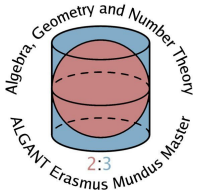
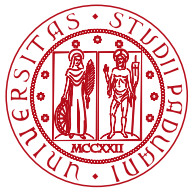
Marco Andrea Garuti

Commutative Algebra Lecture Notes

Version of January 17, 2017





UNIVERSITÀ
DEGLI STUDI
DI PADOVA

This text consists of the notes of a course in Commutative Algebra taught in Padova from 2014-15 to 2016-17. Some topics were also covered during lectures in Stellenbosch in march 2015.

The choice of topics reflects the course structure in Padova, where Commutative Algebra is flanked by *Introduction to Ring Theory* and by *Number Theory 1* and followed by *Algebraic Geometry 1*, sharing most of the audience. There are thus no preliminaries on Category Theory (bare definitions are recalled in the Appendix I, which includes also a short discussion on representable functors) and the theory of modules of finite length is shrunk to a single statement in § 4.2, because these topics are covered in detail in *Introduction to Ring Theory*. We treat extensions of Dedekind domains and their ramification without mentioning the Galois case, which is discussed in *Number Theory 1*. As a preparation to *Algebraic Geometry 1*, we introduce the spectrum of a ring (only as a topological space) already in § 1.1, and we use it to emphasise the topological meaning of the Going Up and Going Down theorems in § 3.2. With applications to line bundles and divisors in mind, the discussion on invertible modules in § 5.2 is extended beyond what is strictly needed for the factorisation of ideals in Dedekind domains, adopting the geometric terminology.

Some other choices were imposed by time constraints and reflect personal taste. The most conspicuous casualty is the theory of primary decomposition, though its absence should not be felt unduly until the end of the last chapter (which is, of course, when things begin to get interesting).

Appendix II contains the solution to some of the exercises, including all those quoted in the main body of text.

Alexander Grothendieck passed away in november 2014. The discussion on the Grothendieck group (of a Dededkind domain) in § 5.4 was meant as a small tribute to this great mathematician, introducing one of the tools that bear his name. His ideas have shaped the development of Commutative Algebra in the second half of the last century and are now woven into its very fabric. Most directly attributable to Grothendieck are the basics of algebraic differential calculus (§ 1.3), faithfully flat descent for modules (§ 2.2) and the theory of Weil and Cartier divisors (§ 5.2).

Contents

Chapter I

Basic notions

§ 1 Rings

Definition 1.1.1 A commutative **ring** with unit in a set $(R, +, \cdot, 1)$ equipped with two binary operations and a fixed element, satisfying the following axioms

a) $(R, +)$ is an abelian group.

b) The multiplication is associative and distributes with respect to addition.

c) The multiplication is commutative.

d) The multiplication has 1 as a neutral element.

Henceforth, we shall simply say "ring" instead of commutative ring with unit.

Remark 1.1.2 For technical reasons, we cannot rule out the **zero ring**. It is the only ring in which $0 = 1$. Indeed, if $0 = 1$ then $x = x \cdot 1 = x \cdot 0 = 0$ for all $x \in R$.

Example 1.1.3 The integers $\mathbb{Z}$, the rationals $\mathbb{Q}$, the reals $\mathbb{R}$ and the complex numbers $\mathbb{C}$ are all examples of rings.

Definition 1.1.4 A subset $R' \subseteq R$ of a ring is a **subring** if R' is a ring with the operations defined on R.

Explicitely, $(R', +)$ is a subgroup of $(R, +)$, the multiplication of two elements in R' stays in R' and $1 \in R'$. For instance $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are subrings of $\mathbb{C}$.

Example 1.1.5 If X is a set and R a ring, the set $F(X, R)$ of all functions $f : X \to R$ is a ring. if we define $f + g$ (resp. fg) as the function taking the value $f(x) + g(x)$ (resp. $f(x)g(x)$) at all elements $x \in X$. The constant functions 0 and 1 provide the neutral elements.

Example 1.1.6 If X is a topological space, the set $C(X)$ of all continuous functions $f : X \to \mathbb{R}$ is a ring, with operations as in example 1.1.5 is a ring.

Example 1.1.7 If R is a ring, the set of polynomials $R[X]$ is a ring, with 0 and 1 as constant polynomials and operations

$$\left(\sum_{i=0}^{n} a_i X^i\right) + \left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{k=0}^{\max\{n,m\}} (a_k + b_k) X^k; \quad (\text{set } a_k = 0 \text{ if } k > n \text{ and } b_k = 0 \text{ if } k > m)$$

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot \left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{k=0}^{n+m} \left(\sum_{h=0}^{k} a_h b_{k-h}\right) X^k$$

with $a_i = 0$ if $i > n$ and $b_j = 0$ if $j > m$. Iterating, we get the polynomial rings $R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$ and the ring of polynomials in infinitely many variables $R[X_1, \ldots, X_n, \ldots]$.

Definition 1.1.8 If R and A are rings, a **ring homomorphism** is a map $\varphi : R \to A$ satisfying

$$\varphi(x + y) = \varphi(x) + \varphi(y); \quad \varphi(xy) = \varphi(x)\varphi(y) \quad \forall\, x, y \in R; \quad \varphi(1) = 1.$$

An **isomomorphism** is a bijective homomorphism.

We leave it as an exercise to check that the composition of ring homomorphisms is a homomorphism.

Example 1.1.9 If R' is a subring of a ring R, the inclusion $R' \hookrightarrow R$ is a ring homomorphism. E.g $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$ are all rings homomorphisms.

Example 1.1.10 If R is a ring, X a set and $x_0 \in X$, the map

$$\begin{array}{rcl} F(X, R) & \longrightarrow & R \\ f & \longmapsto & f(x_0) \end{array}$$

is a ring homomorphism.

Proposition 1.1.11 *If $\varphi : R \to A$ is a ring homomorphism, then $\operatorname{im}\varphi$ is a subring of A.*

Proof. Straightforward from the definitions. Notice $1 = \varphi(1) \in \operatorname{im}\varphi$. □

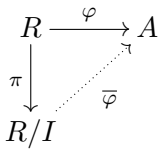
Definition 1.1.12 A subset $I \subset R$ of a ring is an **ideal** if $(I, +)$ is a subgroup of $(R, +)$ and $xy \in I$ for all $x \in R$ and all $y \in I$.

Proposition 1.1.13 *If $\varphi : R \to A$ is a ring homomorphism, and $J \subseteq A$ is an ideal of A then $\varphi^{-1}(J) = \{x \in R \,|\, \varphi(x) \in J\}$ is an ideal in R. In particular $\ker\varphi = \varphi^{-1}(0)$ is an ideal of R.*

Proof. Indeed it is a subgroup and, for all $x \in R$ and $y \in \varphi^{-1}(J)$ we have $\varphi(xy) = \varphi(x)\varphi(y) \in J$ because $\varphi(y) \in J$. □

For instance, if R is a ring and X a set, the set of all functions vanishing at some point $x_0 \in X$ is an ideal, kernel of the homomorphism in example 1.1.10.

Proposition 1.1.14 *If $I \subseteq R$ is an ideal, the quotient R/I is a ring and the projection $\pi : R \to R/I$ is a ring homomorphism. Any ring homomorphism $\varphi : R \to A$ such that $I \subseteq \ker \varphi$ factors uniquely through a ring homomorphism $\overline{\varphi} : R/I \to A$:*



Proof. Recall that R/I is the quotient group of R by the equivalence relation $x \sim y \iff x-y \in I$. The relation is compatible with multiplication ($x \sim y \implies xz \sim yz$ for all $z \in R$, because $xz - yz = z(x-y) \in I$ if $x - y \in I$) and so we can multiply classes in R/I: $\overline{x} \cdot \overline{y} = \overline{xy}$ is well-defined.
For any homomorphism $\varphi : R \to A$ such that $\varphi(y) = 0$ for all $y \in I$ we have that $\varphi(x) = \varphi(x')$ whenever $x \sim x'$. Thus $\overline{\varphi}(\overline{x}) = \varphi(x)$ is well defined, and obviously a ring homomorphism. □

Example 1.1.15 For any ring R there is a unique ring homomorphism $\varphi : \mathbb{Z} \to R$ defined by $\varphi(1) = 1$ (hence $\varphi(n) = 1 + \cdots + 1$ for all $n \in \mathbb{N}$). Its kernel is an ideal of $\mathbb{Z}$. Hence $\ker \varphi = m\mathbb{Z}$ for some integer $m \in \mathbb{N}$ called the **characteristic** of R.

Example 1.1.16 If $I = R$, then R/I is the zero ring. In many arguments it will be necessary to accept the whole ring as an ideal, and this one of the reasons for including the zero ring.

Proposition 1.1.17 *An ideal $I \subseteq R$ gives rise to a bijection*

$$\begin{array}{rcl} \{\text{Ideals in } R \text{ containing } I\} & \longrightarrow & \{\text{Ideals in } R/I\}. \\ J & \longmapsto & J/I \\ \pi^{-1}(\bar{J}) & \longleftarrow\!\shortmid & \bar{J} \end{array}$$

Proof. The two maps are obviously inverse to each other. □

Definition 1.1.18 Let R be a ring and $S \subseteq R$. The set $(S) = \{\sum_i x_i s_i \mid x_i \in R,\, s_i \in S\}$ (finite sums) is clearly an ideal, called the **ideal generated** by S. An ideal is **finitely generated** if it can be generated by a finite subset. For instance the set of all multiples of an element $x \in R$ is a **principal ideal**, denoted (x) or xR.

Definition 1.1.19 Let R be a ring and $x \in R$.

a) We say that x is a **zero-divisor** if $xy = 0$ for some $y \neq 0$.

b) We say that x is a **nilpotent** if $x^n = 0$ for some $n \in \mathbb{N}$.

c) We say that x is a **unit** or **invertible** if $xy = 1$ for some $y \in R$.

Remark 1.1.20 It is straightforward to check that the subset $R^\times$ of invertible elements in a ring is an abelian group with respect to multiplication. In particular, if x is invertible, the element $y \in R^\times$ such that $xy = 1$ is unique and denoted $y = x^{-1}$.

Example 1.1.21 In $\mathbb{Z}/6\mathbb{Z}$, the element $\overline{2}$ is a zero-divisor, as $\overline{2} \cdot \overline{3} = \overline{0}$, while $\overline{5}$ is a unit, since $\overline{5}^2 = \overline{1}$. In $\mathbb{Z}/4\mathbb{Z}$ the element $\overline{2} \neq \overline{0}$ is nilpotent, as $\overline{2}^2 = 0$.

Example 1.1.22 The partitions of unity show that the ring $C(\mathbb{R})$ has plenty of zero-divisors.

Definition 1.1.23 The **nilradical** of a ring is the set $\mathfrak{N}_R$ of all nilpotent elements in R.

The nilradical is an ideal: if $x^n = 0 = y^m$ then $(x+y)^{n+m} = \sum_{i=0}^{n+m} x^i y^{n+m-i} = 0$ because in every monomial at least one of the exponents is bigger than either n or m. Moreover, for every $z \in R$, clearly $(zx)^n = z^n x^n = z^n 0 = 0$.

Remark 1.1.24 The set of zero-divisors in R is not an ideal in general, e.g. $\overline{2} + \overline{3} = \overline{5} \in (\mathbb{Z}/6\mathbb{Z})^\times$.

Definition 1.1.25 A **domain** is a ring in which the only zero-divisor is 0.

Example 1.1.26 The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are domains. If R is a domain, so is $R[X]$. A subring of a domain is a domain.

Remark 1.1.27 The characteristic of a domain R is either zero or a prime number. Indeed if the characteristic is $m \neq 0$, an equation $m = ab$ in $\mathbb{Z}$ implies $(a \cdot 1)(b \cdot 1) = 0$ in R hence either $a \cdot 1 = 0$ or $b \cdot 1 = 0$. By definition of characteristic, either $a \in m\mathbb{Z}$ or $b \in m\mathbb{Z}$, so either $m = \pm a$ or $m = \pm b$. Therefore m is an irreducible element in $\mathbb{Z}$, hence prime.

Definition 1.1.28 A **field** is a ring in which every nonzero element is invertible.

Example 1.1.29 $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields. For $p > 1$, the ring $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is a prime number: by Fermat's little theorem, $x^p \equiv x \bmod p$, so $\overline{x}^{-1} = \overline{x}^{p-2}$ for $\overline{x} \neq 0$. We shall write $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and more generally $\mathbb{F}_q$ for the field with q elements.

Proposition 1.1.30 *Let R be a nonzero ring. The following conditions are equivalent:*

a) R is a field;

b) Any nonzero homomorphism $\varphi : R \to A$ is injective;

c) The only ideals in R are 0 and R.

Proof. a) $\Longrightarrow$ b) If $x \in \ker \varphi$, $x \neq 0$ then $1 = x^{-1}x \in \ker \varphi$, hence φ is the zero homomorphism.
b) $\Longrightarrow$ c) If $I \subsetneq R$ is a proper ideal, $\pi : R \to R/I$ can't be the zero map, so must be injective, hence $I = \ker \pi = 0$.
c) $\Longrightarrow$ a) If $x \neq 0$, then $xR \neq 0$ hence $xR = R$ and then 1 is a multiple of x. □

Definition 1.1.31 A **principal ideal domain**, or **PID** for short, is a domain in which every ideal is principal.

Example 1.1.32 $\mathbb{Z}$ is a PID. For any field k, the polynomial ring $k[X]$ is a PID. Both statements are easy consequences of the euclidean algorithm.

Definition 1.1.33 An element $x \in R$ is **irreducible** if $x \notin R^\times$ and whenever $x = yz$ in R then either y or z is a unit. A domain is a **unique factorisation domain**, also called **factorial**, or **UFD** for short, if every element can be written as a product of irreducible elements multiplied by a unit, the irreducible factors being unique up to order and multiplication by units.

Example 1.1.34 Again, the euclidean algorithm shows that a PID is a UFD. Gauss' lemma states that if R is a UFD then $R[X]$ is a UFD.

Remark 1.1.35 In corollary 6.1.13 we will characterise UFDs in terms of principal ideals.

Prime and Maximal Ideals

Definition 1.1.36 A proper ideal $\mathfrak{p} \subsetneq R$ is a **prime ideal** if for any two elements $x, y \in R$ such that $xy \in \mathfrak{p}$ either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

Example 1.1.37 The ideal $p\mathbb{Z}$ is prime if and only if p is a prime number.

Proposition 1.1.38 *Let R be a ring, $\mathfrak{p} \subsetneq R$ a proper ideal. The following conditions are equivalent:*

a) $\mathfrak{p}$ is prime;

b) $R/\mathfrak{p}$ is a domain.

Proof. By definition $\overline{x} \cdot \overline{y} = \overline{xy} = 0$ in $R/\mathfrak{p}$ if and only if $xy \in \mathfrak{p}$. □

Corollary 1.1.39 *The zero ideal is prime if and only if R is a domain.*

Example 1.1.40 If p is a prime number, $p\mathbb{Z}[X] \subset \mathbb{Z}[X]$ is a prime ideal. Indeed, $p\mathbb{Z}[X] = \ker \pi$, where $\pi : \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$ is $\pi(\sum a_i X^i) = \sum \overline{a}_i X^i$. Hence $\mathbb{Z}[X]/p\mathbb{Z}[X] \cong (\mathbb{Z}/p\mathbb{Z})[X]$. The converse does not hold in general: a classical example is $R = \mathbb{Z}[\sqrt{-5}]$, where $x = 1 + \sqrt{-5}$ is irreducible and $6 = x(2 - x) \in xR$ even though $2, 3 \notin xR$. However, if R is a UFD, then every irreducible element x is prime: if $yz = xt$ then x is an irreducible factor of either y or z.

Example 1.1.41 Let R be a domain. The ideal $(X) \subset R[X]$ is prime, since $R[X]/(X) \cong R$. If X is a set, the set of all functions vanishing at some point $x_0 \in X$ is a prime ideal in $F(X, R)$, since the quotient is isomorphic to R.

Remark 1.1.42 Let R be a domain. We may call $x \in R$ a **prime element** if xR is a prime ideal. A prime element is irreducible: if $x = yz$ then either y or z belongs to xR; if $y = xu$ for some $u \in R$, then $0 = x - yz = x(1 - uz)$, hence $uz = 1$ and $z \in R^\times$.

Proposition 1.1.43 *Let $\varphi : R \to A$ be a ring homomorphism. If $\mathfrak{q} \subset A$ is a prime ideal, then $\varphi^{-1}(\mathfrak{q}) \subset R$ is prime.*

Proof. By proposition 1.1.14, $R/\varphi^{-1}(\mathfrak{q}) \hookrightarrow A/\mathfrak{q}$ and the latter is a domain. □

Definition 1.1.44 A proper ideal $\mathfrak{m} \subsetneq R$ is a **maximal ideal** if there is no proper ideal in R strictly containing $\mathfrak{m}$.

In other words, if $I \subset R$ is an ideal such that $\mathfrak{m} \subseteq I \subseteq R$, then either $\mathfrak{m} = I$ or $I = R$.

Proposition 1.1.45 *Let R be a ring, $\mathfrak{m} \subsetneq R$ a proper ideal. The following conditions are equivalent:*

a) $\mathfrak{m}$ *is maximal;*

b) $R/\mathfrak{m}$ *is a field.*

Proof. If $\mathfrak{m}$ is maximal and $x \notin \mathfrak{m}$ then the ideal generated by $\mathfrak{m}$ and x is R: there exist $z \in \mathfrak{m}$ and $y \in R$ such that $1 = xy + z$. Then $\overline{x}$ is invertible in $R/\mathfrak{m}$ with inverse $\overline{y}$. Conversely, if $R/\mathfrak{m}$ is a field consider $\mathfrak{m} \subseteq I \subseteq R$. If I contains an element $x \notin \mathfrak{m}$, since x is invertible mod $\mathfrak{m}$ there exist $z \in \mathfrak{m}$ and $y \in R$ such that $1 = xy + z \in I$, so $I = R$. □

Corollary 1.1.46 *Every maximal ideal is prime.*

Proof. Indeed the field $R/\mathfrak{m}$ is a domain. □

Example 1.1.47 If p is a prime number, $p\mathbb{Z} \subset \mathbb{Z}$ is a maximal ideal.

Example 1.1.48 Let k be a field. The ideal $(X) \subset k[X]$ is maximal, since $k[X]/(X) \cong k$. If X is a set, the set of all functions vanishing at some point $x_0 \in X$ is a maximal ideal in $F(X, k)$, since the quotient is isomorphic to k.

If $\varphi : R \to A$ is a ring homomorphism and $\mathfrak{m} \subset A$ is a maximal ideal, in general $\varphi^{-1}(\mathfrak{m}) \subset R$ is not maximal. For instance, consider the inclusion $\varphi : \mathbb{Z} \hookrightarrow \mathbb{Q}$ and $\varphi^{-1}(0) = 0$. However:

Proposition 1.1.49 *Let $\varphi : R \to A$ be a surjective ring homomorphism. If $\mathfrak{m} \subset A$ is a maximal ideal, then $\varphi^{-1}(\mathfrak{m}) \subset R$ is maximal.*

Proof. Consider the diagram

$$\begin{array}{ccccc} R & \xrightarrow{\varphi} & A & \xrightarrow{\psi} & A/\mathfrak{m}. \\ {\scriptstyle\pi}\downarrow & & & \nearrow_{\overline{\psi\circ\varphi}} & \\ R/\varphi^{-1}(\mathfrak{m}) & & & & \end{array}$$

Since $\psi \circ \varphi$ is surjective, $\overline{\psi \circ \varphi} \circ \pi$ is surjective, thus $\overline{\psi \circ \varphi}$ is surjective. It is injective by proposition 1.1.14. Hence $R/\varphi^{-1}(\mathfrak{m}) \simeq A/\mathfrak{m}$ is a field, so $\varphi^{-1}(\mathfrak{m})$ is maximal. □

Maximal and prime ideals always exist. This is a simple application of Zorn's lemma which we now recall. A set Σ is **partially ordered** if it admits a reflexive and transitive relation $\leq$ such that

$$\begin{cases} x \leq y \\ y \leq x \end{cases} \quad \Longrightarrow \quad x = y.$$

An element $m \in \Sigma$ is **maximal** if the condition $x \geq m$ implies $x = m$. A **chain** is a subset $C \subseteq \Sigma$ such that for every $x, y \in C$, either $x \leq y$ or $y \leq x$.

Theorem 1.1.50 (Zorn's Lemma) *Let Σ be a partially ordered non-empty set. Suppose that for every chain $C \subseteq \Sigma$ there exists an element $s \in \Sigma$ such that $x \leq s$ for all $x \in C$. Then Σ has maximal elements.* ⊠

Corollary 1.1.51 *Let R be a nonzero ring. Then R contains a maximal ideal.*

Proof. Let Σ be the set of proper ideals of R, partially ordered by inclusion. It is not empty because $0 \in \Sigma$ (proper, since $0 \neq 1$). Let $C = \{\mathfrak{a}_n\}_{n\in\mathbb{N}}$ be a chain in Σ. The set $\mathfrak{a} = \bigcup_{n\in\mathbb{N}} \mathfrak{a}_n$ is an ideal, because for all $x, y \in \mathfrak{a}$ we have $x, y \in \mathfrak{a}_n$ for a sufficiently large n, hence $x + y \in \mathfrak{a}_n \subset \mathfrak{a}$ and $zx \in \mathfrak{a}_n \subset \mathfrak{a}$ for all $z \in R$. Moreover $\mathfrak{a}$ is a proper ideal, because $1 \notin \mathfrak{a}_n$ for all n. Hence $\mathfrak{a} \in \Sigma$ and $\mathfrak{a} \supseteq \mathfrak{a}_n$ for all $\mathfrak{a}_n \in C$. We can thus apply Zorn's lemma to conclude that R has maximal elements.

Corollary 1.1.52 *Every proper ideal $I \subsetneq R$ is contained in a maximal ideal.*

Proof. Recall proposition 1.1.17 and apply corollary 1.1.51 to R/I. □

Corollary 1.1.53 *In a nonzero ring, every $x \notin R^\times$ is contained in a maximal ideal.*

Proof. Apply corollary 1.1.52 to xR. □

Proposition 1.1.54 *The nilradical is the intersection of all the prime ideals.*

Proof. Clearly a nilpotent element belongs to every prime ideal. Conversely, let $x \in R$ be a non-nilpotent element. We look for a prime ideal not containing x. Let Σ be the set of all ideals $\mathfrak{a} \subset R$ such that $x^n \notin \mathfrak{a}$ for all $n \in \mathbb{N}$. Since x is not nilpotent, $0 \in \Sigma$, which is thus non-empty. Again, if $C = \{\mathfrak{a}_n\}_{n\in\mathbb{N}}$ is a chain in Σ then $\mathfrak{a} = \bigcup_{n\in\mathbb{N}} \mathfrak{a}_n \in \Sigma$, hence Σ satisfies the assumption of Zorn's lemma. Let $\mathfrak{p} \in \Sigma$ be a maximal element. We need to show that $\mathfrak{p}$ is prime. If $y, z \notin \mathfrak{p}$ then $\mathfrak{p}$ is properly contained in $(y, \mathfrak{p})$ and $(z, \mathfrak{p})$, so these ideals are not in Σ: there exist integers $n, m \in \mathbb{N}$ and elements $a, c \in R$ and $b, d \in \mathfrak{p}$ such that $x^n = ay + b$ and $x^m = cz + d$. If $yz \in \mathfrak{p}$ we would get $x^{n+m} = acyz + (ayd + czb + bd) \in (yz, \mathfrak{p}) = \mathfrak{p}$, which is a contradiction. □

Definition 1.1.55 The **Jacobson radical** is the intersection $\mathfrak{R}_R$ of all the maximal ideals of R.

The Jacobson radical is clearly an ideal. Its elements can be characterised as follows:

Proposition 1.1.56 *An element $x \in \mathfrak{R}_R$ if and only if $1 - xy \in R^\times$ for all $y \in R$.*

Proof. Let $x \in R$ such that $1 - xy$ is a unit for all $y \in R$ and let $\mathfrak{m}$ be a maximal ideal. If $x \notin \mathfrak{m}$, then $(x, \mathfrak{m}) = R$: there exist $y \in R$ and $z \in \mathfrak{m}$ such that $1 = xy + z$. Hence $\mathfrak{m} = R$, because it contains the unit $z = 1 - xy$. Conversely, if $x \in R$ belongs to every maximal ideal, then for all $y \in R$ and all maximal ideal $\mathfrak{m}$ we have $1 - xy \notin \mathfrak{m}$, otherwise $1 \in \mathfrak{m}$. Corollary 1.1.53 implies that $1 - xy \in R^\times$. □

Definition 1.1.57 A ring is **local** if it has a unique maximal ideal. A **semi-local ring** is a ring with finitely many maximal ideals.

Example 1.1.58 If p is a prime number and $n \geq 1$ an integer, $\mathbb{Z}/p^n\mathbb{Z}$ is a local ring, with maximal ideal $p\mathbb{Z}/p^n\mathbb{Z}$. Indeed, by proposition 1.1.17 the ideals of $\mathbb{Z}/p^n\mathbb{Z}$ are in bijection with the ideals of $\mathbb{Z}$ containing p^n, and by proposition 1.1.49 this bijection preserves maximal ideals. We then notice that $p\mathbb{Z}$ is the only maximal ideal in $\mathbb{Z}$ containing p^n. A similar argument shows that if k is a field, $k[X]/(X^n)$ is local.

Example 1.1.59 $\mathbb{Z}/6\mathbb{Z}$ is a semilocal ring, with maximal ideals $2\mathbb{Z}/6\mathbb{Z}$ and $3\mathbb{Z}/6\mathbb{Z}$. Indeed, by propositions 1.1.17 and 1.1.49 the maximal ideals of $\mathbb{Z}/6\mathbb{Z}$ are in bijection with the ideals of $\mathbb{Z}$ containing 6: the only ones are $2\mathbb{Z}$ and $3\mathbb{Z}$.

Proposition 1.1.60 *Let R be a ring.*

a) If $\mathfrak{a} \subset R$ is a proper ideal such that $R - \mathfrak{a} \subseteq R^\times$, then R is local with maximal ideal $\mathfrak{a}$.

b) Let $\mathfrak{m} \subset R$ be a maximal ideal. If $1 + x \in R^\times$ for all $x \in \mathfrak{m}$, then R is local.

Proof. a) Let $\mathfrak{a} \subseteq I \subseteq R$. If $\mathfrak{a} \neq I$, then I contains an element in $R - \mathfrak{a}$, i.e. a unit. Hence $I = R$, thus $\mathfrak{a}$ is maximal. It is the unique maximal ideal because any other ideal not contained in $\mathfrak{a}$ contains a unit.
b) Let $\mathfrak{b} \subset R$ be any ideal. If $\mathfrak{b} \neq \mathfrak{m}$, let $y \in \mathfrak{b}$, $y \notin \mathfrak{m}$. By maximality, $(y, \mathfrak{m}) = R$. Write $1 = ay + x$ for some $a \in R$, $x \in \mathfrak{m}$. Then $ay = 1 - x \in \mathfrak{b}$ is a unit, hence $\mathfrak{b} = R$. Therefore, every proper ideal is contained in $\mathfrak{m}$. □

Operations on Ideals

Proposition 1.1.61 *Let R be a ring, $\{I_\alpha\}_\alpha$ a family of ideals. The intersection $\bigcap_\alpha I_\alpha$ and the sum $\sum_\alpha I_\alpha = \{\sum_\alpha x_\alpha,\ x_\alpha \in I_\alpha,\ x_\alpha = 0$ for all but finitely many $\alpha\}$ are ideals of R.*

Proof. We know that $\sum_\alpha I_\alpha$ and $\bigcap_\alpha I_\alpha$ are subgroups of R. For $x \in \bigcap_\alpha I_\alpha$ and $y \in R$ we have $yx \in I_\alpha$ for all α because I_α are ideals, hence $yx \in \bigcap_\alpha I_\alpha$. Similarly, for $x_{\alpha_1} \in I_{\alpha_1}, \ldots, x_{\alpha_r} \in I_{\alpha_r}$ we have $yx_{\alpha_j} \in I_{\alpha_j}$, hence $y(x_{\alpha_1} + \cdots + x_{\alpha_r}) = yx_{\alpha_1} + \cdots + yx_{\alpha_r} \in \sum_\alpha I_\alpha$. □

Proposition 1.1.62 *Let I and J be ideals in a ring R. The set $IJ = \{\sum_i x_i y_i,\ \forall\ x \in I,\ y \in J\}$ of finite sums of products of an element in I by an element in J is an ideal, called the* **product ideal**.

Proof. IJ is non-empty because it contains 0. The sum of two elements in IJ is again a finite sum, hence in IJ. For any $a \in R$ we have $a(\sum_i x_i y_i) = \sum_i (ax_i) y_i \in IJ$ because all $ax_i \in I$. □

Example 1.1.63 Let R be a PID, $I = (x)$ and $J = (y)$. Then $I + J = (\gcd(x, y))$, $I \cap J = (\operatorname{lcm}(x, y))$ and $IJ = (xy)$. In particular, $IJ = I \cap J$ if and only if $\gcd(x, y) = 1$.

Definition 1.1.64 Two ideals $I, J \subseteq R$ are **coprime** or **relatively prime** if $I + J = R$.

Proposition 1.1.65 *Let I and J be ideals in a ring R. Then $IJ \subseteq I \cap J$ with equality if I and J are coprime.*

Proof. The inclusion $IJ \subseteq I \cap J$ is obvious from the definitions. Suppose $I + J = R$, write $1 = x + y$ with $x \in I$ and $y \in J$. Then for any $z \in I \cap J$, we have $xz \in I$ and $yz \in J$, hence $z = 1z = xz + yz \in IJ$. □

Corollary 1.1.66 *Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals in a ring R. Then $\prod_{i=1}^n \mathfrak{a}_i \subseteq \bigcap_{i=1}^n \mathfrak{a}_i$ with equality if the ideals are pairwise coprime: $\mathfrak{a}_i + \mathfrak{a}_j = R$ for all $i \neq j$.*

Proof. The inclusion is clear. By induction, let $\mathfrak{b} = \prod_{i=1}^{n-1} \mathfrak{a}_i = \bigcap_{i=1}^{n-1} \mathfrak{a}_i$. For $i \in \{1, \ldots, n-1\}$, choose $x_i \in \mathfrak{a}_i$ and $y_i \in \mathfrak{a}_n$ such that $x_i + y_i = 1$. Then $x = \prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1}(1 - y_i) = 1 + y$ for a suitable $y \in \mathfrak{a}_n$, while by definition $x \in \mathfrak{b}$. The equation $1 = x + y$ shows that $\mathfrak{b}$ and $\mathfrak{a}_n$ are coprime, hence $\prod_{i=1}^n \mathfrak{a}_i = \mathfrak{b}\mathfrak{a}_n = \mathfrak{b} \cap \mathfrak{a}_n = \bigcap_{i=1}^n \mathfrak{a}_i$ by proposition 1.1.65. □

Definition 1.1.67 Let $\{R_\alpha\}_\alpha$ be a collection of rings. The product abelian group $\prod_\alpha R_\alpha$ is a ring, called the **direct product**, with multiplication $(\ldots, a_\alpha, \ldots) \cdot (\ldots, b_\alpha, \ldots) = (\ldots, a_\alpha b_\alpha, \ldots)$ and $1 = (\ldots, 1, \ldots)$. The projections $\pi_\alpha : \prod_\alpha R_\alpha \to R_\alpha$ are ring homomorphisms.

Notice that the injections $R_\beta \to \prod_\alpha R_\alpha$ are not homomorphisms, as they do not map 1 to 1.

Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals in a ring R.The projections $\pi_i : R \to R/\mathfrak{a}_i$ define a natural ring homomorphism

$$\begin{aligned} \varphi : R &\longrightarrow \textstyle\prod_{i=1}^n R/\mathfrak{a}_i. \\ x &\longmapsto (\pi_1(x), \ldots, \pi_n(x)) \end{aligned} \tag{1.1}$$

Clearly, $\ker \varphi = \bigcap_{i=1}^n \mathfrak{a}_i$. We can say more:

Corollary 1.1.68 (Chinese Remainder Theorem) *The morphism φ in (1.1) is surjective if and only if the ideals $\mathfrak{a}_i$ are pairwise coprime.*

Proof. If φ is surjective, for every $i \neq j$ the composite map $R \to \prod_{i=1}^n R/\mathfrak{a}_i \to R/\mathfrak{a}_i \times R/\mathfrak{a}_j$ is surjective too. Take $x \in R$ mapping to $(1, 0)$, i.e. $x \equiv 1 \bmod \mathfrak{a}_i$ and $x \equiv 0 \bmod \mathfrak{a}_j$. Then $1 = (1 - x) + x \in \mathfrak{a}_i + \mathfrak{a}_j$.
Conversely, if the $\mathfrak{a}_i$ are pairwise coprime, for $i = 2, \ldots, n$ choose $x_i \in \mathfrak{a}_1$ and $y_i \in \mathfrak{a}_i$ such that $x_i + y_i = 1$. Then $y = \prod_{i=2}^n y_i \in \mathfrak{a}_i$ for all $i \in \{2, \ldots, n\}$ but also $y = \prod_{i=2}^n (1 - x_i) \equiv 1 \bmod \mathfrak{a}_1$, therefore $\varphi(y) = (1, 0, \ldots, 0)$. Permuting the indices, we see that φ is surjective. □

THE PRIME SPECTRUM

It is fair to say that most of modern Commutative Algebra has been inspired or motivated by Algebraic Geometry and Number Theory. Classically, Algebraic Geometry investigates the properties of algebraic varieties, the loci in affine or projective spaces defined by systems of polynomial equations. The zero locus of a polynomial in one variable over an algebraically closed field k is just a finite collection of points in the affine line, the roots of the polynomial. Any reasonable topology on the affine line should consider these loci as closed sets. Therefore, if polynomials are to be continuous functions on the affine space k^n, the natural topology should be the *Zariski topology*: open sets are complementary to finite unions of zero loci of polynomials.

Thus $k[X_1, \ldots, X_n]$ is viewed as the ring of continuous functions on a basic topological space, the affine n-dimensional space. It was one of Grothendieck's insights to jump from particular to universal and regard every ring R as the ring of continuous functions on a topological space intrinsically attached to it, its spectrum $\operatorname{Spec} R$. This conceptual breakthrough allows to do geometry with arbitrary coefficient rings, not just algebraically closed fields, blending thus Algebraic Geometry and Number Theory into Arithmetic Geometry.

Definition 1.1.69 Let R be a ring and $I \subseteq R$ an ideal. The **zero locus** of I is the set $\mathcal{Z}(I)$ of all the prime ideals in R containing I.

Example 1.1.70 In any ring R, we have $\mathcal{Z}(1) = \varnothing$ (as all prime ideals are assumed to be proper ideals) while $\mathcal{Z}(0)$ is the set of all prime ideals. If $\mathfrak{m} \subset R$ is a maximal ideal, $\mathcal{Z}(\mathfrak{m}) = \{\mathfrak{m}\}$.

Example 1.1.71 In $R = \mathbb{Z}$ we have $\mathcal{Z}((30)) = \{(2), (3), (5)\}$.

Example 1.1.72 In $R = \mathbb{C}[X, Y]$ we have $\mathcal{Z}((X)) = \{(X); (X, Y - y) \; \forall \, y \in \mathbb{C}\}$. Indeed, if $X \in \mathfrak{p}$ and $\mathfrak{p}$ is generated by some polynomials f_i, we must have an equation $X = g_{i_1} f_{i_1} + \cdots + g_{i_r} f_{i_r}$. Taking degrees, we see that this is possible only if one of the generators is a nonzero scalar multiple of X. If $\mathfrak{p} \neq (X)$ then $\mathfrak{p}/(X)$ is a non-trivial prime ideal of $\mathbb{C}[X, Y]/(X) \simeq \mathbb{C}[Y]$. The latter is a PID and its prime ideals are generated by irreducible polynomials, which have degree 1 by the fundamental theorem of algebra. Hence $\mathfrak{p} = (X, Y - y)$ for a suitable $y \in \mathbb{C}$.

Proposition 1.1.73 *Let R be a ring, I, J and $\{I_\alpha\}_\alpha$ ideals.*

a) If $I \subseteq J$ then $\mathcal{Z}(J) \subseteq \mathcal{Z}(I)$;

b) $\mathcal{Z}(IJ) = \mathcal{Z}(I) \cup \mathcal{Z}(J)$;

c) $\mathcal{Z}(\sum_\alpha I_\alpha) = \bigcap_\alpha \mathcal{Z}(I_\alpha)$.

Proof. a) is obvious from the definition. Since IJ is contained in both I and J, this proves $\mathcal{Z}(IJ) \supseteq \mathcal{Z}(I) \cup \mathcal{Z}(J)$. On the other hand, if $IJ \subseteq \mathfrak{p}$ and $I \nsubseteq \mathfrak{p}$, let $x \in I$, $x \notin \mathfrak{p}$. Since for all $y \in J$ we have $xy \in IJ \subseteq \mathfrak{p}$ and $x \notin \mathfrak{p}$, necessarily $y \in \mathfrak{p}$. Therefore $J \subseteq \mathfrak{p}$, whence b).
c) Any prime containing each of the I_α contains their sum and conversely each I_α is contained in the sum, hence any prime containing the sum contains every I_α. □

Definition 1.1.74 The **spectrum** of a ring R is the set $\operatorname{Spec} R$ of all prime ideals in R, equipped with the **Zariski topology** in which an open sets are the subsets of the form $\operatorname{Spec} R - \mathcal{Z}(I)$ for some ideal $I \subseteq R$.

The sets $\mathcal{Z}(I)$ truly define a topology: the empty set and the whole space are both open and closed by example 1.1.70; finite unions and arbitrary intersections of closed subsets are closed by proposition 1.1.73.

Proposition 1.1.75 *A ring homomorphism $\varphi : R \to A$ determines a continuous map*

$$\begin{aligned} \varphi^\sharp : \operatorname{Spec} A &\longrightarrow \operatorname{Spec} R. \\ \mathfrak{q} &\longmapsto \varphi^{-1}(\mathfrak{q}) \end{aligned}$$

In other words, Spec *is a contravariant functor from the category of rings to that of topological spaces.*

Proof. The map $\varphi^\sharp$ is well defined by proposition 1.1.43. If $I \subseteq R$ is an ideal,

$$\begin{aligned}\left(\varphi^\sharp\right)^{-1} \mathcal{Z}(I) &= \left\{\mathfrak{q} \in \operatorname{Spec} A \,|\, \varphi^\sharp(\mathfrak{q}) \in \mathcal{Z}(I)\right\} \\ &= \left\{\mathfrak{q} \in \operatorname{Spec} A \,|\, I \subseteq \varphi^{-1}(\mathfrak{q})\right\} \\ &= \{\mathfrak{q} \in \operatorname{Spec} A \,|\, \varphi(I) \subseteq \mathfrak{q}\} \\ &= \mathcal{Z}\left(\varphi(I)\right).\end{aligned}$$

Therefore $\varphi^\sharp$ is continuous. □

The correspondence between ideals in R and closed subsets in $\operatorname{Spec} R$ is not perfect: if $I \subseteq R$ is an ideal, by proposition 1.1.73 $\mathcal{Z}(I^2) = \mathcal{Z}(I) \cup \mathcal{Z}(I) = \mathcal{Z}(I)$ but in general $I \neq I^2$. This prompts the following definition

Definition 1.1.76 Let R be a ring and $I \subseteq$ an ideal. The **radical** of I is the ideal

$$\sqrt{I} = \{x \in R \,|\, \exists\, n \in \mathbb{N},\ x^n \in I\}.$$

If $I = \sqrt{I}$, we say that I is a **radical ideal**.

To show that $\sqrt{I}$ is indeed an ideal, one can either check it directly or notice that $\sqrt{0} = \mathfrak{N}_R$. In general, if $\pi : R \to R/I$ is the canonical projection, $\sqrt{I} = \pi^{-1}\left(\mathfrak{N}_{R/I}\right)$. It follows now from propositions 1.1.17 and 1.1.54 that $\sqrt{I}$ is the intersection of all the prime ideals containing I.

Example 1.1.77 Any prime ideal is radical. The ideal $6\mathbb{Z}$ is a radical ideal in $\mathbb{Z}$ and $\sqrt{12\mathbb{Z}} = 6\mathbb{Z}$.

