful anyway. We will use the dimension of a ring for the folllowing fact: if $A$ is an integral domain which is not a field, then $A$ is a DVR if and only if $A$ is an integrally closed Noetherian local ring of dimension 1.

## 5.1. Dimension Theory

If we say that $A$ is a ring we will always assume that $A$ is commutative with unit.

DEFINITION 5.1.1. Let $A$ be a non-trivial ring. A chain of $n+1$ different prime ideals

$$P_0 \subset P_1 \subset \ldots \subset P_n$$

is called a chain of prime ideals of *length* $n$.

For a prime ideal $P$, we consider $P$ to be a chain of prime ideals of length 0.

DEFINITION 5.1.2. For a prime ideal $P$ in $A$ the *height* $\mathrm{ht}(P)$ is defined to be the supremum of lenghts of chains $P_0 \subset P_1 \subset \ldots \subset P_n$ of prime ideals with $P_n = P$. If the supremum does not exist we define $\mathrm{ht}(P) = \infty$.

For example, the ideal $(x_1, \ldots, x_r)$ in $K[x_1, \ldots, x_n]$ is a prime ideal of height $r$, with the chain $0 \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \ldots, x_r)$.

DEFINITION 5.1.3. The *dimension* of $A$, denoted by $\dim(A)$ is defined to be the supremum of the heights of all prime ideals in $A$, if it exists, and $\infty$ otherwise.

The dimension of $A$ is also the supremum of the heights of all maximal ideals in $A$, since every prime ideal is contained in a maximal ideal. Moreover, $\dim(A)$ is the supremum over all $n \geq 0$ such that there exists a chain of prime ideals of $A$ of lenght $n$.

EXAMPLE 5.1.4. *A field $K$ has dimension 0. The ring $\mathbb{Z}$ has dimension 1.*

We have $\mathrm{Spec}(K) = 0$, and $P = 0$ is a chain of length 0. Hence $\dim(K) = 0$. There is no chain of prime ideals $P_0 = 0 \subset P_1 \subset P_2$ of lenght 2 in $\mathbb{Z}$, since $P_1$ and $P_2$ would be maximal ideals, i.e., $P_1 = P_2$. On the other hand, $0\mathbb{Z} \subset p\mathbb{Z}$ for a prime $p$ defines a chain of lenght 1. Hence $\dim(\mathbb{Z}) = 1$. Actually, the following result is true:

EXAMPLE 5.1.5. *Every PID which is not a field has dimension 1.*

To see this, use first that every PID $A$ is a factorial ring. If $P$ is a prime ideal of $A$ then $\mathrm{ht}(P) = 1$ if and only if $P = (p)$ for some irreducible element $p$ of $A$. The claim follows.

PROPOSITION 5.1.6. *Let $B \supset A$ be an integral ring extension. Then*

$$\dim(A) = \dim(B).$$

PROOF. Let $Q_0 \subset Q_1 \subset \ldots \subset Q_n$ be a chain of prime ideals of $B$. Denote by $Q_i^c$ the contraction of $Q_i$ with respect to the injective homomorphism $\iota\colon A \to B$. Then it follows from the Incomparability Theorem 4.2.2, that

$$Q_0^c \subset Q_1^c \subset \ldots \subset Q_n^c$$

is a chain of prime ideals in $A$. Hence $\dim(B) \leq \dim(A)$. To see this, recall that the Incomparability Theorem says that if $Q_i, Q_j$ are different and have the same contraction in $A$, then $Q_i$ and $Q_j$ are incomparable in the sense that neither is contained in the other.
Conversely, suppose that

$$P_0 \subset P_1 \subset \ldots \subset P_n$$

is a chain of prime ideals in $A$. By the Lying-over Theorem 4.2.5 there exists $Q_0 \in \operatorname{Spec}(B)$ such that $Q_0^c = P_0$. Applying the Going-up Theorem 4.2.6 it follows that there exists a chain

$$Q_0 \subset Q_1 \subset \ldots \subset Q_n$$

of prime ideals of $B$, so that $\dim(A) \leq \dim(B)$. □

Among the many results which should be covered we only mention the following, and refer the reader to [**7**], Chapter 14 and 15 for more details and theory.

PROPOSITION 5.1.7. *Let $A$ be a Noetherian ring. Then*

$$\dim(A[x_1, \ldots, x_n]) = \dim(A) + n.$$

*In particular,* $\dim(A[x]) = \dim(A) + 1$ *and* $\dim(K[x_1, \ldots, x_n]) = n$.

When $A$ is not Noetherian it might happen that $\dim(A[x]) > \dim(A) + 1$. We have the estimate $\dim(A) + 1 \leq \dim(A[x]) \leq 2\dim(A) + 1$, where $A$ is a commutative ring.

REMARK 5.1.8. In a Noetherian ring, every prime ideal has finite height, but nevertheless there are Noetherian rings of infinite dimension. A well known example can be found in Nagata's book *Local rings*, written in 1962. Here we give a short description of Nagata's example. The details are left as an exercise.
Let $K$ be a field and $A = K[x_1, x_2, \ldots]$ be the polynomial ring in countably infinitely many variables over $K$. Choose an increasing sequence of positive integers $m_1, m_2, m_3, \cdots$ whose differences are also increasing, i.e., with

$$m_{k+1} - m_k > m_k - m_{k-1} > 0$$

for all $k \geq 2$. For example, take $m_i = 2^{i-1}$ for $i \in \mathbb{N}$. Consider the prime ideals $P_i = (x_{m_i+1}, \ldots, x_{m_{i+1}})$ and let $S = A \setminus \cup_{i\in\mathbb{N}} P_i$. This set is multiplicatively closed. Consider the ring of fractions $B := S^{-1}A$. Then one can show that

(1) The maximal ideals of the ring $B$ are the ideals $\mathfrak{m}_i = P_i B$.

(2) We have $B_{\mathfrak{m}_i} = A_{P_i}$, which is a Noetherian local ring of finite dimension.

(3) Each $S^{-1}P_i$ is the smallest prime ideal in a chain of prime ideals of length $m_{i+1} - m_i$.

(4) The ring $B$ is Noetherian and $\dim(B) = \infty$.

## 5.2. Fractional ideals

Throughout this section, let $R$ be an integral domain with quotient field $K$.

DEFINITION 5.2.1. A *fractional ideal* $A$ of $R$ is a $R$-submodule of $K$ for which there is a nonzero element $d$ of $R$ such that $dA \subseteq R$.

One can prove the following result.

LEMMA 5.2.2. *Every finitely generated $R$-submodule of $K$ is a fractional ideal. Conversely, if $R$ is Noetherian, every fractional ideal is a finitely generated $R$-submodule of $K$.*

Let $A^{-1} = \{\alpha \in K \mid \alpha A \subseteq R\}$. Note that $0 \in A^{-1}$. For fractional ideals $A$ and $B$ define $AB$ to be the set of finite linear combinations of elements $ab$ with $a \in A$ and $b \in B$. Note that $A^{-1}$ and $AB$ are fractional ideals. We have $AA^{-1} \subseteq R$, but equality need not hold.

DEFINITION 5.2.3. A fractional ideal $A$ of $R$ is called *invertible*, if $AA^{-1} = R$.

Call two fractional ideals $A$ and $B$ equivalent, if $A = \alpha B$ for some nonzero element $\alpha \in K$. In other words, $A \sim B$ if and only if $A$ and $B$ differ by the principal fractional ideal $(\alpha)$. Let $C(R)$ denote the set of equivalence classes of invertible fractional ideals under this equivalence relation. Define the product of two elements $x = [A]$ and $y = [B]$ in $C(R)$ by $xy = [AB]$.

LEMMA 5.2.4. *The set $C(R)$, together with the multiplication of ideal classes, forms an Abelian group, known as the ideal class group of $R$ (or of $K$, by a common abuse of terminology).*

PROOF. The class of the ideal (1), or of any nonzero element of $K$, is an identity element. Let $[A]$ be an ideal class. Choose an $x \in R, x \neq 0$ such that $xA^{-1}$ is an ideal of $A$. Then its class is the inverse to $[A]$ because $[A][xA^{-1}] = [(x)] = [(1)]$. □

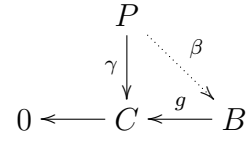
If we define $C(R)$ to be the set of classes of all fractional ideals different from zero, i.e., not necessarily invertible, we will only obtain the structure of a monoid.

REMARK 5.2.5. The ideal class group is a central object to study in algebraic number theory, for rings of integers $\mathcal{O}_K$ in number fields $K$. It turns out, that in this case, the ideal class group $C(\mathcal{O}_K)$ is *finite*. Then its order is called the *class number of* $\mathcal{O}_K$. In general, the class group is not finite, not even for Dedekind rings.

There is an equivalent definition of $C(R)$. For each non-zero element $\alpha \in K$, $\alpha R$ is an invertible fractional ideal, isomorphic to $R$. Then $C(R)$ can be identified with the quotient of all invertible $R$-modules by its subgroup of principal $R$-modules. In this sense $C(R)$ measures how much ideals can differ from being principal. In this context we mention a very natural definition of a *Dedekind ring*, see the next section: it is an integral domain $R$ where all nonzero fractional ideals are invertible. There exist many different (but of course equivalent) definitions for a Dedekind ring.

DEFINITION 5.2.6. An $R$-module $P$ is called *projective* if, for any pair of $R$-modules $B$ and $C$, any surjective $R$-module homomorphism $g\colon B \to C$ and any $R$-module homomorphism $\gamma\colon P \to C$ there is at least one $R$-module homomorphism $\beta\colon P \to B$ such that $\gamma = g \circ \beta$.

Equivalently, the functor $\mathrm{Hom}_R(P, \cdot)$ is exact. The corresponding diagram looks as follows:



The homomorphisms $\beta$ is not unique; this is not a universal property.
Free $R$-modules are projective. Returning to our integral domain $R$, we have the following result.

PROPOSITION 5.2.7. *Any nonzero fractional ideal $A$ of $R$ is invertible if and only if it is projective as an $R$-module. In this case, it is finitely generated.*

## 5.3. The definition of Dedekind rings and DVR's

There are many equivalent definitions of a Dedekind ring and a DVR. We start with the following one.

DEFINITION 5.3.1. An integral domain $R$ is a *Dedekind ring* if every nonzero fractional ideal of $R$ is invertible. A *DVR* is a Dedekind ring which is a local ring.

EXAMPLE 5.3.2. *Every PID is a Dedekind ring. In particular, $\mathbb{Z}$ is a Dedekind ring.*

Let $\mathbb{Z}_{(p)}$ be the ring of *$p$-local integers*, for a prime $p$. This is the localization of the Dedekind ring $\mathbb{Z}$ at the prime ideal generated by $p$. It is a DVR. In fact, any localization of a Dedekind ring at a nonzero prime ideal is a discrete valuation ring; in practice, this is frequently how discrete valuation rings arise.