We can thus refine proposition 1.1.73.a:

Corollary 1.1.78 *If I and J are ideals, $\mathcal{Z}(J) \subseteq \mathcal{Z}(I) \iff \sqrt{I} \subseteq \sqrt{J}$.*

Proof. Since $\mathcal{Z}(I) = \mathcal{Z}(\sqrt{I})$, one implication follows from proposition 1.1.73.a. If $\mathcal{Z}(J) \subseteq \mathcal{Z}(I)$, every prime ideal containing J also contains I. Thus $\sqrt{I} = \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p} \subseteq \bigcap_{J \subseteq \mathfrak{p}} \mathfrak{p} = \sqrt{J}$. □

Remark 1.1.79 As a topological space, $\operatorname{Spec} R$ admittedly presents features that are far from the intuition acquired by dealing with the standard real or complex topology. For instance it is very much non-Hausdorff: if R is a domain, 0 is a prime ideal contained in the neighborhood of every point. Points are not necessarily closed: again in a domain 0 is a point whose closure is the whole space. In general, the closure of a point $\mathfrak{p} \in \operatorname{Spec} R$ is

$$\overline{\{\mathfrak{p}\}} = \bigcap_{I \subseteq \mathfrak{p}} \mathcal{Z}(I) = \bigcap_{I \subseteq \mathfrak{p}} \{\mathfrak{q} \supseteq I\} = \mathcal{Z}(\mathfrak{p}).$$

In particular, the closed points in $\operatorname{Spec} R$ are the *maximal* ideals. In classical Algebraic Geometry, one only considers closed points. An affine *algebraic variety* over an algebraically closed field k, classically defined as the set of points in the afine space k^n whose coordinates are solutions to a system of equations $F_1(X_1, \ldots, X_n) = 0, \ldots F_m(X_1, \ldots, X_n) = 0$, will be identified with the set of closed points in $\mathcal{Z}(F_1, \ldots, F_m) \subseteq \operatorname{Spec} k[X_1, \ldots, X_n]$, by means of Hilbert's Nullstellensatz (corollary 4.3.7).
However, as remarked just before proposition 1.1.49, maximal ideals do not behave well with respect to ring homomorphism and one only gets the whole picture by considering all prime ideals i.e by working with *schemes* instead of varieties.

Remark 1.1.80 We have described the spectrum of a ring simply as a topological space. It has in fact a richer structure, encoded by the extra datum of a *sheaf of rings*.

§ 2 Modules

Definition 1.2.1 Let R be a ring. An R**-module** is an abelian group M equipped with a multiplication

$$\begin{array}{rcl} R \times M & \longrightarrow & M \\ (x, m) & \longmapsto & xm \end{array}$$

such that the following relations hold for every $x, y \in R$ and $m, n \in M$:

$$(x+y)m = xm + ym; \quad x(m+n) = xm + xn; \quad (xy)m = x(ym); \quad 1m = m.$$

Definition 1.2.2 If M and M' are R-modules, an R-module homomorphism, or an R-linear map, is a group homomorphism $f : M \to N$ such that $f(xm) = xf(m)$ for all $x \in R$ and $m \in M$. An isomomorphism is a bijective homomorphism. We shall write $\mathbf{Mod}_R$ for the category of R-modules.

Example 1.2.3 A vector space is a module over its field of scalars.

Example 1.2.4 Any abelian group is a $\mathbb{Z}$-module.

Example 1.2.5 Any ideal $I \subseteq R$ is an R-module.

Example 1.2.6 Let M be an R-module and $f : M \to M$ an R-linear endomorphism. We can view M as an $R[X]$-module by the rule $X \cdot m = f(m)$.

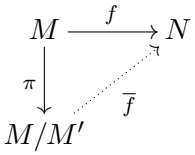
Example 1.2.7 The abelian group $Hom_R(M, N)$ of all homomorphisms between two R-modules is itself an R-module by declaring that, for any $x \in R$ and $\lambda \in Hom_R(M, N)$, the element $x\lambda$ is the homomorphism taking $m \in M$ to $x\lambda(m) \in N$. An R-linear map $f : N \to N'$ induces an R-linear map $f_* : Hom_R(M, N) \to Hom_R(M, N')$ defined by $f_*(\lambda) = \lambda \circ f$. An R-linear map $g : M' \to M$ induces an R-linear map $g^* : Hom_R(M, N) \to Hom_R(M', N)$ defined by $g^*(\lambda) = g \circ \lambda$.

Example 1.2.8 A ring homomorphism $\varphi : R \to A$ allows us to view every A-module as an R-module by the rule $x \cdot m = \varphi(x)m$ (sometimes simply written xm, even though φ is not necessarily injective). We shall sometimes denote this module as $\varphi_*(M)$. It is immediate to check that this construction gives rise to a functor $\varphi_* : \mathbf{Mod}_A \to \mathbf{Mod}_R$.
In particular, φ endows A with an R-module structure: we shall say that A is an R**-algebra**.

Definition 1.2.9 Let M be an R-module. A subset $M' \subseteq M$ is a **submodule** if it is a subgroup and if $xm' \in M'$ for every $x \in R$ and $m' \in M'$.

Example 1.2.10 If $f : M \to N$ is an R-linear map, $\ker f$ is a submodule of M and $\operatorname{im} f$ is a submodule of N.

Proposition 1.2.11 *If $M' \subseteq M$ is a submodule, the quotient M/M' is an R-module and the projection $\pi : M \to M/M'$ is R-linear. Any R-linear map $f : M \to N$ such that $M' \subseteq \ker f$ factors uniquely through a R-linear map $\overline{f} : M/M' \to N$:*



Proof. Recall that M/M' is the quotient group of M by the equivalence relation $m_1 \sim m_2 \iff m_1 - m_2 \in M'$. The relation is compatible with scalar multiplication ($m_1 \sim m_2 \implies xm_1 \sim xm_2$ for all $x \in R$, because $xm_1 - xm_2 = x(m_1 - m_2) \in M'$ if $m_1 - m_2 \in M'$) and so we can multiply classes in M/M': $x \cdot \overline{m} = \overline{xm}$ is well-defined.
For any linear map $f : M \to N$ such that $f(m') = 0$ for all $m' \in M'$ we have that $f(m_1) = f(m_2)$ whenever $m_1 \sim m_2$. Thus $\overline{f}(\overline{m}) = f(m)$ is well defined, and clearly linear. □

Corollary 1.2.12 *Let M be an R-module, $P \subseteq N \subseteq M$ submodules. There is a canonical isomorphism $((M/P)\,/\,(N/P)) \cong M/N$.*

Proof. Let $\pi : M \to M/N$ be the projection. Since $P \subseteq N = \ker \pi$, we get $\overline{\pi} : M/P \to M/N$. Since π is surjective, $\overline{\pi}$ is surjective. Its kernel is easily seen to be N/P. □

Definition 1.2.13 Let $f : M \to N$ be an R-linear map. The R-module $\operatorname{coker} f = N/\operatorname{im} f$ is called the **cokernel** of f.

Example 1.2.14 If R is a ring and $x \in R$, multiplication by x yields an R-linear map $\mu_x : R \to R$ (not a ring homomorphism in general, since $\mu_x(1) = x$) with $\operatorname{coker}\mu_x = R/xR$.

Definition 1.2.15 Let M be an R-module, $N, P \subseteq M$ submodules. Their **index** is the set

$$(P : N) = \{x \in R : \ xn \in P \ \ \forall\, n \in N\}\,.$$

It is immediate to check that $(P : N)$ is an ideal. In particular $(0 : N) = \operatorname{Ann}(N)$ is called the **annihilator** of N. For $m \in M$, write $\operatorname{Ann}(m)$ for $\operatorname{Ann}(Rm)$.

Example 1.2.16 If $I \subset R$ is an ideal, $I = \operatorname{Ann}(R/I)$. Any R-module $M = \pi_*(M)$ is naturally an $R/\operatorname{Ann}(M)$-module (via $\pi : R \to R/\operatorname{Ann}(M)$).

Definition 1.2.17 An R-module M is **faithful** if $\operatorname{Ann}(M) = 0$. An $m \in M$ is a **torsion element** if $\operatorname{Ann}(m) \neq 0$. We say that M is a **torsion module** if $\operatorname{Ann}(m) \neq 0$ for all $m \in M$. We say that M is **torsion-free** if $\operatorname{Ann}(m) = 0$ for all $m \in M$.

Example 1.2.18 The group $\mathbb{Q}/\mathbb{Z}$ is a faithful $\mathbb{Z}$-module, even though it is a torsion module.

If M is an R-module, let M_{tors} be the subset of its torsion elements. In general, it is not a submodule (example: in $M = R = \mathbb{Z}/6\mathbb{Z}$ the elements $\overline{2}$ and $\overline{3}$ are torsion but $\overline{2} + \overline{3} = \overline{5}$ is a unit). However:

Lemma 1.2.19 *If R is a domain and M an R-module, then M_{tors} is a submodule.*

Proof. If $m_1, m_2 \in M_{\mathrm{tors}}$, there exist $0 \neq x_i \in R$ such that $x_i m_i = 0$. Then $x_1 x_2 (m_1 + m_2) = 0$ and $x_1 x_2 \neq 0$. □

Operations on Modules

Proposition 1.2.20 *Let M be an R-module, $\{M_\alpha\}_\alpha$ a family of submodules. The intersection $\bigcap_\alpha M_\alpha$ and the sum $\sum_\alpha M_\alpha = \{\sum_\alpha m_\alpha,\ m_\alpha \in M_\alpha,\ m_\alpha = 0$ for all but finitely many $\alpha\}$ are R-modules.*

Proof. We know that $\sum_\alpha M_\alpha$ and $\bigcap_\alpha M_\alpha$ are subgroups of M. For $m \in \bigcap_\alpha M_\alpha$ and $x \in R$ we have $xm \in M_\alpha$ for all α because M_α are submodules, hence $xm \in \bigcap_\alpha M_\alpha$. In the same way, for $m_{\alpha_1} \in M_{\alpha_1}, \ldots, m_{\alpha_r} \in M_{\alpha_r}$ we have $x m_{\alpha_j} \in M_{\alpha_j}$, therefore $x(m_{\alpha_1} + \cdots + m_{\alpha_r}) = x m_{\alpha_1} + \cdots + x m_{\alpha_r} \in \sum_\alpha M_\alpha$. □

Proposition 1.2.21 *Let M be an R-module, $N, P \subseteq M$ submodules. There is a canonical isomorphism $(N+P)/N \cong P/(N \cap P)$.*

Proof. Let $f : P \hookrightarrow N + P \twoheadrightarrow (N+P)/N$ be the composition of the natural inclusion with the projection mod N. Clearly every element in $N + P$ is congruent to an element in P mod N, so f is surjective. On the other hand, one computes $\ker f = N \cap P$. From proposition 1.2.11 we get an isomorphism $\overline{f}$. □

Definition 1.2.22 The sum of two submodules $M_1, M_2 \subseteq M$ is a **direct sum** if $M_1 \cap M_2 = \{0\}$ and we write $M_1 \oplus M_2$ for such sums. Equivalently, every element in $M_1 \oplus M_2$ can be written uniquely as the sum of an element in each summand.

Definition 1.2.23 Let $\{M_\alpha\}_\alpha$ be a family of R-modules. Their **direct product** $\prod_\alpha M_\alpha$ is defined as the cartesian product of the M_α equipped with the componentwise operations

$$(\ldots, m_\alpha, \ldots) + (\ldots, m'_\alpha, \ldots) = (\ldots, m_\alpha + m'_\alpha, \ldots); \qquad x(\ldots, m_\alpha, \ldots) = (\ldots, x m_\alpha, \ldots).$$

Their **direct sum** $\bigoplus_\alpha M_\alpha$ is the submodule of all elements $(\ldots, m_\alpha, \ldots) \in \prod_\alpha M_\alpha$ such that $m_\alpha = 0$ for all but finitely many α.

Example 1.2.24 As an R-module, the ring of polynomials $R[X]$ can be seen as the direct sum $\bigoplus_{n\in\mathbb{N}} R$. The direct product $\prod_{n\in\mathbb{N}} R$ is the R-module underlying the ring of **formal power series** $R[[X]]$, whose product is defined by the rule

$$\left(\sum_{i=0}^{\infty} a_i X^i\right)\left(\sum_{j=0}^{\infty} b_j X^j\right) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_k b_{n-k}\right) X^n. \tag{1.2}$$

Notice that $R[[X]]$ is not the direct product ring. The unit in $R[[X]]$ is the series $1 + 0 + 0 + \ldots$. For later use, let us remark that the units in $R[[X]]$ are given by the power series $f = \sum_{i=0}^{\infty} a_i X^i$

such that $a_0 \in R^\times$. Indeed, given such a series, we can construct a series $g = \sum_{j=0}^{\infty} b_j X^j$ such that $fg = 1$ by solving recursively the system of equations in $b_0, b_1, \ldots$ arising from (1.2):

$$\begin{cases} a_0 b_0 = 1 \\ a_0 b_1 + a_1 b_0 = 0 \\ \qquad \ddots \\ a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 = 0 \\ \qquad\qquad\qquad \ddots \end{cases}$$

each time the new variable b_n appearing with the invertible coefficient a_0. In particular, if k is a field, $k[[X]]$ is a local ring with maximal ideal (X).

Definition 1.2.25 A **free module** is a module isomorphic to a direct sum of copies of R.

Example 1.2.26 The ring of Gauss integers $\mathbb{Z}[i]$ is a free $\mathbb{Z}$-module of rank 2, with basis 1 and i.

Proposition 1.2.27 *Let F be a free R-module with basis $\{\mathbf{e}_\alpha\}_\alpha$. Let M be an R-module and $\{m_\alpha\}_\alpha$ an arbitrary set of elements of M. There exists a unique finear map $f : F \to M$ such that $f(\mathbf{e}_\alpha) = m_\alpha$.*

Proof. Standard linear algebra argument. □

Definition 1.2.28 An R-module M is generated by elements $\{m_\alpha\}_\alpha \subset M$ if every element in M is a finite R-linear combination of the $\{m_\alpha\}_\alpha$, called generators. We shall say that M is **finitely generated** if it can be generated by finitely many elements.

In view of proposition 1.2.27, an R-module M is finitely generated if and only if there exists a presentation, i.e. a surjective map $\pi : R^n \to M$. Over arbitrary rings, is it useful to introduce a more restrictive condition, requiring finiteness for the number of relations as well:

Definition 1.2.29 An R-module M is **finitely presented** if it admits a presentation $\pi : R^n \twoheadrightarrow M$ such that $\ker \pi$ is a finitely generated module.

For R-algebras we use a slightly different terminology.

Definition 1.2.30 An R-algebra A is **of finite type** over R if it is a quotient of a polynomial algebra $R[X_1, \ldots, X_n]$ for a suitable n. We say that A is a **finitely presented** R-algebra if it admits a presentation $\pi : R[X_1, \ldots, X_n] \to A$ such that $\ker \pi$ is a finitely generated ideal. We say that A is **finite** over R if A is a finitely generated R-module via the natural map $\varphi : R \to A$.

Clearly, a finite R-algebra is of finite type: take $x_1, \ldots, x_n$ generating A as an R module and get a presentation $\pi : R[X_1, \ldots, X_n] \twoheadrightarrow A$ by $\pi(X_i) = x_i$. Corollary 3.1.11 will tell us precisely which R-algebras of finite type are finite.

Proposition 1.2.31 *Let R be a ring.*

a) For any R-module M, the map $\lambda \mapsto \lambda(1)$ defines an isomorphism $Hom_R(R, M) \cong M$.

b) For any R-modules M_1, M_2 and N we have

$$Hom_R(N, M_1 \oplus M_2) \cong Hom_R(N, M_1) \oplus Hom_R(N, M_1).$$

c) For any R-modules M, N_1 and N_2 we have

$$Hom_R(N_1 \oplus N_2, M) \cong Hom_R(N_1, M) \oplus Hom_R(N_2, M).$$

Proof. a) The map is injective, since if $\lambda(1) = 0$ then $\lambda(x) = x\lambda(1) = 0$ for all $x \in R$. It is surjective, because any $m \in M$, the rule $x \mapsto xm$ defines a linear map $R \to M$.
b) Let $\pi_j : M_1 \oplus M_2 \twoheadrightarrow M_j$ be the projection. Then $f \mapsto (\pi_1 \circ f, \pi_2 \circ f)$ is readily seen to be an isomorphism.
c) Similarly, denoting $i_j : N_j \hookrightarrow N_1 \oplus N_2$ the inclusions, the rule $f \mapsto (f \circ i_1, f \circ i_2)$ gives the second isomorphism. □

THE CAYLEY–HAMILTON THEOREM AND NAKAYAMA'S LEMMA

Theorem 1.2.32 (Cayley–Hamilton) *Let M be a finitely generated R-module, $\mathfrak{a} \subseteq R$ an ideal and $f : M \to M$ an R-linear map such that $f(M) \subseteq \mathfrak{a}M$. There exists a monic polynomial $p(X) \in R[X]$ such that $p(f) = 0$ on M.*

Proof. Choose generators $m_1, \ldots, m_n$ for M. By assumption, $f(m_i) \in \mathfrak{a}M$, hence the expressions $f(m_j) = \sum_{i=1}^{n} a_{i,j} m_i$ define an $n \times n$ matrix $A = (a_{i,j})$ with coefficients in $\mathfrak{a}$. As in example 1.2.6, view M as an $R[X]$-module letting X act as f. Notice that in M^n we have

$$(XI_n - A) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Multiplying on the left by the cofactor matrix we conclude that $\det(XI_n - A)m_i = 0$ for all i, hence $\det(XI_n - A)m = 0$ for all $m \in M$. □

Remark 1.2.33 The proof shows that we can take $p(X)$ to be the characteristic polynomial of a matrix with entries in $\mathfrak{a}$. Hence, except for the leading one, the coefficients of $p(X)$ are in $\mathfrak{a}$.

Corollary 1.2.34 *Let M be a finitely generated R-module. An endomorphism $f : M \to M$ is an isomorphism if and only if it is surjective.*

Proof. Let $f : M \to M$ be a surjective map and view M as an $R[T]$-module where T acts as f. Take $\mathfrak{a} = (T) \subset R[T]$: since f is surjective, $\mathfrak{a}M = M$. Applying Cayley–Hamilton to $id : M \to M$ we obtain a polynomial $p(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in R[T][X]$ such that $p(id) = 0$. By remark 1.2.33 we have $a_i \in (T)$ and evaluating in id we get that $(id - Tq(T))\, M = 0$ for a suitable $q(T) \in R[T]$. Recalling that T acts as f we have that $fq(f)$ is the identity on M, hence f is an isomorphism with inverse $q(f)$. □

Corollary 1.2.35 *Any minimal set of generators in R^n is a basis and has cardinality n.*

Proof. Let $m_1 \ldots, m_r$ be a minimal set of generators of R^n. By minimality, $r \leq n$. Define $f : R^n \to R^n$ by $f(\mathbf{e}_i) = m_i$ for $i = 1, \ldots, r$ and $f(\mathbf{e}_j) = 0$ for $j = r+1, \ldots, n$. By construction f is surjective, hence an isomorphism by corollary 1.2.34. Therefore $\ker f = 0$, hence $r = n$. □

Definition 1.2.36 Let M be a finitely generated free R-module. The unique integer n such that $M \simeq R^n$ is called the **rank** of M.

Corollary 1.2.37 *Let M be a finitely generated R-module, $\mathfrak{a} \subseteq R$ an ideal such that $\mathfrak{a}M = M$. Then there exists an element $x \in R$, $x \equiv 1$ mod $\mathfrak{a}$, such that $xM = 0$.*

Proof. Apply Cayley–Hamilton to $f = id : M \to M$. □

Corollary 1.2.38 (Nakayama's Lemma) *Let M be a finitely generated R-module and $\mathfrak{a} \subseteq R$ an ideal contained in the Jacobson radical $\mathfrak{R}_R$. Then $\mathfrak{a}M = M$ if and only if $M = 0$.*

Proof. If $\mathfrak{a}M = M$, by corollary 1.2.37 we have $xM = 0$ for some $x \in 1 + \mathfrak{a} \subseteq 1 + \mathfrak{R}_R$, hence, by proposition 1.1.56, $x \in R^\times$ and therefore $M = 0$. □

Remark 1.2.39 The most common application of Nakayama's Lemma, and of the following corollaries, is to the case where R is a local ring and $\mathfrak{a} = \mathfrak{R}_R$ is the maximal ideal.

Corollary 1.2.40 *Let M be a finitely generated R-module, $N \subseteq M$ a submodule, $\mathfrak{a} \subseteq \mathfrak{R}_R$ an ideal such that $M = \mathfrak{a}M + N$. Then $N = M$.*

Proof. We have $\mathfrak{a}\,(M/N) = (\mathfrak{a}M + N)\,/N = M/N$, hence $M/N = 0$ by Nakayama. □

Corollary 1.2.41 *Let M be a finitely generated R-module, $m_1, \ldots, m_n \in M$ and $\mathfrak{a} \subseteq \mathfrak{R}_R$. The the m_i generate M if and only if their classes generate $M/\mathfrak{a}M$.*

Proof. Apply corollary 1.2.40 to $N = (m_1, \ldots, m_n)$. □

EXACT SEQUENCES

Definition 1.2.42 A sequence of groups or R-modules and homomorphisms

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots \tag{1.3}$$

is **exact** in M_i if $\ker f_{i+1} = \operatorname{im} f_i$. We say the the sequence is exact if it is exact in each spot. A **short exact sequence** is an exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0.$$

Example 1.2.43 An injection $M' \hookrightarrow M$ corresponds to an exact sequence $0 \to M' \to M$. Similarly, a surjection $M \twoheadrightarrow M''$ gives rise to an exact sequence $M \to M'' \to 0$.

Example 1.2.44 If R is a ring and $I \subseteq R$ an ideal, we have a short exact sequence of R-modules

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0$$

Example 1.2.45 An R-module M is finitely generated if it fits in a sequence $R^n \to M \to 0$ for a suitable integer n. It is finitely presented if it fits in an exact sequence $R^m \to R^n \to M \to 0$.

Remark 1.2.46 Any long exact sequence (1.3) can be broken into short ones:

$$0 \longrightarrow \operatorname{im} f_i \longrightarrow M_i \longrightarrow \ker f_{i+2} \longrightarrow 0.$$

.

Lemma 1.2.47 (Snake Lemma) *Given a commutative diagram of R-modules with exact rows*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi'} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi''} & & \\ 0 & \longrightarrow & N' & \xrightarrow{u} & N & \xrightarrow{v} & N'' & \longrightarrow & 0 \end{array}$$

(with optional exactness of the colored arrows) there exists an R-linear map $\delta : \ker \phi'' \to \operatorname{coker}\phi'$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker \phi' & \longrightarrow & \ker \phi & \longrightarrow & \ker \phi'' & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N' & \xrightarrow{u} & N & \xrightarrow{v} & N'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \pi} & & \downarrow & & \downarrow & & \\ & & \operatorname{coker}\phi' & \longrightarrow & \operatorname{coker}\phi & \longrightarrow & \operatorname{coker}\phi'' & \longrightarrow & 0 \end{array} \qquad \delta$$

such that the sequence $0 \to \ker \phi' \to \ker \phi \to \ker \phi'' \to \operatorname{coker}\phi' \to \operatorname{coker}\phi \to \operatorname{coker}\phi'' \to 0$ is exact.

Proof. Let $x \in \ker \phi''$. Choose $y \in M$ such that $g(y) = x$. Since $v(\phi(y)) = \phi''(x) = 0$, we can take $z \in N'$ such that $u(z) = \phi(y)$. Define $\delta(x) = \pi(z) \in \operatorname{coker} \phi$. We leave it as an exercise to check that this procedure really defines a map (i.e. doesn't depend on the choices), that δ is R-linear and that the 6-term sequence is exact. □

Remark 1.2.48 The arguments employed to define the map δ are fairly common in commutative and homological algebra and go under the self-explaining name of *diagram chasing*.

Proposition 1.2.49 *A sequence of R-modules $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$ is exact if and only if $0 \longrightarrow Hom_R(N, M') \xrightarrow{f_*} Hom_R(N, M) \xrightarrow{g_*} Hom_R(N, M'')$ is exact for every R-module N.*

A sequence of R-modules $M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ is exact if and only if the induced sequence $0 \longrightarrow Hom_R(M'', N) \xrightarrow{g^*} Hom_R(M, N) \xrightarrow{f^*} Hom_R(M', N)$ is exact for every R-module N.

Proof. Let $\lambda' : N \to M'$ be an R-linear map. To say $f \circ \lambda' = 0$ means $f(\lambda'(n)) = 0$ for all $n \in N$. Since f is injective, this means $\lambda'(n) = 0$ for all $n \in N$, i.e. f_* is injective.
Clearly $g_* \circ f_* = (g \circ f)_* = 0_* = 0$ so $\operatorname{im} f_* \subseteq \ker g_*$. If $g \circ \lambda = 0$ for some $\lambda : N \to M$, then $\lambda(n) \in \ker g = \operatorname{im} f$ for all $n \in N$. There exists thus an R-linear $\mu : N \to M'$ such that $\lambda = f \circ \mu$. The proof of the second statement is analogous and left as an exercise. □

Definition 1.2.50 Let R and A be rings. A functor $F : \mathbf{Mod}_R \to \mathbf{Mod}_A$ is

a) **additive** if $F(M \oplus N) = F(M) \oplus F(N)$. Moreover, we require $F(0) = 0$.

b) **left–exact** if it is additive and for every exact sequence $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$ of R-modules, the sequence of A-modules $0 \longrightarrow F(M') \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(M'')$ is exact.

c) **right–exact** if it is additive and for every exact sequence $M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ of R-modules, the sequence of A-modules $F(M') \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(M'') \longrightarrow 0$ is exact.

d **exact** if both left and right–exact.

We can thus rephrase proposition 1.2.49 saying that $Hom_R(N, -) : \mathbf{Mod}_R \to \mathbf{Mod}_R$ is a left-exact functor.

Definition 1.2.51 A **splitting** of an exact sequence is a homomorphism σ such that $g \circ \sigma = id_{M''}$

$$0 \longrightarrow M' \xrightarrow{f} M \underset{\sigma}{\overset{g}{\rightleftarrows}} M'' \longrightarrow 0.$$

An exact sequence admitting a splitting is called **split exact**.

Lemma 1.2.52 *A splitting of an exact sequence of R-modules $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ induces an isomorphism $M \simeq M' \oplus M''$.*

Proof. Let σ be a splitting of the sequence. The sum $M' + \operatorname{im} \sigma$ is direct: if $\sigma(m'') \in M' = \ker g$, then $m'' = g(\sigma(m'') = 0$. The injection $M' \oplus \operatorname{im} \sigma \subseteq M$ is an equality: every $m \in M$ can be written as $[m - \sigma((g(m))] + \sigma((g(m))$. □

Proposition 1.2.53 *An exact sequence of R-modules $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ splits if and only if $g_* : Hom_R(M'', M) \to Hom_R(M'', M'')$ is surjective.*

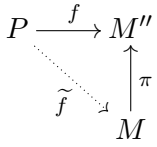
Proof. If g_* is surjective, any map $\sigma : M'' \to M$ such that $g_*(\sigma) = g \circ \sigma = id_{M''}$ splits the sequence. Conversely, if $\sigma : M'' \to M$ splits the sequence, for any $h \in Hom_R(M'', M'')$ the map $\sigma \circ h : M'' \to M$ satisfies $g_*(\sigma \circ h) = g \circ \sigma \circ h = h$, hence g_* is surjective. □

Corollary 1.2.54 *If $\sigma : M'' \to M$ splits the exact sequence $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$, then any other splitting σ' is of the form $\sigma' + \lambda$ for a suitable $\lambda \in Hom_R(M'', M')$.*

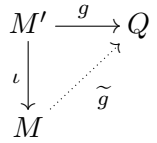
Proof. The set of splittings is $g_*^{-1}(id_{M''}) \subset Hom_R(M'', M)$. The claim now follows from proposition 1.2.49. □

One says that the set of splittings of $0 \to M' \to M \to M'' \to 0$, if non-empty, is an **affine space**, or **principal homogeneous space** or **torsor** under $Hom_R(M'', M')$.

Definition 1.2.55 An R-module P is **projective** if for every surjection $\pi : M \to M''$ and every homomorphism $f : P \to M''$ there exists a homomorphism $\widetilde{f} : P \to M$ such that $f = \pi \circ \widetilde{f}$.



An R-module Q is **injective** if for every injection $\iota : M' \to M$ and every homomorphism $g : M' \to Q$ there exists a homomorphism $\widetilde{g} : M \to Q$ such that $g = \widetilde{g} \circ \iota$.



Example 1.2.56 A free module is projective, as follows easily from proposition 1.2.27.

Example 1.2.57 $\mathbb{Q}$ is an injective $\mathbb{Z}$-module. Let $\iota : M' \hookrightarrow M$ and $g : M' \to \mathbb{Q}$. Consider the set Σ of submodules $M' \subseteq N \subseteq M$ such that g extends to $g_N : N \to \mathbb{Q}$. Declare $(N, g_N) \leq (N', g_{N'})$ if $N \subseteq N'$ and $g_{N'}$ extends g_N. The set Σ is non-empty (it contains M') and if $\{(N_i, g_{N_i})\}_i$ is a chain in Σ then $\bigcup_i N_i$ is in Σ. Hence Σ satisfies the conditions of Zorn's lemma. Let $(N, g_N) \in \Sigma$ be a maximal element: we want to show that $N = M$. If $x \in M - N$ then $N + \mathbb{Z}x \notin \Sigma$. Consider the index ideal $(N : N + \mathbb{Z}x) = a\mathbb{Z} \subseteq \mathbb{Z}$. If $a \neq 0$, the rule $\widetilde{g}(x) = \frac{1}{a} g_N(ax) \in \mathbb{Q}$ defines an extension of g_N to $N + \mathbb{Z}x$, which is a contradiction. If $a = 0$, the sum $N + \mathbb{Z}x$ is direct and $\widetilde{g}(x) = 0$ also defines an extension, so again we get a contradiction.

Proposition 1.2.58 *Let P be an R-module. The following conditions are equivalent:*

a) P is projective;

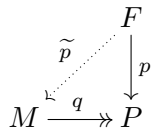
b) $\pi_* : Hom_R(P, M) \to Hom_R(P, M'')$ is surjective for every surjection $\pi : M \to M''$;

c) For every presentation $F \overset{p}{\twoheadrightarrow} P$ with F a free module, $Hom_R(P, F) \overset{p_*}{\to} Hom_R(P, P)$ is surjective;

d) P is a direct summand of a free module;

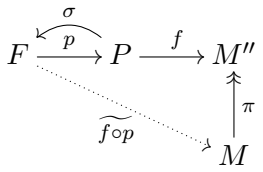
e) Every surjection $q : M \twoheadrightarrow P$ admits a splitting.

Proof. The implications a) $\iff$ b) $\implies$ c) are obvious. For c) $\implies$ d) apply proposition 1.2.53 and lemma 1.2.52 to a presentation $0 \to \ker p \to F \xrightarrow{p} P \to 0$ with F a free module.
For d) $\implies$ e), choose a presentation $p : F \to P$ with F free and consider the diagram



where $\widetilde{p}$ exists because F is free and thus projective. Then any splitting $\sigma : P \to F$ of p yields a splitting $\widetilde{p} \circ \sigma$ of q. The implication e) $\implies$ d) is now obvious.

For d) $\Longrightarrow$ a), again choose a presentation $p : F \to P$ with F free and consider the diagram



to get a lifting $(\widetilde{f \circ p}) \circ \sigma$ of f. □

Example 1.2.59 Let $R = \mathbb{Z}[\sqrt{-5}]$ and $\mathfrak{a} = (2, 1 + \sqrt{-5})$. The R-module $\mathfrak{a}$ is not free: the generators are not a basis, since $3 \cdot 2 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. We shall see in theorem 5.3.9 that if $\mathfrak{a}$ were free, it would be principal. The element $1 + \sqrt{-5}$ is prime: if $z = a + b\sqrt{-5}$ divides $1 + \sqrt{-5}$ then $|z|^2 = a^2 + 5b^2$ must divide $|1 + \sqrt{-5}|^2 = 6$, but $a^2 + 5b^2 = 2$ and $a^2 + 5b^2 = 3$ have no solutions $a, b \in \mathbb{Z}$. So if $\mathfrak{a}$ were free, it would have to be generated by $1 + \sqrt{-5}$, which would then divide 2, but then 6 would divide $|2|^2 = 4$. However $\mathfrak{a}$ is projective: take $p : R^2 \twoheadrightarrow \mathfrak{a}$ defined by $p(\mathbf{e}_1) = 2$ and $p(\mathbf{e}_2) = 1 + \sqrt{-5}$; a splitting is given by $\sigma(2) = -2\mathbf{e}_1 + (1 - \sqrt{-5})\mathbf{e}_2$, $\sigma(1 + \sqrt{-5}) = -(1 + \sqrt{-5})\mathbf{e}_1 + 3\mathbf{e}_2$.

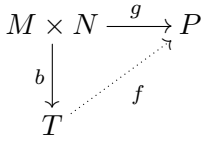
TENSOR PRODUCTS

Definition 1.2.60 Let M, N and P be R-modules. A map $f : M \times N \to P$ is **bilinear** if $f(x, y)$ is R-linear in x for any fixed $y \in N$ and R-linear in y for any fixed $x \in M$. The set of bilinear maps $M \times N \to P$ is denoted $\mathrm{Bil}_R(M \times N, P)$.

The set $\mathrm{Bil}_R(M \times N, P)$ is an R-module by declaring that αf is the map $(x, y) \mapsto \alpha f(x, y)$ for all $\alpha \in R$.

Theorem 1.2.61 *For every $M, N \in \mathbf{Mod}_R$, the functor $\mathrm{Bil}_R(M \times N, -) : \mathbf{Mod}_R \to \mathbf{Mod}_R$ is representable.*

Proof. The statement means that there exists an R-module T equipped with a bilinear map $b : M \times N \to T$ satisfying the following universal property: for every R-module P and bilinear map $g : M \times N \to P$, there exists a unique R-linear map $f : T \to P$ making the following diagram commute:



Let F be the free R-module generated by $M \times N$: its elements are thus finite sums $\sum_i \alpha_i(x_i, y_i)$, with $\alpha_i \in R$, $x_i \in M$ and $y_i \in N$. Let $S \subseteq F$ be the submodule generated by the elements

$$(x+x', y)-(x, y)-(x', y); \quad (x, y+y')-(x, y)-(x, y'); \quad (\alpha x, y)-\alpha(x, y); \quad (x, \alpha y)-\alpha(x, y) \tag{1.4}$$

for all $x, x' \in M$, $y, y' \in N$ and $\alpha \in R$. Set $T = F/S$, write $x \otimes y$ for (x, y) mod S and define $b(x, y) = x \otimes y$. It is now immediate to check that (T, b) satisfies the required propreties. □

Definition 1.2.62 By corollary A.14 the R-module representing $\mathrm{Bil}_R(M \times N, -)$ is unique up to unique isomorphism: we call it the **tensor product** of M and N and denote it $M \otimes_R N$.

Remark 1.2.63 A pair of linear maps $f : M \to P$ and $g : N \to Q$ defines a bilinear map

$$\begin{array}{rl} f \times g : M \times N & \longrightarrow P \otimes_R Q \\ (x, y) & \longmapsto f(x) \otimes g(y) \end{array}$$

whence an R-linear map $f \otimes g : M \otimes_R N \longrightarrow P \otimes_R Q$.

Example 1.2.64 $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$: indeed $\overline{a} \otimes \frac{b}{c} = \overline{a} \otimes \frac{nb}{nc} = \overline{n}a \otimes \frac{b}{nc} = \overline{0} \otimes \frac{b}{nc} = \overline{0} \otimes 0\frac{b}{nc} = \overline{0} \otimes 0$.

Proposition 1.2.65 *For every $M, N, P \in \mathbf{Mod}_R$, there are canonical isomorphisms*

$$\begin{array}{rl} M \otimes_R N & \longrightarrow N \otimes_R M \\ x \otimes y & \longmapsto y \otimes x \end{array} ; \qquad \begin{array}{rl} (M \otimes_R N) \otimes_R P & \longrightarrow M \otimes_R (N \otimes_R P) \\ (x \otimes y) \otimes z & \longmapsto x \otimes (y \otimes z) \end{array} ;$$

$$\begin{array}{rl} (\bigoplus_\alpha M_\alpha) \otimes_R N & \longrightarrow \bigoplus_\alpha (M_\alpha \otimes_R N) \\ (\dots, x_\alpha, \dots) \otimes y & \longmapsto (\dots, x_\alpha \otimes y, \dots) \end{array} ; \qquad \begin{array}{rl} R \otimes_R M & \longrightarrow M \\ \alpha \otimes x & \longmapsto \alpha x \end{array} .$$

Proof. One should first show that these maps are well defined and then check that they are isomorphism. For instance the map $M \times N \to N \times M$ given by $(x, y) \mapsto (y, x)$ is very clearly bilinear, hence so is the composition $M \times N \to N \otimes_R N$ whence a linear map $M \otimes_R N \to N \otimes_R M$. It is an isomorphism because we can construct the inverse map $N \otimes_R M \to M \otimes_R N$, $y \otimes x \mapsto x \otimes y$ in a similar way. The rest of the proof is an exercise left to the reader. □

Remark 1.2.66 The second isomorphism in proposition 1.2.65 (associativity of the tensor product) allows to write without ambiguity the tensor product $M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M_n$ of several modules. Notice that the latter represents the functor $\mathbf{Mod}_R \to \mathbf{Mod}_R$ taking P to the module of *multilinear* maps $M_1 \times M_2 \times \cdot \times M_n \to P$.

Definition 1.2.67 Let M be an R-module, $\varphi : R \to A$ an R-algebra. Then $A \otimes_R M$ is an A-module, called **extension of the scalars** from R to A by setting $a \cdot (b \otimes m) = ab \otimes m$.

Example 1.2.68 It follows from the isomorphisms in proposition 1.2.65 that $A \otimes_R R^n \cong A^n$. If $M(m \times n, R)$ is the module of $m \times n$ matrices with coefficients in R, then $A \otimes_R M(m \times n, R) = M(m \times n, A)$.

Definition 1.2.69 Let A and B be rings. An (A, B)-**bimodule** is an abelian group N equipped with an A-module structure and an B-module structure such that $(a \cdot_A x) \cdot_B b = a \cdot_A (x \cdot_B b)$ for all $a \in A$, $b \in B$ and $x \in N$.

Example 1.2.70 Let $\varphi : R \to A$ and $\psi : R \to B$ be two R-algebras. Then $A \otimes_R B$ is an (A, B)-bimodule. Notice that $A \otimes_R B$ has a ring structure: the map

$$\begin{array}{rl} A \times B \times A \times B & \longrightarrow A \otimes_R B. \\ (a, b, a', b') & \longmapsto aa' \otimes bb' \end{array}$$

is multilinear in the four variables, whence an R-linear map $A \otimes_R B \otimes_R A \otimes_R B \to A \otimes_R B$, $a \otimes b \otimes a' \otimes b' \mapsto aa' \otimes bb'$ which in turn corresponds to an R-bilinear map

$$\begin{array}{rl} (A \otimes_R B) \times (A \otimes_R B) & \longrightarrow A \otimes_R B \\ (a \otimes b, a' \otimes b') & \longmapsto aa' \otimes bb' \end{array}$$

easily seen to satisfy the axioms or ring multiplication, with unit $1 \otimes 1$. Beware that $A \otimes_R B$ could be the zero ring, as in example 1.2.64.
The special case $A \otimes_R A$ will play a crucial role in § I.3 (algebraic differential calculus) and especially in § II.2 (descent theory). It is worth remarking that $A \otimes_R A$ has several non-equivalent A-module structures, chief among them the right $a \cdot (x \otimes y) = ax \otimes y$ and left $a \cdot (x \otimes y) = x \otimes ay$ structures.