DEFINITION 5.3.3. An integral domain $R$ is called a *valuation ring*, if it is not a field and $x \in K \setminus R$ implies $x^{-1} \in R$.

A valuation ring is a local ring.

LEMMA 5.3.4. *If $I$ and $J$ are ideals in a valuation ring $R$, then either $I \subseteq J$ or $J \subseteq I$. In particular, $R$ is a local ring.*

PROOF. Let $x \in I$ and $x \notin J$. For $y \in J$ with $y \neq 0$ we have $x/y \notin R$, hence $y/x \in R$ since $R$ is a valuation ring. It follows $y = (y/x)x \in I$, and hence $J \subseteq I$. □

DEFINITION 5.3.5. A *discrete valuation* on a field $K$ is a function

$$\nu \colon K \to \mathbb{Z} \cup \{\infty\}$$

that satisfies the following properties.

(1) $\nu(x) = \infty$ if and only if $x = 0$.
(2) $\nu$ is surjective.
(3) $\nu(xy) = \nu(x) + \nu(y)$
(4) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$.

The second property says that $\nu_{|K^\times} \colon K^\times \to \mathbb{Z}$ is a surjective group homomorphism, i.e., $\nu_{|K^\times} = \mathbb{Z}$. The valuation is called *trivial*, if $\nu(K) = \{0, \infty\}$.

LEMMA 5.3.6. *Let $\nu$ be a discrete valuation on a field $K$. Then*

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

*is a valuation ring.*

PROOF. We first show that $R$ is a subring of $K$. If $x, y \in R$ then $\nu(x) \geq 0$ and $\nu(y) \geq 0$. Hence $\nu(xy) = \nu(x) + \nu(y) \geq 0$, so that $xy \in R$. Furthermore

$$\nu(x + y) \geq \min\{\nu(x), \nu(y)\} \geq 0,$$

so that $x + y \in R$. Since $\nu(1) = \nu(1 \cdot 1) = \nu(1) + \nu(1)$ we have $\nu(1) = 0$ and $1 \in R$. Also, $0 = \nu(1) = \nu((-1)(-1)) = \nu(-1) + \nu(-1)$, so that $\nu(-1) = 0$. Then we have $\nu(-x) = \nu(x) + \nu(-1) = \nu(x) \geq 0$.
Let $x \in K \setminus R$. We must show that $x^{-1} \in R$. We have

$$0 = \nu(1) = \nu(x \cdot x^{-1}) = \nu(x) + \nu(x^{-1}).$$

Since $x \notin R$ we have $\nu(x) < 0$, hence $\nu(x^{-1}) > 0$. This says $x^{-1} \in R$. □

DEFINITION 5.3.7. Let $\nu$ be a discrete valuation on a field $K$. Then $R = \{x \in K \mid \nu(x) \geq 0\}$ is called the *valuation ring* of $(K, \nu)$.

LEMMA 5.3.8. *Let $\nu$ be a discrete valuation on a field $K$ and $R$ its valuation ring. Then the following statements hold.*

(1) $E(R) = \{x \in K \mid \nu(x) = 0\}$.
(2) $M_\nu = \{x \in K \mid \nu(x) > 0\}$ *is the only maximal ideal in $R$.*
(3) *$R$ is a PID, and hence integrally closed. It is not a field if and only if the valuation is not trivial.*

PROOF. (1): Let $x \in K$. If $\nu(x) \geq 0$ then $\nu(x^{-1}) = -\nu(x) \leq 0$. But $x$ is invertible in $R$ if $x$ and $x^{-1}$ in $R$, i.e., if $\nu(x) \geq 0$ and $\nu(x) \leq 0$.
(2): Note that $M_\nu$ is an ideal in $R$. For $x \in M_\nu$ and $y \in R$ we have $\nu(xy) = \nu(x) + \nu(y) > 0$, hence $xy \in M_\nu$. Since $R \setminus M_\nu = E(R)$, it follows that $R$ has exactly one maximal ideal. Of course, we know already that $R$ is a local ring by lemma 5.3.4.
(3): Let $I \subset R$ be an ideal different from 0. Then choose an $a \in I$ such that $\nu(a)$ is minimal among all $\nu(x)$ with $x \in I$. This is possible since $\nu(x) \geq 0$. Then $I = (a)$ is a principal ideal. To see this, let $b \in I$. Then $b = a(b/a)$ with $a \in I$ and

$$\nu\left(\frac{b}{a}\right) = \nu(b) - \nu(a) \geq 0,$$

since $\nu(a)$ was minimal. It follows that $b/a \in R$, hence $a \mid b$ and $b \in (a)$. □

REMARK 5.3.9. Note that it suffices to define a discrete valuation $\nu$ on $R$, since if $x = r/s \in K$, then we can (and we must) define $\nu(x) = \nu(r) - \nu(s)$.

Now we come to our second definition for a DVR.

DEFINITION 5.3.10. A DVR is an integral domain $R$ that is the valuation ring of a valuation on $K = \mathrm{Quot}(R)$.

We know already that a DVR is a PID. However, we can show more.