Proposition 1.2.71 *Let M be an A-module, P an B-module and N an (A, B)-bimodule. There is a canonical isomorphism*

$$\begin{array}{rl} (M \otimes_A N) \otimes_B P & \longrightarrow M \otimes_A (N \otimes_B P) \\ (x \otimes y) \otimes z & \longmapsto x \otimes (y \otimes z) \end{array}$$

Proof. Tedious exercise left to the reader. ⊠

Corollary 1.2.72 *Let M be an R-module, $\varphi : R \to R'$ an R-algebra and $\psi : R' \to R''$ an R'-algebra. There are canonical isomorphisms*

$$R'' \otimes_{R'} (R' \otimes_R M) \cong (R'' \otimes_{R'} R') \otimes_R M \cong R'' \otimes_R M.$$

Proof. The isomorphism to the left is given in proposition 1.2.71, the one to the right is the last in proposition 1.2.65. □

The following result establishes the crucial relation between the Hom and $\otimes$ functors:

Lemma 1.2.73 *Let M, N and P be R-modules. There is a canonical isomorphism*

$$\Phi : Hom_R(M \otimes_R N, P) \cong Hom_R(M, Hom_R(N, P)).$$

Proof. Let $f : M \otimes_R N \to P$ be a linear map. By construction, it corresponds to a bilinear map $g : M \times N \to P$: by definition, for every fixed $m \in M$, the map $g(m, -) : N \to P$ is linear. The rule $\Phi(f) = [m \mapsto g(m, -)]$ clearly defines a linear map Φ. Conversely, if $\lambda : M \to Hom_R(N, P)$ is a linear map, the rule $(m, n) \mapsto (\lambda(m))(n)$ defines a bilinear form $M \times N \to P$, whence a linear map $\Psi(\lambda) : M \otimes_R N \to P$. One checks easily that Ψ is inverse to Φ. □

Definition 1.2.74 Let $\mathfrak{C}$ and $\mathfrak{D}$ be categories. Two functors $L : \mathfrak{C} \to \mathfrak{D}$ and $R : \mathfrak{D} \to \mathfrak{C}$ are called **adjoint** if for every pair of objects C in $\mathfrak{C}$ and D in $\mathfrak{D}$ there is a bijection

$$Hom_{\mathfrak{D}}(L(C), D) \cong Hom_{\mathfrak{C}}(C, R(D)).$$

"functorial" in C and D i.e. for every $f : C \to C'$, $g : D \to D'$ the following diagram commutes:

$$\begin{array}{ccccc} Hom_{\mathfrak{D}}(L(C'), D) & \xrightarrow{L(f)^*} & Hom_{\mathfrak{D}}(L(C), D) & \xrightarrow{g_*} & Hom_{\mathfrak{D}}(L(C), D') \\ \cong\downarrow & & \cong\downarrow & & \cong\downarrow \\ Hom_{\mathfrak{C}}(C', R(D)) & \xrightarrow{f^*} & Hom_{\mathfrak{C}}(C, R(D)) & \xrightarrow{R(g)_*} & Hom_{\mathfrak{C}}(C, R(D')). \end{array} \tag{1.5}$$

We say that L is left adjoint to R and that R is right adjoint to L.

Remark 1.2.75 If $L : \mathfrak{C} \to \mathfrak{D}$ and $R : \mathfrak{D} \to \mathfrak{C}$ are adjoint functors, then $R^{\mathrm{op}} : \mathfrak{D}^{\mathrm{op}} \to \mathfrak{C}^{\mathrm{op}}$ and $L^{\mathrm{op}} : \mathfrak{C}^{\mathrm{op}} \to \mathfrak{D}^{\mathrm{op}}$ are also adjoint, with R^{op} left adjoint and L^{op} right adjoint.

We can rephrase lemma 1.2.73 by saying that $L(-) = - \otimes_R N$ is adjoint to $R(-) = Hom_R(N, -)$ (the verification of diagram (1.5) is left to the reader).

Proposition 1.2.76 *Let A and B be rings, $L : \mathbf{Mod}_A \to \mathbf{Mod}_B$ and $R : \mathbf{Mod}_B \to \mathbf{Mod}_A$ two adjoint additive functors. Then L is right exact and R is left exact.*

Proof. Let $M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ be an exact sequence of A-modules. By proposition 1.2.49, for every B-module N the top sequence in the following diagram is exact

$$\begin{array}{ccccccc} 0 & \longrightarrow & Hom_A\left(M'', R(N)\right) & \longrightarrow & Hom_A\left(M, R(N)\right) & \longrightarrow & Hom_A\left(M', R(N)\right) \\ & & \cong\downarrow & & \cong\downarrow & & \cong\downarrow \\ 0 & \longrightarrow & Hom_B\left(L(M''), N\right) & \longrightarrow & Hom_B\left(L(M), N\right) & \longrightarrow & Hom_B\left(L(M'), N\right). \end{array}$$

The diagram is commutative and the vertical arrows are isomorphism, so the bottom row is also exact. Again by proposition 1.2.49 we conclude that $L(M') \longrightarrow L(M) \longrightarrow L(M)'' \longrightarrow 0$ is an exact sequence of B-modules, hence L is right-exact. We now get for free that R^{op} is right-exact: for every exact sequence $N'' \longrightarrow N \longrightarrow N' \longrightarrow 0$ in $\mathbf{Mod}_B^{\mathrm{op}}$ (i.e. for every exact sequence $0 \longrightarrow N' \longrightarrow N \longrightarrow N''$ of B-modules) the sequence $R^{\mathrm{op}}(N'') \longrightarrow R^{\mathrm{op}}(N) \longrightarrow R^{\mathrm{op}}(N') \longrightarrow 0$ in $\mathbf{Mod}_B^{\mathrm{op}}$ (i.e. the sequence $0 \longrightarrow R(N') \longrightarrow R(N) \longrightarrow R(N'')$) is exact. Thus R is left-exact. □

Corollary 1.2.77 *If $N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$ is an exact sequence of R-modules, then for every R-module M the sequence $M \otimes_R N' \longrightarrow M \otimes_R N \longrightarrow M \otimes_R N'' \longrightarrow 0$ is exact.*

Corollary 1.2.78 *Let M be a finitely generated (respectively presented) R-module and $\varphi : R \to A$ an R-algebra. Then $A \otimes_R M$ is a finitely generated (resp. presented) A-module.*

Proof. Take a presentation $(R^m \longrightarrow) R^n \longrightarrow M \longrightarrow 0$, apply $A \otimes_R -$ and use example 1.2.68. □

Example 1.2.79 The functor $M \otimes_R -$ is not always left-exact: tensoring $0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q}$ by $\mathbb{Z}/n\mathbb{Z}$ we get the sequence $0 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$ which is far from being exact.

Definition 1.2.80 An R-module M is **flat** if the functor $M \otimes_R -$ is exact. A ring homomorphism $\varphi : R \to A$ is flat if it makes A into a flat R-module. We shall say then that A is a **flat R-algebra**.

Example 1.2.81 $\mathbb{Q}$ is a flat $\mathbb{Z}$-algebra: this is a special case of a statement we shall prove later, corollary 2.1.21. A free module is flat, since $(\bigoplus_\alpha R) \otimes_R M \cong \bigoplus_\alpha M$.

Remark 1.2.82 If $\varphi : R \to R'$ is a flat R-algebra and $\psi : R' \to R''$ a flat R'-algebra, it follows immediately from corollary 1.2.72 that R'' is a flat R-algebra via $\psi \circ \varphi$. Notice however that it may happen that φ and $\psi \circ \varphi$ are flat but ψ is not. For example take $\varphi : R \to R[X]$ the inclusion and $\psi : R[X] \to R = R$ defined by $\psi(X) = 0$. Then φ is flat ($R[X]$ is free) and $\psi \circ \varphi = id_R$ but

$$R \otimes_{R[X]} \Big[0 \longrightarrow XR[X] \longrightarrow R[X] \xrightarrow{\psi} R \longrightarrow 0\Big] = 0 \longrightarrow R \otimes_{R[X]} XR[X] \longrightarrow R \xrightarrow{id_R} R \longrightarrow 0$$

is not exact, since $R \otimes_{R[X]} XR[X] \neq 0$.

Proposition 1.2.83 *Let M be an R-module. The following conditions are equivalent:*

a) M is flat;

b) for every injection $f : N' \hookrightarrow N$ the map $id_M \otimes f : M \otimes_R N' \to M \otimes_R N$ is injective;

c) $id_M \otimes f : M \otimes_R N' \to M \otimes_R N$ is injective for every injection $f : N' \hookrightarrow N$ between finitely generated R-modules;

d) for every ideal $I \subseteq R$ the multiplication map

$$\begin{aligned} I \otimes_R M &\longrightarrow M \\ x \otimes m &\longmapsto xm \end{aligned}$$

is injective.

Proof. The implications a) $\implies$ b) $\implies$ c) are obvious. For b) $\implies$ a), if $\longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N''$ is exact, tensoring by M the exact sequence $0 \longrightarrow \operatorname{im} f \longrightarrow \ker g \longrightarrow 0$ we get an injection $\operatorname{im}(id_M \otimes f) \subseteq \ker(id_M \otimes g)$, and in fact an isomorphism, since $M \otimes_R -$ is left-exact anyway.
b) $\implies$ d) follows by tensoring by M the sequence $0 \longrightarrow I \longrightarrow R$ and recalling that the multiplication $R \otimes_R M \to M$ is an isomorphism.
c) $\implies$ b): let $f : N' \hookrightarrow N$ be an injection and $x = \sum_i m_i \otimes n_i \in \ker id_M \otimes f$, i.e. $\sum_i m_i \otimes f(n_i) = 0$. Let N'_0 be the R-submodule of N' generated by the n_i. Recall from theorem 1.2.61 that $M \otimes_R N$ is the quotient of the free module on $M \times N$ by the submodule S generated by the relations (1.4). Hence $\sum_i m_i \otimes f(n_i) = 0$ in $M \otimes_R N$ means $\sum_i (m_i, f(n_i)) \in S$. Write $\sum_i (m_i, f(n_i)) = \sum_j \alpha_j s_j$, with $\alpha_j \in R$, $s_j \in S$ and let $N_0 \subseteq N$ be the submodule generated by $f(N'_0)$ and the N-components of the s_j. By construction, $y_0 = \sum_i m_i \otimes f(n_i) = 0$ in $M \otimes_R N_0$ because $\sum_i (m_i, f(n_i))$ is in the corresponding submodule generated by the relations (1.4). The restriction $f : N'_0 \hookrightarrow N_0$ is an injection of finitely generated R-modules, hence $id_M \otimes f : M \otimes_R N'_0 \hookrightarrow M \otimes_R N_0$ is injective. It maps x_0 to $y_0 = 0$, thus $x_0 = 0$ and so its image $x \in M \otimes_R N'$ vanishes too.
d) $\implies$ c): let $f : N' \hookrightarrow N$ be an injection of finitely generated modules. Suppose first that N is free of rank r. If $r = 1$ the statement is precisely condition d). We proceed by induction on r: write $N = N_1 \oplus N_2$ with N_i free of rank $r_i < r$ and consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N'_1 & \longrightarrow & N' & \longrightarrow & N'_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_2} & & \\ 0 & \longrightarrow & N_1 & \longrightarrow & N & \longrightarrow & N_2 & \longrightarrow & 0 \end{array} \tag{1.6}$$

where $N'_1 = f^{-1}(N_1)$, f_1 is the restriction of f, $N'_2 = N'/N'_1$ and f_2 the induced map. A simple diagram chase shows that f_2 is also injective. By inductive assumption $id_M \otimes f_i$ are injective, so the snake lemma applied to diagram (1.6) tensored by M shows that $id_M \otimes f$ is injective too. If N is an arbitrary finitely generated R-module, pick a presentation $\pi : R^r \twoheadrightarrow N$ and consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker \pi & \longrightarrow & \pi^{-1}(f(N')) & \longrightarrow & N' & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & \ker \pi & \longrightarrow & R^r & \xrightarrow{\pi} & N & \longrightarrow & 0 \end{array} \tag{1.7}$$

where ι is the inclusion. Tensoring (1.7) by M, we have $id_M \otimes id_{\ker \pi} = id_{M \otimes_R \ker \pi}$ and $id_M \otimes \iota$ is injective by the free case just treated. By the snake lemma we conclude $\ker(id_M \otimes f) = 0$. $\square$

Proposition 1.2.84 *Let R' be R-algebra, M and N two R-modules. There is an R'-linear map*

$$\vartheta_{M,N} : R' \otimes Hom_R(M,N) \to Hom_{R'}(R' \otimes M, R' \otimes N).$$

It is an isomorphism if R' is flat over R and M is a finitely presented R-module.

Proof. The map $\lambda \mapsto id_{R'} \otimes \lambda$ defines a homomorphism $Hom_R(M,N) \to Hom_{R'}(R' \otimes M, R' \otimes N)$ of R-modules, whence an R-bilinear map $R' \times Hom_R(M,N) \to Hom_{R'}(R' \otimes M, R' \otimes N)$ given by $(x, \lambda) \mapsto x \otimes \lambda$. This induces the map $\vartheta_{M,N}$ in the statement.
By proposition 1.2.31 we have $Hom_R(R^n, N) \cong N \oplus \cdots \oplus N$, hence $\vartheta_{R^n,N}$ is an isomorphism.
Suppose now that that R' is a flat and M has a finite presentation: $R^m \to R^n \to M \to 0$. Applying the Hom functor to this sequence, we obtain the following commutative diagram, where M', N' stand for $R' \otimes M$ and $R' \otimes N$

$$\begin{array}{ccccccc}
0 & \longrightarrow & R' \otimes Hom_R(M,N) & \longrightarrow & R' \otimes Hom_R(R^n,N) & \longrightarrow & R' \otimes Hom_R(R^m,N) \\
 & & \downarrow{\scriptstyle \vartheta_{M,N}} & & \downarrow{\scriptstyle \vartheta_{R^n,N}} & & \downarrow{\scriptstyle \vartheta_{R^m,M}} \\
0 & \longrightarrow & Hom_{R'}(M',N') & \longrightarrow & Hom_{R'}({R'}^n,N') & \longrightarrow & Hom_{R'}({R'}^m,N').
\end{array}$$

The diagram has exact rows and the maps $\vartheta_{R^n,N}$ and $\vartheta_{R^m,N}$ are isomorphism. A little diagram chase shows that $\vartheta_{M,N}$ is an isomorphism. □

§ 3 Differentials

Definition 1.3.1 *Let $\varphi : R \to A$ be a ring homomorphism and M an A-module. An R-***derivation** *$d : A \to M$ is an R-linear map satisfying* **Leibnitz rule***:*

$$d(xy) = xdy + ydx.$$

We denote $\mathrm{Der}_R(A,M)$ the set of all R-linear derivations $A \to M$.

Notice that $\mathrm{Der}_R(A,M)$ is an A-module: for $a \in A$ and $d \in \mathrm{Der}_R(A,M)$, define $ad : A \to M$ as $(ad)x = a(dx)$.

Proposition 1.3.2 *The functor $\mathrm{Der}_R(A,-) : \mathbf{Mod}_A \to \mathbf{Mod}_A$ is representable. In other words, there exists and A-module $\Omega^1_{A/R}$ and an R-linear derivation $d_{A/R}$ (the universal element, see remark A.16) such that for every A-module M and every R-derivation δ there is a unique A-linear map ϑ such that $\delta = \vartheta \circ d_{A/R}$:*

(1.8)
$$\begin{array}{ccc}
A & \xrightarrow{\ \delta\ } & M \\
{\scriptstyle d_{A/R}}\downarrow & \nearrow_{\vartheta} & \\
\Omega^1_{A/R} & &
\end{array}$$

Proof. Let F be the free A module generated by the elements dx, for all $x \in A$. Let $S \subseteq F$ be the submodule generated by the relations

$$d(x+y) - dx - dy; \quad d(\alpha x) - \alpha dx; \quad d(xy) - xdy - ydx \qquad \forall\, x, y \in A,\ \forall\, \alpha \in R.$$

Put $\Omega^1_{A/R} = F/S$. Let $d_{A/R} : A \to F \to \Omega^1_{A/R}$ be the map $x \mapsto dx \bmod S$. By construction $d_{A/R}$ is an R-derivation and for every derivation $\delta : A \to M$, one checks that $\vartheta(dx) = \delta(x)$ is a well defined map making diagram (1.8) commute.

Definition 1.3.3 *The pair* $(\Omega^1_{A/R}, d_{A/R})$ *is called the* **universal module of differentials**.

Notice that as a consequence of the construction in proposition 1.3.2, the A-module $\Omega^1_{A/R}$ is generated by the image of $d_{A/R}$. When there is no risk of confusion, we will write d_A or just d instead of $d_{A/R}$.

Example 1.3.4 If $A = R[X_1, \ldots, X_n]$ then $\Omega^1_{A/R} = \bigoplus_{i=1}^n A dX_i$. Indeed by Leibnitz rule we have

$$d(X_1^{\nu_1} \ldots X_n^{\nu_n}) = \sum_{i=1}^n \nu_i \frac{X_1^{\nu_1} \ldots X_n^{\nu_n}}{X_i} dX_i \quad \Longleftrightarrow \quad dF = \sum_{i=1}^n \frac{\partial F}{\partial X_i} dX_i \quad \forall\, F \in R[X_1, \ldots, X_n].$$

Therefore $\Omega^1_{A/R}$ is generated by $dX_1, \ldots, dX_n$, whence a surjection $\pi : A^n \twoheadrightarrow \Omega^1_{A/R}$. The map

$$\begin{array}{rcl} \nabla : A & \longrightarrow & A^n \\ F & \longmapsto & \left(\frac{\partial F}{\partial X_1}, \ldots, \frac{\partial F}{\partial X_n}\right) \end{array}$$

is clearly an R-derivation, whence an A-linear map $\vartheta : \Omega^1_{A/R} \to A^n$. One checks immediately that ϑ is an inverse to π.

Example 1.3.5 Let $A = R[X_1, \ldots, X_n]/(F_1, \ldots, F_m)$, and denote by x_i the image of X_i in A. Since $F_i = 0$ in A, necessarily $dF_i = d0 = 0$ in $\Omega^1_{A/R}$: from example 1.3.4 we get that $\Omega^1_{A/R}$ is the quotient of $\bigoplus_{i=1}^n A dx_i$ by the submodule $\left(\sum_{i=1}^n \frac{\partial F_j}{\partial X_i}(x_1, \ldots, x_n) dx_i \mid 1 \leq j \leq m\right)$. Therefore if A is an R-algebra of finite type, $\Omega^1_{A/R}$ is a finitely generated A-module.

Example 1.3.6 If K is a field and L a finite separable extension, then $\Omega^1_{L/K} = 0$. Indeed, by Abel's theorem there exists a separable polynomial $f(X) \in K[X]$ such that $L \simeq K[X]/(f)$. By example 1.3.5, $\Omega^1_{L/K}$ is the L-vector space generated by dx modulo the relation $f'(x)dx$, and by the separability assumption, $f'(x) \in L^\times$.

Example 1.3.7 If K is a field of characteristic $p > 0$ and $L = K[X]/(f)$ a monogenic inseparable extension. Then $\Omega^1_{L/K} = L$. Indeed, since f is inseparable, $f(X) = g(X^p)$ for some $g \in K[X]$. By example 1.3.5, $\Omega^1_{L/K}$ is the L-vector space generated by dx modulo the relation $f'(x)dx$, and $f'(x) = px^{p-1}g'(x^p) = 0$.

Remark 1.3.8 There is an alternative construction of the module $\Omega^1_{A/R}$. Let $\mu : A \otimes_R A \to A$ be the multiplication map $\mu(x \otimes y) = xy$. Then $I = \ker(\mu)$ is the submodule of $A \otimes_R A$ generated by the elements $1 \otimes x - x \otimes 1$ for all $x \in A$. Indeed, we can write $x \otimes y = xy \otimes 1 + (x \otimes 1)(1 \otimes y - y \otimes 1)$.

By definition, an element $\sum_i x_i \otimes y_i$ is in I if and only if $\sum_i x_i y_i = 0$ and thus $\sum_i x_i \otimes y_i = \sum_i (x_i \otimes 1)(1 \otimes y_i - y_i \otimes 1)$.
The quotient I/I^2 is an $A \otimes_R A/I = A$-module and the R-linear map

$$\begin{aligned} d : A &\longrightarrow I/I^2 \\ x &\longmapsto 1 \otimes x - x \otimes 1 \bmod I^2 \end{aligned}$$

is a derivation, since $1 \otimes xy - xy \otimes 1 = (x \otimes 1)(1 \otimes y - y \otimes 1) + (1 \otimes y)(1 \otimes x - x \otimes 1)$. The fact that $(I/I^2, d)$ satisfies the universal property (1.8) is proven in exercise 1.23.

If $R \to R'$ is a ring homomorphism, let $A' = R' \otimes_R A$, viewed as an A-algebra via the map $A \to A'$ given by $a \mapsto 1 \otimes a$

Proposition 1.3.9 *The map $A' \otimes_A \Omega^1_{A/R} \to \Omega^1_{A'/R'}$, given by $x \otimes dy \mapsto xd(1 \otimes y)$ is an isomorphism.*

Proof. The composition $A \to A' \to \Omega^1_{A'/R'}$ is an R-linear derivation, whence an A-linear map ϑ

$$\begin{array}{ccccc} A & \longrightarrow & A' & \xrightarrow{d_{A'/R'}} & \Omega^1_{A'/R'} \\ {\scriptstyle d_{A/R}}\downarrow & & & \nearrow_{\vartheta} & \\ \Omega^1_{A/R} & & & & \end{array}$$

given by $\vartheta(dy) = d(1 \otimes y)$. This induces the A'-linear map in the statement. On the other hand, tensoring $d_{A/R}$ by A' we get an R'-derivation $A' = R' \otimes_R A \to A' \otimes_A \Omega^1_{A/R'}$, whence

$$\begin{array}{ccc} A' & \xrightarrow{id_{R'} \otimes d_{A/R}} & A' \otimes_A \Omega^1_{A/R}. \\ {\scriptstyle d_{A'/R'}}\downarrow & \nearrow_{\vartheta'} & \\ \Omega^1_{A'/R'} & & \end{array}$$

Since $\vartheta'(d(1 \otimes y)) = dy$ for all $y \in A$, we see that ϑ' is the inverse of ϑ. □

Proposition 1.3.10 (First fundamental sequence) *Let $\varphi : R \to A$ and $\psi : A \to B$ be homomorphisms. The following sequence of B-modules is exact:*

$$B \otimes_A \Omega^1_{A/R} \xrightarrow{v} \Omega^1_{B/R} \xrightarrow{u} \Omega^1_{B/A} \longrightarrow 0$$

where $v(b \otimes d_{A/R}(a)) = b d_{B/R}(\psi(a))$ and $u(d_{B/R}(b)) = d_{B/A}(b)$.

Proof. It is obvious that u is surjective and that $u \circ v = 0$. To check exactness in the middle we may apply the functor $Hom_B(-, N)$, for all B-module N. We have a commutative diagram

$$\begin{array}{ccccc} Hom_B(\Omega^1_{B/A}, N) & \xrightarrow{u^*} & Hom_B(\Omega^1_{B/R}, N) & \xrightarrow{v^*} & Hom_B(B \otimes_A \Omega^1_{A/R}, N) \\ \cong\downarrow & & \downarrow\cong & & \downarrow\alpha \\ \mathrm{Der}_A(B, N) & \longrightarrow & \mathrm{Der}_R(B, N) & \xrightarrow{\psi^*} & \mathrm{Der}_R(A, N). \end{array}$$

and the map α is the composition of the isomorphism $Hom_B(B\otimes_A\Omega^1_{A/R},N)\cong Hom_A(\Omega^1_{A/R},N)$ given in exercise 1.16, with the natural identification $Hom_A(\Omega^1_{A/R},N)\cong \mathrm{Der}_A(A,N)$. Since the vertical arrows are isomorphisms, it suffices to check exactness of the bottom row. But this is clear: $\psi_*(\delta)=\delta\circ\psi=0$ means $(\delta\circ\psi)(a)=\delta(\psi(a))=0$ for all $a\in A$ and this is equivalent to saying that the R-linear derivation δ is A-linear. □

Corollary 1.3.11 *The first fundamental sequence can be extended by a 0 on the left if and only if every R-linear derivation $\delta: A\to N$ with values in a B-module N can be extended to an R-linear derivation $\tilde{\delta}: B\to N$.*

Proof. This is a byproduct of the proof of proposition 1.3.10: v is injective if and only if ψ^* is surjective. □

Corollary 1.3.12 *Let $k\subseteq K\subseteq L$ be fields, with L/K finite separable. Then $v: L\otimes_K\Omega^1_{K/k}\to\Omega^1_{L/k}$ is an isomorphism.*

Proof. $\Omega^1_{L/K}=0$ by example 1.3.6, so v is surjective. Let's check that the condition of corollary 1.3.11 is satisfied. By Abel's theorem, $L\simeq K[X]/(f)$ for some $f=\sum_{i=0}^n a_iX^i\in K[X]$ separable and write x for the image of X. Let $\delta: K\to N$. If it can be extended, by Leibnitz rule

$$0=\tilde{\delta}(0)=\tilde{\delta}\left(f(x)\right)=\sum_{i=0}^n\delta(a_i)x^i+\sum_{i=1}^n ia_ix^{i-1}\tilde{\delta}(x)=\sum_{i=0}^n\delta(a_i)x^i+f'(x)\tilde{\delta}(x).$$

Since $f'(x)\neq 0$, this formula can be reversed to define $\tilde{\delta}(x)=-(f'(x))^{-1}(\sum_{i=0}^n\delta(a_i)x^i)$. It is now easy to check that this defines a derivation $\tilde{\delta}: L\to N$ extending δ. □

Corollary 1.3.13 *If $\psi: A\twoheadrightarrow B$ is surjective, $\Omega^1_{B/A}=0$.*

Proof. If ψ is surjective, $v: B\otimes_A\Omega^1_{A/R}\to\Omega^1_{B/R}$ is surjective because $\Omega^1_{B/R}$ is generated by the elements db. □

If ψ is surjective, we can continue the sequence. If $B=A/J$, then J/J^2 is a $B=A/J$-module.

Proposition 1.3.14 (Second fundamental sequence) *Let $B=A/J$. The following sequence of B-modules is exact:*

$$J/J^2\xrightarrow{\ w\ }B\otimes_A\Omega^1_{A/R}\xrightarrow{\ v\ }\Omega^1_{B/R}\longrightarrow 0$$

where $w(a \bmod J^2)=1\otimes da$.

Proof. Let's first check that w is well defined. Indeed, if $x,y\in J\subset A$ then $1\otimes d(xy)=1\otimes xdy+1\otimes ydx=\psi(x)\otimes dy+\psi(y)\otimes dx=0$, since $\psi(x)=\psi(y)=0$.
The surjectivity of v is given in corollary 1.3.13. To check exactness, we may again apply $Hom_B(-,N)$ to get

$$\begin{array}{ccccc} Hom_B(\Omega^1_{B/R},N) & \xrightarrow{v^*} & Hom_B(B\otimes_A\Omega^1_{A/R},N) & \xrightarrow{w^*} & Hom_B(J/J^2,N) \\ \cong\downarrow & & \downarrow\cong & & \downarrow\beta \\ \mathrm{Der}_R(B,N) & \xrightarrow{\psi^*} & \mathrm{Der}_R(A,N) & \xrightarrow{\text{restriction}} & Hom_A(J,N). \end{array} \tag{1.9}$$

Notice that if $\delta : A \to N$ is an R-derivation, its restriction to J is A-linear because N is a $B = A/J$-module: for $a \in A$ and $x \in J$ we have $\delta(ax) = a\delta(x) + x\delta(a) = a\delta(x)$. The map β is an isomorphism by exercise 1.22, so it suffices to check exactness of the bottom row. But $\delta(x) = 0$ for all $x \in J$ if and only if $\delta : A \to N$ factors through $A/J = B$. □

Corollary 1.3.15 *If A is an R-algebra of finite presentation, $\Omega^1_{A/R}$ is a finitely presented A-module.*

Corollary 1.3.16 *Let k be a field, $\varphi : k \to A$ a local k algebra with maximal ideal $\mathfrak{m}$ such that $A/\mathfrak{m} \simeq k$. Then $w : \mathfrak{m}/\mathfrak{m}^2 \to k \otimes_A \Omega^1_{A/k}$ is an isomorphism.*

Proof. Under these assumption, $\psi \circ \varphi : k \to A \to k$ is the identity map, so φ splits the surjection ψ and we get a decomposition $A = \mathfrak{m} \oplus k$ as k-vector spaces. Since $\Omega^1_{k/k} = 0$, w is surjective. It is injective if and only if its dual is surjective. Inspecting the right square in diagram (1.9), this is equivalent to showing that the restriction map

$$\mathrm{Der}_k(A, k) \longrightarrow Hom_k(\mathfrak{m}/\mathfrak{m}^2, k)$$

is surjective. For every $x \in A$, let $\overline{x} = \varphi(\psi(x))$, thus $x - \overline{x} \in \mathfrak{m}$ and $x = (x - \overline{x}) + \overline{x}$ is the unique decomposition of x in $A = \mathfrak{m} \oplus k$. If $\lambda : \mathfrak{m}/\mathfrak{m}^2 \to k$ is a k-linear map, define $\delta(x) = \lambda(x - \overline{x})$. This map is clearly k-linear and its restriction to $\mathfrak{m}$ is λ. Let's check Leibnitz rule:

$$\begin{aligned}
\delta(xy) &= \delta\left((x - \overline{x})(y - \overline{y}) + \overline{x}(y - \overline{y}) + \overline{y}(x - \overline{x}) + \overline{xy}\right) \\
&= \lambda\left((x - \overline{x})(y - \overline{y}) + \overline{x}(y - \overline{y}) + \overline{y}(x - \overline{x})\right) \\
&= \overline{x}\lambda(y - \overline{y}) + \overline{y}\lambda(x - \overline{x}) \\
&= \overline{x}\delta(y) + \overline{y}\delta(x).
\end{aligned}$$

Therefore δ is a k-derivation and we have shown that the restriction map is surjective. □

Remark 1.3.17 Since $\mathfrak{m}/\mathfrak{m}^2$ is isomorphic to the space of differentials, its dual $(\mathfrak{m}/\mathfrak{m}^2)^\vee$ deserves the name of **tangent space** to $\mathrm{Spec}\, A$ at the point $\mathcal{Z}(\mathfrak{m})$. So far, this makes sense only for local rings, but in § 2.1 we shall learn how to turn every ring into a local one and every prime into a maximal ideal by the process of localisation.

Building upon the ideas in the proof of corollary 1.3.16, we can give another useful characterisation of the tangent space. Define the ring of **dual numbers** $k[\varepsilon]$ as the quotient $k[X]/(X^2)$. With notation as in the proof of corollary 1.3.16, a linear form $\lambda : \mathfrak{m}/\mathfrak{m}^2 \to k$ extends to a k-linear map $f : A \to k[\varepsilon]$ by the formula $f(x) = \overline{x} + \lambda(x - \overline{x})\varepsilon = \overline{x} + \delta(x)\varepsilon$. This map is in fact a k-algebra homomorphism. To see this, recall that δ is a derivation, thus

$$f(xy) = \overline{xy} + \delta(xy)\varepsilon = \overline{xy} + \overline{x}\delta(y)\varepsilon + \overline{y}\delta(x)\varepsilon = (\overline{x} + \delta(x)\varepsilon)\,(\overline{y} + \delta(y)\varepsilon) = f(x)f(y).$$

We have thus constructed a map $(\mathfrak{m}/\mathfrak{m}^2)^\vee \to Hom_{k\text{-alg}}(A, k[\varepsilon])$. Notice that, if $\pi : k[\varepsilon] \to k$ is the natural projection, $\pi \circ f = \psi$ (as above, $\psi : A \to A/\mathfrak{m} = k$ is the quotient map $\psi(x) = \overline{x}$).

Corollary 1.3.18 *Let k be a field, A a local k algebra with maximal ideal $\mathfrak{m}$ such that $A/\mathfrak{m} \simeq k$. The construction above gives a bijection between $(\mathfrak{m}/\mathfrak{m}^2)^\vee$ and the subset $\{f \in Hom_{k\text{-alg}}(A, k[\varepsilon]) \mid \pi \circ f = \psi\}$.*

Proof. The map constructed above is obviously injective. Let $f : A \to k[\varepsilon]$ be a k-algebra homomorphism such that $\pi \circ f = \psi$. Then $\pi(f(\mathfrak{m})) = \psi(\mathfrak{m}) = 0$, thus $f(\mathfrak{m}) \subseteq \ker \pi = (\varepsilon)$. Moreover, since $\varepsilon^2 = 0$, we have $f(\mathfrak{m}^2) = 0$. The ideal (ε) is isomorphic to k, hence the restriction of f to $\mathfrak{m}$ defines a linear map $\lambda : \mathfrak{m}/\mathfrak{m}^2 \to k$ by $f(x) = \lambda(x)\varepsilon$. □

For a generalisation of corollary 1.3.18, see exercise 2.5.

§ 4 Exercises

Exercise 1.1 Show that for every ring R there exists a unique ring homomorphism $\varphi : \mathbb{Z} \to R$ (category theory language: $\mathbb{Z}$ is the *initial object* in the category of rings).

Exercise 1.2 Let $I = (X)$ and $J = (Y)$ in $\mathbb{C}[X, Y]$. Show that $I \cap J = IJ$ but I and J are not coprime.

Exercise 1.3 Let R be a ring, $\mathfrak{a}_1, \mathfrak{a}_2$ ideals and $\pi_i : R \to R/\mathfrak{a}_i$ the projection. Show that $\pi_1 \times \pi_2$ defines a ring homomorphism $\psi : R/\mathfrak{a}_1\mathfrak{a}_2 \to R/\mathfrak{a}_1 \times R/\mathfrak{a}_2$. Show that this is surjective if and only if $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are coprime and that in this case ψ is an isomorphism. Give an example in which ψ is injective but not surjective.

Exercise 1.4 Let R be a ring, $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ ideals. Show that, if $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, $\mathfrak{a}\mathfrak{b} + \mathfrak{c} = (\mathfrak{a} + \mathfrak{c}) \cap (\mathfrak{b} + \mathfrak{c})$.

Exercise 1.5 Describe all the prime ideals in the ring $\mathbb{Z}[X]/(2X)$.

Exercise 1.6 Let $R_1 \times R_2$ be the product of two rings. Show that $e_1 = (1, 0)$ and $e_2 = (0, 1)$ form an *orthogonal basis of idempotents* i.e.

$$e_i^2 = e_i; \qquad e_1 e_2 = 0; \qquad e_1 + e_2 = 1.$$

Conversely, show that if a ring R contains two elements e_1, e_2 satisfying the above property, then R is isomorphic to the product of two rings.

Exercise 1.7 Let R be a PID. Show that any increasing sequence $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_i \subseteq \mathfrak{a}_{i+1} \subseteq \ldots$ of ideals in R eventually stabilizes: $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \ldots$ for n sufficiently large.

Exercise 1.8 Let R be a PID. Denote by $M(m \times n, R)$ the (noncommutative) ring of $m \times n$ matrices with coefficients in R and by $\mathrm{GL}_n(R) \subset M(n \times n, R)$ the group of invertible matrices. Recall that elementary operations on the rows (resp. columns) of a matrix are given by left (resp. right) multiplication by an invertible matrix. A matrix $A = (a_{i,j}) \in M(m \times n, R)$ is in **Smith normal form** if $a_{i,j} = 0$ for $i \neq j$ and $a_{i,i} | a_{i+1,i+1}$ $\forall\, i = 1, \ldots, m-1$.
Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2 \times 2, R)$.

a) Suppose that $b = c = 0$ and that $\gcd(a, d) = 1$. Use the identity $ar + ds = 1$ (for suitable $r, s \in R$) to transform A, by row and column operations, into the matrix $\begin{pmatrix} 1 & 0 \\ 0 & ad \end{pmatrix}$.

b) Let $e_1 = \gcd(a, c)$ and write $e_1 = ax + cy$. Check that $S_1 = \begin{pmatrix} x & y \\ \frac{c}{e_1} & -\frac{a}{e_1} \end{pmatrix} \in \mathrm{GL}_2(R)$.

c) Check that $S_1 A$ is a matrix of the form $\begin{pmatrix} e_1 & * \\ 0 & * \end{pmatrix}$.

d) Show that there exists a matrix $T_2 \in \mathrm{GL}_2(R)$ such that S_1AT_2 is of the form $\begin{pmatrix} e_2 & 0 \\ * & * \end{pmatrix}$ with $e_2|e_1$.

e) Show that there exist $S, T \in \mathrm{GL}_2(R)$ such that SAT is of the form $\begin{pmatrix} e & f \\ 0 & g \end{pmatrix}$ or $\begin{pmatrix} e & 0 \\ f & g \end{pmatrix}$ with $e|f$. [Hint: consider the sequence of ideals $(e_1) \subseteq (e_2) \subseteq \ldots$.]

f) Show that there exist $S, T \in \mathrm{GL}_2(R)$ such that SAT is of the form $\begin{pmatrix} e & 0 \\ 0 & g \end{pmatrix}$.

g) Show that there exist $S, T \in \mathrm{GL}_2(R)$ such that SAT is in Smith normal form.

h) Compute a Smith normal form for $\begin{pmatrix} 84 & 18 & 141 \\ 66 & 12 & 108 \end{pmatrix}$ by row and column operations.

More generally, let now $A = (a_{ij}) \in M(m \times n, R)$.

i) Show that there exist $S_1 \in \mathrm{GL}_m(R)$ such that S_1A is of the form $\begin{pmatrix} e_1 & * & \ldots & * \\ 0 & * & \ldots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \ldots & * \end{pmatrix}$.

j) Show that there exist $T_1 \in \mathrm{GL}_n(R)$ such that $S_1AT_1 = \begin{pmatrix} e_2 & 0 & \ldots & 0 \\ * & * & \ldots & * \\ \vdots & \vdots & & \vdots \\ * & * & \ldots & * \end{pmatrix}$ with $e_2|e_1$.

k) Show that there exist $S \in \mathrm{GL}_m(R)$, $T \in \mathrm{GL}_n(R)$ such that $SAT = \begin{pmatrix} e & 0 & \ldots & 0 \\ 0 & * & \ldots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \ldots & * \end{pmatrix}$.

l) Show that there exist $S \in \mathrm{GL}_m(R)$, $T \in \mathrm{GL}_n(R)$ such that SAT is in Smith normal form.

Exercise 1.9 Let R be a PID and M a finitely presented[1] R-module.

a) Show that M is isomorphic to a product $R/\mathfrak{a}_1 \oplus R/\mathfrak{a}_2 \oplus \cdots \oplus R/\mathfrak{a}_n$ where $\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots \supseteq \mathfrak{a}_n$ is a sequence of ideals in R. This is known as the **elementary divisors' theorem**.

b) Show that M is the direct sum of a free module and a torsion module.

c) Show that M is free if and only[2] if $M_{tors} = 0$.

d) Show that any finitely presented submodule of a free R-module is free.

e) Let A be a finitely generated abelian group. Show that $A \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^r$ for suitable integers r and $n_1|n_2|\ldots|n_k$.

[1] We shall see in corollary 4.1.9 that any finitely generated module over a PID has a finite presentation.
[2] This fails if M is not finitely generated: $\mathbb{Q}$ has no torsion but it is not a free $\mathbb{Z}$-module.

Exercise 1.10 Show that if A_1 and A_2 are R-algebras of finite type then $A_1 \times A_2$ is an R-algebra of finite type.

Exercise 1.11 Let X be a Hausdorff (i.e. compact and separated) topological space. Recall that for any two points $x, y \in X$ one can construct a continuous function $f : X \to \mathbb{R}$ such that $f(x) = 0$ and $f(y) = 1$ (Urysohn's lemma). Let $C = C^0(X)$ be the ring of continuous real-valued functions on X. For any subset $S \subseteq C$, put $Z(S) = \{x \in X \mid f(x) = 0 \; \forall f \in S\}$ and let M be the set of all maximal ideals in C.

a) Show that $Z(S) = Z((S))$ (where (S) is the ideal generated by a subset S).

b) Show that if $I \subsetneq C$ is an ideal then $Z(I) \neq \varnothing$.

c) Show that the map

$$\begin{array}{rcl} X & \longrightarrow & M \\ x & \longmapsto & \mathfrak{m}_x = \{f \in C \mid f(x) = 0\} \end{array}$$

is a bijection.

Exercise 1.12 (Kummer's Lemma) Let R be a local ring with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. Let $f \in R[X]$ be a monic irreducible polynomial, $\overline{f} = \prod_{i=1}^{r} \overline{g}_i^{e_i} \in k[X]$ a decomposition of the reduction of f mod $\mathfrak{m}$, with the $\overline{g}_i \in k[X]$ monic irreducible, $(\overline{g}_i, \overline{g}_j) = 1$ for $i \neq j$. Choose $g_i \in R[X]$ lifting $\overline{g}_i$, for each $i = 1, \ldots, r$, and denote $\mathfrak{m}_i$ the ideal of $A = R[X]/(f)$ generated by $\mathfrak{m}$ and g_i. Show that $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$ is the set of all maximal ideals of A

Exercise 1.13 Let R be a ring and $J \subset R$ an ideal. If $P(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$ denote $\overline{P}(X_1, \ldots, X_n) \in R/J[X_1, \ldots, X_n]$ the polynomial obtained by reducing mod J the coefficients of P. Show that

$$R[X_1, \ldots, X_n]/(F_1, \ldots, F_m) \otimes_R R/J \cong R/J[X_1, \ldots, X_n]/\left(\overline{F}_1, \ldots, \overline{F}_m\right).$$

Exercise 1.14 Compute the tensor products $\mathbb{Z}[X, Y]/(X^2 - Y^2) \otimes_{\mathbb{Z}} \mathbb{Z}[X, Y](X^2 + Y^2 - 1)$ and $\mathbb{Z}[X, Y]/(X^2 - Y^2) \otimes_{\mathbb{Z}[X,Y]} \mathbb{Z}[X, Y](X^2 + Y^2 - 1)$.