LEMMA 5.3.11. *Let $R$ be a DVR of $(K, \nu)$. Then $\nu\colon R \setminus 0 \to \mathbb{N}$ is a Euclidean norm. Hence $R$ is a Euclidean ring.*

PROOF. Let $x, y \in R \setminus 0$. By (3) of definition 5.3.5 we have $\nu(x) \leq \nu(xy)$. If $\nu(x) \geq \nu(y)$, then $\nu(x/y) \geq 0$, so that $x/y \in R$. The equations

$$x = (x/y)y + 0, \quad \text{if } \nu(x) \geq \nu(y),$$
$$x = 0 \cdot y + x \quad \text{if } \nu(x) < \nu(y)$$

verify the other defining condition for a Euclidean norm: there exist $q, r \in R$ such that $x = qy + r$ with either $r = 0$ or $\nu(r) < \nu(y)$. □

EXAMPLE 5.3.12. *Let $K = \mathbb{Q}$ and $\nu_p\colon \mathbb{Q} \to \mathbb{Z}$ defined by*

$$\nu_p\left(\frac{p^n a}{b}\right) = n$$

*for a prime $p$, where $a$ and $b$ are integers which are coprime to $p$. Then the valuation ring of $(\mathbb{Q}, \nu_p)$ is $R = \mathbb{Z}_{(p)}$.*

EXAMPLE 5.3.13. *Let $K$ be a field and $f \in K[x]$ be an irreducible polynomial. Then the localization $K[x]_{(f)} = K[x][f^{-1}]$ is the valuation ring of the discrete valuation $\nu\colon K(x) \to \mathbb{Z}$ given by*

$$\nu_f(f^n \frac{g}{h}) = n,$$

*where $g, h$ are polynomials in $K[x]$ which are prime to $f$.*

DEFINITION 5.3.14. Let $R$ be an DVR. An element $t$ of $R$ is called a *uniformizing parameter*, abbreviated UP, if $\nu(t) = 1$.

LEMMA 5.3.15. *Let $R$ be a DVR with fraction field $K$ and UP $t$. Then the following statements hold:*

(1) *If $r \neq 0$ in $R$, then $r = ut^n$ where $u \in E(R)$ and $n = \nu(r) \geq 0$.*
(2) *If $x \neq 0$ in $K$, then $x = ut^n$ where $u \in E(R)$ and $n = \nu(x) \in \mathbb{Z}$.*
(3) *The only nonzero proper ideals of $R$ are $(t^n)$ with $n \geq 1$.*
(4) *The only nonzero prime ideal of $R$ is the maximal ideal $M = (t)$, which is given by $M = \{a \in R \mid \nu(a) > 0\}$.*
(5) *The only nonzero fractional ideals of $R$ are the $(t^n)$ for $n \in \mathbb{Z}$.*

PROOF. (1): Let $u = rt^{-n}$. Then $\nu(u) = 0$, and hence $u$ is a unit in $R$ by lemma 5.3.8, part (1). Then $ut^n = r$.

(2): Let $u = xt^{-n}$. Again $u$ is a unit in $R$ and $ut^n = x$.

(3): If $I \subset R$ is a nonzero proper ideal and $n$ is minimal such that there exists $a \in I$ with $\nu(a) = n$, then $a = ut^n$ for a unit $u$ by (1), and $(t^n) \subseteq I$. Conversely, if $b \in I$, then $b = ut^q$ where $u$ is a unit and $q \geq n$, hence $b \in (t^n)$. This shows (3). The rest is left as an exercise. □

We come to the basic characterization theorem for DVR's.

THEOREM 5.3.16. *The following statements are equivalent for a given integral domain $R$ which is not a field.*

(1) *$R$ is the valuation ring of a discrete valuation on $K = \mathrm{Quot}(R)$, i.e., $R$ is a DVR in the sense of definition* 5.3.10.
(2) *$R$ is a local PID.*
(3) *$R$ is a factorial ring with a unique irreducible element $t$, up to associates.*
(4) *$R$ is a Noetherian local ring with a principal maximal ideal.*
(5) *$R$ is an integrally closed Noetherian local ring of dimension* 1.
(6) *$R$ is a local ring such that every nonzero fractional ideal of $R$ is invertible, i.e., $R$ is a DVR in the sense of definition* 5.3.1.

PROOF. We use the above lemma repeatedly without mentioning it. We first show that (1) ⇒ (2) ⇒ (3) ⇒ (1). We have already shown that (1) ⇒ (2): a valuation ring is a local ring, and it is a PID, see lemma 5.3.8.
Assume (2): let $(t)$ be the maximal ideal of $R$. Then $t$ is irreducible, since if $t = xy$ with neither $x$ nor $y$ a unit, we would have $(x) \subset (t)$ and $(y) \subset (t)$, because of the maximality of $(t)$. This would mean $t \mid x$ and $t \mid y$, so that $t^2 \mid xy = t$, hence $t \mid 1$, i.e., $t$ is a unit. Moreover $t$ is the unique irreducible by the maximality of $(t)$, so that (3) holds.
Assume (3): then the ideal $(t)$ is prime. It is even maximal by the uniqueness of $t$. For any $r \in R$, there exists $n \geq 1$ such that $r \in (t^n)$ and $r \notin (t^{n+1})$. We set $\nu(r) = n$ and find that $\nu$ induces a discrete valuation on $K$, the fraction field of $R$, with valuation ring $R$. Hence (1)

holds.
Clearly (2) ⇒ (4), because a PID is a Noetherian ring.
The equivalent conditions (1), (2) and (3) also imply (5) and (6). The only ideals in $R$ are $(t^n)$ for a UP $t$ by assumption, and similarly for fractional ideals. This shows (6). Also, $R$ is obviously integrally closed: no element of $K$ not in $R$ can satisfy an equation of integral dependence over $R$. This shows (5), since a PID has dimension 1.
(4) ⇒ (2): Let $M = (t)$ be the maximal ideal of $R$. We must show that any ideal $I \subset R$ is principal. Since $R$ is Noetherian, $I$ is finitely generated. Hence there is a maximal $n \geq 1$ such that $I \subset M^n$. For an element $a \in I$ that is not in $M^{n+1}$ we have $a = ut^n$ for some unit $u \in R$, see again lemma 5.3.15. Thus $a \in (t^n)$. Since this holds for all such $a$ and since $M^{n+1} \subset (t^n)$, it follows $I = (t^n)$.
(6) ⇒ (4): Since invertible ideals are finitely generated, $R$ is Noetherian. We need only show that the maximal ideal $M$ is principal. We use Nakayama's lemma, see corollary 3.1.12, with $I = M$. Then $M^2 = M$ would imply $M = 0$ which is impossible. Hence we have $M \neq M^2$. Let $t \in M \setminus M^2$. Since $t \in M$ we have $tM^{-1} \subset R$. Since $t \notin M^2$ we have $tM^{-1} \not\subset M$. Therefore $tM^{-1} = R$ and $(t) = M$.
(5) ⇒ (4): This is the hardest part. We must find a way to use the assumption that $R$ is integrally closed. Let $M$ be the unique maximal ideal of $R$. We have to show that $M$ is a principal ideal. Again, $M \neq M^2$ by Nakayama's lemma, and we can choose $t \in M \setminus M^2$. Of course, $(t) \subset M$. We claim that equality holds. Since $M$ is the unique nonzero prime ideal, it is the radical of $(t)$,i.e. $M = \sqrt{(t)}$. Here we use that $\sqrt{(t)}$ is a prime ideal since the radical is an intersection of prime ideals. Let $n \geq 1$ be minimal such that $M^n \subset (t)$. We claim that $n = 1$. Assume that $n > 1$. We will obtain a contradiction. Let $x \in M^{n-1} \setminus (t)$. Then $xM \subset M^n \subset (t)$. Let $y = x/t \in K$. Then $y \notin R$ since otherwise $x = yt \in (t)$, which is not true. We claim that $y$ is integral over $R$. This would imply that $y \in R$, since $R$ is integrally closed. But $y \notin R$ and we have obtained a contradiction. Since $xM \subset (t)$ we have $yM \subset R$, and $yM$ is an ideal. If $yM = R$, then $ym = 1$ for some $m \operatorname{im} M$, and $xm = tym = t$ is in $M^n \subset M^2$, contradicting the choice of $t$. Thus $yM$ is a proper ideal of $R$, and $yM \subset M$. This leads to the required equation, as we have already seen earlier. Indeed, let $M$ be generated by $m_1, \ldots, m_r$. Then $ym_j = \sum a_{ij} m_i$ with $a_{ij} \in R$, which can be written

$$\sum_i (\delta_{ij} y - a_{ij}) m_i = 0.$$

Let $d = \det(\delta_{ij} y - a_{ij})$. By Cramer's rule, or taking the adjoint matrix, we obtain $dm_i = 0$ for all $i$, and thus $dM = 0$. Since $M \neq 0$ it follows $d = 0$, which is the required equation of integral dependence for $y$. □

Corollary 5.3.17. *A valuation ring $R$ is a DVR if and only if it is Noetherian.*

Proof. A DVR is a PID and therefore is Noetherian. Conversely, let $R$ be a Noetherian valuation ring. Let $I$ be any ideal. It is generated by finitely many elements $a_i$. By lemma 5.3.4 one of the ideals $(a_i)$ must contain all of the others and therefore must be $I$. Hence every ideal is a principal ideal and $R$ is local. This is just (2) of the theorem, so that $R$ is a DVR. □

Corollary 5.3.18. *Suppose that $P$ is a minimal nonzero prime ideal in an integrally closed Noetherian integral domain. Then the localization $R_P$ is a DVR.*

Proof. Indeed, $R_P$ is an integrally closed Noetherian local integral domain. By the theorem $R_P$ is a DVR. □

The following proposition is also useful.

PROPOSITION 5.3.19. *A ring $R$ is integrally closed if and only if $R_P$ is integrally closed for all prime ideals $P$, or equivalently, for all maximal ideals $P$.*

PROOF. Let $I\colon R \to S$ be the inclusion of $R$ in its integral closure in $K$. Thus $R$ is integrally closed if and only if $i$ is an epimorphism. Of course, $K$ is also the field of fractions of $K_P$ for all primes $P$, and the integral closure of $R_P$ is $i_P\colon R_P \to S_P$. Since $i$ is an epimorphism if and only if $i_P$ is an epimorphism for all prime ideals $P$ or, equivalently, all maximal ideals $P$, the conclusion follows. □

Here is an important example of a DVR:

EXAMPLE 5.3.20. *The ring $\mathbb{Z}_p$ of $p$-adic integers is a local ring with unique maximal ideal $(p)$, and a PID. Hence $\mathbb{Z}_p$ is a DVR. Its quotient field is the field $\mathbb{Q}_p$ of $p$-adic numbers. Any $x \in \mathbb{Q}_p$ is of the form $up^n$, where $u$ is a unit in $\mathbb{Z}_p$, and $n$ is an integer. The required valuation $\nu_p$ is given by $\nu_p(x) = n$.*