Exercise 1.15 Let R be a ring, $\varphi : R \to A$ a flat R-algebra and I, J two ideals in R. Show that $\varphi(I)A \cap \varphi(J)A = \varphi(I \cap J)A$.

Exercise 1.16 Let $\psi : A \to B$ be a ring-homomorphism. If M is an A-module and N a B-module, view $Hom_A(M, N)$ as a B-module via multiplication on the target (so $b \cdot f$ is the function whose value at $m \in M$ is $bf(m)$). Show that the map

$$\begin{array}{rcl} Hom_B(M \otimes_A B, N) & \longrightarrow & Hom_A(M, N) \\ g & \longmapsto & [m \mapsto g(m \otimes 1)] \end{array}$$

is an isomorphism of B-modules.

Exercise 1.17 Let N and Q be two R-modules. An R-module E is called an **extension of Q by N** if it sits in an exact sequence of R-modules

$$0 \longrightarrow N \xrightarrow{\iota} E \xrightarrow{\pi} Q \longrightarrow 0. \tag{1.10}$$

The extension $E = N \oplus Q$ is called the trivial extension. A morphism between two extensions E_1 and E_2 is a homomorphism $\eta : E_2 \to E_2$ such that the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{\iota_1} & E_1 & \xrightarrow{\pi_1} & Q & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \eta} & & \| & & \\ 0 & \longrightarrow & N & \xrightarrow{\iota_2} & E_2 & \xrightarrow{\pi_2} & Q & \longrightarrow & 0. \end{array} \tag{1.11}$$

commutes. If $\alpha : N \to N'$ is a morphism, the **pushout** $\alpha_* E$ is defined as the quotient of $N' \oplus E$ by the submodule $S = \{(-\alpha(x), \iota(x)) \in N' \oplus E, \forall x \in N\}$. If $\beta : Q' \to Q$ is a morphism, the module $\beta^* E = \{(x, y) \in E \oplus Q' \,|\, \pi(x) = \beta(y)\}$ is called the **pullback** of E. If E_1 and E_2 are two extensions of Q by N, the module $E_1 \boxplus E_2 = \{(x, y) \in E_1 \oplus E_2 \,|\, \pi_1(x) = \pi_2(y)\}/D$, where $D = \{(\iota_1(z), -\iota_2(z)) \in E_1 \oplus E_2, \forall z \in N\}$ is called the **Baer sum** of E_1 and E_2.

a) Check that a morphism of extensions is always an isomorphism.

b) Check that an extension E is isomorphic to the trivial extension and only if (1.10) admits a splitting $\sigma : Q \to E$ (i.e. $\pi \circ \sigma = id_Q$).

c) Check that $\alpha_* E$ is an extension of Q by N' and that $\beta^* E$ is an extension of Q' by N.

d) Check that $E_1 \boxplus E_2$ is again an extension of Q by N.

Denote by $Ext^1_R(Q, N)$ the set of isomorphism classes of extensions of Q by N. If E is an extension, write $[E] \in Ext^1_R(Q, N)$ for its class.

e) Check that $[E_1] + [E_2] = [E_1 \boxplus E_2]$ defines an abelian group structure on $Ext^1_R(Q, N)$, with neutral element $[N \oplus Q]$.

To a short exact sequence of R-modules

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0.$$

associate the following

$$\begin{array}{l} 0 \longrightarrow Hom_R(N, M') \longrightarrow Hom_R(N, M) \longrightarrow Hom_R(N, M'') \xrightarrow{\delta} \\ \longrightarrow Ext^1_R(N, M') \longrightarrow Ext^1_R(N, M) \longrightarrow Ext^1_R(N, M'') \end{array}$$

where, to $g : N \to M''$, we set $\delta(g) = [g_*(M)]$.

f) Show that the latter is a sequence of abelian groups extending the $Hom_R(N, -)$ sequence.

Exercise 1.18 Let R_1 and R_2 be rings. Show that $\mathrm{Spec}\ (R_1 \times R_2) = \mathrm{Spec}\, R_1 \coprod \mathrm{Spec}\, R_2$ (disjoint union).

Exercise 1.19 Recall that if X is a topological space, a closed subset $Z \subseteq X$ is called **irreducible** if any expression of $Z = Z_1 \cup Z_2$ as the union of two closed subset implies $Z = Z_1$ or $Z = Z_2$.

a) Let Z be an irreducible subset of the topological space X and $U \subseteq X$ an open subset such that $U \cap Z \neq \varnothing$. Show that the closure of $U \cap Z$ is equal to Z.

b) Let R be a ring. Show that a closed subset $Z \subseteq \operatorname{Spec} R$ is irreducible if and only if $Z = \mathcal{Z}(\mathfrak{p})$, for $\mathfrak{p}$ a prime ideal uniquely determined by Z.

Exercise 1.20 Recall that if X is a topological space, a subset $S \subseteq X$ is called **dense** if the closure of S is equal to X. Let $\varphi : R \to A$ be a ring homomorphism and $\varphi^\sharp : \operatorname{Spec} A \to \operatorname{Spec} R$ the induced map. Show that $\operatorname{Im} \varphi^\sharp$ is dense in $\operatorname{Spec} R$ if and only if $\ker \varphi$ is contained in the nilradical $\mathfrak{N}_R$ of R.

Exercise 1.21 Let R be a ring and $\mathbb{A}^1_R = \operatorname{Spec} R[X]$, the affine line over R.

a) Let $A = R[X_1, \ldots, X_n]/(F_1, \ldots, F_m)$. Show that any $a \in A$ defines a continuous function $\operatorname{Spec} A \to \mathbb{A}^1_R$.

b) Show that any element $x \in R$ defines a continuous function $\operatorname{Spec} R \to \mathbb{A}^1_{\mathbb{Z}}$.

Exercise 1.22 Let A be a ring, $J \subset A$ an ideal and $B = A/J$. View J/J^2 as a B-module by $b \cdot x = ax \bmod J^2$, where a is any element in A whose reduction is b (check that this does not depend on the particular choice of a). Let $\pi : J \to J/J^2$ be the projection. Show that for any B-module N, the map

$$\begin{array}{rcl} Hom_B(J/J^2, N) & \longrightarrow & Hom_A(J, N) \\ f & \longmapsto & f \circ \pi \end{array}$$

is an isomorphism of A-modules.

Exercise 1.23 Let $\varphi : R \to A$ be a ring homomorphism, $\mu : A \otimes_R A \to A$ the multiplication map $\mu(a \otimes b) = ab$ and $I = \ker \mu$. View $A \otimes_R A$ as an A-algebra via the left structure: $a \cdot (b \otimes c) = ab \otimes c$. For any A-module N, define a multiplication on the A-module $A \oplus N$ by

$$(a, x) * (b, y) = (ab, ay + bx), \qquad \forall a, b \in A,\ x, y \in N. \tag{1.12}$$

a) Check that (1.12) defines an A-algebra structure on $A \oplus N$, henceforth denoted $A * N$.

b) Check that N, identified with the subset $\{(0, x),\ \forall x \in N\} \subset A * N$, is an ideal. Compute N^2.

c) Let $\delta : A \to N$ be an R-linear derivation. Check that

$$\begin{array}{rcl} \eta : A \otimes_R A & \longrightarrow & A * N \\ a \otimes b & \longmapsto & (ab, a\delta(b)) \end{array}$$

is an A-algebra homomorphism and that $\eta(I) \subseteq N$.

d) Check that η factors through $(A \otimes_R A)/I^2$.

e) Recall the map $d : A \to I/I^2$ given by $d(a) = 1 \otimes a - a \otimes 1$. Show that $(I/I^2, d) \cong (\Omega^1_{A/R}, d)$.

Chapter II

Local properties

§ 1 Localisation

The technique of taking fractions, allowing to construct $\mathbb{Q}$ from $\mathbb{Z}$, can be generalised to arbitrary rings.

Definition 2.1.1 Let R be a ring. A subset $S \subseteq R$ is **multiplicative** if $1 \in S$ and for every $s, t \in S$ we have $st \in S$.

Example 2.1.2 If $f \in R$, $S = \{1, f, f^2, \dots, f^n, \dots\}$ is multiplicative.

Example 2.1.3 If $\mathfrak{p} \subset R$ is a prime ideal, $S = R - \mathfrak{p}$ is multiplicative. A useful special case: R a domain and $\mathfrak{p} = 0$.

If $S \subseteq R$ is multiplicative, define a relation on the set $R \times S$ by declaring $(x, s) \sim (y, t)$ if there exists $u \in S$ such that $u(xt - ys) = 0$. Taking $u = 1$, one sees immediately that this relation is reflexive and symmetric. It is also transitive:

$$\begin{cases} (x,s) \sim (y,t) \\ (y,t) \sim (z,w) \end{cases} \iff \begin{cases} u(xt-ys) = 0 \\ v(yw-zt) = 0 \end{cases} \implies uvt(xw - zs) \iff (x,s) \sim (z,w).$$

We can thus form the quotient set $(R \times S) / \sim$, in which the class of (x, s) is denoted $\frac{x}{s}$.

Definition 2.1.4 Let R be a ring, $S \subseteq R$ a multiplicative set. The ring $S^{-1}R$ is the set $(R \times S) / \sim$ with the operations

$$\frac{x}{s} + \frac{y}{t} = \frac{xt + ys}{st}; \qquad \frac{x}{s} \cdot \frac{y}{t} = \frac{xy}{st}; \qquad 1 = \frac{1}{1}. \tag{2.1}$$

There is a canonical ring homomorphism $\varphi : R \to S^{-1}R$ defined by $\varphi(x) = \frac{x}{1}$.

We leave it as an exercise to check that the operations (2.1) are well defined and satisfy the ring axioms. Notice that $\varphi : R \to S^{-1}R$ is not always injective.

Example 2.1.5 Let $R = \mathbb{Z}/6\mathbb{Z}$ and $S = \{\overline{1}, \overline{3}\}$. By definition, $(x, s) \sim (0, 1)$ if there exists some $u \in S$ such that $ux = 0$. Hence $\ker \varphi = \{\overline{0}, \overline{2}, \overline{4}\}$, whence an exact sequence

$$0 \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/6\mathbb{Z} \xrightarrow{\varphi} S^{-1}(\mathbb{Z}/6\mathbb{Z})$$

and an injection $\overline{\varphi} : \mathbb{Z}/2\mathbb{Z} \hookrightarrow S^{-1}(\mathbb{Z}/6\mathbb{Z})$. The latter is an isomorphism, since $(x, s) \nsim (0, 1)$ is equivalent to $\overline{3}x \neq 0$, which is in turn equivalent to $x \in S$. Computing, we see that $(\overline{3}, \overline{1}) \sim (\overline{1}, \overline{3}) \sim (\overline{1}, \overline{1})$, as $\overline{3}(\overline{3} - \overline{1}) = \overline{0}$. Hence the only elements in $S^{-1}(\mathbb{Z}/6\mathbb{Z})$ are 0 and 1.

Example 2.1.6 If R is a domain and $S = R - \{0\}$ then $S^{-1}R = \operatorname{Frac} R$ is a field, called the **fraction field** of R. The map $\varphi : R \to \operatorname{Frac} R$ is clearly injective. Let us mention two important special cases, for k is a field: the field of **rational functions** $k(X_1, \dots, X_n) = \operatorname{Frac} k[X_1, \dots, X_n]$ and the field of **Laurent power series** $k((X)) = \operatorname{Frac} k[[X]]$.

Example 2.1.7 If $0 \in S$ then $S^{-1}R = 0$. Indeed $0(x - 0) = 0$ so $(x, s) \sim (0, 1)$ for all x and s.

Example 2.1.8 If $f \in R$ and $S = \{1, f, f^2, \dots, f^n, \dots\}$, then $S^{-1}R = \{\frac{x}{f^n},\ \forall x \in R,\ n \in \mathbb{N}\}$ is denoted $R\left[\frac{1}{f}\right]$ or R_f. For instance, since every power series in $k[[X]]$ with non-zero constant term is invertible, $k((X)) = k[[X]]\left[\frac{1}{X}\right]$.

Example 2.1.9 If $\mathfrak{p} \subset R$ is a prime ideal and $S = R - \mathfrak{p}$, then $S^{-1}R = \{\frac{x}{s},\ \forall x \in R,\ s \notin \mathfrak{p}\}$ is denoted $R_{\mathfrak{p}}$ and is called the **localisation** of R at $\mathfrak{p}$. The name will be justified in corollary 2.1.13. For example, if p is a prime number:

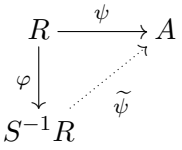
$$\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbb{Q},\ (a, b) = 1,\ p \nmid b\right\}.$$

Proposition 2.1.10 *Let R be a ring, $S \subset R$ a multiplicative subset. Then $J \mapsto \varphi^{-1}(J)$ is an injection from the set of ideals $J \subset S^{-1}R$ to the set of ideals $I \subset R$ such that $I \cap S = \varnothing$. It preserves inclusions and intersections and induces a bijection on the subsets of prime ideals.*

Proof. For any ideal $I \subseteq R$ such that $I \cap S = \varnothing$ consider the ideal $\varphi(I)S^{-1}R \subseteq S^{-1}R$ and notice that the inclusion $\varphi(\varphi^{-1}(J))\, S^{-1}R \subseteq J$ is an equality for any $J \subseteq S^{-1}R$: indeed, any $\frac{x}{s} \in J$ can be written as $\frac{1}{s}\varphi(x)$ and, since $\varphi(x) = \frac{s}{1} \cdot \frac{x}{s} \in J$, we have $x \in \varphi^{-1}(J)$. Hence $J \mapsto \varphi^{-1}(J)$ is injective and one checks immediately that it preserves inclusions and intersections.
If $\mathfrak{p} \subset R$ is a prime ideal such that $\mathfrak{p} \cap S = \varnothing$, it is clear from the definition that $S^{-1}\mathfrak{p}$ is prime. Moreover the inclusion $\mathfrak{p} \subseteq \varphi^{-1}(S^{-1}\mathfrak{p})$ is an equality: if $\varphi(y) \in S^{-1}\mathfrak{p}$, there exist $x \in \mathfrak{p}$ and $s \in S$ such that $(y, 1) \sim (x, s)$, hence $t(x - ys) = 0$ for some $t \in S$. Then $sty = -tx \in \mathfrak{p}$ and, since $st \in S$, we conclude $y \in \mathfrak{p}$. □

Remark 2.1.11 If $f \in R$, recall that $\mathcal{Z}(f) = \{\mathfrak{p} \subset R \mid f \in \mathfrak{p}\}$ is a closed subset of $\operatorname{Spec} R$. Hence, by proposition 2.1.10, $\operatorname{Spec} R_f = \operatorname{Spec} R - \mathcal{Z}(f)$ is an open subset. The map $\varphi : R \to R_f$ plays in Algebraic Geometry the role of the map taking a function defined on a topological space to its restriction to an open subset.

Proposition 2.1.12 (Universal property of rings of fractions) *Let R be a ring, $S \subset R$ a multiplicative subset. Any $\psi : R \to A$ such that $\psi(S) \subseteq A^\times$ factors uniquely through $S^{-1}R$:*



Proof. Put $\widetilde{\psi}\left(\frac{x}{s}\right) = \psi(x)\psi(s)^{-1}$. It is well defined: if $u(xt - ys) = 0$, then $0 = \psi(xut - yus) = \psi(x)\psi(ut) - \psi(y)\psi(us)$, thus

$$\widetilde{\psi}\left(\frac{y}{t}\right) = \psi(y)\psi(t)^{-1} = \psi(yus)\psi(sut)^{-1} = \psi(xut)\psi(sut)^{-1} = \psi(x)\psi(s)^{-1} = \widetilde{\psi}\left(\frac{x}{s}\right).$$

One checks immediately that $\widetilde{\psi}$ is a ring homomorphism. As for uniqueness, let $\vartheta : S^{-1}R \to A$ be another map also making the diagram commute. Then $\vartheta\left(\frac{x}{1}\right) = \vartheta(\varphi(x)) = \psi(x)$, for all $x \in R$, hence $\vartheta\left(\frac{x}{s}\right) = \vartheta(x)\vartheta(s)^{-1} = \psi(x)\psi(s)^{-1} = \widetilde{\psi}\left(\frac{x}{s}\right)$ for all $x \in R$, $s \in S$. □

Corollary 2.1.13 *Let $\mathfrak{p} \subset R$ be a prime ideal and $\varphi : R \to R_\mathfrak{p}$. Then $R_\mathfrak{p}$ is a local ring with maximal ideal $\varphi(\mathfrak{p})R_\mathfrak{p}$ (denoted $\mathfrak{p}R_\mathfrak{p}$ by abuse of notation). The quotient $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ is the fraction field of $R/\mathfrak{p}$.*

Proof. Any ideal $J \subseteq R_\mathfrak{p}$ is of the form $\varphi(I)R_\mathfrak{p}$ for some ideal $I \cap (R - \mathfrak{p}) = \varnothing$, which is equivalent to $I \subseteq \mathfrak{p}$. Hence $R_\mathfrak{p}$ is local. Clearly, $\mathfrak{p}$ is the kernel of the composite map $R \to R_\mathfrak{p} \to R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$, hence $R/\mathfrak{p} \subseteq R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$. By proposition 2.1.12, we get an injection $\operatorname{Frac} R/\mathfrak{p} \subseteq R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$. The inverse map sends the class of $\frac{x}{s}$ mod $\mathfrak{p}R_\mathfrak{p}$ to $\overline{x}\,\overline{s}^{-1}$, where $\overline{x}, \overline{s}$ are the classes mod $\mathfrak{p}$. □

Lemma 2.1.14 *Let $\varphi : R \to A$ be a ring homomorphism, $\mathfrak{p} \subset R$ a prime. The following are equivalent:*

a) There exists a prime $\mathfrak{q} \subset A$ such that $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$;

b) $\varphi^{-1}(\varphi(\mathfrak{p})A) = \mathfrak{p}$.

Proof. Obviously, $\mathfrak{p} \subseteq \varphi^{-1}(\varphi(\mathfrak{p})A)$. If $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$ then $\varphi(\mathfrak{p}) \subseteq \mathfrak{q}$, hence $\varphi(\mathfrak{p})A \subseteq \mathfrak{q}$ and thus $\varphi^{-1}(\varphi(\mathfrak{p})A) \subseteq \varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$.
To prove the converse, consider the multiplicative set $S = \varphi(R - \mathfrak{p}) \subseteq A$. If $\varphi^{-1}(\varphi(\mathfrak{p})A) = \mathfrak{p}$, then $\varphi(\mathfrak{p})A \cap S = \varnothing$. The ideal $\varphi(\mathfrak{p})S^{-1}A$, generated in $S^{-1}A$ by the image of $\mathfrak{p}$, is not the unit ideal: $1 \in \varphi(\mathfrak{p})S^{-1}A$ means that there exists $y \in \varphi(\mathfrak{p})A$ and $t \in S$ such that $ty \in S$, contradicting $\varphi(\mathfrak{p})A \cap S = \varnothing$. Now let $\overline{\mathfrak{q}}$ be any prime ideal in $S^{-1}A/\varphi(\mathfrak{p})S^{-1}A$: it corresponds to a prime ideal $\widetilde{\mathfrak{q}} \subset S^{-1}A$ containing $\varphi(\mathfrak{p})S^{-1}A$. In turn, $\widetilde{\mathfrak{q}}$ corresponds to a prime ideal $\mathfrak{q} \subset A$ such that $\mathfrak{q} \cap S = \varnothing$. Moreover, $\varphi(\mathfrak{p})A \subseteq \mathfrak{q}$: for any $x \in \varphi(\mathfrak{p})A$ we have $\frac{x}{1} = \frac{z}{s}$ for suitable $z \in \mathfrak{q}$ and $s \in S$, hence $usx = uz \in \mathfrak{q}$, for some $u \in S$. Since $us \in S \subseteq A - \mathfrak{q}$ and $\mathfrak{q}$ is prime, we conclude $x \in \mathfrak{q}$. From $\varphi(\mathfrak{p})A \subseteq \mathfrak{q}$ we get $\mathfrak{p} = \varphi^{-1}(\varphi(\mathfrak{p})A) \subseteq \varphi^{-1}(\mathfrak{q})$ and this is an equality because $\mathfrak{q} \cap \varphi(R - \mathfrak{p}) = \varnothing$. □

The construction of fractions works verbatim for modules. Let $S \subseteq R$ be a multiplicative subset in a ring and M an R-module. Define an equivalence relation on the set $M \times S$ by declaring $(m, s) \sim (m', s')$ if there exists $u \in S$ such that $u(s'm - sm') = 0$. We can then form the quotient set $(M \times S) / \sim$, in which the class of (m, s) is denoted $\frac{m}{s}$.

Definition 2.1.15 Let R be a ring, $S \subseteq R$ a multiplicative set and M an R-module. The $S^{-1}R$-module $S^{-1}M$ is the set $(M \times S) / \sim$ with the operations

$$\frac{m}{s} + \frac{m'}{s'} = \frac{s'm + sm'}{ss'}; \qquad \frac{x}{t} \cdot \frac{m}{s} = \frac{xm}{ts}.$$

Example 2.1.16 If $f \in R$ and $S = \{1, f, f^2, \dots, f^n, \dots\}$, then $S^{-1}M = \{\frac{m}{f^n},\ \forall m \in M,\ n \in \mathbb{N}\}$ is denoted M_f.

Example 2.1.17 If $\mathfrak{p} \subset R$ is a prime ideal and $S = R - \mathfrak{p}$, then $S^{-1}M = \{\frac{m}{s},\ \forall m \in R,\ s \notin \mathfrak{p}\}$ is denoted $M_{\mathfrak{p}}$ and is called the **localisation** of M at $\mathfrak{p}$.

If $\alpha : M \to N$ is a morphism of R-modules, one checks immediately that

$$S^{-1}\alpha : S^{-1}M \to S^{-1}N; \qquad S^{-1}\alpha\left(\frac{m}{s}\right) = \frac{\alpha(m)}{s}$$

is a morphism of $S^{-1}R$-modules, denoted $\alpha_{\mathfrak{p}}$ when S is the complement of a prime ideal $\mathfrak{p}$.

Proposition 2.1.18 *For any exact sequence $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ of R-modules, the sequence of $S^{-1}R$-modules $S^{-1}M' \xrightarrow{S^{-1}\alpha} S^{-1}M \xrightarrow{S^{-1}\beta} S^{-1}M''$ is exact*

Proof. It follows immediately from the definitions that $S^{-1}\beta \circ S^{-1}\alpha = S^{-1}(\beta \circ \alpha) = 0$. If $\frac{m}{s} \in S^{-1}M \in \ker(S^{-1}\beta)$, there is some $u \in S$ such that $u\beta(m) = \beta(um) = 0$. Then $um = \alpha(m')$ for some $m' \in M'$ and we get $\frac{m}{s} = \frac{um}{us} = \frac{\alpha(m')}{us} = S^{-1}\alpha\left(\frac{m'}{us}\right) \in \operatorname{Im} S^{-1}(\alpha)$.

In other words, $M \mapsto S^{-1}M$ is an exact functor $\mathbf{Mod}_R \to \mathbf{Mod}_{S^{-1}R}$.

Corollary 2.1.19 *Let $N \subseteq M$ be a submodule. Then $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.*

Proof. Apply S^{-1} to the sequence $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$. □

Proposition 2.1.20 *Let R be a ring, $S \subseteq R$ a multiplicative set and M an R-module. There is a canonical isomorphism $\varphi : S^{-1}R \otimes_R M \cong S^{-1}M$ satisfying $\varphi\left(\frac{x}{s} \otimes m\right) = \frac{xm}{s}$.*

Proof. φ is defined by the universal property of tensor products applied to the R-bilinear map

$$S^{-1}R \times M \longrightarrow S^{-1}M; \qquad \left(\frac{x}{s}, m\right) \longmapsto \frac{xm}{s}.$$

It is therefore unique, and obviously surjective. Every element in $S^{-1}R \otimes_R M$ can be written as $\frac{1}{s} \otimes m$, for some $s \in S$ and $m \in m$. Indeed

$$\sum_i \frac{x_i}{s_i} \otimes m_i = \frac{1}{s} \otimes \left[\sum_i \left(\prod_{j \neq i} s_j\right) x_i m_i\right], \qquad s = \prod_i s_i.$$

Now $\varphi\left(\frac{1}{s} \otimes m\right) = \frac{m}{s} = 0$ means $um = 0$ for some $u \in S$. Then $\frac{1}{s} \otimes m = \frac{1}{us} \otimes um = \frac{1}{us} \otimes 0 = 0$. Therefore $\ker \varphi = 0$. □

Corollary 2.1.21 *The canonical morphism $\varphi : R \to S^{-1}R$ is flat.*

Proof. Combine propositions 2.1.18 and 2.1.20. □

Corollary 2.1.22 *Let R be a ring, $S \subseteq R$ a multiplicative set and M, N two R-modules. There is a canonical isomorphism $S^{-1}M \otimes_{S^{-1}R} S^{-1}N \cong S^{-1}(M \otimes_R N)$.*

Proof. Indeed $S^{-1}M \otimes_{S^{-1}R} S^{-1}N \cong (S^{-1}R \otimes_R M) \otimes_{S^{-1}R} (S^{-1}R \otimes_R N) \cong S^{-1}(M \otimes_R N)$. □

Proposition 2.1.23 *Let R be a ring, $S \subseteq R$ a multiplicative set. Then $\Omega^1_{S^{-1}R/R} = 0$. For any R-algebra A, the natural map $S^{-1}\Omega^1_{A/R} \cong S^{-1}A \otimes_A \Omega^1_{A/R} \to \Omega^1_{S^{-1}A/R}$ is an isomorphism.*

Proof. The first assertion follows from the fact that $\mathrm{Der}_R(S^{-1}R, M) = 0$ for any $S^{-1}R$-module M: indeed for any such derivation δ and any $x \in R$, $s \in S$ we have

$$0 = \delta\left(s\frac{x}{s}\right) = s\,\delta\left(\frac{x}{s}\right) + \frac{x}{s}\delta(s).$$

Since $\delta(s) = 0$ and s is a unit in $S^{-1}R$, we conclude that $\delta\left(\frac{x}{s}\right) = 0$.
Since $\Omega^1_{S^{-1}A/A} = 0$, we get a surjection $v : S^{-1}\Omega^1_{A/R} \cong S^{-1}A \otimes_A \Omega^1_{A/R} \twoheadrightarrow \Omega^1_{S^{-1}A/R}$ from the first fundamental sequence of differentials. To conclude that it is an isomorphism, applying the functor $Hom_{S^{-1}A}(-, N)$ we have to show that for any $S^{-1}A$-module N the map $\mathrm{Der}_R(S^{-1}A, N) \to \mathrm{Der}_R(A, N)$ is surjective. Any R-linear derivation $\partial \in \mathrm{Der}_R(A, N)$ extends:

$$\partial(a) = \partial\left(s\frac{a}{s}\right) = s\,\partial\left(\frac{a}{s}\right) + \frac{a}{s}\,\partial(a) \quad \Longrightarrow \quad \partial\left(\frac{a}{s}\right) = \frac{s\partial(a) - a\partial(s)}{s^2}.$$

□

A property of rings, modules, morphisms,... is called *local* if it can be checked by localisation. The following propositions provide some examples.

Proposition 2.1.24 *Let M be an R-module. The following conditions are equivalent:*

a) $M = 0$;

b) $M_{\mathfrak{p}} = 0$ *for every prime ideal* $\mathfrak{p}$;

c) $M_{\mathfrak{m}} = 0$ *for every maximal ideal* $\mathfrak{m}$.

Proof. The implications a) $\Longrightarrow$ b) $\Longrightarrow$ c) are clear. Suppose $M_{\mathfrak{m}} = 0$ for every maximal ideal $\mathfrak{m}$ in R and suppose $m \in M$ is a non-zero element. Then $1 \notin \mathrm{Ann}(m)$, so $\mathrm{Ann}(m)$ is a proper ideal in R, hence $\mathrm{Ann}(m) \subseteq \mathfrak{m}$ for some maximal ideal of R. Since $\frac{m}{1} = 0$ in $M_{\mathfrak{m}}$, there exists some $s \in R - \mathfrak{m}$ such that $sm = 0$, hence $s \in \mathrm{Ann}(m)$ but $s \notin \mathfrak{m}$ which is a contradiction. □

Proposition 2.1.25 *Let $f : M \to N$ be a homomorphism of R-modules. The following conditions are equivalent:*

a) f *is injective;*

b) $f_{\mathfrak{p}}$ *is injective for every prime ideal* $\mathfrak{p}$;

c) $M_{\mathfrak{m}}$ is injective for every maximal ideal $\mathfrak{m}$.

Proof. The implication a) $\Longrightarrow$ b) follows immediately from proposition 2.1.20 and corollary 2.1.21. b) $\Longrightarrow$ c) is obvious. For c) $\Longrightarrow$ a), tensor the sequence $0 \longrightarrow \ker(f) \longrightarrow M \longrightarrow N$ by $R_{\mathfrak{m}}$ and apply proposition 2.1.20 and exactness of localisation to get that $\ker(f_{\mathfrak{m}}) = \ker(f)_{\mathfrak{m}}$ for all $\mathfrak{m}$. Conclude by proposition 2.1.24. □

Proposition 2.1.26 *Let M be an R-module. The following conditions are equivalent:*

a) M is flat;

b) $M_{\mathfrak{p}}$ is flat for every prime ideal $\mathfrak{p}$;

c) $M_{\mathfrak{m}}$ is flat for every maximal ideal $\mathfrak{m}$.

Proof. Let $N' \hookrightarrow N$ be an injection of $R_{\mathfrak{p}}$-modules. Since $M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} [N' \to N] \cong M \otimes_R [N' \to N]$ and the second map is injective when M is flat, we conclude that $M_{\mathfrak{p}}$ is flat if M is, so a) $\Longrightarrow$ b). b) $\Longrightarrow$ c) is obvious. For c) $\Longrightarrow$ a), let $N' \hookrightarrow N$ be an injection of R-modules: proposition 2.1.25 implies that if $R_{\mathfrak{m}} \otimes_R [M \otimes_R N' \hookrightarrow M \otimes_R N] = M_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} N'_{\mathfrak{m}} \hookrightarrow M_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} N_{\mathfrak{m}}$ is injective for all $\mathfrak{m}$ then $M \otimes_R N' \hookrightarrow M \otimes_R N$ is injective. □

§ 2 Faithfully flat modules and descent

Definition 2.2.1 Let R be a ring. An R-module M is **faithfully flat** if for every sequence

$$N' \xrightarrow{f} N \xrightarrow{g} N'' \tag{2.2}$$

of R-modules, (2.2) is exact if and only if

$$M \otimes N' \xrightarrow{id_M \otimes f} M \otimes N \xrightarrow{id_M \otimes g} M \otimes N''$$

is exact. If $\varphi : R \to A$ is a ring homomorphism, we say that A (or φ) is faithfully flat if A is a faithfully flat R-module.

Proposition 2.2.2 *Let $\varphi : R \to A$ be a flat ring homomorphism. The following are equivalent:*

a) A is faithfully flat;

b) $A \otimes_R M \neq 0$ for every nonzero R-module M;

c) $\varphi^\sharp : \operatorname{Spec} A \to \operatorname{Spec} R$ is surjective.

Proof. a) $\Longrightarrow$ b). If A is faithfully flat and M is an R-module such that $A \otimes_R M = 0$ then the sequence $A \otimes_R M \xrightarrow{0} A \otimes_R M \longrightarrow 0$ is exact, which implies that the sequence $M \xrightarrow{0} M \longrightarrow 0$ is exact, which is equivalent to $M = 0$.

b) $\Longrightarrow$ a). Tensor sequence (2.2) by A and suppose we get an exact sequence. First we remark that $\operatorname{im}\,(id_A \otimes (g \circ f)) = A \otimes \operatorname{im}\,(g \circ f) = 0$, therefore $\operatorname{im}\,(id_A \otimes f) \subseteq \ker(id_A \otimes g)$. Furthermore $0 = \ker(id_A \otimes g)/\operatorname{im}\,(id_A \otimes f) = A \otimes (\ker(g)/\operatorname{im}\,(f))$, and we can apply assumption b) to conclude that (2.2) is exact.

b) $\Longrightarrow$ c). In view of the correspondence established in proposition 2.1.10, in order to show that a prime $\mathfrak{p} \subset R$ is in the image of $\varphi^\sharp$, we may replace R by $R_\mathfrak{p}$ and A by $A_\mathfrak{p}$. We thus assume that R is local and $\mathfrak{p}$ is maximal. Tensoring $0 \longrightarrow \mathfrak{p} \longrightarrow R \longrightarrow R/\mathfrak{p} \longrightarrow 0$ by the flat R-algebra A, we get $0 \longrightarrow \varphi(\mathfrak{p})A \longrightarrow A \longrightarrow A \otimes R/\mathfrak{p} \longrightarrow 0$. Thus $A/\varphi(\mathfrak{p}) = A \otimes R/\mathfrak{p} \neq 0$, hence $\varphi(\mathfrak{p})$ is a proper ideal and as such it is contained in some maximal ideal $\mathfrak{m} \subset A$. Thus $\varphi^{-1}(\mathfrak{m}) \supseteq \varphi^{-1}(\varphi(\mathfrak{p})) \supseteq \mathfrak{p}$. Since $\mathfrak{p}$ is maximal, we conclude $\varphi^\sharp(\mathfrak{m}) = \varphi^{-1}(\mathfrak{m}) = \mathfrak{p}$.

c) $\Longrightarrow$ b) First notice that for every prime ideal $\mathfrak{p} \subset R$, the ideal $\varphi(\mathfrak{p})A$ is proper, because $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$ for some prime $\mathfrak{q} \subset A$, hence $\varphi(\mathfrak{p})A \subseteq \mathfrak{q}$. Let now M be an R-module, $0 \neq m \in M$ and set $N = Rm$. It suffices to show that $A \otimes N \neq 0$, because $A \otimes N$ injects into $A \otimes M$ by flatness of A. Hence $N = R/\operatorname{Ann}\,(m)$. If $\operatorname{Ann}\,(m) \neq R$, it is contained in some prime ideal $\mathfrak{p} \subset R$, hence $\varphi(\operatorname{Ann}\,(m))A \subseteq \varphi(\mathfrak{p})A \neq A$ and therefore $A \otimes N \cong A/\varphi(\operatorname{Ann}\,(m))A$ is not 0. $\square$

Example 2.2.3 Let $f_1, \ldots, f_s \in R$ such that $(f_1, \ldots, f_s) = R$. The R-algebra $A = \prod_{i=1}^s R_{f_i}$ is faithfully flat. Indeed, it is flat because the R_{f_i} are flat by corollary 2.1.21 and finite products commute with tensor products by proposition 1.2.65. Moreover, the induced map

$$\operatorname{Spec} A = \coprod_{i=1}^{s} \operatorname{Spec} R_{f_i} \longrightarrow \operatorname{Spec} R$$

(see exercise 1.18) is surjective because for every prime $\mathfrak{p} \subset R$, at least one of the $f_i \notin \mathfrak{p}$ (otherwise $R = (f_1, \ldots, f_r) \subseteq \mathfrak{p}$), hence $\mathfrak{p}$ corresponds to a prime ideal of R_{f_i} in the bijection of proposition 2.1.10.

Example 2.2.4 $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is flat but not faithfully flat. $\operatorname{Spec}\mathbb{Q}$ only has one point, so can't possibly surject onto $\operatorname{Spec}\mathbb{Z}$. Moreover, for any $n > 1$ we have $\mathbb{Z}/n\mathbb{Z} \neq 0$ while $\mathbb{Q} \otimes \mathbb{Z}/n\mathbb{Z} = 0$.

Example 2.2.5 The map $\varphi : \mathbb{C}[X] \to \mathbb{C}[Y]$ defined by $\varphi(X) = Y^2$ is faithfully flat. As a $\mathbb{C}[X]$-module, $\mathbb{C}[Y] = \mathbb{C}[X] \oplus Y\mathbb{C}[X]$ is free, hence φ is flat. Clearly $\varphi^{-1}(0) = 0$, and for any $\alpha \in \mathbb{C}$ the inclusion $(X - \alpha) \subseteq \varphi^{-1}(Y - \sqrt{\alpha})$ is an equality, since $(X - \alpha)$ is maximal and $1 \notin \varphi^{-1}(Y - \sqrt{\alpha})$.

Remark 2.2.6 A flat morphism $\varphi : R \to A$ is not necessarily injective, as $\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}\left[\frac{1}{3}\right] \cong \mathbb{Z}/2\mathbb{Z}$ shows. On the other hand a faithfully flat morphism is injective: $xR \otimes A \cong \varphi(x)A \neq 0$ for all $x \neq 0$.

Definition 2.2.7 Let R and A be local rings with maximal ideals $\mathfrak{m}_R$ and $\mathfrak{m}_A$. A ring homomorphism $\varphi : R \to A$ is a **local homomorphism** if $\varphi^{-1}(\mathfrak{m}_A) = \mathfrak{m}_R$.

Lemma 2.2.8 *A flat local homomorphism is faithfully flat.*

Proof. In order to show that $A \otimes_R M \neq 0$ for any R-module $M \neq 0$, it suffices to prove it for the modules of the form $M = Rm \cong R/\mathrm{Ann}\,(m)$. Since $m \neq 0$, $\mathrm{Ann}\,(m) \neq R$ so $\mathrm{Ann}\,(m) \subseteq \mathfrak{m}_R$. Then $\mathrm{Ann}\,(m)A \subseteq \mathfrak{m}_R A \subseteq \mathfrak{m}_A \neq A$, hence $A \otimes_R M \cong A \otimes_R R/\mathrm{Ann}\,(m) \cong A/\mathrm{Ann}\,(m)A \neq 0$. □

.

Proposition 2.2.9 *Let R be a ring, M'' a finitely presented R-module. An exact sequence of R-modules*

$$0 \longrightarrow M' \longrightarrow M \xrightarrow{\pi} M'' \longrightarrow 0 \tag{2.3}$$

splits if and only if there exists a faithfully flat R-algebra A such that the sequence

$$0 \longrightarrow A \otimes M' \longrightarrow A \otimes M \xrightarrow{id_A \otimes \pi} A \otimes M'' \longrightarrow 0$$

of A-modules splits.

Proof. By proposition 1.2.53, the sequence (2.3) splits if and only if the induced homomorphism $\pi_* : Hom_R(M'', M) \to Hom_R(M'', M'')$ is surjective. Since M'' is finitely presented, by proposition 1.2.84 we have $A \otimes Hom_R(M'', N) \simeq Hom_A(A \otimes M'', A \otimes N)$ for any R-module N. Again by faithful flatness of A we get that π_* is surjective if and only if $(id_A \otimes \pi)_*$ is surjective. □

Proposition 2.2.9 is a first instance of a property of modules over a ring that can be recovered after replacing the ring by a faithfully flat extension. This is similar to a local property, that can be tested by replacing the ring by its localisations. This analogy has led Grothendieck to introduce the flat topologies (fppf and fpqc) to compensate for the coarseness of the Zariski topology.

In Topology, one often defines a function $f : X \to Y$ by covering X by open subsets and defining functions $f_i : X_i \to Y$. The collection $\{f_i\}$ defines a function f if f_i and f_j agree on the intersection $X_i \cap X_j$, for all i, j. In a similar fashion, one can construct a space X by glueing a collection of spaces X_i, which will become open subsets covering X. The glueing is achieved by selecting in each X_i an open subset U_{ij} for each $j \neq i$ and an isomorphism $\phi_{ij} : U_{ij} \to U_{ji}$: in this way, U_{ij} will become the intersection of X_i with X_j inside X. For this construction to work, one has to require compatibilities between the maps $\phi_{i,j}$.

In Algebraic Geometry, this reconstruction process goes under the name of *descent theory*. Faithfully flat descent for modules over rings can be presented in purely algebraic terms. The starting point is the construction of the following exact sequence.