There are several different ways to define $\mathbb{Z}_p$ and $\mathbb{Q}_p$. One way is to define the ring $\mathbb{Z}_p$ as the projective limit $\mathbb{Z}_p = \varprojlim A_n$ of rings $A_n = \mathbb{Z}/p^n\mathbb{Z}$ with respect to the homomorphisms $\varphi_n\colon A_n \to A_{n-1}$ of reduction modulo $p^{n-1}$. The sequence

$$\cdots \xrightarrow{\varphi_{n+1}} A_n \xrightarrow{\varphi_n} A_{n-1} \xrightarrow{\varphi_{n-1}} \cdots \xrightarrow{\varphi_3} A_2 \xrightarrow{\varphi_2} A_1$$

forms a so called projective system, indexed by positive integers $n \geq 1$. The *projective limit* of a projective system is defined as a ring

$$A = \varprojlim A_n$$

with the following universal property. There are uniquely defined projections $\pi_n\colon A \to A_n$ such that for an arbitrary ring $B$ and a system of ring homomorphisms $\psi_n\colon B \to A_n$, compatible with each other under the condition $\psi_{n-1} = \varphi_n \circ \psi_n$ for all $n \geq 2$, there exists a unique homomorphism $\psi\colon B \to A$ such that $\psi_n = \pi_n \circ \psi$. As usual, the universal property implies the uniqueness of $A$, which is $\mathbb{Z}_p$ in our case. This ring is local PID, hence a DVR with residue field

$$\mathbb{Z}_p/(p) \simeq \mathbb{F}_p.$$

The field $\mathbb{Q}_p$ of $p$-adic numbers is just the fraction field of $\mathbb{Z}_p$.

Here is another way to describe $\mathbb{Z}_p$ and $\mathbb{Q}_p$. For a fixed prime number $p$, any nonzero rational number $x$ can be written as $p^a \cdot m/n$ where $a, m, n \in \mathbb{Z}$ and $m$ and $n$ are prime to $p$. Define $\nu_p(x) = a$ for $x \neq 0$ and $\nu_p(0) = \infty$. Then

$$\nu_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$$

is a valuation on $\mathbb{Q}$, with valuation ring $\mathbb{Z}_{(p)}$. This valuation induces a non-Archimedian norm $|.|_p$ on $\mathbb{Q}$ by

$$|x|_p = \begin{cases} \frac{1}{p^{\nu_p(x)}}, & x \neq 0 \\ 0, & x = 0 \end{cases}$$

The completion of $\mathbb{Q}$ with respect to this metric associated with this norm is the field of $p$-adic numbers $\mathbb{Q}_p$. In general, there is a construction of adjoining the limits of Cauchy sequences to a given field $K$ with an absolute value $|.|$, which leads to the so-called *completion* of $K$, denoted by $\widehat{K}$. The completion is given by the set of Cauchy sequences in $K$, where we consider two sequences as equivalent if they differ by a sequence converging to zero. In our case we have

$K = \mathbb{Q}$, and we obtain with the $p$-adic metric $\widehat{\mathbb{Q}} = \mathbb{Q}_p$. It is well-known that any completion of $\mathbb{Q}$ is either $\mathbb{R}$ or some $\mathbb{Q}_p$. We can also complete the valuation ring $\mathbb{Z}_{(p)}$. Then we obtain $\widehat{\mathbb{Z}_{(p)}} = \mathbb{Z}_p$. One way to think of this is to represent elements of $\mathbb{Q}_p$ as $p$-adic Laurent series

$$a = \sum_{i \in \mathbb{Z}} a_i p^i, \quad 0 \leq a_i < p,$$

with $\nu_p(a)$ being the minimal $n$ such that $a_n \neq 0$. We have

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}.$$

Now we come back to Dedekind rings, see definition 5.3.1. Of course, $\mathbb{Z}$ is a Dedekind ring (any PID is). We have the following result.

THEOREM 5.3.21. *The ring $\mathcal{O}_L$ of integers in an algebraic number field $L$ is a Dedekind ring. More generally, if $R$ is a Dedekind ring, $L$ is a finite field extension of $K$, and $C$ is the integral closure of $R$ in $L$, then $C$ is a Dedekind ring.*

PROOF. The first statement follows from the second if we take $R = \mathbb{Z}$, $K = \mathbb{Q}$, $L$ the algebraic number field, and $C = \mathcal{O}_L$. To prove the second statement one shows that $C$ is a Noetherian integrally closed integral domain of Krull dimension 1. This means that $C$ is a Dedekind ring, as we will see. We refer the reader to a book on algebraic number theory for more details. Certainly $C$ is integrally closed since it is an integral closure. For the rest of the proof one assumes first that the field extension is separable. Then the proof is not difficult. Afterwards one treats the general case where $L$ is a purely inseparable extension of a separable extension $L_s$ of $K$. □

Here is the characterization theorem for Dedekind rings.

THEOREM 5.3.22. *Let $R$ be an integral domain which is not a field. The following statements are equivalent for $R$.*

1. *$R$ is Noetherian, integrally closed, and of Krull dimension 1.*
2. *$R$ is Noetherian and each localization $R_P$ at a prime ideal $P$ is a DVR.*
3. *$R$ is a Dedekind ring in the sense of definition 5.3.1, i.e., every nonzero fractional ideal of $R$ is invertible.*
4. *Every nonzero proper ideal of $R$ is a product of maximal ideals.*
5. *Every nonzero proper ideal of $R$ is a product of prime ideals.*

*Moreover, the product decomposition in (4) is then unique.*

PROOF. (1) ⇔ (2): Since prime ideals of $R_P$ correspond to prime ideals contained in $P$ in $R$, we see that the dimension of $R$ is one if and only if the dimension of each $R_P$ is one. Similarly, the Noetherian property is local, and so is the integral closure by proposition 5.3.19. Thus, by theorem 5.3.16 part (5) we see that (1) is equivalent to (2).
(2) ⇔ (3): Again by theorem 5.3.16, part (5) and (6), it suffices to show that every nonzero ideal of $R$ is invertible if and only if every nonzero ideal of each $R_P$ is invertible. In the fraction field $K$ of $R_P$ we have

$$(A^{-1})_P = (A_P)^{-1},$$
$$(AB)_P = A_P B_P$$

for finitely generated fractional ideals $A$ and $B$ of $R$. Moreover, just as for ideals, each fractional ideal of $R_P$ has the form $R_P A$ for some fractional ideal $A$ of $R$. Assume (3). This implies that

$R$ is Noetherian, since invertible ideals are finitely generated. As said above, to conclude (2), it is enough to show that $AA^{-1} = R$ implies $A_P(A_P)^{-1} = R_P$ for all $P$. But this is now clear from the above discussion. For the converse, if $A_P(A_P)^{-1} = R_P$ for all $P$, then also $(AA^{-1})_P = R_P$ for all $P$. This gives $AA^{-1} = R$ and we are done. To see the last step in an elementary way, assume that there is an ideal $A$ such that $AA^{-1}$ is properly contained in $R$, hence properly contained in some maximal ideal $P$. We are done if we arrive at a contradiction. Now $A_P$ is a principal ideal, say generated by $a/s$ with $a \in A$ and $s \in R \setminus P$. The ideal $A$ is generated by finitely many elements $b_i$. Each $b_i$ can be written as

$$\frac{r_i}{s_i}\frac{a}{s}$$

for some elements $r_i \in R$ and $s_i \in R \setminus P$. Let $t$ be the product of s and all the $s_i$. Then $t \in R \setminus P$, and $t/a \in A^{-1}$, since each $\frac{b_i t}{a}$ is in $R$. But then $t = a\frac{t}{a}$ is in $AA^{-1} \subset P$, which is the desired contradiction.
(3) $\Rightarrow$ (4): There are several proofs available. Here is an argument which we have already seen in the section on primary decompositions. Before starting, note that (3) implies that $R$ is Noetherian, see above. Let $\mathcal{S}$ be the set of all nonzero proper ideals that are not finite products of maximal ideals. Since $R$ is Noetherian, every such non-empty set $\mathcal{S}$ contains a maximal ideal. If $\mathcal{S}$ is empty we are done. If not, it contains a maximal element $I$. This cannot be a maximal ideal, so it must be properly contained in some maximal ideal $M$. By assumption $M$ is invertible. Let $J = M^{-1}I$. Then $J \subset R$ and the inclusion is proper. Now $I = MJ \subset J$, and again the inclusion is proper since $MJ = J$ would imply $M = R$. It follows from the maximality of $I$ that $J$ must be a product of maximal ideals. But then so is $I$, which is a contradiction. Hence we have shown (4). The uniqueness of this factorization will be shown in lemma 5.3.23, see below.
(4) $\Rightarrow$ (5): This is obvious, since a maximal ideal is prime.
(5) $\Rightarrow$ (3): The proof will consist of three lemmas, which will be given afterwards (the last one is lemma 5.3.26). □

LEMMA 5.3.23. *Let $I$ be an ideal in an integral domain $R$. If $I$ can be factored as a product of invertible prime ideals, then the factorization is unique.*

PROOF. Suppose that $P_1 \cdots P_m$ and $Q_1 \cdots Q_n$ are two such factorizations of $I$. We must show that $m = n$ and, after reordering, $P_i = Q_i$. Take $Q_1$ to be minimal among the $Q_j$, so that $Q_1 \supset Q_j$ implies $Q_1 = Q_j$. Since $I \subset Q_1$, we have $P_i \subset Q_1$ for some $i$. Reordering, we may assume that $P_1 \subset Q_1$. Similarly, $P_1 \supset Q_j$ for some $j$. But then $Q_j \subset P_1 \subset Q_1$ and these are all equal, since $Q_1$ was minimal. Multiplying by $Q_1^{-1}$ we obtain $P_2 \cdots P_m$ and $Q_2 \cdots Q_n$. Now it is clear that the conclusion follows by induction. □

LEMMA 5.3.24. *Let $R$ be an integral domain and let $x \neq 0$ be in the fraction field $K$. Suppose that $xR = A_1 \cdots A_q$ for fractional ideals $A_i$. Then each $A_i$ is invertible.*

PROOF. Indeed, the inverse of $A_i$ is $x^{-1}A_1 \cdots A_{i-1}A_{i+1} \cdots A_n$. □

LEMMA 5.3.25. *Let $R$ be an integral domain such that all ideals in $R$ are finite products of prime ideals. Then every invertible prime ideal is maximal.*