Proposition 2.2.10 *Let $\varphi : R \to A$ be a faithfully flat morphism and M an R-module. The sequence*

$$0 \longrightarrow M \xrightarrow{\delta_0} M \otimes A \xrightarrow{\delta_1} M \otimes A \otimes A \xrightarrow{\delta_2} M \otimes A \otimes A \otimes A. \tag{2.4}$$

is exact. Here

$$\delta_0(m) = m \otimes 1; \qquad \delta_1(m \otimes a) = m \otimes 1 \otimes a - m \otimes a \otimes 1;$$

$$\delta_2(m \otimes a \otimes b) = m \otimes 1 \otimes a \otimes b - m \otimes a \otimes 1 \otimes b + m \otimes a \otimes b \otimes 1.$$

Proof. It is clear from the definitions (and does not require flatness of A) that (2.4) is a *complex* (called Amitsur's complex for M), i.e. the composition of two consecutive maps is zero. Let $0 \neq m \in M$. By proposition 2.2.2, $Rm \otimes A \neq 0$, hence δ_0 is injective.

Suppose that φ has a section, i.e. a morphism $\psi : A \to R$ such that $\psi \circ \varphi = id_R$. Define

$$\begin{array}{rcl} h_0 : M \otimes A & \longrightarrow & M \\ m \otimes a & \longmapsto & \psi(a)m \end{array} ; \qquad \begin{array}{rcl} h_1 : M \otimes A \otimes A & \longrightarrow & M \otimes A \\ m \otimes a \otimes b & \longmapsto & \psi(a)m \otimes b \end{array} ;$$

$$\begin{array}{rcl} h_2 : M \otimes A \otimes A \otimes A & \longrightarrow & M \otimes A \otimes A. \\ m \otimes a \otimes b \otimes c & \longmapsto & \psi(a)m \otimes b \otimes c \end{array}$$

These maps are *homotopies* for the complex (2.4) i.e. satisfy

$$h_1 \circ \delta_1 + \delta_0 \circ h_0 = id_{M \otimes A}; \qquad h_2 \circ \delta_2 + \delta_1 \circ h_1 = id_{M \otimes A \otimes A}.$$

Let us check the first identity, leaving the second as a (tedious) exercise:

$$\begin{array}{rl} (h_1 \circ \delta_1 + \delta_0 \circ h_0)(m \otimes a) & = h_1(m \otimes 1 \otimes a - m \otimes a \otimes 1) + \delta_0(\psi(a)m) \\ & = (m \otimes a - \psi(a) \otimes 1 \otimes 1) + \psi(a)m \otimes 1 \\ & = m \otimes a. \end{array}$$

It follows then from lemma 2.2.11 below that the sequence (2.4) is exact if φ has a section. To prove exactness in general, we may tensor (2.4) by any faithfully flat R-algebra. Tensoring then by A we have an obvious section of $\varphi \otimes id_A : A \to A \otimes_R A$, given by $a \otimes b \mapsto ab$. □

Lemma 2.2.11 *Let $N' \xrightarrow{f} N \xrightarrow{g} N''$ be a sequence of R-modules. Suppose there exist R-linear maps $\sigma : N \to N'$ and $\tau : N'' \to N$ such that $\tau \circ g + f \circ \sigma = id_N$. Then the sequence is exact.*

Proof. For any $x \in \ker g$ we have $x = \tau(g(x)) + f(\sigma(x)) = f(\sigma(x)) \in \operatorname{im} f$. □

Let $\varphi : R \to A$ be a faithfully flat morphism. There are two natural A-algebra structures $\varphi_i : A \to A \otimes_R A$, given by $\varphi_1(a) = a \otimes 1$ and $\varphi_2(a) = 1 \otimes a$. Therefore for any A-module N we get two A-module structures on $N \otimes_R A \otimes_R A$. In order to avoid confusion, we write $\otimes_i$ for the tensor product over A with $A \otimes_R A$ via φ_i. Hence

$$N \otimes_1 (A \otimes_R A) \quad \text{with} \quad (a_1 \otimes a_2)(x \otimes_1 b_1 \otimes b_2) = (x \otimes_1 a_1 b_1 \otimes a_2 b_2) = (a_1 b_1 x \otimes_1 1 \otimes a_2 b_2)$$

$$N \otimes_2 (A \otimes_R A) \quad \text{with} \quad (a_1 \otimes a_2)(x \otimes_1 b_1 \otimes b_2) = (x \otimes_2 a_1 b_1 \otimes a_2 b_2) = (a_2 b_2 x \otimes_2 a_1 b_1 \otimes 1).$$

As R-modules, both are isomorphic to $N \otimes_R A$, but $x \otimes_1 a \otimes b = ax \otimes b$ while $x \otimes_2 a \otimes b = bx \otimes a$. If $N = M \otimes_R A$ for some R-module M, we have an $A \otimes_R A$-linear isomomorphism ϕ:

$$\begin{array}{rcl} \phi : (M \otimes_R A) \otimes_1 (A \otimes_R A) & \longrightarrow & (M \otimes_R A) \otimes_2 (A \otimes_R A). \\ (m \otimes a) \otimes_1 (b_1 \otimes b_2) & \longmapsto & (m \otimes a) \otimes_2 (b_2 \otimes b_1) \end{array}$$

The R-module M can be recovered from the pair (N, ϕ): indeed it follows from the exactness of sequence (2.4) that $M = \operatorname{im}(\delta_0) = \ker(\delta_1)$, i.e.

$$M = \{x \in N \mid x \otimes_2 1 \otimes 1 = \phi(x \otimes_1 1 \otimes 1) \text{ in } N \otimes_2 A \otimes_R A\}. \tag{2.5}$$

Next, there are three natural $A \otimes_R A$-algebra structures $\varphi_{i,j} : A \otimes_R A \to A \otimes_R A \otimes_R A$, given by

$$\varphi_{3,2}(a \otimes b) = 1 \otimes a \otimes b; \qquad \varphi_{3,1}(a \otimes b) = a \otimes 1 \otimes b; \qquad \varphi_{2,1}(a \otimes b) = a \otimes b \otimes 1.$$

If (N,ϕ) is an A-module with an $A\otimes_R A$-linear isomorphism $\phi : N\otimes_1(A\otimes_R A)\simeq N\otimes_2(A\otimes_R A)$, define $N\otimes_{h,i,j}(A\otimes A\otimes A) = N\otimes_h(A\otimes A)\otimes_{\varphi_{i,j}}(A\otimes A\otimes A)$. From ϕ we obtain $A\otimes A\otimes A$-linear isomorphisms:

$$\phi_{i,j} = \phi\otimes_{i,j} id_{A\otimes A\otimes A} : N\otimes_{1,i,j}(A\otimes A\otimes A)\xrightarrow{\sim} N\otimes_{2,i,j}(A\otimes A\otimes A).$$

Once again, if $N = M\otimes A$ for some R-module M, the the exactness of sequence (2.4), specifically the equation $\mathrm{im}\,(\delta_1) = \ker(\delta_2)$, translates into a relation

$$\phi_{3,1} = \phi_{3,2}\circ\phi_{2,1} \tag{2.6}$$

the verification of which is an excruciating exercise left to the reader.

Definition 2.2.12 Let $\varphi : R\to A$ be a morphism and N an A-module. A **descent datum** on N is the datum of an isomorphism $\phi : A\otimes_R A$-linear isomorphism $\phi : N\otimes_1(A\otimes_R A)\simeq N\otimes_2(A\otimes_R A)$ such that the induced isomorphisms $\phi_{i,j} = \phi\otimes_{i,j} id_{A\otimes A\otimes A}$ satisfy the **cocycle condition** (2.6). A morphism $f : (N,\phi)\to(N',\phi')$ is an A-linear map $f : N\to N'$ making the following diagram commute:

$$\begin{array}{ccc} N\otimes_1(A\otimes_R A) & \xrightarrow{\phi} & N\otimes_2(A\otimes_R A) \\ {\scriptstyle f\otimes_1 id_{A\otimes A}}\downarrow & & \downarrow{\scriptstyle f\otimes_2 id_{A\otimes A}} \\ N'\otimes_1(A\otimes_R A) & \xrightarrow{\phi'} & N'\otimes_2(A\otimes_R A). \end{array} \tag{2.7}$$

The discussion above shows that if $\varphi : R\to A$ is a faithfully flat morphism, any R-module M defines a A-module with descent datum. The following results shows that descent data are precisely the requirements for an A-module to descend to R.

Theorem 2.2.13 *Let $\varphi : R\to A$ be a faithfully flat morphism. The functor $M\mapsto(M\otimes_R A,\phi)$ is an equivalence of categories between $\mathbf{Mod}_R$ and the category of A-modules with descent data.*

Proof. The functor is faithful: for any R-linear map $g : M\to M'$, tensoring by A the exact sequence $0\longrightarrow\ker(g)\longrightarrow M\longrightarrow M'$ we get $0\longrightarrow\ker(g\otimes id_A)\longrightarrow M\otimes_R A\longrightarrow M'\otimes_R A$. Hence, if $g\otimes id_A = 0$, we have that $\ker(g\otimes id_A)\to M\otimes_R A$ is an isomorphism, which implies that $\ker(g)\to M$ is an isomorphism.

It is also fully faithful: let M, M' be R-modules and $f : (M\otimes_R A,\phi)\to(M'\otimes_R A,\phi')$ a morphism. For any $m\in M$, from diagram (2.7) we deduce that

$$\begin{aligned}\phi'(f(m\otimes 1)\otimes_1 1\otimes 1) &= (f\otimes_2 id_{A\otimes A})(\phi(m\otimes 1\otimes_1 1\otimes 1)) \\ &= (f\otimes_2 id_{A\otimes A})(m\otimes 1\otimes_2 1\otimes 1) \\ &= f(m\otimes 1)\otimes_2 1\otimes 1.\end{aligned}$$

Hence, from formula (2.5) we get that $f(m\otimes 1)\in M'$. We therefore get an R-linear map $g : M\to M'$ defined by $g(m) = f(m\otimes 1)$, and clearly $f = g\otimes id_A$.

A functor in the opposite direction is defined by associating to any A-module with descent datum (N,ϕ) the R-module $M = \{x\in N\mid x\otimes_2 1\otimes 1 = \phi(x\otimes_1 1\otimes 1)\text{ in }N\otimes_2 A\otimes_R A\}$. To check that this is an inverse functor we use the A-linear map

$$\begin{aligned}\vartheta : M\otimes_R A &\longrightarrow N. \\ x\otimes a &\longmapsto ax\end{aligned}$$

To prove that ϑ is an isomorphism, consider the following diagrams

$$\begin{array}{ccccc} M \otimes_R A & \xrightarrow{\gamma} & N \otimes_1 A \otimes A & \underset{\beta\otimes id_A}{\overset{\alpha\otimes id_A}{\rightrightarrows}} & N \otimes_{1,3,2} (A \otimes A \otimes A) \\ \downarrow{\scriptstyle \vartheta} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi_{3,2}} \\ N & \xrightarrow{\delta_{0,N}} & N \otimes_2 A \otimes A & \underset{id_N\otimes\varphi_{3,1}}{\overset{id_N\otimes\varphi_{3,2}}{\rightrightarrows}} & N \otimes_{2,3,2} (A \otimes A \otimes A) \end{array}$$

where $\alpha(x \otimes 1 \otimes a) = x \otimes 1 \otimes 1 \otimes a$, $\beta(x \otimes 1 \otimes 1) = \phi(x \otimes 1 \otimes 1) \otimes a$ and $\gamma(x) = x \otimes 1$. We write $\delta_{i,N}$ for the maps in the exact sequence (2.4) relative to the module N and ring morphism $\varphi_2 : A \to A \otimes A$. The diagram using the top arrows commutes by definition, the one using the bottom arrows commutes because of the cocycle condition. By definition, we have that $M \otimes_R A = \ker[\alpha \otimes id_A - \beta \otimes id_A]$. Moreover $\delta_{1,N} = id_N \otimes \varphi_{3,2} - id_N \otimes \varphi_{3,1}$, so it follows from propostition 2.2.10 that N is the kernel of the double arrow at the bottom. Since the vertical arrows ϕ and $\phi_{3,2}$ are isomorphism, we get that ϑ is an isomorphism too. □

§ 3 Flatness and projective modules

Definition 2.3.1 An R-module M is **locally free** if for every prime ideal $\mathfrak{p} \subset R$ the $R_\mathfrak{p}$-module $M_\mathfrak{p}$ is free.

Theorem 2.3.2 *Let M be a finitely generated R-module. Consider the following conditions:*

a) M is free;

b) M is projective;

c) M is flat;

d) M is locally free.

Then a) $\Longrightarrow$ b) $\Longrightarrow$ c) $\Longrightarrow$ d). Moreover, if M is finitely presented, locally free and if $\mathfrak{p} \mapsto \operatorname{rk}_{R_\mathfrak{p}} M_\mathfrak{p}$ is a constant function on $\operatorname{Spec} R$, then M is projective.

Proof. a) $\Longrightarrow$ b) is obvious. For b) $\Longrightarrow$ c), choose $\pi : R^n \twoheadrightarrow M$ and a splitting $\sigma : M \hookrightarrow R^n$ of π. For any R-module N, the composite map $M \otimes N \to R^n \otimes N \to M \otimes N$ is the identity, hence $\sigma \otimes id_N$ is injective. For any injection $f : N' \hookrightarrow N$ of R-modules, the diagram

$$\begin{array}{ccc} M \otimes N' & \xrightarrow{id_M\otimes f} & M \otimes N \\ \downarrow{\scriptstyle \sigma\otimes id_{N'}} & & \downarrow{\scriptstyle \sigma\otimes id_N} \\ R^n \otimes N' & \xrightarrow{id_{R^n}\otimes f} & R^n \otimes N \end{array}$$

shows that $id_M \otimes f : M \otimes N' \to M \otimes N$ is injective, hence M is flat by proposition 1.2.83.

For c) $\Longrightarrow$ d), replacing R by its localisations, we may assume that R is local with maximal ideal $\mathfrak{m}$. Let $m_1, \dots, m_r \in M$ lift a basis of $M \otimes R/\mathfrak{m}$. They generate M, by Nakayama's lemma, and we shall prove by induction on $s \leq r$ that $m_1, \dots, m_s$ are linearly independent over R. For $s = 1$, let $m \in M$ whose reduction mod $\mathfrak{m}M$ is non-zero. Let $\alpha \in R$ such that $\alpha m = 0$. Since M is flat, tensoring the exact sequence $0 \longrightarrow \operatorname{Ann}(\alpha) \longrightarrow R \longrightarrow R$ by M we get an exact sequence

$$0 \longrightarrow \operatorname{Ann}(\alpha)M \longrightarrow M \xrightarrow{\mu_\alpha} M$$

where μ_α is the multiplication by α. Hence, there exist $\beta_1, \dots, \beta_r \in \operatorname{Ann}(\alpha)$ such that $m = \sum \beta_j m_j$. Since $m \notin \mathfrak{m}M$, at least one of the $\beta_j \notin \mathfrak{m}$. This means that $\operatorname{Ann}(\alpha)$ contains a unit, and thus $\operatorname{Ann}(\alpha) = R$, hence $\alpha = 0$.

Let now $\sum_{i=1}^s \alpha_i m_i = 0$ be a linear dependence relation over R. Extend it to $\sum_{i=1}^r \alpha_i m_i = 0$ by $\alpha_{s+1} = \cdots = \alpha_r = 0$. By lemma 2.3.3 below, there exist elements $\beta_{i,j} \in R$ such that $m_i = \sum_{j=1}^r \beta_{i,j} m_j$ and $\sum_{i=1}^r \alpha_i \beta_{i,j} = 0$ for all $j = 1, \dots, r$. Since $m_s \notin \mathfrak{m}M$, one of the $\beta_{s,j}$ is a unit. Fix such an index j and write

$$\alpha_s = -\sum_{i=1}^{s-1} \frac{\beta_{i,j}}{\beta_{s,j}} \alpha_i \qquad \Longrightarrow \qquad 0 = \sum_{i=1}^{s} \alpha_i m_i = \sum_{i=1}^{s-1} \alpha_i \left(m_i - \frac{\beta_{i,j}}{\beta_{s,j}} m_s \right).$$

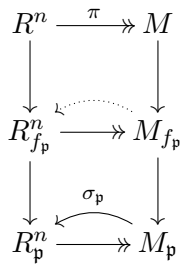
Put $m_i' = m_i - \frac{\beta_{i,j}}{\beta_{s,j}} m_s$. The elements $m_1', \dots, m_{s-1}', m_s, \dots, m_r$ lift a basis of $M \otimes R/\mathfrak{m}$ and $\sum_{i=1}^{s-1} \alpha_i m_i' = 0$. By induction we deduce $\alpha_1 = \cdots = \alpha_{s-1} = 0$ and also $\alpha_s = -\sum_{i=1}^{s-1} \frac{\beta_{i,j}}{\beta_{s,j}} \alpha_i = 0$.

Assume now that M is locally free, that $r = \operatorname{rk}_{R_\mathfrak{p}} M_\mathfrak{p}$ is independent of $\mathfrak{p}$ and that there exists a finite presentation

$$0 \longrightarrow N \longrightarrow R^n \xrightarrow{\pi} M \longrightarrow 0. \tag{2.8}$$

To show that M is projective, it suffices to show that this sequence splits. By proposition 2.2.9 this can be tested after tensoring by some faithfully flat R-algebra A. We are going to show that this can be achieved over an algebra of the kind $A = \prod_i R_{f_i}$ considered in in example 2.2.3

Let $m_i = \pi(\mathbf{e}_i)$ be the generators for M given by sequence (2.8). For every prime $\mathfrak{p} \subset R$, select a splitting $\sigma_\mathfrak{p} : M_\mathfrak{p} \simeq R_\mathfrak{p}^r \to R_\mathfrak{p}^n$ of the sequence (2.8) tensored by $R_\mathfrak{p}$. This map is determined by the values $\sigma_\mathfrak{p}(1 \otimes m_i) = \sum_{j=1}^n \alpha_{i,j} \mathbf{e}_j$, where $\alpha_{i,j} \in R_\mathfrak{p}$. Since there are only finitely many coefficients, we can find an element $f_\mathfrak{p} \in R - \mathfrak{p}$ such that $\alpha_{i,j} = \frac{a_{i,j}}{f_\mathfrak{p}}$, with $a_{i,j} \in R$, for all $i, j \in \{1, \dots, n\}$. In other words, $\sigma_\mathfrak{p}$ extends to a splitting of sequence (2.8) tensored by $R_{f_\mathfrak{p}}$:



Let $I = (f_\mathfrak{p})_\mathfrak{p} \subseteq R$ be the ideal generated by all these elements. By construction, for every prime $\mathfrak{p}$ the ideal $I_\mathfrak{p}$ contains an element outside $\mathfrak{p}$, hence $I_\mathfrak{p} = R_\mathfrak{p}$ and therefore $I = R$. Writing $1 = b_1 f_{\mathfrak{p}_1} + \cdots + b_s f_{\mathfrak{p}_s}$ for suitable $b_i \in R$, we see that $(f_{\mathfrak{p}_1}, \dots, f_{\mathfrak{p}_s}) = R$. By construction sequence (2.8) splits when tensored by $A = \prod_{i=1}^s R_{f_{\mathfrak{p}_i}}$, which is faithfully flat as seen in example 2.2.3. $\square$

Lemma 2.3.3 *Let M be an R-module generated by elements $m_1, \dots, m_r$. The following are equivalent:*

a) M is flat;

b) For any linear relation $\sum_{i=1}^r \alpha_i m_i = 0$ there exist elements $\beta_{i,j} \in R$ such that $m_i = \sum_{j=1}^r \beta_{i,j} m_j$ and $\sum_{i=1}^r \alpha_i \beta_{i,j} = 0$ for all $j = 1, \dots, r$.

Proof. Suppose that M is flat and consider the exact sequence

$$0 \longrightarrow N \longrightarrow R^r \xrightarrow{\lambda} R$$

where $\lambda(x_1, \dots, x_r) = \sum_{i=1}^r \alpha_i x_i$ and $N = \ker \lambda$. Tensoring by M we get the exact sequence

$$0 \longrightarrow N \otimes M \xrightarrow{\varepsilon} M^r \xrightarrow{\lambda_M} M$$

where $\lambda_M(y_1, \dots, y_r) = \sum_{i=1}^r \alpha_i y_i$ and $\varepsilon\left((z_1, \dots, z_r) \otimes m\right) = (z_1 m, \dots, z_r m)$. Hence the vector $(m_1, \dots, m_r) \in \ker \lambda_M$ can be written as $(m_1, \dots, m_r) = \varepsilon\left(\sum_{j=1}^r \mathbf{b}_j \otimes m_j\right)$ for suitable $\mathbf{b}_j \in N$. Writing $\mathbf{b}_j = (\beta_{1,j}, \dots, \beta_{r,j})$ we get $\sum_{i=1}^r \alpha_i \beta_{i,j} = 0$ because $\mathbf{b}_j \in \ker \lambda$ and

$$(m_1, \dots, m_r) = \varepsilon\left(\sum_{j=1}^r (\beta_{1,j}, \dots, \beta_{r,j}) \otimes m_j\right) = \left(\sum_{j=1}^r \beta_{1,j} m_j, \dots, \sum_{j=1}^r \beta_{r,j} m_j\right).$$

Conversely, suppose M satisfies condition b) and let $I \subset R$ be an ideal. We want to show that $\mu : I \otimes M \to IM$ is injective. Let $\sum_{i=1}^r \alpha_i \otimes m_i \in \ker \mu$ i.e. $\sum_{i=1}^r \alpha_i m_i = 0$ and write $m_i = \sum_{j=1}^r \beta_{i,j} m_j$. Then in $I \otimes M$ we have

$$\sum_{i=1}^r \alpha_i \otimes m_i = \sum_{i=1}^r \alpha_i \otimes \sum_{j=1}^r \beta_{i,j} m_j = \sum_{j=1}^r \left[\sum_{i=1}^r \alpha_i \beta_{i,j}\right] \otimes m_j = \sum_{j=1}^r 0 \otimes m_j = 0.$$

□

Let R be a ring. For any prime ideal $\mathfrak{p} \subset R$ write $\kappa(\mathfrak{p}) = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$. Recall that $\kappa(\mathfrak{p})$ is the fraction field of $R/\mathfrak{p}$ (corollary2.1.13). If M is a free module of finite rank r, clearly the function $\mathfrak{p} \mapsto \dim_{\kappa(\mathfrak{p})} M \otimes \kappa(\mathfrak{p}) = r$ is constant on $\operatorname{Spec} R$. Conversely:

Proposition 2.3.4 *Let R be a domain, M a finitely generated R-module. If $\mathfrak{p} \mapsto \dim_{\kappa(\mathfrak{p})} M \otimes \kappa(\mathfrak{p})$ is a constant function on $\operatorname{Spec} R$, then M is locally free.*

Proof. Without loss of generality, we may assume that R is local with maximal ideal $\mathfrak{m}$. Let $m_1, \dots, m_r \in M$ lift a basis of $M \otimes \kappa(\mathfrak{m}) = M \otimes R/\mathfrak{m} \cong M/\mathfrak{m}M$ and let $\varphi : R^r \twoheadrightarrow M$ defined by $\varphi(\mathbf{e}_i) = m_i$. By assumption, $\dim_{\kappa(\mathfrak{p})} M \otimes \kappa(\mathfrak{p}) = \dim_{\kappa(\mathfrak{m})} M \otimes \kappa(\mathfrak{m}) = r$ for every prime $\mathfrak{p} \subset R$, hence $\ker \varphi \subseteq \mathfrak{p}R^r$ for all $\mathfrak{p}$. Therefore $\ker \varphi \subseteq \bigcap_\mathfrak{p} \mathfrak{p}R^r = \mathfrak{N}_R R^r = 0$, so φ is an isomorphism. □

Example 2.3.5 A submodule of a locally free module is not necessarily locally free. Let $R = k[t]/t^2$ and $M = tR$. Then M is an ideal of R, hence a submodule of a free module of rank 1. Tensoring the sequence $0 \to tR \to R \to R/tR \to 0$ by tR we obtain

$$0 \longrightarrow tR \otimes_R tR \xrightarrow{\mu} tR \longrightarrow 0 \longrightarrow 0$$

where $\mu(at \otimes bt) = abt^2 = 0$, so μ is the zero map. Since $tR \neq 0$, this sequence is not exact.

§ 4 Exercises

Exercise 2.1 Let R be a ring, $S \subseteq R$ a multiplicative set, $M, N \in \mathbf{Mod}_R$. Check that the rule

$$\begin{array}{rl} Hom_R(M,N) \times S & \longrightarrow Hom_{S^{-1}R}(S^{-1}M, S^{-1}N) \\ (f,s) & \longmapsto \frac{1}{s} S^{-1} f \end{array}$$

defines an $S^{-1}R$-linear map $\vartheta : S^{-1}Hom_R(M,N) \to Hom_{S^{-1}R}(S^{-1}M, S^{-1}N)$.

a) Show that ϑ is injective.

b) Show that ϑ is an isomorphism if M is finitely generated and $N \to S^{-1}N$ is injective.

Exercise 2.2 Let k be a field, $R = k[X_{i,j}]_{i \geq 1;\ 1 \leq j \leq i}$. Let $\mathfrak{p}_i = (X_{i,1}, \ldots, X_{i,i})$ and $S = R - \bigcup_{i=1}^{\infty} \mathfrak{p}_i$. Check that S is multiplicative and put $A = S^{-1}R$.

a) Show that $R_{\mathfrak{p}_i} = k\left(X_{h,j};\, \forall\, h \neq i\right)\left[X_{i,j}\right]_{(X_{i,1},\ldots,X_{i,i})}$.

b) Show that any $0 \neq f \in R$ belongs to only finitely many of the $\mathfrak{p}_i$.

c) Using lemma 6.1.22, show that the natural map $\varphi : A \to \prod_{i=1}^{\infty} R_{\mathfrak{p}_i}$ is faithfully flat.

d) For any ideal $0 \neq I \subset A$, show that there exists $n \in \mathbb{N}$ such that $IA_{S^{-1}\mathfrak{p}_i} = A_{S^{-1}\mathfrak{p}_i}$ for $i \geq n$.

e) For $1 \leq i < n$, write $IA_{S^{-1}\mathfrak{p}_i} = (\frac{x_{i,1}}{s_{i,1}}, \ldots, \frac{x_{i,r_i}}{s_{i,r_i}})$ and choose $y \in I$, $y \notin \bigcup_{i \geq n} \mathfrak{p}_i$. Let $J = (x_{i,j}, y) \subseteq I$. Show that $J = I$. [Hint: use c).]

Exercise 2.3 Let $A = k[X]$, $B = k[X,Y]$ and $C = k[X,Y]/(X^2 + Y^2 - 1)$, where k be a field of characteristic $\neq 2$. Denote x and y the classes of X and Y in C. As usual, write R_f for $S^{-1}R$, where $S = \{1, f, f^2, \ldots\}$.

a) Compute $\Omega^1_{A/k}$, $\Omega^1_{B/k}$, $\Omega^1_{C/k}$, and $\Omega^1_{B/A}$.

b) Compute the localisations $(\Omega^1_{C/k})_x$, $(\Omega^1_{C/k})_y$ and $(\Omega^1_{C/A})_y$.

c) Compute the dimension of $\Omega^1_{C/A}$ as a k-vector space.

d) Write down the first fundamental sequence of differentials for $k \subset A \subset C$. Is it exact on the left?

e) Write down the second fundamental sequence of differentials for $k \subset B \to C$. Is it exact on the left?

Definition 2.4.1 *An R-algebra A is called an* **formally smooth** *(resp.* **formally unramified**, *resp.* **formally étale**) *if for every R-algebra B and every nilpotent ideal $J \subset B$, the map*

$$\begin{array}{rl} \rho : Hom_{R-\text{algebras}}(A,B) & \longrightarrow Hom_{R-\text{algebras}}(A, B/J) \\ u & \longmapsto \pi \circ u \end{array}$$

(where $\pi : B \to B/J$ is the projection) is surjective (resp. injective, resp. bijective). If moreover A is finitely presented as an R-algebra, we drop the adverb "formally".

Exercise 2.4 Let A be an R-algebra.

a) Check that in the conditions in the definition above it suffices to assume $J^2 = 0$.

b) Let A' be an A algebra. Show that if A is formally smooth (resp. form. unramified, resp. form. étale) over R and A' is formally smooth (resp. form. unramified, resp. form. étale) over A then A' is formally smooth (resp. form. unramified, resp. form. étale) over R.

c) Let $S \subset A$ be a multiplicative subset. Show that if A is formally smooth (resp. formally unramified, resp. formally étale), then $S^{-1}A$ has the same property.

d) Let $f \in R$. Show that R_f is an étale R-algebra.

Exercise 2.5 Let A and B be R-algebras and $J \subset B$ a square-zero ideal.

a) Let $\bar{u} : A \to B/J$ be an R-algebra homomorphism and denote $\bar{u}_* J$ the B/J-module J viewed as an A-module via $\bar{u}$. Suppose that there exists some $u : A \to B$ such that $\rho(u) = \bar{u}$. Show that $\delta \mapsto u + \delta$ is a bijection between $Der_R(A, \bar{u}_* J)$ and the set $\rho^{-1}(\bar{u})$.

b) Show that A is formally unramified if and only if $\Omega^1_{A/R} = 0$.

c) Show that A is formally unramified over $R \iff A_{\mathfrak{p}}$ is formally unramified over R for every prime ideal $\mathfrak{p} \subset A \iff A_{\mathfrak{m}}$ is formally unramified over R for every maximal ideal $\mathfrak{m} \subset A$.

Exercise 2.6 Let A be a finitely presented R-algebra. Write $P = R[X_1, \ldots, X_n]$ and fix a presentation $\psi : P \twoheadrightarrow A$ with $\mathfrak{a} = \ker \psi = (F_1(X_1, \ldots, X_n), \ldots, F_m(X_1, \ldots, X_n))$. The jacobian matrix is denoted

$$J(\psi) = \left(\frac{\partial F_i}{\partial X_j} \right)_{i=1,\ldots,n;\, j=1,\ldots,m} \in M\left(m \times n, P\right).$$

a) Show that P is a smooth R-algebra.

b) Let $\bar{u} : A \to B/J$ be an R-algebra homomorphism and put $\bar{v} = \bar{u} \circ \psi : P \to B/J$. Choose a lifting $v : P \to B$. Show that $\bar{u}$ can be lifted to $u : A \to B$ if and only if there exists an R-linear derivation $\delta : P \to \bar{u}_* J$ such that $\delta(a) = v(a)$ for all $a \in \mathfrak{a}$.

c) Show that A is a smooth R-algebra if and only if the second fundamental sequence of differentials for $R \to P \to A$ is injective on the left and splits (hence $\Omega^1_{P/R} \otimes A \cong \mathfrak{a}/\mathfrak{a}^2 \oplus \Omega^1_{A/P}$).

d) Show that A is a smooth R-algebra if and only if $A_{\mathfrak{p}}$ is a formally smooth R-algebra for every prime ideal $\mathfrak{p} \subset A$. [Hint: use theorem 2.3.2]

e) Let $m \leq n$ and suppose that the image of $J(\psi)$ in $M\left(m \times n, A\right)$ has rank m. Show that A is a smooth R-algebra. Show moreover that, up to reordering the variables, A is étale over $R[X_{m+1}, \ldots, X_n]$.

f) Again let $m \leq n$ and let $f \in A$. Suppose that the image of $J(\psi)$ in $M\left(m \times n, A_f\right)$ has rank m. Show that A_f is a smooth R-algebra and (possibly reordering the variables) an étale $R[X_{m+1}, \ldots, X_n]$-algebra. [Hint: write A_f as a quotient of $R[X_1, \ldots, X_n, X_{n+1}]$.]

g) Conversely, let $\mathfrak{p} \subset A$ be a prime ideal and suppose that $A_{\mathfrak{p}}$ is formally smooth over R. Show that there exist $r \leq n$ among the polynomials F_i such that their classes generate $(\mathfrak{a}/\mathfrak{a}^2)_{\mathfrak{p}}$ and the image in $M(r \times n, A_{\mathfrak{p}})$ of the jacobian matrix has rank r.

h) Show that A is a smooth R-algebra if and only if for every prime ideal $\mathfrak{p} \subset A$ there exists $f \in A - \mathfrak{p}$ such that A_f is isomorphic to an algebra as in f) above.

Chapter III

Integral dependence, valuations and completions

§ 1 Integral elements

Let A be a ring and $R \subseteq A$ a subring.

Definition 3.1.1 An element $x \in A$ is **integral** over R if there exists a *monic* polynomial $f(X) \in R[X]$ such that $f(x) = 0$.

Example 3.1.2 Any element $a + ib \in \mathbb{Z}[i]$ is integral over $\mathbb{Z}$, root of $X^2 - 2aX + a2 + b^2$.

In general it is tricky to show directly that if $x, y \in A$ are integral, then $x + y$ is integral. It is better to linearize the problem and work with modules.

Proposition 3.1.3 *Let A be a ring, $R \subseteq A$ a subring and $x \in A$. The following conditions are equivalent:*

a) x is integral over R;

b) $R[x] = \{\sum_i \alpha_i x^i,\ \alpha_i \in R\}$ is a finitely generated R-module;

c) There exists an intermediate subring $R[x] \subseteq B \subseteq A$ with B finitely generated as an R-module;

d) There exists a faithful $R[x]$-module which is finitely generated as R-module.

Proof. a) $\Longrightarrow$ b) If x is integral, $R[x]$ is generated by $1, x, \ldots, x^{\deg f - 1}$. b) $\Longrightarrow$ c) Take $B = R[x]$. c) $\Longrightarrow$ d) Let $M = B$: it is a faithful module because $1 \in B$, hence for any $a \in \operatorname{Ann}_{R[x]}(B)$ we have $a = a \cdot 1 = 0$.
d) $\Longrightarrow$ a) Let $\mu_x : M \to M$ the multiplication by x (i.e. $\mu_x(m) = xm$). By the Cayley–Hamilton theorem, there exists a monic $p(T) \in R[T]$ such that $p(\mu_x)$ is the zero endomorphism of M. That means $p(x)m = 0$ for every $m \in M$. Since M is faithful, this implies $p(x) = 0$. □

Corollary 3.1.4 *Let A be a ring and $R \subseteq A$ a subring. If $x_1, \ldots, x_n$ are integral over R then $R[x_1, \ldots, x_n] = \{\sum_{i_1,\ldots,i_n} \alpha_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n},\ \alpha_{i_1,\ldots,i_n} \in R\}$ is a finitely generated R-module.*

Proof. By induction on n. If $R[x_1, \ldots, x_{n-1}]$ is a finitely generated R-module and $R[x_1, \ldots, x_n]$ is a finitely generated $R[x_1, \ldots, x_{n-1}]$-module, then $R[x_1, \ldots, x_n]$ is a finitely generated R-module. □

Corollary 3.1.5 *Let A be a ring and $R \subseteq A$ a subring. The susbset $\{x \in A \mid x \text{ is integral over } R\}$ is a subring of A called the* **integral closure** *of R in A.*

Proof. If $x, y \in A$ are integral over R then $R[x, y]$ is a finitely generated R-module. It contains $R[x + y]$ and $R[xy]$ as submodules. By applying condition c) in proposition 3.1.3 we get that $x + y$ and xy are integral over R. □

Definition 3.1.6 Let A be a ring and $R \subseteq A$ a subring. We say that R is **integrally closed** in A if R coincides with its integral closure in A. We say that a domain R is **integrally closed** if R is integrally closed in its fraction field.

Example 3.1.7 A UFD is integrally closed. If $\frac{x}{y}$ satisfies an integral equation

$$\left(\frac{x}{y}\right)^n + a_{n-1}\left(\frac{x}{y}\right)^{n-1} + \cdots + a_0 = 0 \quad \Longrightarrow \quad x^n + y\left(a_{n-1}x^{n-1} + \cdots + a_0 y^{n-1}\right) = 0.$$

We deduce that $y|x^n$. Hence $y|x$ and thus $\frac{x}{y} \in R$.

Definition 3.1.8 A finite field extension K of $\mathbb{Q}$ is called a **number field**. The integral closure of $\mathbb{Z}$ in a number field K is denoted $\mathcal{O}_K$ and called the **ring of integers** of K.

Example 3.1.9 Let $d \in \mathbb{N}$ be a squarefree integer and $K = \mathbb{Q}(\sqrt{d})$. Then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \bmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \bmod 4. \end{cases}$$

To prove this, recall that the Galois group is $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma\}$, where $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$ and $z \in K$ belongs to $\mathbb{Q}$ if and only if $\sigma(z) = z$. If $z = x + y\sqrt{d} \in K$ is integral over $\mathbb{Z}$, then $\sigma(z)$ is also integral, root of the same polynomial as z:

$$0 = \sigma(0) = \sigma(z^n + a_{n-1}z^{n-1} + \cdots + a_0) = \sigma(z)^n + a_{n-1}\sigma(z)^{n-1} + \cdots + a_0$$

since we assume that $a_i \in \mathbb{Z}$. As any UFD, $\mathbb{Z}$ is integrally closed (example 3.1.7), therefore

$$z + \sigma(z) = 2x \in \mathcal{O}_K \cap \mathbb{Z} = \mathbb{Z}; \qquad z\sigma(z) = x^2 - dy^2 \in \mathcal{O}_K \cap \mathbb{Z} = \mathbb{Z}.$$

Since $2x \in \mathbb{Z}$, multiplying the second equation by 4 we get that $4dy^2 \in \mathbb{Z}$. Write $y = \frac{u}{v}$ with $(u, v) = 1$ and consider a prime divisor p of v. Since $4d\frac{u^2}{v^2}$ is an integer, p^2 divides $4du^2$. Since d is squarefree, if p is odd, then p must divide u^2, hence p divides u, which is impossible since we assumed $(u, v) = 1$. So 2 is the only possible prime divisor for the denominators of x and y. Write $x = \frac{a}{2}$ and $y = \frac{b}{2}$, with $a, b \in \mathbb{Z}$. The equation $x^2 - dy^2 \in \mathbb{Z}$ becomes $a^2 - db^2 \in 4\mathbb{Z}$. If $2|b$,

then $a^2 \in 4\mathbb{Z}$, hence $2|a$ and $x, y \in \mathbb{Z}$. If $2 \nmid b$, since the only squares mod 4 are 0 and 1, we get $b^2 \equiv 1 \bmod 4$ and $a^2 \equiv 0, 1 \bmod 4$. Since $d \not\equiv 0 \bmod 4$ (it is squarefree), it must be $a^2 \equiv 1 \bmod 4$. Hence $2 \nmid b$ implies $a^2 - db^2 \equiv 1 - d \equiv 0 \bmod 4$. So for $d \equiv 2, 3 \bmod 4$, we get a and b even, hence $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.
On the other hand, if $d \equiv 1 \bmod 4$ then $\frac{1+\sqrt{d}}{2}$ is integral, root of $X^2 - X - \frac{d-1}{4}$ and if a, b are odd we have $\frac{a}{2} + \frac{b}{2}\sqrt{d} = \frac{a-b}{2} + b\frac{1+\sqrt{d}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

Definition 3.1.10 Let A be a ring and $R \subseteq A$ a subring. We say that A is **integral** over R if every element $x \in A$ is integral over R. More generally, if $\varphi : R \to A$ is a ring homomorphism, we say that A is **integral** over R if every element $x \in A$ is integral over the subring $\varphi(R)$.

Corollary 3.1.11 *For an R-algebra A the following conditions are equivalent:*

a) A is a finite R-algebra.

b) A is integral and of finite type over R.

Proof. a) $\Longrightarrow$ b) is obvious. For the converse, choose $x_1, \ldots, x_n$ generating A as an R-algebra and apply corollary 3.1.4. □

Corollary 3.1.12 *Let $R \subseteq A \subseteq B$ be rings. If A is integral over R and B is integral over A then B is integral over R.*

Proof. Let $x \in B$ and $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ be an integral equation with $a_i \in A$. Since the a_i are integral over R, the subring $A' = R[a_0, \ldots, a_{n-1}]$ is a finitely generated R-module. Moreover $A'[x]$ is a finitely generated A'-module. Therefore $x \in A'[x] = R[a_0, \ldots, a_{n-1}, x]$ and the latter is a finitely generated R-module, hence x is integral over R. □

Corollary 3.1.13 *Let A be a ring, $R \subseteq A$ a subring and $\widetilde{R}$ the integral closure of R in A. Then $\widetilde{R}$ is integrally closed in A.*

Proof. If $x \in A$ is integral over $\widetilde{R}$ it is integral over R and thus belongs to $\widetilde{R}$. □

Corollary 3.1.14 *Let R be a domain and $K = \operatorname{Frac} R$. Let $K \subseteq L$ and $L \subseteq M$ be finite field extensions, A the integral closure of R in L and B the integral closure of A in M. Then B is the integral closure of R in M.*

Proof. If $\widetilde{R}$ is the integral closure of R in M, then $B \subseteq \widetilde{R}$ by corollary 3.1.12. On the other hand, any $x \in \widetilde{R} \subseteq M$ satisfies an integral equation with coefficients in $R \subseteq A$ and is thus integral over A. Hence $x \in B$ and therefore $\widetilde{R} \subseteq B$. □

Proposition 3.1.15 *Let A be a ring and $R \subseteq A$ a subring. Assume A is integral over R.*

a) Let $I \subset A$ be an ideal and $J = R \cap I$. Then A/I is integral over R/J.

b) Let $S \subset R$ be a multiplicative set. Then $S^{-1}A$ is integral over $S^{-1}R$.

Proof. a) Let $\overline{x} \in A/I$ and $x \in A$ a representative. Then $x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0 = 0$ for suitable $\alpha_i \in R$ and therefore $\overline{x}^n + \overline{\alpha}_{n-1}\overline{x}^{n-1} + \cdots + \overline{\alpha}_0 = 0$.
b) Let $\frac{x}{s} \in S^{-1}A$, with $x \in A$ and $s \in S$. From an integral equation $x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0 = 0$ we deduce the equation $\left(\frac{x}{s}\right)^n + \frac{\alpha_{n-1}}{s}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{\alpha_0}{s^n} = 0$. □

Corollary 3.1.16 *Let A be a ring, $R \subseteq A$ a subring, $\widetilde{R}$ the integral closure of R in A and $S \subset R$ a multiplicative set. Then $S^{-1}\widetilde{R}$ is the integral closure of $S^{-1}R$ in $S^{-1}A$.*

Proof. Let $\frac{x}{s} \in S^{-1}A$, with $x \in A$ and $s \in S$. If it is integral over $S^{-1}R$ there is an equation

$$\left(\frac{x}{s}\right)^n + \frac{\alpha_{n-1}}{s_{n-1}}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{\alpha_0}{s_0} = 0 \tag{3.1}$$

for some $\alpha_i \in R$ and $s_i \in S$. Put $t = s_0 \cdots s_{n-1} \in S$. Multiplying (3.1) by $(st)^n$ we get an integral equation $(xt)^n + \beta_{n-1}(xt)^{n-1} + \cdots + \beta_0 = 0$, for suitable $\beta_i \in R$. Hence $xt \in \widetilde{R}$ and thus $\frac{x}{s} = \frac{xt}{st} \in S^{-1}\widetilde{R}$. □

Corollary 3.1.17 *Let R be a domain. The following conditions are equivalent.*

a) R is integrally closed:

b) $R_{\mathfrak{p}}$ is integrally closed for every prime ideal $\mathfrak{p}$;

c) $R_{\mathfrak{m}}$ is integrally closed for every maximal ideal $\mathfrak{m}$.

Proof. Let K be the common fraction field of R, $R_{\mathfrak{p}}$ and $R_{\mathfrak{m}}$. Then a) $\Longrightarrow$ b) follows from corollary 3.1.16; b) $\Longrightarrow$ c) is trivial. For c) $\Longrightarrow$ a), let $\widetilde{R}$ be the integral closure of R and denote $\varphi : R \hookrightarrow \widetilde{R}$ the inclusion. Again corollary 3.1.16 implies that φ_m is an isomorphism for all maximal ideals $\mathfrak{m}$, hence φ is an isomorphism. □

§ 2 Going Up and Going Down

Proposition 3.2.1 *Let A be a domain integral over a subring R. Then A is a field if and only if R is a field.*

Proof. Suppose R is a field and $0 \neq x \in A$. Let $x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0 = 0$ be an integral equation. Since A is a domain, we may assume $\alpha_0 \neq 0$. Then $\frac{1}{x} = \frac{-1}{\alpha_0}(x^{n-1} + \cdots + \alpha_1) \in A$.
Suppose A is a field and $0 \neq z \in R$. Then $\frac{1}{z} \in A$ satisfies an integral equation

$$\left(\frac{1}{z}\right)^n + \beta_{n-1}\left(\frac{1}{z}\right)^{n-1} + \cdots + \beta_0 = 0 \qquad \Longrightarrow \qquad \frac{1}{z} = -\beta_{n-1} - \cdots - \beta_0 z^{n-1} \in R. \qquad \square$$

Corollary 3.2.2 *Let A be a ring integral over a subring R. Let $\mathfrak{q} \subset A$ be a prime ideal and $\mathfrak{p} = \mathfrak{q} \cap R$. Then $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.*

Proof. By proposition 3.1.15.a, $A/\mathfrak{q}$ is integral over $R/\mathfrak{p}$. □

Corollary 3.2.3 *Let A be a ring integral over a subring R. Let $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subset A$ be prime ideals such that $\mathfrak{q}_1 \cap R = \mathfrak{q}_2 \cap R$. Then $\mathfrak{q}_1 = \mathfrak{q}_2$.*

Proof. Let $\mathfrak{p} = \mathfrak{q}_1 \cap R = \mathfrak{q}_2 \cap R$. We may replace $R \subseteq A$ by $R_\mathfrak{p} \subseteq A_\mathfrak{p}$. Then $\mathfrak{p}$ is maximal, so both $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are maximal. Since $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$, they must be equal. □

Proposition 3.2.4 (Lying over) *Let A be a ring integral over a subring R. Let $\mathfrak{p} \subset R$ be a prime ideal. Then there exists a prime ideal $\mathfrak{q} \subset A$ such that $\mathfrak{p} = \mathfrak{q} \cap R$.*

Proof. Again we may replace $R \subseteq A$ by $R_\mathfrak{p} \subseteq A_\mathfrak{p}$. Pick any maximal ideal $\mathfrak{m} \subseteq A$, then $\mathfrak{m} \cap R$ is maximal, hence $\mathfrak{m} \cap R = \mathfrak{p}$.

Corollary 3.2.5 *Let A be a ring integral over a subring R and $I \subseteq R$ an ideal. Then $\sqrt{I} = \sqrt{IA} \cap R$.*

Proof. Clearly $\sqrt{I} \subseteq \sqrt{IA} \cap R$. An element $x \in \sqrt{IA}$ if and only if it belongs to every prime $\mathfrak{q} \subset A$ containing IA. For every prime $\mathfrak{p} \subset R$, proposition 3.2.4 provides a prime $\mathfrak{q}$ such that $\mathfrak{p} = \mathfrak{q} \cap R$. If $I \subseteq \mathfrak{p}$ then $IA \subseteq \mathfrak{p}A \subseteq \mathfrak{q}$. So if $x \in \sqrt{IA} \cap R$, then $x \in \mathfrak{q} \cap R = \mathfrak{p}$ for every such $\mathfrak{p} \supseteq I$, hence $x \in \sqrt{I}$. □

Proposition 3.2.4 can be interpreted geometrically: if $\varphi : R \hookrightarrow A$ is an injective homomorphism and A is integral over R then $\varphi^\sharp : \operatorname{Spec} A \to \operatorname{Spec} R$ is surjective. Moreover:

Corollary 3.2.6 *Suppose $\varphi : R \hookrightarrow A$ is an injective homomorphism and A integral is over R. Then $\varphi^\sharp : \operatorname{Spec} A \to \operatorname{Spec} R$ is a closed map.*

Proof. Clearly, for every ideal $I \subseteq A$ we have $\varphi^\sharp(\mathcal{Z}(I)) \subseteq \mathcal{Z}(\varphi^{-1}(I))$. Let us show that it is an equality. If $\mathfrak{p} \in \mathcal{Z}(\varphi^{-1}(I))$ then $\mathfrak{p} \supseteq \varphi^{-1}(I)$. By proposition 3.1.15.a, $\overline{\varphi} : R/\varphi^{-1}(I) \hookrightarrow A/I$ is an integral homomorphism. Proposition 3.2.4 ensures that there exists a prime $\overline{\mathfrak{q}} \subset A/I$ such that $\overline{\varphi}^{-1}(\overline{\mathfrak{q}}) = \overline{\mathfrak{p}}$. Denoting by $\pi : A \to A/I$ the projection, we get $\mathfrak{q} = \pi^{-1}(\mathfrak{q}) \in \mathcal{Z}(I)$ and by construction $\varphi^\sharp(\mathfrak{q}) = \varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$. □

Corollary 3.2.7 *Let R be a domain, $\varphi : R \hookrightarrow A$ be an injective homomorphism making A into a finitely generated R-algebra. Then the image of $\varphi^\sharp : \operatorname{Spec} A \to \operatorname{Spec} R$ contains a non-empty open subset of $\operatorname{Spec} R$.*

Proof. Choose a presentation $\pi : R[X_1, \dots, X_n] \twoheadrightarrow A$. Suppose one of the generators, say $\pi(X_1)$, is not algebraic over R. Then we can factor φ as $R \subset R[X_1] \subset A$. Repeating this, we may assume that φ factors as $R \subseteq R' = R[X_1, \dots, X_m] \subseteq A = R'[X_{m+1}, \dots, X_n]/I$ where, for all $m < i \leq n$ the element $x_i = X_i \bmod I$ satisfies a polynomial equation

$$a_{i,d_i} X_i^{d_i} + a_{i,d_i-1} X_i^{d_i-1} + \cdots + a_{i,0} = 0, \qquad 0 \neq a_{i,d_i} \in R'.$$

Let $f \in R$ be any non-zero coefficient of the polynomial $\prod_{i=m+1}^n a_{i,d_i} \in R'$. Then $\operatorname{im} \varphi^\sharp$ contains the open subset $\operatorname{Spec} R - \mathcal{Z}(f)$. Indeed, every prime $\mathfrak{p} \subset R$ is the image of the ideal $\mathfrak{p}' = \mathfrak{p}[X_1, \dots, X_m]$ (the set of polynomials with coefficients in $\mathfrak{p}$), which is prime because $R[X_1, \dots, X_m]/\mathfrak{p}[X_1, \dots, X_m] \cong (R/\mathfrak{p})[X_1, \dots, X_m]$ is a domain. If moreover $f \notin \mathfrak{p}$, then $\prod_{i=m+1}^n a_{i,d_i} \notin \mathfrak{p}'$, so $A_{\mathfrak{p}'}$ is integral over $R'_{\mathfrak{p}'}$. By proposition 3.2.4, there exists a prime $\mathfrak{q} \subset A$ lying over $\mathfrak{p}'$ and $\mathfrak{q} \cap R = \mathfrak{q} \cap R' \cap R = \mathfrak{p}' \cap R = \mathfrak{p}$. □

Corollary 3.2.7 is a special case (and a crucial step in the proof) of theorem 6.1.37, to be established later. Proposition 3.2.4 can be refined to arbitrary finite increasing chains of primes:

Theorem 3.2.8 (Going Up) *Let A be a ring integral over a subring R. Let $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n \subset R$ be a chain of prime ideals, $m \leq n$ and $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m \subset A$ a chain of primes such that $\mathfrak{p}_i = \mathfrak{q}_i \cap R$ for $1 \leq i \leq m$. Then there exist primes $\mathfrak{q}_m \subseteq \mathfrak{q}_{m+1} \subseteq \cdots \subseteq \mathfrak{q}_n \subset A$ such that $\mathfrak{p}_i = \mathfrak{q}_i \cap R$ for $1 \leq i \leq n$.*

Proof. We are easily reduced to the case $n = m+1$. We may replace R and A by their localisation at $\mathfrak{p}_{m+1}$. We may then replace R by $R/\mathfrak{p}_m$ and A by $A/\mathfrak{q}_m$, thereby reducing to the case $m = 1$, $n = 2$, both rings are domains, $\mathfrak{p}_1 = 0$ and $\mathfrak{q}_1 = 0$. Apply now proposition 3.2.4 to find $\mathfrak{q}_2 \subseteq A$ such that $\mathfrak{q}_2 = \mathfrak{p}_2$. □

Definition 3.2.9 We shall say that a ring homomorphism $\varphi : R \to A$ has the **going down property** if for any two primes $\mathfrak{p}_1 \supseteq \mathfrak{p}_2$ in R and for every prime $\mathfrak{q}_1 \subset A$ such that $\varphi^{-1}(\mathfrak{q}_1) = \mathfrak{p}_1$ there exists a prime $\mathfrak{q}_1 \supseteq \mathfrak{q}_2$ in A such that $\varphi^{-1}(\mathfrak{q}_2) = \mathfrak{p}_2$.

Remark 3.2.10 As before, we may refine the going down property and consider a descending chain $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$ of prime ideals in R and, for $m \leq n$, a chain $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$ of primes in A such that $\mathfrak{p}_i = \varphi^{-1}(\mathfrak{q}_i)$ for $1 \leq i \leq m$. The requirement is then that there exist prime ideals $\mathfrak{q}_m \supseteq \mathfrak{q}_{m+1} \supseteq \cdots \supseteq \mathfrak{q}_n$ in A such that $\mathfrak{p}_i = \varphi^{-1}(\mathfrak{q}_i)$ for $1 \leq i \leq n$.
We leave it as an exercise to check that if $\varphi : R \to A$ satisfies the going down property in the sense of definition 3.2.9, then it satisfies the stronger property just stated.

While apparently similar, the going up and going down properties are of a very different nature, as becomes apparent from their geometric translations (corollary 3.2.6 above for going up, propositions 3.2.13 below for going down). See also proposition 3.2.15 and remark 3.2.17.

Proposition 3.2.11 *A homomorphism $\varphi : R \to A$ has the going down property if and only if for every prime $\mathfrak{p}_1 \subset R$ and $\mathfrak{q}_1 \subset A$ such that $\varphi^{-1}(\mathfrak{q}_1) = \mathfrak{p}_1$, the induced map $\varphi^\sharp : \operatorname{Spec} A_{\mathfrak{q}_1} \to \operatorname{Spec} R_{\mathfrak{p}_1}$ is surjective.*

Proof. Follows directly from the bijections given by proposition 2.1.10. □

Corollary 3.2.12 *A flat homomorphism $\varphi : R \to A$ has the going down property.*

Proof. The map $\varphi_{\mathfrak{p}_1} : R_{\mathfrak{p}_1} \to A_{\mathfrak{q}_1}$ is a flat local homomorphism. By lemma 2.2.8, is faithfully flat, hence $\varphi^\sharp : \operatorname{Spec} A_{\mathfrak{q}_1} \to \operatorname{Spec} R_{\mathfrak{p}_1}$ is surjective by proposition 2.2.2. □

The following proposition is a direct translation of the going down property in geometric terms. Recall the discussion in remark 1.1.79 on non-closed points in spectra.

Proposition 3.2.13 *A homomorphism $\varphi : R \to A$ has the going down property if and only if the induced map $\varphi^\sharp : \operatorname{Spec} A \to \operatorname{Spec} R$ satisfies the following property: for every $\mathfrak{p}_1 = \varphi^\sharp(\mathfrak{q}_1)$ and $\mathfrak{p}_1 \in \mathcal{Z}(\mathfrak{p}_2) = \overline{\{\mathfrak{p}_2\}}$, there exists $\mathfrak{q}_2 \in A$ with $\mathfrak{q}_1 \in \mathcal{Z}(\mathfrak{q}_2)$ such that $\mathfrak{p}_2 = \varphi^\sharp(\mathfrak{q}_2)$.*

Even more explicitely: if $\mathfrak{p}_1$ is the image of $\mathfrak{q}_1$, for any irreducible subset $\mathcal{Z}(\mathfrak{p}_2) \subseteq \operatorname{Spec} R$ containing $\mathfrak{p}_1$ there exists an irreducible subset $\mathcal{Z}(\mathfrak{q}_2) \subseteq \operatorname{Spec} A$ such that $\varphi^\sharp(\mathcal{Z}(\mathfrak{q}_2)) = \mathcal{Z}(\mathfrak{p}_2)$.

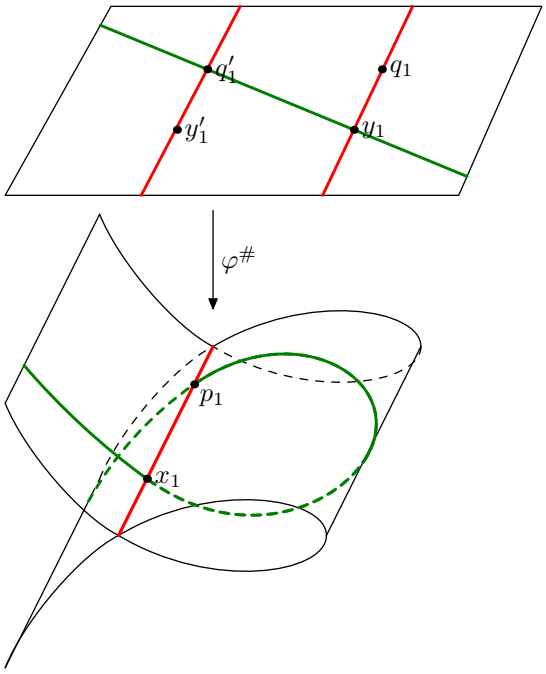
Example 3.2.14 Let $R = \mathbb{C}[X,Y,Z]/(X^3 - Y^2 + XY)$ and $A = \mathbb{C}[T,Z]$. Define $\varphi : R \hookrightarrow A$ by

$$\varphi(X) = T^2 - T; \quad \varphi(Y) = T^3 - T^2; \quad \varphi(Z) = Z.$$

Let $\mathfrak{p}_1 = (X,Y,Z)$, $\mathfrak{p}_2 = \varphi^{-1}(T-Z)$ and $\mathfrak{q}_1 = (T-1,Z)$. Put $q_1 = \mathcal{Z}(\mathfrak{q}_1)$ and $y_1' = \mathcal{Z}(T, Z-1)$. Then

$$(\varphi^\sharp)^{-1}\left(\mathcal{Z}(\mathfrak{p}_2)\right) = \{\mathcal{Z}(T-Z), q_1, y_1'\}.$$

In this set, $(T-Z)$ is the only ideal mapping to $\mathfrak{p}_2$, but $q_1 \notin \mathcal{Z}(T-Z)$.



We give now a simple sufficient topological condition for the going down property to hold. The proof we present forces us to introduce an (unnecessary) technical assumption in the statement: we assume that the rings are *noetherian* (see definition 4.1.2). This class of rings, the most widely used in algebraic geometry and number theory, will be studied in detail from the next chapter. Notice that the map $\varphi^\sharp$ in example 3.2.14 is not open: $U = \operatorname{Spec} A - [\mathcal{Z}(T-Z) \cup \mathcal{Z}(T)]$ is an open subset but $\varphi^\sharp(U) = [\operatorname{Spec} R - \mathcal{Z}(\mathfrak{p}_2)] \cup \{p_1\}$ is not.

Proposition 3.2.15 *Let $\varphi : R \to A$ be morphism of noetherian rings such that $\varphi^\sharp : \operatorname{Spec} A \to \operatorname{Spec} R$ is open. Then φ has the going down property.*

Proof. Let us first remark that if $\mathfrak{p}_2 \subseteq \mathfrak{p}_1$ then $\mathfrak{p}_2$ belongs to *every* open neighborhood of $\mathfrak{p}_1$ in $\operatorname{Spec} R$. Indeed, such neighborhoods are of the form $U = \operatorname{Spec} R - \mathcal{Z}(I)$ for some ideal $I \subset R$ and $\mathfrak{p}_1 \in U$ means $I \nsubseteq \mathfrak{p}_1$. This forces $I \nsubseteq \mathfrak{p}_2$, hence $\mathfrak{p}_2 \in U$.
If $\operatorname{im}(\varphi^\sharp)$ is open and contains $\mathfrak{p}_1$, it is an open neighborhood of it and as such $\mathfrak{p}_2 \in \operatorname{im}(\varphi^\sharp)$: there exists some $\mathfrak{q}_2 \in \operatorname{Spec} A$ such that $\mathfrak{p}_2 = \varphi^{-1}(\mathfrak{q}_2)$. We need to show that at least one such prime $\mathfrak{q}_2$ is contained in $\mathfrak{q}_1$.

Since we are only interested in primes above $\mathfrak{p}_2$, we may assume $\mathfrak{p}_2 = 0$ (replace R by $R/\mathfrak{p}_2$ and A by $A/\varphi(\mathfrak{p}_2)A$; the induced map $\operatorname{Spec} A/\varphi(\mathfrak{p}_2)A) = \mathcal{Z}(\varphi(\mathfrak{p}_2)A) \to \operatorname{Spec} R/\mathfrak{p}_2 = \mathcal{Z}(\mathfrak{p}_2)$ is just the restriction of $\varphi^\sharp$, hence still open; we shall see in corollary 4.1.13 that the rings remain noetherian).
Let us consider the minimal prime ideals in A (i.e. prime ideals minimal with respect to inclusion). A simple application of Zorn's lemma shows that every prime ideal contains a minimal prime (see corollary 6.1.10). Therefore, every non-empty open set $U \subseteq \operatorname{Spec} A$ contains some minimal prime. Since $\varphi^\sharp(U)$ is open, it contains 0, hence some prime $\mathfrak{q} \in U$ maps to 0. If $\mathfrak{n} \subseteq \mathfrak{q}$ is a minimal prime, then $0 \in \varphi^{-1}(\mathfrak{n}) \subseteq \varphi^{-1}(\mathfrak{q}) = 0$. Hence, for every open subset in $U \subseteq \operatorname{Spec} A$, some of the minimal primes in U map to 0.
We now use the assumption that A is noetherian: it implies that the set of minimal primes in A is finite (we shall prove this in corollary 6.1.11). Let $\mathfrak{n}_1, \dots, \mathfrak{n}_r$ be these minimal primes. The set $U_i = \operatorname{Spec} A - \bigcup_{j \neq i} \mathcal{Z}(\mathfrak{n}_j)$ is open, therefore $\varphi^\sharp(\mathfrak{n}_i) = 0$, since $\mathfrak{n}_i$ is the only minimal prime in U_i. Thus every minimal prime maps to 0.
Therefore any prime $\mathfrak{q}_1 \subset A$ mapping to $\mathfrak{p}_1$ contains a minimal prime mapping to 0. □

Remark 3.2.16 The result holds without the noetherian assumption, but the proof requires more techniques. If A is a domain, one argues as follows: write $A_{\mathfrak{q}_1} = \bigcup_{f \notin \mathfrak{q}_1} A_f \subset \operatorname{Frac} A$. Then $\operatorname{Spec} A_{\mathfrak{q}_1} = \bigcap_{f \notin \mathfrak{q}_1} \operatorname{Spec} A_f$. Since $\operatorname{Spec} A_f \subseteq \operatorname{Spec} A$ is open, $\operatorname{Spec} R_{\mathfrak{p}_1} \subseteq \varphi^\sharp(\operatorname{Spec} A_f)$ for all $f \notin \mathfrak{q}_1$, hence $\operatorname{Spec} R_{\mathfrak{p}_1} \subseteq \bigcap_f \varphi^\sharp(\operatorname{Spec} A_f) = \varphi^\sharp(\operatorname{Spec} A_{\mathfrak{q}_1})$. For a general ring A, the same proof will work by replacing the union of the A_f with their direct limit, a notion which we will not cover in this course (somehow dual to that of inverse limit discussed in § 3.6).

Remark 3.2.17 Let R be noetherian and A a finitely generated R-algebra (hence A is noetherian too, corollary 4.1.19). In corollary 6.1.38 we will show that if $\varphi : R \to A$ has the going down property, then $\varphi^\sharp : \operatorname{Spec} A \to \operatorname{Spec} R$ is open. Hence, for noetherian rings,

$$\text{flat} \implies \text{going down} \iff \text{open}.$$

A direct proof of flat $\implies$ open can be found in [10], theorem I.2.12.

The ring R in example 3.2.14 is not integrally closed. A domain integral over an integrally closed domain has the going down property, as we shall see in theorem 3.2.21 below. We need some preliminary results.

Definition 3.2.18 Let A be a ring, $R \subseteq A$ a subring and $I \subseteq R$ an ideal. We say that $x \in A$ is integral over I if there exists a monic polynomial $f(X) = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_0 \in R[X]$ with $\alpha_i \in I$ such that $f(x) = 0$. Let $\widetilde{I} = \{x \in A \mid x \text{ is integral over } I\}$ be the integral closure of I in A.

Lemma 3.2.19 *$\widetilde{I} = \sqrt{I\widetilde{R}}$. In particular, $\widetilde{I}$ is an ideal in $\widetilde{R}$.*

Proof. If $x \in \widetilde{I}$, then $x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0 = 0$, with $\alpha_i \in I$. Therefore $x \in \widetilde{R}$ and $x^n = -(\alpha_{n-1}x^{n-1} + \cdots + \alpha_0) \in I\widetilde{R}$, hence $x \in \sqrt{I\widetilde{R}}$. Conversely, if $x^n \in I\widetilde{R}$, write $x^n = \sum_{i=1}^m \beta_i x_i$ with $\beta_i \in I$ and $x_i \in \widetilde{R}$. The R-module $M = R[x_1, \dots, x_m]$ is finitely generated and the multiplication by x^n map $\mu_{x^n} : M \to M$ has image in IM. By the Cayley-Hamilton theorem (and remark 1.2.33), we conclude that x^n is integral over I, hence x is integral over I. □

Lemma 3.2.20 *Let A be a domain, integral over an integrally closed subdomain R and $K = \operatorname{Frac} R$. Let $x \in A$ be integral over an ideal $I \subseteq R$. Then if $g(X) = X^n + \beta_{n-1}X^{n-1} + \cdots + \beta_0 \in K[X]$ is the minimal polynomial of x, the coefficients β_i belong to $\sqrt{I}$.*

Proof. Let L be a splitting field of g, denote $x_1 = x, \ldots, x_r$ the roots of g in L. For any x_j, fix a K-linear automorphism $\sigma_j : L \to L$ such that $x_j = \sigma_j(x)$. By assumption, x satisfies an equation $x^m + \alpha_{m-1}x^{m-1} + \cdots + \alpha_0 = 0$, with $\alpha_i \in I$. Applying σ_j, we see that x_j satisfies the same equation and is thus integral over I. The coefficients β_i are polynomials in $x_1, \ldots, x_r$, hence also integral over I. Since they belong to K and are integral over $I \subseteq R$ and R is integrally closed, we conclude $\beta_i \in \widetilde{I} \cap R = \sqrt{I\widetilde{R}} \cap R = \sqrt{I}$, the last equality being corollary 3.2.5. □

Theorem 3.2.21 (Going Down) *Let A be a domain, integral over an integrally closed subdomain R. Then $R \hookrightarrow A$ has the going down property.*

Proof. Let $\mathfrak{p}_1 \supseteq \mathfrak{p}_2$ in R and $\mathfrak{q}_1 \subset A$ a prime such that $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$. We may replace R by $R_{\mathfrak{p}_1}$ and A by $A_{\mathfrak{p}_1}$. By lemma 2.1.14, it suffices to show that $\mathfrak{p}_2 A_{\mathfrak{q}_1} \cap R = \mathfrak{p}_2$. The inclusion $\mathfrak{p}_2 \subseteq \mathfrak{p}_2 A_{\mathfrak{q}_1} \cap R$ being obvious, let $x \in \mathfrak{p}_2 A_{\mathfrak{q}_1} \cap R$, written as $x = \frac{z}{s}$, with $z \in \mathfrak{p}_2 A$ and $s \in A - \mathfrak{q}_1$. Then $z \in \mathfrak{p}_2 A \subseteq \sqrt{\mathfrak{p}_2 A}$, so by lemma 3.2.19, it is integral over $\mathfrak{p}_2$. By lemma 3.2.20, its minimal polynomial $g(Z) = Z^n + \beta_{n-1}Z^{n-1} + \cdots + \beta_0 \in K[Z]$ has coeffficients $\beta_i \in \sqrt{\mathfrak{p}_2} = \mathfrak{p}_2$. On the other hand, $x \in R$, so $x^{-1} \in K$, hence the minimal polynomial $h(S) = S^n + \frac{\beta_{n-1}}{x}S^{n-1} + \cdots + \frac{\beta_0}{x^n}$ for $s = \frac{z}{x}$ over K is obtained dividing g by x^n. But $s \in A - \mathfrak{q}_1$, so it is integral over R: applying lemma 3.2.20 to $I = R$ we get that $\alpha_j = \frac{\beta_j}{x^{n-j}} \in R$ for $j = 0, \ldots, n-1$. Therefore, $x^{n-j}\alpha_j = \beta_j \in \mathfrak{p}_2$. If $x \notin \mathfrak{p}_2$, then $\alpha_j \in \mathfrak{p}_2$ and then $s^n = -\alpha_{n-1}s^{n-1} - \cdots - \alpha_0 \in \mathfrak{p}_2 A \subseteq \mathfrak{q}_1$, contadicting $s \in A - \mathfrak{q}_1$. Therfore, any $x \in \mathfrak{p}_2 A_{\mathfrak{q}_1} \cap R$ belongs to $\mathfrak{p}_2$. □

§ 3 Norm, trace, discriminant

Let R be a ring and F a free R-module of finite rank. Define the characteristic polynomial, trace and determinant of an endomorphism $F \to F$ as in linear algebra. If A is an R-algebra, which is free of finite rank as an R-module, for any $x \in A$, the multiplication by x is an R-linear endomorphism $\mu_x : A \to A$.

Definition 3.3.1 Let A be an R-algebra, which is free of finite rank as an R-module and $x \in A$. The **trace** of x is $\operatorname{Tr}_{A/R}(x) = \operatorname{Tr}(\mu_x)$. The **norm** of x is $N_{A/R}(x) = \det(\mu_x)$.

The following result lists well-known properties from linear algebra.

Proposition 3.3.2 *Let A be an R-algebra, which is free of rank n as an R-module. For any $x, y \in A$ and $\alpha, \beta \in R$,*

$$\operatorname{Tr}_{A/R}(\alpha x + \beta y) = \alpha \operatorname{Tr}_{A/R}(x) + \beta \operatorname{Tr}_{A/R}(y);$$

$$N_{A/R}(xy) = N_{A/R}(x)N_{A/R}(y); \quad N_{A/R}(\alpha x) = \alpha^n N_{A/R}(x).$$

Proposition 3.3.3 *Let A be an R-algebra, free of finite rank as an R-module and B an A-algebra, free of finite rank as an A-module. Then B is a free R-module and for any $x \in B$,*

$$\mathrm{Tr}_{B/R}(x) = \mathrm{Tr}_{A/R}(\mathrm{Tr}_{B/A}(x)).$$

Proof. For any R-basis $\mathcal{A} = \{a_1, \ldots, a_n\}$ of A and A-basis $\mathcal{B} = \{b_1, \ldots, b_m\}$ of B we have the R-basis $\mathcal{C} = \{a_i b_j \,|\, 1 \le i \le n;\ 1 \le j \le m\}$ for B. Denote $(\beta_{i,j}(x)) \in M_m(A)$ be the matrix of μ_x in $\mathcal{B}$ i.e. $xb_j = \sum_{i=1}^m \beta_{i,j}(x) b_i$. Moreover, for $y \in A$, let $(\alpha_{p,q}(y)) \in M_n(R)$ be the matrix of μ_y in $\mathcal{A}$, i.e. $ya_q = \sum_{p=1}^n \alpha_{p,q}(y) a_p$. Then, applying linearity of the trace,

$$\mathrm{Tr}_{A/R}\left(\mathrm{Tr}_{B/A}(x)\right) = \sum_{j=1}^m \mathrm{Tr}_{A/R}\left(\beta_{j,j}(x)\right) = \sum_{i=1}^n \sum_{j=1}^m \alpha_{i,i}\left(\beta_{j,j}(x)\right). \tag{3.2}$$

On the other hand

$$\mu_x(a_i b_j) = x a_i b_j = \sum_{q=1}^m \left[a_i \beta_{q,j}(x)\right] b_q = \sum_{p=1}^n \sum_{q=1}^m \alpha_{p,i}\left(\beta_{q,j}(x)\right) a_p b_q$$

so the matrix of μ_x in the basis $\mathcal{C}$ is $\left(\alpha_{p,i}\left(\beta_{q,j}(x)\right)\right)_{1 \le i,p \le n;\, 1 \le j,q \le m}$ and its trace coincides with the result of (3.2). □

Example 3.3.4 Let $K \subseteq L$ be a finite field extension and $x \in L$. Let $f(X) \in K[X]$ be the minimal polynomial of x over K and $x_1 = x, \ldots, x_n$ the (possibly repeated) roots of f in a splitting field. Then $\mathrm{Tr}_{K[x]/K}(x) = x_1 + \cdots + x_n$ and $N_{K[x]/K}(x) = x_1 \cdots x_n$. Indeed, the matrix M_x of μ_x in the basis $\{1, x, \ldots, x^{n-1}\}$ of $K[x]$ is just the companion matrix of $f(X)$. It follows from proposition 3.3.3 that $\mathrm{Tr}_{L/K}(x) = [L : K[x]] \cdot \mathrm{Tr}_{K[x]/K}(x)$. We can say more: if $y_1, \ldots, y_m$ is a $K[x]$-basis of L, then the matrix of $\mu_x : L \to L$ in the basis $\{x^i y_j \,|\, 0 \le i \le n-1;\ 1 \le j \le m\}$ is block diagonal, with blocks all equal to M_x. Hence the characteristic polynomial of μ_x on L is the $m = [L : K[x]]$-th power of $f(X)$. In particular, $N_{L/K}(x) = N_{K[x]/K}(x)^{[L:K[x]]}$.

The trace defines a bilinear symmetric form

$$\begin{aligned} A \times A &\longrightarrow R \\ (x, y) &\longmapsto \mathrm{Tr}_{A/R}(xy) \end{aligned}$$

Definition 3.3.5 If $\{x_1, \ldots, x_n\}$ is a basis for the free R-module A, its **discriminant** is

$$\Delta_{A/R}(x_1, \ldots, x_n) = \det\left(\mathrm{Tr}_{A/R}(x_i x_j)\right).$$

If $\{y_1, \ldots, y_n\}$ is another basis, let $y_j = \sum_{i=1}^n a_{i,j} x_i$ and $U = (a_{i,j})$ be the change of basis matrix. Then $\left(\mathrm{Tr}_{A/R}(y_p y_q)\right) = U\left(\mathrm{Tr}_{A/R}(x_i x_j)\right) U^t$, hence

$$\Delta_{A/R}(y_1, \ldots, y_n) = (\det U)^2 \Delta_{A/R}(x_1, \ldots, x_n). \tag{3.3}$$

Since $U \in \mathrm{GL}_n(R)$, the two differ by a unit. If A is a free R-module, we can thus define the **discriminant ideal** as the principal ideal $\mathfrak{d}_{A/R} \subseteq R$ generated by the discriminant of any basis.

We shall be mostly concerned with the following situation. R is an integrally closed domain with fraction field K. We consider a finite field extension $K \subseteq L$ and a subring $A \subset L$, integral over R and such that $L = \mathrm{Frac}\, A$. If $x \in A$, let $f(X) = X^n + \alpha_{n-1} X^{n-1} + \cdots + \alpha_0 \in K[X]$ be the the minimal polynomial of x. By example 3.3.4, $\mathrm{Tr}_{K[x]/K}(x) = \alpha_{n-1}$, so by lemma 3.2.20 (with $I = R$) we get $\mathrm{Tr}_{K[x]/K}(x) \in R$. Hence $\mathrm{Tr}_{L/K}(x) = [L : K[x]]\, \mathrm{Tr}_{K[x]/K}(x) \in R$ for every $x \in A$.

Definition 3.3.6 Let R be an integrally closed domain, K its fraction field, L a finite field extension of K and $A \subset L$ a subring, integral over R. Assume furthermore that A contains a K-basis for L. The **discriminant ideal** is the ideal $\mathfrak{d}_{A/R} \subseteq R$ generated by the discriminants $\Delta_{L/K}(x_1, \ldots, x_n)$ of all the K-bases $\{x_1, \ldots, x_n\}$ of L contained in A.

If A is a free R-module, this definition coincides with the one given above, in view of formula (3.3), but in general it won't be a principal ideal. It can be computed by localisation.

Lemma 3.3.7 *Let $S \subset R$ be a multiplicative subset. Then $\mathfrak{d}_{S^{-1}A/S^{-1}R} = S^{-1}\mathfrak{d}_{A/R}$.*

Proof. Since $A \subseteq S^{-1}A$, any K-basis of L contained in A is in $S^{-1}A$, hence $\mathfrak{d}_{A/R} \subseteq \mathfrak{d}_{S^{-1}A/S^{-1}R}$ so $S^{-1}\mathfrak{d}_{A/R} \subseteq \mathfrak{d}_{S^{-1}A/S^{-1}R}$. If $x_1, \ldots, x_n \in S^{-1}A$ are a K-basis for L then, for a suitable $s \in S$ we have that $sx_1, \ldots, sx_n \in A$, hence $\Delta_{L/K}(sx_1, \ldots, sx_n) = s^{2n}\Delta_{L/K}(x_1, \ldots, x_n) \in \mathfrak{d}_{A/R}$. Therefore $\mathfrak{d}_{S^{-1}A/S^{-1}R} \subseteq S^{-1}\mathfrak{d}_{A/R}$. □

As usual, the bilinear form allows us to define K-linear (respectively R-linear) maps

$$\begin{array}{rcl} L & \longrightarrow & \mathrm{Hom}_K(L, K) \\ x & \longmapsto & \left[y \mapsto \mathrm{Tr}_{L/K}(xy)\right] \end{array} ; \qquad \begin{array}{rcl} A & \longrightarrow & \mathrm{Hom}_R(A, R) \\ x & \longmapsto & \left[y \mapsto \mathrm{Tr}_{L/K}(xy)\right] \end{array} .$$

Definition 3.3.8 Let R be an integrally closed domain, K its fraction field, L a finite field extension of K and $A \subset L$ a subring, integral over R and containing a K-basis for L. The **codifferent**

$$\mathfrak{D}_{A/R}^{-1} = \{x \in L \,|\, \mathrm{Tr}_{L/K}(xy) \in R \;\forall\, y \in A\}$$

is the largest sub-A-module $M \subseteq L$ such that $Tr_{L/K}(M) \subseteq R$. Notice that $A \subseteq \mathfrak{D}_{A/R}^{-1}$.

Also the codifferent can be computed by localisation.