PROOF. Let $P$ be an invertible prime ideal in $R$ and $a \in R \setminus P$. We claim that $P+(a) = R$, so that $P$ is maximal. If $P + (a) \neq R$, we can write

$$P + (a) = P_1 \cdots P_m,$$
$$P + (a^2) = Q_1 \cdots Q_n$$

as products of prime ideals. Clearly $P$ is contained in each $P_i$ and $Q_i$. Let $b$ be the image of $a$ in the integral domain $R/P$. Note that $b^2$ is the image of $a^2$. Then

$$(b) = (P_1/P) \cdots (P_m/P)$$

is the product of prime ideals $P_i/P$, and

$$(b^2) = (Q_1/P) \cdots (Q_n/P)$$

is the product of prime ideals $Q_j/P$. By lemma 5.3.24, each $P_i/P$ and $Q_j/P$ is invertible. We have

$$(P_1/P)^2 \cdots (P_m/P)^2 = Q_1/P \cdots Q_n/P.$$

This means $n = 2m$ by lemma 5.3.23, and each $P_i/P$ appears twice among the $Q_j/P$. This proves that all inclusions in the following display, which are obvious, are actually equalities:

$$P \subset P + (a^2) = (P + (a^2))^2 \subset P^2 + (a).$$

If $x \in P$, then $x = y + ra$ with some $y \in P^2$ and some $r \in R$, since $P = P^2 + (a)$. We have $ra = x - y \in P$. Since $a \notin P$ we have $r \in P$. Thus $P \subset P^2 + aP \subset P$ and hence

$$P = P^2 + aP = P(P + (a)).$$

Since $P$ is invertible this implies $R = P + (a)$ as claimed. □

LEMMA 5.3.26. *Let $R$ be an integral domain such that all ideals in $R$ are finite products of prime ideals. Then every nonzero prime ideal is invertible.*

PROOF. Let $a \in P$ be nonzero. Then $(a) = P_1 \cdots P_n$ with $P_i$ prime. Each $P_i$ is invertible and therefore maximal by lemmas 5.3.24 and 5.3.25. Since $(a) \subset P$ we have $P_i \subset P$ for some $i$, and then $P = P_i$ is invertible. □

Note that the lemma implies the conclusion (5) ⇒ (3) in theorem 5.3.22.

COROLLARY 5.3.27. *A Dedekind ring $R$ is a PID if and only if it is factorial.*

PROOF. Any PID is factorial. Conversely, assume that $R$ is a UFD, i.e., factorial and let $P$ be a prime ideal. Let $a$ be a nonzero element of $P$. Some irreducible factor $t$ of $a$ is in $P$ and so $(t) \subset P$. Since $R$ has dimension 1 we have $P = (t)$. Thus every prime ideal is principal. Since every ideal is a product of prime ideals by the theorem, every ideal is principal. □

COROLLARY 5.3.28. *Let $I$ be a nonzero proper ideal of a Dedekind ring $R$. Then the following statements hold.*

1. *There is an ideal $J$ of $R$ such that $IJ$ is principal.*
2. *Every ideal in $R/I$ is principal and $R/I$ is Noetherian of dimension zero, i.e., it is Artinian.*
3. *If $I \subset J$ for an ideal $J$, then $J = I + (b)$ for some $b \in R$.*
4. *$I$ can be generated by two elements.*

PROOF. (1): Let $I = P_1^{r_1} \cdots P_n^{r_n}$, where the $P_i$ are distinct maximal ideals and $r_i \in \mathbb{N}$. Distinct maximal ideals are coprime, i.e., $P + Q = R$, and it follows that any powers $P^r$ and $Q^s$ are also coprime. Therefore we can apply the CRT (Chinese remainder theorem) to conclude that $R/I$ is the product of the $R/P_i^{r_i}$, and if $b_i \in R \setminus P_i^{r_i+1}$, then there exists an $a \in R$ such that

$$a \equiv b_i \mod P_i^{r_i+1} \ \forall i$$

We can even choose $b_i \in P^{r_i}$ for each $i$, and then $a \in I$. Now let $J = aI^{-1}$. Then $J \subset R$ and $IJ = (a)$, which proves (1).
(2): Any of the factors of $R/I$, say $R/P^r$ is isomorphic to $R_P/R_P P^r$, which is principal since it is a quotient of a DVR. Therefore $R/I$ is a principal ideal ring, hence Noetherian of dimension 0.
(3): If we take the quotient by $I$ we see that (3) is just a reinterpretation of (2) in $R$.
(4): If $a$ is a nonzero element of $I$, we can apply (3) to the inclusion $(a) \subset I$ to obtain a $b \in R$ such that $I = (a, b)$. □

COROLLARY 5.3.29. *Let $R$ a Dedekind ring. Then any nonzero fractional ideal $A$ has a unique factorization*

$$A = P_1^{r_1} \cdots P_q^{r_q},$$

*where the $P_i$ are maximal ideals and the $r_i$ are nonzero integers.*

PROOF. If $A$ is an ideal, the claim follows from lemma 5.3.23. If we apply this to the ideals $(d)$ and $dA$ where $dA \subset R$, it follows in general. □

# Bibliography


[1] M. F. Atiyah, I. G. Macdonald: *Introduction to commutative algebra.* Addison-Wesley Publishing Co. (1969).

[2] D. Cox, J. Little, D. O'Shea: *Ideals, varieties and algorithms*, Springer-Verlag (1997).

[3] G. H Hardy, E. M. Wright: *An Introduction to the Theory of Numbers.* Oxford University Press (1979).

[4] M. Harper: $\mathbb{Z}[\sqrt{14}]$ *is Euclidean.* Canad. J. Math. **56** (2004), 55–70.

[5] J. C. Jantzen, J. Schwermer: *Algebra.* Springer-Verlag (2006).

[6] J. P. May: *Munshi's proof of the Nullstellensatz.* Amer. Math. Monthly **110** (2003), no. 2, 133–140.

[7] R. Y. Sharp: *Steps in Commutative Algebra.* LMS (2000).