Lemma 3.3.9 *Let $S \subset R$ be a multiplicative subset. Then $S^{-1}\mathfrak{D}_{A/R}^{-1} \subseteq \mathfrak{D}_{S^{-1}A/S^{-1}R}^{-1}$ and equality holds if A is finitely generated as an R-module.*

Proof. By definition, if $x \in \mathfrak{D}_{A/R}^{-1}$ then $\mathrm{Tr}_{L/K}(xy) \in R$ for all $y \in A$. Then, for $s, t \in S$, we have $\mathrm{Tr}_{L/K}(\frac{x}{s}\frac{y}{t}) = \frac{1}{st}\mathrm{Tr}_{L/K}(xy) \in S^{-1}R$. Thus $S^{-1}\mathfrak{D}_{A/R}^{-1} \subseteq \mathfrak{D}_{S^{-1}A/S^{-1}R}^{-1}$. For the reverse inclusion, let $y_1, \ldots, y_r$ be generators for A. If $x \in \mathfrak{D}_{S^{-1}A/S^{-1}R}^{-1}$, select $s \in S$ such that $s\mathrm{Tr}_{L/K}(xy_i) \in R$ for all $i = 1, \ldots, r$. Then for all $y = \alpha_1 y_1 + \cdots + \alpha_r y_r \in A$, with $\alpha_i \in R$, we get $\mathrm{Tr}_{L/K}(sxy) = \sum_{i=1}^{r} \alpha_i s\mathrm{Tr}_{L/K}(xy_i) \in R$, hence $sx \in \mathfrak{D}_{A/R}^{-1}$ and therefore $x \in S^{-1}\mathfrak{D}_{A/R}^{-1}$. □

Proposition 3.3.10 *Let R be an integrally closed domain, K its fraction field, $f(X) \in R[X]$ a monic separable polynomial, $L = K[X]/(f(X))$ and $A = R[X]/(f(X))$. Let $x \in A$ be the class of X. Then the pairing $\mathrm{Tr}_{L/K} : L \times L \to K$ is non-degenerate and $\mathfrak{D}_{A/R}^{-1}$ is the free A-module generated by $\frac{1}{f'(x)}$.*

Proof. Under these assumption, A is a free R-module with basis $1, x, \ldots, x^{n-1}$, where $n = \deg f$. Put $r_{i,j} = \mathrm{Tr}_{L/K}\left(\frac{x^i x^j}{f'(x)}\right)$, for $i, j \in \{0, \ldots, n-1\}$. Lemma 3.3.12 below shows that $r_{i,j} = 0$ for $0 \leq i + j \leq n - 2$ and $r_{i,j} = 1$ for $i + j = n - 1$. Moreover, for $i + j \geq n$ we have,

$$r_{i,j} = \mathrm{Tr}_{L/K}\left(x^n \cdot \frac{x^{i+j-n}}{f'(x)}\right) = \mathrm{Tr}_{L/K}\left(\sum_{k=0}^{n-1} \beta_k \frac{x^k}{f'(x)}\right) = \sum_{k=0}^{n-1} \beta_k \mathrm{Tr}_{L/K}\left(\frac{x^k}{f'(x)}\right) \in R$$

for suitable $\beta_0, \dots, \beta_{n-1} \in R$. Therefore the matrix $(r_{i,j}) = \left(\mathrm{Tr}_{L/K}\left(\frac{x^i x^j}{f'(x)}\right)\right)$ is in $\mathrm{GL}_n(R)$ and

$$\det\left(\mathrm{Tr}_{L/K}\left(\frac{x^i x^j}{f'(x)}\right)\right) = \det\begin{pmatrix} 0 & \dots & 0 & 1 \\ 0 & \dots & 1 & * \\ \vdots & \iddots & \iddots & \vdots \\ 1 & * & \dots & * \end{pmatrix} = (-1)^{\frac{n(n-1)}{2}}.$$

Therefore the basis $(1, x, \dots, x^{n-1})$ admits $\left(\frac{1}{f'(x)}, \dots, \frac{x^{n-1}}{f'(x)}\right)(r_{i,j})^{-1} = (y_1, \dots, y_n) \in L^n$ as dual basis with respect to the pairing $\mathrm{Tr}_{L/K} : L \times L \to K$, which is thus non-degenerate. By definition, $z = \sum_{i=1}^n \alpha_i y_i \in L$ is in $\mathfrak{D}_{A/R}^{-1}$ if and only if $\mathrm{Tr}_{L/K}(zx^i) = \alpha_i \in R$ for $i = 0, \dots, n_1$. Since $(r_{i,j}) \in \mathrm{GL}_n(R)$, the R-submodules generated by $y_1, \dots, y_n$ and $\frac{1}{f'(x)}, \dots, \frac{x^{n-1}}{f'(x)}$ coincide. □

Corollary 3.3.11 $\Delta_{L/K}(1, x, \dots, x^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(x))$.

Proof. Let $M \in \mathrm{GL}_n(K)$ be the matrix of the multiplication by $f'(x)$, in the basis $1, x, \dots, x^{n-1}$. By linearity of the trace, we have $\left(\mathrm{Tr}_{L/K}\left(\frac{x^i x^j}{f'(x)}\right)\right) = \left(\mathrm{Tr}_{L/K}\left(x^i x^j\right)\right) M^{-1}$. Thus

$$\begin{aligned} \Delta(1, x, \dots, x^{n-1}) &= \det\left(\mathrm{Tr}_{L/K}\left(x^i x^j\right)\right) \\ &= \det\left(\mathrm{Tr}_{L/K}\left(\frac{x^i x^j}{f'(x)}\right)\right)\det(M) \\ &= (-1)^{\frac{n(n-1)}{2}} N_{L/K}\left(f'(x)\right). \end{aligned}$$

□

Lemma 3.3.12 (Euler) $\mathrm{Tr}_{L/K}\left(\frac{x^i}{f'(x)}\right) = 0$ *for* $0 \le i \le n-2$ *and* $\mathrm{Tr}_{L/K}\left(\frac{x^{n-1}}{f'(x)}\right) = 1$.

Proof. Let $x_1 = x, x_2, \dots, x_n$ the roots of f in its splitting field. Decompose the rational fraction $\frac{1}{f(X)}$ into simple elements, substitute $Y = \frac{1}{X}$ and expand the geometric series:

$$\begin{aligned} \frac{1}{f(X)} &= \sum_{j=1}^n \frac{1}{f'(x_j)(X - x_j)} \\ &= \sum_{j=1}^n \frac{Y}{f'(x_j)} \frac{1}{(1 - x_j Y)} \\ &= \sum_{j=1}^n \frac{Y}{f'(x_j)}(1 + x_j Y + x_j^2 Y^2 + \dots + x_j^{n-1} Y^{n-1} + \dots) \\ &= \left(\sum_{j=1}^n \frac{1}{f'(x_j)}\right) Y + \left(\sum_{j=1}^n \frac{x_j}{f'(x_j)}\right) Y^2 + \dots + \left(\sum_{j=1}^n \frac{x_j^{n-1}}{f'(x_j)}\right) Y^n + \dots \\ &= \mathrm{Tr}_{L/K}\left(\frac{1}{f'(x)}\right) Y + \mathrm{Tr}_{L/K}\left(\frac{x}{f'(x)}\right) Y^2 + \dots + \mathrm{Tr}_{L/K}\left(\frac{x^{n-1}}{f'(x)}\right) Y^n + \dots \end{aligned} \tag{3.4}$$

the last equality follows from example 3.3.4. On the other hand, if $f(X) = a_0 + a_1 X + \dots + X^n$, we can expand directly

$$\frac{1}{f(X)} = \frac{1}{a_0 + a_1 \frac{1}{Y} + \dots + \frac{1}{Y^n}} = \frac{Y^n}{1 + \dots + a_1 Y^{n-1} + a_0 Y^n} = Y^n\left(1 + \sum_{h=1}^{\infty} c_h Y^h\right) \tag{3.5}$$

for suitable $c_i \in R$. The identities in the statement now follow by comparing the coefficients of $Y, Y^2, \ldots, Y^n$ in (3.4) and (3.5). □

Theorem 3.3.13 *Let $K \subseteq L$ be a finite field extension. The following are equivalent:*

a) L/K *is separable;*

b) $\mathrm{Tr}_{L/K} : L \times L \to K$ *is a non-degenerate bilinear form.*

Proof. If L/K is separable, we can invoke Abel's theorem to apply proposition 3.3.10 to conclude that the trace pairing is non-degenerate.
On the contrary, if L/K is not separable, one can find an intermediate extension $K \subseteq F \subseteq L$ such that

i) $[L : F] = p^m$ for some $m \geq 1$, where $p = \mathrm{char}\, K$;

ii) $x^p \in F$ for all $x \in L$.

Let us show that $\mathrm{Tr}_{L/K}(xy) = 0$ for all $y \in L$ and all $x \in L$ but $x \notin F$. There are two cases. If $xy \notin F$, since $a = (xy)^p \in F$, the minimal polynomial of xy over F is $T^p - a$. The characteristic polynomial of the multiplication map $\mu_{xy} : L \to L$ is $(T^p - a)^{p^{m-1}}$. Hence $\mathrm{Tr}_{L/F}(xy) = 0$. On the other hand, if $xy \in F$, we get $\mathrm{Tr}_{L/F}(xy) = xy\mathrm{Tr}_{L/F}(1) = xyp^m = 0$.
Either way, $\mathrm{Tr}_{L/F}(xy) = 0$ and by transitivity of the trace (proposition 3.3.3) we conclude that $\mathrm{Tr}_{L/K}(xy) = \mathrm{Tr}_{F/K}(\mathrm{Tr}_{L/F}(xy)) = \mathrm{Tr}_{F/K}(0) = 0$. □

Corollary 3.3.14 *Let R be an integrally closed domain, K its fraction field, $K \subseteq L$ a finite separable extension, A the integral closure of R in L. Then A is a submodule of a free R-module of rank $[L : K]$.*

Proof. Let $\{x_1, \ldots, x_n\}$ be a basis for L/K. Each x_i is algebraic. If $a_n x_i^n + \cdots + a_1 x_i + a_0 = 0$ with $a_j \in K$, $a_n \neq 0$, then multiplying by a common denominator of the a_j we may assume $a_j \in R$. Multiplying by a_n^{n-1} we get an integral equation $(a_n x_i)^n + \cdots + a_n^{n-2} a_1 (a_n x_i) + a_n^{n-1} a_0 = 0$ for $a_n x_i$.
Therefore, there exists a basis $\{y_1, \ldots, y_n\}$ be a basis for L/K with $y_i \in A$. Let $\{y_1^*, \ldots, y_n^*\}$ be the dual basis with respect to the trace form. For $x \in A$, let $x = \sum_{j=1}^n \alpha_j y_j^*$, with $\alpha_j \in K$. Then

$$\mathrm{Tr}_{L/K}(xy_i) = \sum_{j=1}^{n} \alpha_j \mathrm{Tr}_{L/K}(y_i y_j^*) = \alpha_i.$$

Since $xy_i \in A$ we conclude that $\alpha_i = \mathrm{Tr}_{L/K}(xy_i) \in R$. Hence $A \subseteq Ry_1^* \oplus \cdots \oplus Ry_n^*$. □

Corollary 3.3.15 *Let R be an PID, K its fraction field, L a finite separable extension of K and A the integral closure of R in L. Then A is a free R-module of finite rank $[L : K]$.*

Proof. As a submodule of a free R-module, A is torsion-free. Since A is a finitely generated, the claim follows from the elementary divisors theorem. □

§ 4 Valuation rings

In this section, K is a field and $R \subset K$ is a subring.

Definition 3.4.1 $R \subset K$ is a **valuation ring** if for every $x \in K^\times$ either $x \in R$ or $x^{-1} \in R$. As a consequence, K is the fraction field of R.

Example 3.4.2 For any prime number p, the ring $\mathbb{Z}_{(p)}$ is a valuation ring: let $\frac{a}{b} \in \mathbb{Q}^\times$ with $(a,b) = 1$. If $p|b$ (i.e. $\frac{a}{b} \notin \mathbb{Z}_{(p)}$), then $p \nmid a$, thus $\frac{b}{a} \in \mathbb{Z}_{(p)}$.

Example 3.4.3 If k is a field, the ring $k[X]_{(X)}$ is a valuation ring: let $\frac{f}{g} \in k(X)^\times$ with $(f,g) = 1$. If $X|g$ (i.e. $\frac{f}{g} \notin k[X]_{(X)}$), then $X \nmid f$, hence $\frac{g}{f} \in k[X]_{(X)}$.

Proposition 3.4.4 *Any valuation ring is a local ring, with maximal ideal* $\mathfrak{m} = \{x \in R \,|\, x^{-1} \notin R\}$.

Proof. The set $\mathfrak{m}$ is closed under multiplication: for any $x \in \mathfrak{m}$ and $y \in R$, if $xy \notin \mathfrak{m} \subset R$, then $(xy)^{-1} \in R$, therefore $x^{-1} = (xy)^{-1}y \in R$, which is a contradiction.
It is also closed under addition: if $x, z \in \mathfrak{m} - \{0\}$ then either $xz^{-1} \in R$ or $x^{-1}z \in R$. Say the first inclusion occurs, then $x + z = (xz^{-1} + 1)z \in \mathfrak{m}$.
Finally, if $u \in R$ but $u \notin \mathfrak{m}$ then $u^{-1} \in R$. Hence $R^\times = R - \mathfrak{m}$, thus R is a local ring. □

Example 3.4.5 The ring $k[X,Y]_{(X,Y)}$ is local but not a valuation ring: both $\frac{X}{Y}, \frac{Y}{X} \notin k[X,Y]_{(X,Y)}$.

Proposition 3.4.6 *Any valuation ring is integrally closed.*

Proof. Let $x \in K$ be integral over R, say $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, with $a_i \in R$. If $x \notin R$, then $x^{-1} \in R$, hence $x^{1-n} \in R$, therefore

$$x = x^{1-n}x^n = -x^{1-n}(a_{n-1}x^{n-1} + \cdots + a_0) = -a_{n-1} - \cdots - a_0x^{1-n} \in R$$

which is a contradiction. □

Valuation rings are intimately related to the integral closure of domains, as we shall see in theorem 3.4.9 below. We need a preliminary result.

Proposition 3.4.7 *Let K be a field and Σ the set of all subdomains $A \subset K$ which are local, with maximal ideal $\mathfrak{m}_A \neq 0$. Order Σ by $(A, \mathfrak{m}_A) \leq (B, \mathfrak{m}_B)$ if $A \subseteq B$ and $\mathfrak{m}_A = A \cap \mathfrak{m}_B$.*

a) If Σ is non-empty, it contains maximal elements.

b) For any subring $R \subset K$, R not a field, there exists a maximal element $A \in \Sigma$ such that $R \subseteq A$.

c) The maximal elements in Σ are the non-trivial valuation rings with fraction field K.

Proof. If $\{(A_n, \mathfrak{m}_{A_n})\}_n$ is a chain in Σ then $A = \bigcup_n A_n$ is a subdomain in K, local with maximal ideal $\mathfrak{m}_A = \bigcup_n \mathfrak{m}_{A_n}$. Hence Σ satisfies the assumptions of Zorn's lemma and has thus maximal elements. The same holds for the subset $\Sigma_R \subseteq \Sigma$ consisting of the A containing R. Notice that $\Sigma_R \neq \varnothing$: it contains $(R_\mathfrak{p}, \mathfrak{p}R_\mathfrak{p})$ for any prime $\mathfrak{p} \subset R$.
Let A be a valuation ring with fraction field K. As a local ring, it is belongs to Σ. Let $(B, \mathfrak{m}_B)$ be a local subdomain in K containing A; if B properly contains A, for any $b \in B$, $b \notin A$ we have $b^{-1} \in A$. Moreover $b^{-1} \notin A^\times$ (otherwise $b \in A^\times \subset A$), so $b^{-1} \in \mathfrak{m}_A \subseteq \mathfrak{m}_B$. This means that $\mathfrak{m}_B$ contains a unit, a contradiction. Valuation rings are thus maximal in Σ.

Conversely, let $(A, \mathfrak{m}_A)$ be a maximal element in Σ. Fix $0 \neq y \in K$ and consider the subrings $A[y]$ and $A[y^{-1}]$ of K. We shall prove that if both $y \notin A$ and $y^{-1} \notin A$ then either $A[y]$ or $A[y^{-1}]$ belongs to Σ, contradicting maximality. So either $y \in A$ or $y^{-1} \in A$, hence A is a valuation ring. Let us thus assume that both y and y^{-1} do not belong to A. We first check that either $\mathfrak{m}_A A[y]$ or $\mathfrak{m}_A A[y^{-1}]$ is a proper ideal. Otherwise, we would have

$$1 = a_0 + a_1 y + \cdots + a_n y^n, \qquad a_0, \ldots, a_n \in \mathfrak{m}_A; \tag{3.6}$$

$$1 = b_0 + b_1 y^{-1} + \cdots + b_m y^{-m}, \qquad b_0, \ldots, b_m \in \mathfrak{m}_A. \tag{3.7}$$

Since $\mathfrak{m}_A \neq A$, $m, n \geq 1$. Choose m, n minimal. By symmetry, we may assume $n \geq m$. From (3.7) we get $(1 - b_0)y^m = b_1 y^{m-1} + \cdots + b_m$. Multiplying (3.6) by $1 - b_0$ and substituting gives

$$1 - b_0 = a_0(1 - b_0) + \cdots + a_{n-1}(1 - b_0)y^{n-1} + a_n[b_1 y^{m-1} + \cdots + b_m]y^{n-m}$$

which is an equation like (3.6) but of degree strictly smaller than n, contradicting minimality. So either $\mathfrak{m}_A A[y]$ or $\mathfrak{m}_A A[y^{-1}]$ is a proper ideal. Say $\mathfrak{m}_A A[y] \subsetneq A[y]$ and pick a maximal ideal $\mathfrak{n}$ in $A[y]$ containing $\mathfrak{m}_A A[y]$. Notice that $\mathfrak{n} \cap A \supseteq \mathfrak{m}_A$ and the latter is maximal, hence $\mathfrak{n} \cap A = \mathfrak{m}_A$. Then $(A[y]_{\mathfrak{n}}, \mathfrak{n}) \in \Sigma$ with $(A, \mathfrak{m}_A) \leq (A[y], \mathfrak{n})$ and $A[y]$ properly containing A, contradicting the maximality of A. □

Example 3.4.8 The prime field $\mathbb{F}_p$ contains no local subrings.

Theorem 3.4.9 *Let K be a field, $R \subset K$ a subdomain which is not a field. The integral closure of R in K is the intersection of all the valuation rings of K containing R.*

Proof. Let $\widetilde{R}$ be the integral closure of R in K. If $R \subseteq A \subset K$ is a valuation ring, any $x \in K$ integral over R is integral over A, hence $x \in A$ because A is integrally closed. Thus $\widetilde{R}$ is contained in every valuation ring.
On the other hand, for $y \in K$, $y \notin \widetilde{R}$ we shall construct a valuation ring A of K with $y \notin A$. Consider $R[y^{-1}]$. The ideal $y^{-1}R[y^{-1}] \subseteq R[y^{-1}]$ is proper, otherwise $1 = a_1 y^{-1} + \cdots + a_n y^{-n}$ for suitable $a_i \in R$ and, multiplying by y^n, we would get $y^n = a_1 y^{n-1} + a_2 y^{n-2} + \cdots + a_n$, which implies y integral over R. Take any prime ideal $y^{-1}R[y^{-1}] \subseteq \mathfrak{p} \subset R[y^{-1}]$. By proposition 3.4.7 there exists a valuation ring $(A, \mathfrak{m}_A)$ in K with $A \supseteq R[y^{-1}]_{\mathfrak{p}}$ such that $\mathfrak{p}R[y^{-1}]_{\mathfrak{p}} = \mathfrak{m}_A \cap R[y^{-1}]_{\mathfrak{p}}$. In particular, $y^{-1} \in \mathfrak{p} \subseteq \mathfrak{m}_A$, so $y \notin A$. □

Another useful consequence of proposition 3.4.7 is the following existence theorem for extensions of valuation rings.

Theorem 3.4.10 *Let R be a valuation ring, K its fraction field and L a finite extension of K. There exists a valuation ring $A \subseteq L$ such that $R \subseteq A$.*

Proof. The statement is obvious if $R = K$. The non-trivial case follows immediately from proposition 3.4.7.b applied to $R \subset L$. □

Remark 3.4.11 Let R be a valuation ring and L a finite extension of $K = \operatorname{Frac} R$. By theorem 3.4.9, the integral closure $\widetilde{R}$ of R in L is contained in any valuation ring $R \subseteq A \subseteq L$. In general $\widetilde{R}$ has more than one maximal ideal, so can't be a valuation ring itself. We shall see in theorem 3.6.11 that $\widetilde{R}$ is a valuation ring if R is complete.

Definition 3.4.12 For any valuation ring R, denote $\Gamma = K^\times/R^\times$. The projection $v : K^\times \twoheadrightarrow \Gamma$ is called a **valuation**. The abelian group $\Gamma = K^\times/R^\times$ is ordered by the relation $v(x) \geq v(y)$ if $xy^{-1} \in R$. Notice that $R = \{x \in K^\times \,|\, v(x) \geq v(1) = 0\} \cup \{0\}$. We extend v to 0 by setting $v(0) = +\infty$.

Proposition 3.4.13 *The valuation map $v : K^\times \to \Gamma$ satisfies*

$$v(x+y) \geq \min\{v(x), v(y)\} \qquad \forall\ x, y \in K^*; \tag{3.8}$$

$$v(x+y) = \min\{v(x), v(y)\} \qquad \textit{if } v(x) \neq v(y). \tag{3.9}$$

Proof. Say $v(x) \geq v(y)$ (i.e. $xy^{-1} \in R$). Then $(x+y)y^{-1} = xy^{-1} + 1 \in R$, which is equivalent to $v(x+y) \geq v(y)$. This proves (3.8).
The inequality $v(x) > v(y)$ holds if and only if $xy^{-1} \in \mathfrak{m}$ (since $x^{-1}y \notin R$). In this case, $(x+y)y^{-1} \in 1+\mathfrak{m}$, so $(x+y)^{-1}y \in R$, hence $v(y) \geq v(x+y)$. Together with (3.8) we get (3.9). □

Remark 3.4.14 If Γ is an ordered abelian group, K a field and $v : K^\times \to \Gamma$ a group homomorphism satisfying (3.8), it is a simple exercise to check that $R = \{x \in K^\times \,|\, v(x) \geq 0\} \cup \{0\}$ is a valuation ring.

Example 3.4.15 Any field K is a valuation ring with the trivial valuation $v : K^\times \to \{0\}$. Notice that $R = K$ and $\mathfrak{m} = \{0\}$.

Example 3.4.16 Let p be prime number. Any nonzero integer $a \in \mathbb{Z}$ can be written uniquely as $a = up^{v_p(a)}$, with $(u, p) = 1$. For any $\frac{a}{b} \in \mathbb{Q}^\times$, set $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$. Obviously $v_p(x) \geq 0$ if and only if $x \in \mathbb{Z}_{(p)}$. The map $v_p : \mathbb{Q}^\times \to \mathbb{Q}^\times/\mathbb{Z}_{(p)}^\times \simeq \mathbb{Z}$ is called the **p-adic valuation** on $\mathbb{Q}$.

Example 3.4.17 Let k be a field. Any nonzero polynomial $f \in k[X]$ can be written uniquely as $f = X^{v_X(f)}h$, with $v_X(f) \in \mathbb{N}$ and $(h, X) = 1$. For any $\frac{f}{g} \in k(X)^\times$, set $v_X(\frac{f}{g}) = v_X(f) - v_X(g)$. Also in this case, for the valuation group we have $k(X)^\times/k[X]_{(X)}^\times \simeq \mathbb{Z}$.
In the same vein, any nonzero Laurent series $f = \sum_{i=n}^\infty a_i X^i \in k((X))$, with $a_n \neq 0$, setting $v_X(f) = n \in \mathbb{Z}$ defines a valuation and $k((X))^\times/k[[X]]^\times \simeq \mathbb{Z}$.

Definition 3.4.18 Valuation rings with valuation group isomorphic to $\mathbb{Z}$ are called **discrete**.

The algebraic properties of discrete valuation rings will be investigated in detail in § 5.1. For these, we'll get a much simpler proof of the existence theorem 3.4.10.

§ 5 Absolute values

Valuations can also be used to introduce very useful analytic tools. The starting point is to notice that a real-valued valuation on a field induces a metric (example 3.5.4 below). Let us begin with a more general definition:

Definition 3.5.1 An **absolute value** on a field K is a map $|\ | : K \longrightarrow \mathbb{R}$ satisfying:

a) $|x| \geq 0$ for all $x \in K$ and $|x| = 0$ if and only if $x = 0$;

b) $|xy| = |x||y|$ for all $x, y \in K$;

c) $|x + y| \leq |x| + |y|$ for all $x, y \in K$ (triangle inequality).

We say that $|\ |$ is **non-archimedean** if the following stronger condition holds:

c') $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in K$.

If $(K, |\ |)$ and $(K', |\ |')$ are fields with an absolute value, an embedding $\varphi : K \to K'$ is an **isometric embedding** if $|x| = |\varphi(x)|'$ for all $x \in K$.

Remark 3.5.2 If $|\ |$ is non-archimedean and $|x| \neq |y|$, then $|x + y| = \max\{|x|, |y|\}$. Indeed, suppose $|x| < |y|$. On the one hand $|x + y| \leq \max\{|x|, |y|\} = |y|$. On the other

$$|y| = |x + y - x| \leq \max\{|x + y|, |x|\} = |x + y|$$

(if $\max\{|x + y|, |y|\} = |x|$, we would get $|y| \leq |x|$, a contradiction).

Example 3.5.3 The usual modulus

$$|x| = \begin{cases} x & x \geq 0 \\ -x & x \leq 0 \end{cases}$$

is an absolute value on $\mathbb{Q}$ and $\mathbb{R}$. We shall denote it $|\ |_\infty$. The complex modulus $|z| = \sqrt{z\overline{z}}$ is an absolute value on $\mathbb{C}$.

Example 3.5.4 Let $v : K^\times \to \Gamma$ be a valuation with values in a subgroup $\Gamma \subseteq \mathbb{R}$ (e.g. a discrete valuation). Choose a real number $0 < c < 1$ and put $|x|_v = c^{v(x)}$ for $x \neq 0$ and $|0|_v = 0$. Then $|\ |_v$ is a non-archimedean absolute value on K: axioms a) and b) follow because $v : K^\times \to \Gamma$ is a group homomorphism and the triangle inequality follows from proposition 3.4.13: if $v(y) \leq v(x)$ then

$$|x + y|_v = c^{v(x+y)} \leq c^{v(y)} = |y|_v = \max\{|x|_v, |y|_v\}.$$

For example, any field can be given the **trivial absolute value**, defined by $|0| = 0$ and $|x| = 1$ for $x \neq 0$. It is attached to the trivial valuation of example 3.4.15.
More interesting is the **p-adic absolute value** on $\mathbb{Q}$, attached to the p-adic valuation, given by $|0|_p = 0$ and $|x|_p = p^{-v_p(x)}$ for $x \neq 0$ (i.e. we have chosen $c = \frac{1}{p}$).

We have used here a lax notation: the absolute value attached to the valuation v also depends on the choice of the constant c, so we should rather write $|\ |_{c,v}$. Changing the constant will raise the absolute value to an exponent:

$$|x|_{b,v} = b^{v(x)} = c^{\frac{v(x)}{\log_b c}} = |x|_{c,v}^{\frac{1}{\log_b c}}.$$

The absolute values $|\ |_{c,v}$ and $|\ |_{b,v}$ are thus equivalent in the sense of the next definition.

Definition 3.5.5 Two absolute values $|\ |_1$ and $|\ |_2$ on a field K are **equivalent** if there exists a real number $\alpha > 0$ such that $|x|_2 = |x|_1^\alpha$ for all $x \in K$.

It is trivial to check that this notion defines an equivalence relation on the set of all possible absolute values on K. In the literature, an equivalence class of absolute values on a field is called a **place**, and sometimes also a valuation. The latter term is justified by the following

Proposition 3.5.6 *Let $|\ |$ be a non-trivial non-archimedean absolute value on a field K. Then*

$$R = \{x \in K \mid |x| \leq 1\}$$

is a valuation ring with maximal ideal $\mathfrak{m} = \{x \in K \mid |x| < 1\}$ and units $R^\times = \{x \in K \mid |x| = 1\}$. Two equivalent non-archimedean absolute values on K define the same ring.

Proof. It follows immediately from the axioms in definition 3.5.1 that R is closed under addition and multiplication. Notice that $|1| = |1|^2$, hence $|1| = 1$, since $|\ |$ is nontrivial (if $|1| = 0$ then $|x| = |1||x| = 0$ for all $x \in K$). Therefore $1 \in R$. This also implies that $|-1|^2 = 1$, thus $|-1| = 1$ and then $|-x| = |x|$ for all $x \in K$, which implies that R is an abelian group and thus a ring. For $x \in K^\times$, from $|xx^{-1}| = |1| = 1$ it follows that $|x^{-1}| = |x|^{-1}$, so R is a valuation ring: if $|x| > 1$, then $|x^{-1}| < 1$. The statement on equivalent absolute values is also obvious. □

Example 3.5.7 Let k be a field, $|\ |$ the absolute value on $k((X))$ induced by the valuation v_X of example 3.4.17. Then $k[[X]] = \{f \in k((X)) \mid |f| \leq 1\}$ and $Xk[[X]] = \{f \in k((X)) \mid |f| < 1\}$.

There is a simple test to check whether an absolute value on a field K is archimedean or not. Recall from example 1.1.15 that there is a canonical ring homomorphism $\varphi : \mathbb{Z} \to K$ given by $\varphi(n) = n \cdot 1$.

Lemma 3.5.8 *An absolute value $|\ |$ on a field K is non-archimedean if and only if $\{|\varphi(n)|\}_{n\in\mathbb{Z}} \subset \mathbb{R}$ is a bounded set.*

Proof. If $|\ |$ is non-archimedean, it follows from c') that $|\varphi(n)| = |1+\cdots+1| \leq \max\{1, \ldots, 1\} = 1$, so the set is bounded. Conversely, suppose $|\varphi(n)| \leq B$ for all $n \in \mathbb{Z}$ and let $x, y \in K$. For all $n \in \mathbb{N}$ we have

$$|x+y|^n = \left|\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right|^n \leq \left|\sum_{k=0}^{n} \binom{n}{k}\right| |x|^k |y|^{n-k} \leq (n+1)B \max\{|x|, |y|\}^n.$$

Therefore $|x+y| \leq (n+1)^{\frac{1}{n}} B^{\frac{1}{n}} \max\{|x|, |y|\}$ for all $n \in \mathbb{N}$. Taking the limit for $n \to \infty$ we get the strict triangle inequality c'). □

Corollary 3.5.9 *Any absolute value on a field of positive characteristic is non-archimedean.*

Theorem 3.5.10 (Ostrowski) *Any nontrivial absolute value on $\mathbb{Q}$ is equivalent to $|\ |_\infty$ or to $|\ |_p$ for some prime number p.*

Proof. Let $m > 1$ be an integer. Any $\nu \in \mathbb{Z}$ can be written uniquely as $\nu = a_k m^k + \cdots + a_1 m + a_0$, with $0 \leq a_i < m$ and $\nu \leq m^k$. Let $M = \max\{1, |m|\}$. We have

$$|\nu| \leq \sum_{i=0}^{k} |a_i||m|^i \leq \sum_{i=0}^{k} |a_i| M^k. \tag{3.10}$$

Since $a_i < m$, we have $|a_i| = |1 + 1 + \cdots + 1| \leq a_i|1| < m$. Since $k \leq \frac{\log \nu}{\log m}$, from (3.10) we get:

$$|\nu| \leq (k+1)mM^k \leq \left(\frac{\log \nu}{\log m} + 1\right) mM^{\frac{\log \nu}{\log m}}. \tag{3.11}$$

Applying (3.11) to $\nu = n^t$ and taking t-roots on both sides we get

$$|n| \leq \left(t\frac{\log n}{\log m} + 1\right)^{\frac{1}{t}} m^{\frac{1}{t}} M^{\frac{\log n}{\log m}}$$

for every integer $n \in \mathbb{Z}$ and every $t \in \mathbb{N}$. Taking the limit for $t \to \infty$ we get

$$|n| \leq M^{\frac{\log n}{\log m}} = \max\{1, |m|\}^{\frac{\log n}{\log m}} \qquad \forall\, n \in \mathbb{Z}. \tag{3.12}$$

There are now two cases. If $|m| > 1$ for all integers $m > 1$, inequality (3.12) yields $|n|^{\frac{1}{\log n}} \leq |m|^{\frac{1}{\log m}}$ for all $n, m > 1$, hence by symmetry $|n|^{\frac{1}{\log n}} = |m|^{\frac{1}{\log m}}$. Writing $c = |n|^{\frac{1}{\log n}} \in \mathbb{R}$ for the constant value of these expressions, we get $|n| = c^{\log n}$ for all $n > 1$. Since $|\ |$ is multiplicative, we get $|\frac{n}{m}| = c^{\log \frac{n}{m}}$ for all positive rational numbers and, since $|-x| = |x|$ we conclude that $|x| = c^{\log |x|_\infty}$ for all $x \in \mathbb{Q}^\times$. Therefore $|x| = |x|_\infty^\alpha$ for all $x \in \mathbb{Q}$, with $\alpha = \log c$.

On the contrary, suppose that there exists an integer $m > 1$ such that $|m| \leq 1$. Then inequality (3.12) yields $|n| \leq 1$ for all integers, so $|\ |$ is non-archimedean by lemma 3.5.8. By proposition 3.5.6, $R = \{x \in \mathbb{Q} \,|\, |x| \leq 1\}$ is a subring of $\mathbb{Q}$ containing $\mathbb{Z}$ and $\{x \in \mathbb{Q} \,|\, |x| < 1\} \cap \mathbb{Z} = p\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. It can't be the zero ideal, otherwise $|m| = 1$ for all $m \in \mathbb{Z} - \{0\}$ and, by multiplicativity of $|\ |$ this would imply that $|x| = 1$ for all $x \in \mathbb{Q}^\times$, contrary to the assumption that $|\ |$ is nontrivial. Now every $x \in \mathbb{Q}$ can be written uniquely as $x = up^{v_p(x)}$, with $u \in \mathbb{Z}_{(p)}^\times$. Therefore $|x| = |p^{v_p(x)}| = |p|^{v_p(x)}$, hence $|x| = |x|_p^\alpha$, with $\alpha = -\log_p |p|$. □

§ 6 Completion

Definition 3.6.1 Let K be a field with an absolute value $|\ |$. A sequence $\{a_n\}_{n\in\mathbb{N}}$ in K

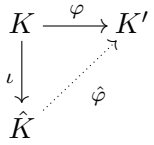
a) **converges** to $a \in K$ if for every $\varepsilon > 0$ there exists $N_\varepsilon \in \mathbb{N}$ such that $|a_n - a| < \varepsilon$ for all $n \geq N_\varepsilon$.

b) is a **Cauchy sequence** if for every $\varepsilon > 0$ there exists an $N_\varepsilon \in \mathbb{N}$ such that $|a_n - a_m| < \varepsilon$ for all $n, m \geq N_\varepsilon$.

It is elementary to check that a convergent sequence is Cauchy. The field $(K, |\ |)$ is **complete** if every Cauchy sequence converges.

It is well known from calculus that $\mathbb{R}$ and $\mathbb{C}$ are complete fields. The field of Laurent series is complete: since checking this directly is quite messy, we shall rather get it as a byproduct of the technique of completion (corollary 3.6.19 below). The classical construction of $\mathbb{R}$ from $(\mathbb{Q}, |\ |_\infty)$ by adjoining all the limits of Cauchy sequences can be carried out in the general setting.

Theorem 3.6.2 *Let K be a field with an absolute value $|\ |$. There exists a field $\hat{K}$, complete with respect to an absolute value also denoted $|\ |$ and an isometric embedding $\iota : K \hookrightarrow \hat{K}$ such that for every complete field K' and isometric embedding $\varphi : K \hookrightarrow K'$, there exists an isometric embedding $\hat{\varphi} : \hat{K} \to K'$ such that $\varphi = \hat{\varphi} \circ \iota$.*



The pair $(\hat{K}, \iota)$ is unique up to unique isomorphism and called the **completion** *of K with respect to $|\ |$.*

Proof. The unicity is clear from the universal property. Let $CS(K)$ the set of all Cauchy sequences in K and $NS(K)$ the subset of null sequences, i.e sequences $\{a_n\} \in CS(K)$ such that $\lim_{n\to\infty} |a_n| = 0$. Using standard calculus techniques, one can show (exercise 3.8) that $CS(K)$ is a ring with termwise addition and multiplication and $NS(K)$ is a maximal ideal. Let $\hat{K} = CS(K)/NS(K)$ and denote $[a_n]$ the class of $\{a_n\}$. Define $|[a_n]| = \lim_{n\to\infty} |a_n|$. This is clearly well defined and provides an absolute value on $\hat{K}$. Embedding $K \subset CS(K)$ as the constant sequences and projecting onto $\hat{K}$ we get an isometric embedding $\iota : K \hookrightarrow \hat{K}$. The universal property is also clear: if $\varphi : K \to K'$ is an isometric embedding and $\{a_n\}$ is a Cauchy sequence in K then $|a_n - a_m| = |\varphi(a_n - a_m)|' = |\varphi(a_n) - \varphi(a_m)|'$, so $\{\varphi(a_n)\}$ is Cauchy and we can define $\tilde{\varphi} : CS(K) \to K'$ by $\tilde{\varphi}(\{a_n\}) = \lim_{n\to\infty} \varphi(a_n)$. If $\{a_n\} \in NS(K)$, then $|\tilde{\varphi}(\{a_n\})|' = \lim_{n\to\infty} |\varphi(a_n)|' = \lim_{n\to\infty} |a_n| = 0$, so $\tilde{\varphi}(\{a_n\}) = 0$, hence $NS(K) \subseteq \ker \tilde{\varphi}$ and this defines the map $\hat{\varphi}$. As a nonzero field homomorphism preserving absolute values, $\hat{\varphi}$ is an isometric embedding.
The tricky bit is to show that $\hat{K}$ is complete. Let $\{\alpha_n\}_{n\in\mathbb{N}}$ be a Cauchy sequence in $\hat{K}$ i.e. for each $n \in \mathbb{N}$, α_n is the class of a Cauchy sequence $\{\alpha_{n,\nu}\}_{\nu\in\mathbb{N}}$ in K. To say that $\{\alpha_n\}$ is Cauchy in $\hat{K}$ means that for every $\varepsilon > 0$ there exists N_ε such that

$$|\alpha_n - \alpha_m| = |[\alpha_{n,\nu}] - [\alpha_{m,\nu}]| = \lim_{\nu\to\infty} |\alpha_{n,\nu} - \alpha_{m,\nu}| < \varepsilon \tag{3.13}$$

for $n, m \geq N_\varepsilon$. Fix $n \in \mathbb{N}$. Since $\{\alpha_{n,\nu}\}_{\nu\in\mathbb{N}}$ is a Cauchy sequence, there exists an integer M_n such that $|\alpha_{n,\nu} - \alpha_{n,\mu}| < \frac{1}{n}$ for all $\nu, \mu \geq M_n$. Put $a_n = \alpha_{n,M_n}$. This defines a sequence $\{a_n\}$ in K such that $|\alpha_n - a_n| < \frac{1}{n}$. Let us check that $\{a_n\} \in CS(K)$: for every $\varepsilon > 0$ we have

$$|a_n - a_m| = |a_n - \alpha_n + \alpha_n - \alpha_m + \alpha_m - a_m| \leq |a_n - \alpha_n| + |\alpha_n - \alpha_m| + |\alpha_m - a_m| \leq \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon$$

for all $n, m \geq \max\{N_{\frac{\varepsilon}{3}}, \frac{3}{\varepsilon}\}$. We are done if we show that $\{\alpha_n\}$ converges to $\alpha = [a_n]$ in $\hat{K}$. But for every $\varepsilon > 0$ we have

$$|\alpha_n - \alpha| = |\alpha_n - a_n + a_n - \alpha| \leq |\alpha_n - a_n| + |a_n - \alpha| = |\alpha_n - a_n| + \lim_{\nu\to\infty} |a_n - a_\nu| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

for all $n \geq \max\{N_{\frac{\varepsilon}{6}}, \frac{6}{\varepsilon}\}$. □

Corollary 3.6.3 *If $|\ |$ is a non-archimedean absolute value on K, then $\hat{K}$ is also non-archimedean.*

Proof. Follows from lemma 3.5.8, since the canonical map $\varphi : \mathbb{Z} \to \hat{K}$ factors through K. □

Corollary 3.6.4 *If $|\ |$ is an absolute value on K induced by a discrete valuation, then $|K| = |\hat{K}| \subset \mathbb{R}$.*

Proof. Indeed, representing any $\alpha \in \hat{K}$ as $\alpha = [a_n]$, we have $|\alpha| = \lim_{n\to\infty} |a_n|$ and the values $|a_n|$ range in the discrete group $c^{\mathbb{Z}} \subset \mathbb{R}$, so $|a_n|$ is constant for large n. □

Remark 3.6.5 If K is a discrete valuation field, we may in fact represent every $\alpha \in \hat{K}$ by a sequence $\{a_n\}_{n\in\mathbb{N}}$ with $|a_n| = |\alpha|$ for all $n \in \mathbb{N}$: we know that there exists an N such that $|a_n| = |\alpha|$ for $n \geq N$ and we may replace $\{a_n\}$ by the sequence $\{a'_n\}$ defined as $a'_n = a_N$ for $n \leq N$ and $a'_n = a_n$ for $n \geq N$ without changing the class mod $NS(K)$.

Example 3.6.6 The completion $\mathbb{Q}_p$ of $\mathbb{Q}$ with respect to the p-adic absolute value $|\ |_p$ is the field of **p-adic numbers**. Elements in the ring $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \,|\, |x| \leq 1\}$ are called **p-adic integers**.

In order to investigate finite extensions of complete fields, it is convenient to discuss vector spaces over such fields.

Definition 3.6.7 Let K be a field with an absolute value $|\ |$ and V a K-vector space. A **norm** on V compatible with $|\ |$ is a function $\|\ \| : V \to \mathbb{R}$ such that

a) $\|\mathbf{v}\| \geq 0$ for all $\mathbf{v} \in V$ and $\|\mathbf{v}\| = 0$ if and only if $\mathbf{v} = \mathbf{0}$;

b) $\|x\mathbf{v}\| = |x|\|\mathbf{v}\|$ for all $x \in K$ and $\mathbf{v} \in V$;

c) $\|\mathbf{v} + \mathbf{w}\| \leq \|\mathbf{v}\| + \|\mathbf{w}\|$ for all $\mathbf{v}, \mathbf{w} \in V$ (triangle inequality).

Two norms $\|\ \|_1$ and $\|\ \|_2$ on V compatible with $|\ |$ are **equivalent** if there exist $c_1, c_2 \in \mathbb{R}$ such that $c_1\|\mathbf{v}\|_1 \leq \|\mathbf{v}\|_2 \leq c_2\|\mathbf{v}\|_1$ for all $\mathbf{v} \in V$.

Definition 3.6.8 Let K be a field with an absolute value $|\ |$ and V a K-vector space with a compatible norm $\|\ \|$. A sequence $\{\mathbf{v}_n\}_{n\in\mathbb{N}}$ in V

a) **converges** to $\mathbf{v} \in V$ if for every $\varepsilon > 0$ there exists $N_\varepsilon \in \mathbb{N}$ such that $\|\mathbf{v}_n - \mathbf{v}\| < \varepsilon$ for all $n \geq N_\varepsilon$.

b) is a **Cauchy sequence** if for every $\varepsilon > 0$ there exists an $N_\varepsilon \in \mathbb{N}$ such that $\|\mathbf{v}_n - \mathbf{v}_m\| < \varepsilon$ for all $n, m \geq N_\varepsilon$.

We say that V is **complete** if every Cauchy sequence converges.

Example 3.6.9 If $V = K^d$ then $\|(x_1, \ldots, x_d)\|_{\max} = \max\{|x_1|, \ldots, |x_d|\}$ is a compatible norm. If K is complete, K^d is clearly complete, since taking coordinates in a Cauchy sequence of vectors yields a Cauchy sequence in K.

Proposition 3.6.10 *Let K be a field complete with respect to a nontrivial absolute value and V a finite dimensional vector space. Any two compatible norms on V are equivalent and V is complete.*

Proof. Choose a basis $\{\mathbf{e}_1, \dots, \mathbf{e}_d\}$ of V and write each vector as $\mathbf{v} = x_1(\mathbf{v})\mathbf{e}_1 + \cdots + x_d(\mathbf{v})\mathbf{e}_d$. This gives an isomorphism $V \simeq K^d$ and a norm $\| \ \|_{\max}$ on V for which V is complete. Let $\| \ \|$ be any other norm on V: we are done if we prove that $\| \ \|$ and $\| \ \|_{\max}$ are equivalent. Clearly

$$\|\mathbf{v}\| \leq \sum_{i=1}^{d} |x_i(\mathbf{v})| \|\mathbf{e}_i\| \leq \max_{i=1,\dots,d} \|\mathbf{e}_i\| \cdot \sum_{i=1}^{d} |x_i(\mathbf{v})| \leq c_2 \|\mathbf{v}\|_{\max}$$

where $c_2 = d \max\{\|\mathbf{e}_i\|\}$. To prove inequality $c_1\|\mathbf{v}\|_{\max} \leq \|\mathbf{v}\|$, replacing $\mathbf{v}$ by a non-zero multiple, we may assume that $\|\mathbf{v}\| \leq 1$. We proceed by induction on d. If $d = 1$ the claim is trivial: $\mathbf{v} = x_1(\mathbf{v})\mathbf{e}_1$ hence $c_1 = \|\mathbf{e}_1\|$. So assume that every $(d-1)$-dimensional K-vector space is complete and all norms on it are equivalent. Let us first assume that for each $i = 1, \dots, d$ there exists $b_i \in \mathbb{R}$ such that

$$|x_i(\mathbf{v})| \leq b_i \qquad \forall\ \mathbf{v} \text{ such that } \|\mathbf{v}\| \leq 1. \tag{3.14}$$

Fix $\pi \in K$ such that $0 < |\pi| < 1$. For $\mathbf{0} \neq \mathbf{v} \in V$, let $m \in \mathbb{N}$ such that $|\pi^{m+1}| \leq \|\mathbf{v}\| \leq |\pi^m|$. Then

$$\|\mathbf{v}\|_{\max} = \max_{i=1,\dots,d} |x_i(\mathbf{v})| = |\pi^m| \max_{i=1,\dots,d} \left| x_i\left(\frac{\mathbf{v}}{\pi^m}\right)\right| \leq |\pi^m| \max_{i=1,\dots,d} b_i \leq \left(|\pi|^{-1} \max_{i=1,\dots,d} b_i\right) \|\mathbf{v}\|$$

hence $c_1\|\mathbf{v}\|_{\max} \leq \|\mathbf{v}\|$ for all $\mathbf{v} \in V$, with $c_1 = |\pi|(\max\{b_i\})^{-1}$.
We now use the induction assumption to prove bound (3.14) for the coordinate x_1 (the general case follows by permutation). Suppose that the values $|x_1(\mathbf{v})|$ are unbounded: for every $n \in \mathbb{N}$, there exists a vector $\mathbf{v}_n$ with $\|\mathbf{v}_n\| \leq 1$ and $|x_1(\mathbf{v}_n)| \geq n$. For $n \geq 1$, let $\mathbf{u}_n = \frac{1}{x_1(\mathbf{v}_n)}\mathbf{v}_n$. Then

$$\|\mathbf{u}_n\| = \frac{\|\mathbf{v}_n\|}{|x_1(\mathbf{v}_n)|} \leq \frac{1}{n}$$

so the sequence $\{\mathbf{u}_n\}$ converges to $\mathbf{0}$ in V. By construction, $\mathbf{u}_n = \mathbf{e}_1 + x_2(\mathbf{u}_n)\mathbf{e}_2 + \cdots + x_d(\mathbf{u}_n)\mathbf{e}_d$, so the sequence $\{x_2(\mathbf{u}_n)\mathbf{e}_2 + \cdots + x_d(\mathbf{u}_n)\mathbf{e}_d\}$ converges to $-\mathbf{e}_1$. But the latter is a sequence of vectors in the subspace $V' =< \mathbf{e}_2, \dots, \mathbf{e}_d >$ which has dimension $d-1$ and is thus complete by inductive assumption. Hence $\mathbf{e}_1 \in V'$, contradicting the fact that $\{\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_d\}$ is a basis. □

Theorem 3.6.11 *Let K be a field, complete with respect to a nontrivial non-archimedean absolute value $|\ |$ and L a finite extension of K. There exists a unique absolute value on L, also denoted $|\ |$, such that $K \subseteq L$ is an isometric embedding. L is complete for this absolute value. The valuation ring of L is the integral closure of the valuation ring of K.*

Proof of uniqueness. Two extensions $|\ |_1$ and $|\ |_2$ of $|\ |$ to L define two compatible norms on the finite dimensional vector space L, so by proposition 3.6.10 they are equivalent in the sense of definition 3.6.7. Let $0 \neq y \in L$ such that $|y|_1 < 1$. Then the sequence $\{y^n\}$ converges to 0 in L for the norm $|\ |_1$ and thus also for the equivalent norm $|\ |_2$: this forces $|y|_2 < 1$. Now fix $x \in K$ with $0 < |x| < 1$ and consider the positive real number $\frac{\log|y|_1}{\log|x|}$. For any rational $\frac{n}{m} \geq \frac{\log|y|_1}{\log|x|}$ we have $|x|^n \leq |y|_1^m$, hence $\left|\frac{x^n}{y^m}\right|_1 \leq 1$, thus $\left|\frac{x^n}{y^m}\right|_2 \leq 1$ and therefore $|x|^n \leq |y|_2^m$, which implies $\frac{n}{m} \geq \frac{\log|y|_2}{\log|x|}$. In a similar way, one proves that any rational $\frac{n}{m} \leq \frac{\log|y|_1}{\log|x|}$ satisfies $\frac{n}{m} \leq \frac{\log|y|_2}{\log|x|}$. Taking sequences or rational numbers approaching from above and from below, we conclude

that $\frac{\log|y|_1}{\log|x|} = \frac{\log|y|_2}{\log|x|}$, hence $|y|_1 = |y|_2$ for all $y \in L$ such that $|y|_1 < 1$. It suffices now to remark that for any $y \in L$ there is a $z \in K$ such that $|zy|_1 < 1$ and then compute

$$|y|_1 = \frac{|yz|_1}{|z|} = \frac{|yz|_2}{|z|} = |y|_2.$$

Proof of existence. Let $R = \{x \in K \mid |x| \leq 1\}$ and recall from theorem 3.4.10 that we have a valuation ring $R \subseteq A \subset L$. To get an absolute value on L, we need to show that the valuation group $L^\times/A^\times$ is a subgroup of $\mathbb{R}$, as in example 3.5.4. We have a commutative diagram

$$\begin{array}{ccc} K^\times & \xrightarrow{v} & K^\times/R^\times \\ \downarrow & & \downarrow \\ L^\times & \xrightarrow{w} & L^\times/A^\times \end{array}$$

where the horizontal maps are the valuations and the vertical ones are induced by the inclusion $K \subseteq L$. Any $y \in L^\times$ is algebraic over K: take a minimal equation $a_n y^n + \cdots + a_1 y + a_0 = 0$ with $a_i \in K$ and $n \leq [L : K]$. If there exists $j \leq n$ such that $a_j \neq 0$ and $w(a_j y^j) > w(a_i y^i)$ for all other $i \leq n$ such that $a_i \neq 0$, then by condition (3.9) in proposition 3.4.13 we get $w(a_j y^j) = w(a_n y^n + \cdots + a_1 y + a_0) = w(0) = +\infty$, which is absurd. Therefore there exist $i \neq j$ such that $w(a_i y^i) = w(a_j y^j)$. Hence $w(y^{i-j}) = w(a_j a_i^{-1}) = v(a_j a_i^{-1}) \in K^\times/R^\times$. Therefore

$$\begin{array}{rcl} \sigma : L^\times/A^\times & \longrightarrow & L^\times/A^\times \\ y & \longmapsto & y^{[L:K]!} \end{array}$$

maps $L^\times/A^\times$ to $K^\times/R^\times$. The map σ is injective: if $y^n = 1$ then $y \in A$ because A is integrally closed. We thus get the injection $L^\times/A^\times \xrightarrow{\sigma} K^\times/R^\times \hookrightarrow \mathbb{R}$ we were looking for.

Finally, by theorem 3.4.9 the integral closure in L of the valuation ring R of K is the intersection of all the valuation rings of L containing R. In the proof of existence, we have shown that any such valuation ring corresponds to an absolute value on L and we know that there is only one of those. □

Now that we know that an extension exists, we can give a formula for it:

Corollary 3.6.12 *Let K be a field, complete with respect to a nontrivial non-archimedean absolute value $|\ |$ and L a finite extension of K. For any $y \in L$*

$$|y| = \left|N_{L/K}(y)\right|^{\frac{1}{[L:K]}} \tag{3.15}$$

is the unique absolute value on L such that $K \subseteq L$ is an isometric embedding.

Proof. Pick a finite normal extension $K \subseteq L \subseteq E$. Then there is also a unique extension of $|\ |$ to E. For any K-linear automorphism $\sigma : E \to E$ define $|\ |_\sigma$ by $|z|_\sigma = |\sigma(z)|$. This is clearly an absolute value and $|x|_\sigma = |x|$ for all $x \in K$. By uniqueness $|\ |_\sigma = |\ |$, so $|z| = |\sigma(z)|$ for all $z \in E$. For $z \in E$ we have $N_{E/K}(z) = \prod_\sigma \sigma(z)$ where σ ranges among all K-linear automorphisms of E (see example 3.3.4). Then for all $y \in L$

$$\left|N_{L/K}(y)\right| = \left|N_{E/K}(y)\right|^{\frac{1}{[E:L]}} = \left|\prod_\sigma \sigma(y)\right|^{\frac{1}{[E:L]}} = |y|^{\frac{[E:K]}{[E:L]}} = |y|^{[L:K]}.$$

□

Remark 3.6.13 We could try to define an absolute value directly by formula (3.15), bypassing the existence part of theorem 3.6.11. Clearly (3.15) satifies conditions a) and b) in definition 3.5.1 and coincides with $|\ |$ on K, but checking condition c) is subtler. See exercise 3.13.

Remark 3.6.14 Theorem 3.6.11 also holds for fields with an archimedean absolute value. In fact, a much stronger result holds: any field complete with respect to an archimedean absolute value is isometrically isomorphic to either $\mathbb{R}$ or $\mathbb{C}$. See [3]. theorem II.4.1. Formula (3.15) also fits: if $z = x + iy$ then $N_{\mathbb{C}/\mathbb{R}}(z) = x^2 + y^2$ and $|z| = \sqrt{x^2 + y^2}$.

Let us now discuss in more detail completions of fields with a nontrivial discrete valuation.

Lemma 3.6.15 *Let K be a field with a nontrivial discrete valuation v and $\hat{K}$ its completion. Then the maximal ideals $\mathfrak{m} = \{x \in K \mid |x| < 1\}$ and $\hat{\mathfrak{m}} = \{\xi \in \hat{K} \mid |\xi| < 1\}$ are principal and any generator of $\mathfrak{m}$ also generates $\hat{\mathfrak{m}}$.*

Proof. The ideal $\mathfrak{m}$ is generated by any element $\pi \in K$ such that $v(\pi) = 1 \in \mathbb{Z} = K^\times/R^\times$, since for any $x \in \mathfrak{m}$ we can write $x = \pi^{v(x)}u$ and $v(u) = 0$ so $u \in R^\times$. By corollary 3.6.4, for any $\xi \in \hat{\mathfrak{m}}$, there is an $x \in \mathfrak{m}$ such that $|\xi| = |x|$; then $|\xi\pi^{-v(x)}| = 1$, so it is a unit and $\xi = \left(\xi\pi^{-v(x)}\right)\pi^{v(x)}$. □

If K is a field with a non-archimedean absolute value and $\{\alpha_n\}$ is a Cauchy sequence in $\hat{R} = \{\alpha \in \hat{K} \mid |\alpha| \leq 1\}$, its limit α is also in $\hat{R}$, because $|\alpha| \leq 1 + \varepsilon$ for all $\varepsilon > 0$, as can be seen by writing $|\alpha| = |\alpha - \alpha_n + \alpha_n| \leq |\alpha - \alpha_n| + 1$. For an arbitrary absolute value, we can't reasonably expect a sequence in $\hat{\mathfrak{m}}$ to converge in $\hat{\mathfrak{m}}$, as a sequence of real numbers strictly smaller than 1 may very well converge to 1. But if the valuation is discrete, then $\hat{\mathfrak{m}} = \{\alpha \in \hat{K} \mid |\alpha| \leq |\pi|\}$, and so the limit of any Cauchy sequence in $\hat{\mathfrak{m}}$ belongs to $\hat{\mathfrak{m}}$. Of course, the same property holds for the ideals $\hat{\mathfrak{m}}^n = \{\alpha \in \hat{K} \mid |\alpha| \leq |\pi|^n\}$, generated by π^n. We can be more precise:

Proposition 3.6.16 *Let K be a field with a nontrivial discrete valuation and $\hat{K}$ its completion. Then for every $n \in \mathbb{N}$ the inclusion $R \subseteq \hat{R}$ induces an isomorphism $R/\mathfrak{m}^n \cong \hat{R}/\hat{\mathfrak{m}}^n$.*

Proof. Let $\alpha \in \hat{R} - \hat{\mathfrak{m}}$, represented by a sequence $\{a_n\}_{n\in\mathbb{N}}$. By remark 3.6.5, we may assume $|a_n| = 1 = |\alpha|$ for all n. Since $\{a_n\}$ is Cauchy, there exists $N \in \mathbb{N}$ such that $|a_n - a_m| < |\pi|$ for all $n \geq N$ (as before, π denotes a generator of $\mathfrak{m}$). Replacing $\{a_n\}$ by a sequence whose first N terms are equal to $a = a_N$ as in remark 3.6.5, we may assume that $a_n \equiv a \bmod \mathfrak{m}$ for all $n \in \mathbb{N}$. Therefore $\alpha \in a + \hat{\mathfrak{m}}$. We conclude that $\hat{R} = R + \hat{\mathfrak{m}}$. We can refine further: take $\xi \in \hat{R}$, write it as $\xi = x + \pi\eta$, with $x \in R$ and $\eta \in \hat{R}$; then $\eta \equiv y \bmod \hat{\mathfrak{m}}$ for some $y \in R$, hence $\xi \in x + \pi y + \hat{\mathfrak{m}}^2$. Repeating, we conclude that $\hat{R} = R + \hat{\mathfrak{m}}^n$ for all n. Since $\hat{\mathfrak{m}}^n = \pi^n\hat{R}$, we have $\hat{\mathfrak{m}}^n \cap R = \mathfrak{m}^n$. Thus

$$\hat{R}/\hat{\mathfrak{m}}^n = \left(R + \hat{\mathfrak{m}}^n\right)/\hat{\mathfrak{m}}^n \cong R/\left(R \cap \hat{\mathfrak{m}}^n\right) = R/\mathfrak{m}^n$$

where the isomorphism is provided by proposition 1.2.21. □

The proposition suggest an alternative representation for elements in $\hat{K}$. Fix a generator π for $\mathfrak{m}$ and a subset $S \subset R$ consisting of one representative for each element in the field $R/\mathfrak{m}$. We assume that $0 \in S$ has been chosen.

Lemma 3.6.17 *Every element $\alpha \in \hat{K}$ can be written uniquely as a formal power series*

$$\alpha = \pi^m(s_0 + s_1\pi + \cdots + s_n\pi^n + \dots)$$

where $m \in \mathbb{Z}$ is defined by $|\alpha| = |\pi|^m$ and $s_i \in S$ with $s_0 \neq 0$.

Proof. It clearly suffices to check the case $m = 0$, i.e. $\alpha \in \hat{R}^\times$. By definition, there exists a unique $0 \neq s_0 \in S$ representing α mod $\mathfrak{m}$. Moreover $\alpha - s_0 = \pi\alpha_1$ for a unique $\alpha_1 \in \hat{R}$. If $\alpha_1 \in \hat{\mathfrak{m}}^{n_1}$, set $s_1 = \cdots = s_{n_1-1} = 0$ and let $s_{n_1} \in S$ be the unique representative of $\alpha_1\pi^{-n_1}$ mod $\hat{\mathfrak{m}}$. Then $\alpha - (s_0 + \cdots + s_{n_1}\pi^{n_1}) = \pi^{n_1+1}\alpha_2$ for a unique $\alpha_2 \in \hat{R}$. Repeating the process, we obtain the power series expansion of α. □

Notice that the series $\sum_{n=0}^{\infty} s_n\pi^n$ converges in $\hat{K}$. Indeed the sequence $a_n = \sum_{i=0}^{n} s_i\pi^i$ is a Cauchy sequence: for $m \leq n$

$$|a_n - a_m| = \left|\sum_{i=m}^{n} s_i\pi^i\right| \leq \max_{i=m,\dots,n} |s_i||\pi|^i \leq \max_{i=m,\dots,n} |\pi|^i = |\pi|^m < \varepsilon \quad \forall\, m, n > \log_{|\pi|}\varepsilon.$$

Corollary 3.6.18 *Let R be a discrete valuation ring, $\mathfrak{m}$ the maximal ideal, $\pi \in \mathfrak{m}$ a generator and $k = R/\mathfrak{m}$. If R is a k-algebra, there exists a k-algebra isomorphism $\varphi : \hat{R} \simeq k[[X]]$ such that $\varphi(\pi) = X$.*

Proof. Indeed, we may take $S = k$ in lemma 3.6.17. □

Corollary 3.6.19 *$k((X))$ is the completion of $k(X)$ with respect to the valuation v_X.*

Example 3.6.20 p-adic numbers are usually expanded as $x = p^m(s_0 + s_1p + \cdots + s_np^n + \dots)$ with $s_i \in S = \{0, \dots, p-1\}$. Sometimes, it is more convenient to choose $S = \{0, 1, \zeta, \dots, \zeta^{p-2}\}$, where $\zeta \in \mathbb{Z}_p$ is a $p-1$-th root of unity (see example 3.6.34 below), since an expansion with a multiplicative set of representatives S is preserved under multiplication of power series.

Corollary 3.6.21 *Let R be a complete discrete valuation ring, L a finite extension of $K = \operatorname{Frac} R$ and A the integral closure of R in L. Then A is a discrete valuation ring, free of rank $[L : K]$ as R-module.*

Proof. With notation as in the existential part of the proof of theorem 3.6.11, we have an injection $L^\times/A^\times \xrightarrow{\sigma} K^\times/R^\times \simeq \mathbb{Z}$, so the valuation group of L is a subgroup of $\mathbb{Z}$, hence cyclic of infinite order. Therefore A is a discrete valuation ring.
Let $\mathfrak{m} \subset R$ be the maximal ideal, $\pi \in \mathfrak{m}$ a generator and $k = R/\mathfrak{m}$. Let $x_1, \dots, x_r \in A$ and $\alpha_1x_1 + \cdots + \alpha_rx_r = 0$ a K-linear relation in L. Multiplying by a suitable power of π, we may assume that $\alpha_i \in R$ for all i and at least one of the α_i is a unit. Reducing mod $\mathfrak{m}$ we get that the x_i are k-linearly dependent. Hence $\dim_k A/\mathfrak{m}A \leq [L : K]$.
Suppose now that the reduction mod $\mathfrak{m}$ of $x_1, \dots, x_r \in A$ is a basis of $A/\mathfrak{m}A$ and let $A' \subseteq A$ be the R-submodule generated by the x_i. Let $y \in A$. There exist $z_0 \in A'$ and $y_1 \in A$ such that $y = z_0 + \pi y_1$. Apply the same argument to y_1 and repeat to construct a sequence $y'_n = z_0 + \pi z_1 \cdots + \pi^n z_n$ in A' such that $|y - y'_n| \leq |\pi|^{n+1}$ for all n. Therefore $\lim_{n\to\infty} y'_n = y$. On the other hand, let $V \subseteq L$ be the K-subspace generated by $x_1, \dots, x_n$. The absolute value on L restricts to a norm on V and $A' = V \cap A$. By proposition 3.6.10, V is complete, so $y \in V \cap A = A'$.
We have thus that A is a finitely generated module over the PID R. It is torsion-free, hence free by the elementary divisors' theorem, of rank $r = \dim_k A/\mathfrak{m}A$. Hence $r = \dim_K A \otimes_R K = \dim_K L = [L : K]$. □

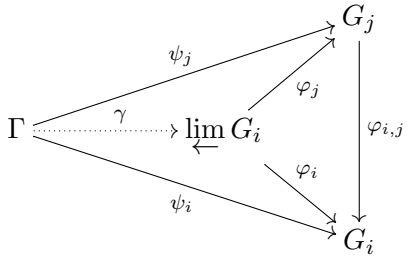
Remark 3.6.22 The proof of corollary 3.6.21 presents a typical situation where one is tempted to apply Nakayama's lemma wrongly: conclude right away that the inclusion $A' \subseteq A$ is an identity because the two R-modules coincide mod $\mathfrak{m}$. We can't do that, because we don't know yet that A is finitely generated.

Proposition 3.6.16 is also a bridge towards another type of completion, valid for general rings, that plays a major role in Algebraic Geometry and Number theory. It is based on the notion of inverse, or projective, limit.

Definition 3.6.23 Let I be a partially ordered set. We say that I is **directed** if for every $i, j \in I$ there exists $k \in I$ such that $i \leq k$ and $j \leq k$.

For instance, a totally ordered set is directed: this is in fact the case we shall restrict to most of the time. Example 3.6.26 illustrates the interest of the more general notion.

Definition 3.6.24 An **inverse system** of groups (rings, modules) $\{(G_i, \varphi_{i,j})\}_{i \in I}$ is a collection of groups (rings, modules) indexed by a directed set and homomorphisms $\varphi_{i,j} : G_j \to G_i$ for every $i \leq j$ in I such that $\varphi_{i,j} \circ \varphi_{j,k} = \varphi_{i,k}$ for every $i \leq j \leq k$. The **inverse limit** of the system is a group (ring, module) $\varprojlim G_i$, equipped with a homomorphism $\varphi_i : \varprojlim G_i \to G_i$ such that $\varphi_i = \varphi_{i,j} \circ \varphi_j$ for every $i \leq j$ and such that for every group (ring, module) Γ with morphisms $\psi_j : \Gamma \to G_i$ such that $\psi_i = \varphi_{i,j} \circ \psi_j$ for all $i \leq j$, there exists a unique morphism $\gamma : \Gamma \to \varprojlim G_i$ such that $\psi_j = \varphi_j \circ \gamma$.



The universal property in the definition makes the inverse limit unique up to unique isomorphism. It can be constructed as the subset of the direct product $\prod_i G_i$ consisting of *coherent sequences* i.e. elements $(\dots, x_i, \dots)$ such that $\varphi_{i,j}(x_j) = x_i$. One checks immediately that the set of coherent sequences forms a subgroup (ring, module) of $\prod_i G_i$. The map φ_i is just the restriction of the projection onto the i-th factor. As for the universal property, given Γ as above, define $\gamma(y) = (\dots, \psi_i(y), \dots)$.

Example 3.6.25 Let $\{(G_n, \iota_n)\}$ be a chain of subgroups of a group G, with $\iota_n : G_{n+1} \hookrightarrow G_n$ the inclusion maps. Then $\varprojlim G_n = \bigcap_{n \in \mathbb{N}} G_n$, as one easily checks from the universal property.

Example 3.6.26 Let K be a field and K^{sep} its separable closure. The collection of all intermediate extensions $K \subseteq L \subseteq K^{\mathrm{sep}}$ such that L is finite and Galois over K is a directed set. If $K \subseteq E \subseteq L$ is an intermediate extension, the Galois correspondence yields a map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$. We obtain thus an inverse system and the absolute Galois group of K is defined as $\mathrm{Gal}(K^{\mathrm{sep}}/K) = \varprojlim \mathrm{Gal}(L/K)$.

Example 3.6.27 If R is a discrete valuation ring with maximal ideal $\mathfrak{m}$ then $\hat{R} \cong \varprojlim R/\mathfrak{m}^n$. Indeed, proposition 3.6.16 gives rise to a sequence of maps $\hat{R} \to R/\mathfrak{m}^n$, so by the universal property we get a morphism $\gamma : \hat{R} \to \varprojlim R/\mathfrak{m}^n$. For the inverse map, notice that if $(\dots, x_n, \dots)$ is coherent sequence, for all $n, m \in \mathbb{N}$ we have $x_{m+n} \equiv x_m \bmod \mathfrak{m}^n$. Choosing arbitrary representatives $\tilde{x}_n \in R$, we get a sequence $\{\tilde{x}_n\}$ in R which is Cauchy: $|\tilde{x}_{n+m} - \tilde{x}_n| \leq |\pi|^n$. One checks immediately that $\lim_{n\to\infty} \tilde{x}_n \in \hat{R}$ does not depend on the choice of the liftings, hence $(\dots, x_n, \dots) \mapsto \lim_{n\to\infty} \tilde{x}_n$ defines an inverse map to γ.

This prompts the following

Definition 3.6.28 Let R be a ring, $\mathfrak{a} \subset R$ an ideal and M an R-module. The ring $\hat{R}_\mathfrak{a} = \varprojlim R/\mathfrak{a}^n$ (resp. the module $\hat{M}_\mathfrak{a} = \varprojlim M/\mathfrak{a}^n M$) is called the **$\mathfrak{a}$-adic completion** of R (resp. M).

When the ideal $\mathfrak{a}$ is understood, we shall often drop it from the notation. The universal property provides a map $R \to \hat{R}_\mathfrak{a}$ (which is just $x \mapsto (\dots, x, \dots)$) whose kernel is $\bigcap_n \mathfrak{a}^n$. Notice that $\mathfrak{a}^n = \ker[R \to \hat{R}_\mathfrak{a}/\hat{\mathfrak{a}}^n]$, so $R/\mathfrak{a}^n \hookrightarrow \hat{R}/\hat{\mathfrak{a}}^n$: it is an isomorphism because $\hat{R}_\mathfrak{a} \to R/\mathfrak{a}^n \to \hat{R}/\hat{\mathfrak{a}}^n$ is surjective. Hence the $\hat{\mathfrak{a}}$-adic completion of $\hat{R}_\mathfrak{a}$ is again $\hat{R}_\mathfrak{a}$. This justifies the definition:

Definition 3.6.29 Let R be a ring, $\mathfrak{a} \subset R$ an ideal. We say that R is **$\mathfrak{a}$-adically complete** if the natural map $R \to \hat{R}_\mathfrak{a}$ is an isomorphism.

Remark 3.6.30 If R is $\mathfrak{a}$-adically complete, then $\mathfrak{a}$ is in the Jacobson radical $\mathfrak{R}_R$: indeed for any $x \in 1 + \mathfrak{a}$ the sequence $(\dots, \sum_{k=0}^n (-1)^k x^k, \dots)$ is coherent and thus defines an element $y \in R$ (we could rephrase this by saying that the geometric series $\sum_{k=0}^\infty (-1)^k x^k$ converges in R) such that $(1+x)y = 1 + z$ with $z = (\dots, (-1)^n x^{n+1}, \dots)$. Since $\varphi_n(z) = (-1)^n x^{n+1} = 0$ in $R/\mathfrak{a}^n$, we conclude that $z = 0$, hence $1 + x \in R^\times$. From proposition 1.1.56 we conclude $\mathfrak{a} \subseteq \mathfrak{R}_R$.

The remark explains why the completions most often considered are with respect to maximal ideals. Nevertheless, general adic completions can be useful, as in the following example.

Example 3.6.31 Let R be a ring, $A = R[X_1, \dots, X_m]$ and $\mathfrak{a} = (X_1, \dots, X_m)$. The $\mathfrak{a}$-adic completion of A is formal power series ring $R[[X_1, \dots, X_m]]$. Indeed for all n we have an obvious map $R[[X_1, \dots, X_m]] \to R[X_1, \dots, X_m]/\mathfrak{a}^n$, whence a map $R[[X_1, \dots, X_m]] \to \hat{A}_\mathfrak{a}$ by universal property. Any coherent sequence can be represented as $(\dots, f_n, \dots)$ where the $f_n \in A$ and $f_{n+1} - f_n \in \mathfrak{a}^{n+1}$. Whence an inverse map $(\dots, f_n, \dots) \mapsto f_1 + \sum_{n\geq 1}(f_{n+1} - f_n)$.

The following classical result well illustrates the usefulness of completions.

Proposition 3.6.32 (Hensel's Lemma) *Let R be a local ring, $\mathfrak{m}$ its maximal ideal and $k = R/\mathfrak{m}$. Let $F \in R[X]$ be a polynomial whose reduction $\overline{F} \in k[X]$ mod $\mathfrak{m}$ is not identically 0. Suppose that $g, h \in k[X]$ are coprime polynomials such that $gh = \overline{F}$. If R is $\mathfrak{m}$-adically complete, there exist $G, H \in R[X]$ such that $\overline{G} = g$, $\deg G = \deg g$, $\overline{H} = h$, $\deg H \leq \deg F - \deg g$ and $F = GH$.*

Proof. Starting from arbitrary polynomials $G_1 \equiv g$ and $H_1 \equiv h \bmod \mathfrak{m}$, with $\deg G_1 = \deg g > 0$, we shall construct inductively polynomials $G_n, H_n \in R[X]$ such that

$$G_{n+1} \equiv G_n \bmod \mathfrak{m}^n; \qquad H_{n+1} \equiv H_n \bmod \mathfrak{m}^n; \qquad F \equiv G_n H_n \bmod \mathfrak{m}^n \tag{3.16}$$

with $\deg H_n \leq \deg F - \deg g$ and such that G_{n+1} and G_n have the same leading coefficient. If we manage that, then writing $G_n = \sum_p b_{p,n}X^p$ and $H_n = \sum_q c_{q,n}X^q$, for every p, q we obtain sequences $(\dots, b_{p,n}, \dots)$ and $(\dots, c_{q,n}, \dots)$ which are coherent by the first two congruences in (3.16), hence converge to elements $b_p, c_q \in R$, and we define $G = \sum_p b_p X^p$ and $H = \sum_q c_q X^q$. Since the sequence of leading coefficients is constant, $\deg G = \deg g$. Moreover, if $F = \sum_r a_r X^r$, the last congruence in (3.16) shows that $a_r = \sum_{p+q=r} b_p c_q$ because their difference is in $\mathfrak{m}^n$ for all n. Hence $F = GH$.

Suppose G_n, H_n have been constructed, so $F - G_n H_n = \sum_i t_i L_i$ with $t_i \in \mathfrak{m}^n$, $L_i \in R[X]$ and $\deg L_i \leq \deg F$. Since $(g, h) = 1$ we can find $u_i, v_i \in k[X]$ such that $L_i \equiv u_i g + v_i h \bmod \mathfrak{m}$. Without loss of generality, we may assume $\deg v_i < \deg g$ and $\deg u_i \leq \deg F - \deg g$. Indeed writing $v_i = v_i'' g + v_i'$ with $\deg v_i' < \deg g$ and setting $u_i' = u_i + v_i''$, we have $L_i \equiv u_i' g + v_i' h$ and $\deg u_i' g = \deg(\overline{L}_i - v_i' h) \leq \deg F$, hence $\deg u_i' \leq \deg F - \deg g$.
Now choose $U_i, V_i \in R[X]$ such that $U_i \equiv u_i$ and $V_i \equiv v_i \bmod \mathfrak{m}$ with $\deg V_i = \deg v_i < \deg g$ and $\deg U_i = \deg u_i \leq \deg F - \deg g$. Then $G_{n+1} = G_n + \sum_i t_i V_i$ and $H_{n+1} = H_n + \sum_i t_i U_i$ satisfy (3.16) and

$$F - G_{n+1}H_{n+1} = \sum_i t_i(L_i - G_n U_i - H_n V_i) - \sum_{i,j} t_i t_j U_i V_j \equiv 0 \bmod \mathfrak{m}^{n+1}.$$

□

Corollary 3.6.33 *Let R be a complete local ring with residue filed k. Let $F \in R[X]$ be a monic polynomial whose reduction $\overline{F} \in k[X]$ factors as the product of two coprime monic polynomials $g, h \in k[X]$. Then there exist $G, H \in R[X]$ monic such that $\overline{G} = g$, $\deg G = \deg g$, $\overline{H} = h$, $\deg H = \deg h$ and $F = GH$.*

Proof. Follows from the proof of Hensel's lemma: we can impose the sequence of leading coefficients in H_n to be constant as that of the G_n. Indeed, since F, G_n, H_n are monic, from the expression $F - G_n H_n = \sum_i t_i L_i$ we get $\deg L_i < \deg F$ and all the inequalities derived from this one are strict. □

Example 3.6.34 $\mathbb{Z}_p$ contains the $p-1$-th roots of unity, since $X^{p-1} - 1 \equiv \prod_{i=1}^{p-1}(X - i) \bmod p$.

We conclude by discussing exactness properties of inverse limits and completions. Given three inverse systems of R-modules $\{(M_n, \varphi_n)\}$, $\{(M_n', \varphi_n')\}$ and $\{(M_n'', \varphi_n'')\}$ indexed by the integers, an exact sequence of inverse systems will be a compatible system of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M'_{n+1} & \xrightarrow{f_{n+1}} & M_{n+1} & \xrightarrow{g_{n+1}} & M''_{n+1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi'_n} & & \downarrow{\scriptstyle \varphi_n} & & \downarrow{\scriptstyle \varphi''_n} & & \\ 0 & \longrightarrow & M'_n & \xrightarrow{f_n} & M_n & \xrightarrow{g_n} & M''_n & \longrightarrow & 0. \end{array} \tag{3.17}$$

Proposition 3.6.35 *Any exact sequence of inverse systems (3.17) induces an exact sequence*

$$0 \longrightarrow \varprojlim M'_n \xrightarrow{f} \varprojlim M_n \xrightarrow{g} \varprojlim M''_n.$$

If the maps φ_n' are surjective for all $n \in \mathbb{N}$, then g is surjective.

Proof. The system defines a commutative diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \prod_n M'_n & \xrightarrow{f} & \prod_n M_n & \xrightarrow{g} & \prod_n M''_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \delta'} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta''} & & \\ 0 & \longrightarrow & \prod_n M'_n & \xrightarrow{f} & \prod_n M_n & \xrightarrow{g} & \prod_n M''_n & \longrightarrow & 0 \end{array}$$

where $\delta(\dots, m_n, \dots) = (\dots, \varphi_n(m_{n+1}) - m_n, \dots)$ and the two other maps are defined similarly. Since $\ker\delta = \varprojlim M_n$, the first claim is a consequence of the snake lemma. The second claim follows as well if we show that δ' is surjective. Given $(\dots, x_n, \dots) \in \prod_n M'_n$ we have to solve the system

$$\begin{cases} x_1 &= \varphi'_1(Y_2) - Y_1 \\ x_2 &= \varphi'_2(Y_3) - Y_2 \\ \vdots &= \quad \vdots \end{cases}$$

and this can be done by the surjectivity of the maps φ'_n: take $y_1 = 0$, choose $y_2 \in M'_2$ such that $\varphi'_2(y_2) = x_1$, then $y_3 \in M'_3$ such that $\varphi'_2(y_3) = x_2 + y_2$ and so on. □

Let R be a ring, $\mathfrak{a} \subset R$ an ideal. Write $\hat{M}$ for the $\mathfrak{a}$-adic completion of an R-module M and consider the functor $\mathbf{Mod}_R \to \mathbf{Mod}_{\hat{R}}$ taking M to $\hat{M}$. It follows easily from proposition 3.6.35 that this functor is additive, but its exactness properties are more delicate. It is certainly not left exact: $0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q}$ is an exact sequence of $\mathbb{Z}$-modules but for any prime p, since $\mathbb{Q}/p^n\mathbb{Q} = 0$, taking p-adic completion we get $0 \longrightarrow \mathbb{Z}_p \longrightarrow 0$ which is most definitely not exact. The only positive result that holds in general is the following:

Lemma 3.6.36 *With notation as above, if $M \longrightarrow M'' \longrightarrow 0$ is exact, then $\hat{M} \longrightarrow \hat{M}'' \longrightarrow 0$ is exact.*

Proof. Let $M' = \ker[M \longrightarrow M'']$. For every $n \geq 1$ we have an exact sequence

$$0 \longrightarrow M'/(M' \cap \mathfrak{a}^n M) \longrightarrow M/\mathfrak{a}^n \longrightarrow M''/\mathfrak{a}^n M'' \longrightarrow 0.$$

These build up to an exact sequence of inverse systems. We can conclude by proposition 3.6.35, since the maps $M'/(M' \cap \mathfrak{a}^{n+1}M) \to M'/(M' \cap \mathfrak{a}^n M)$ are surjective. □

A better behaved functor $\mathbf{Mod}_R \to \mathbf{Mod}_{\hat{R}}$ is $M \mapsto \hat{R} \otimes M$. As a tensor product, it is right-exact and it is exact for noetherian rings (corollary 3.6.42 below). To compare the two functors, notice that the R-linear map $M \to \hat{M}$ given by the universal property induces $\hat{R}$-linear maps

$$\hat{R} \otimes_R M \longrightarrow \hat{R} \otimes_R \hat{M} \longrightarrow \hat{R} \otimes_{\hat{R}} \hat{M} \cong \hat{M}. \tag{3.18}$$

In general, the composite is neither injective nor surjective (and the middle module quite nasty).

Proposition 3.6.37 *For any finitely generated R-module M, the map $\hat{R} \otimes_R M \to \hat{M}$ is surjective.*

Proof. Choose a presentation $0 \longrightarrow N \longrightarrow R^n \xrightarrow{\pi} M \longrightarrow 0$ and tensor with $\hat{R}$ to get

$$\begin{array}{ccccccccc} & & \hat{R} \otimes_R N & \longrightarrow & \hat{R} \otimes_R R^r & \xrightarrow{id_{\hat{R}^n} \otimes \pi} & \hat{R} \otimes_R M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \lambda_{R^n}} & & \downarrow{\scriptstyle \lambda_M} & & \\ 0 & \longrightarrow & \varprojlim N/(N \cap \mathfrak{a}^n R^r) & \longrightarrow & \hat{R}^n & \xrightarrow{\hat{\pi}} & \hat{M} & \longrightarrow & 0 \end{array} \tag{3.19}$$

where λ_{R^n} and λ_M are the maps in (3.18) and γ is induced by the universal property of inverse limits. The top row is exact because tensor products are right-exact and the bottom row is exact by proposition 3.6.35. Since λ_{R^n} is an isomorpism (the functor $M \mapsto \hat{M}$ is additive), it follows from the snake lemma that λ_M is surjective. □

This is as far as the theory for general rings may go. Sharper results are obtained assuming that the ring R is noetherian, a condition that will be investigated in the next chapter.

Proposition 3.6.38 *Let R be a noetherian ring, $\mathfrak{a} \subset R$ and ideal and $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ an exact sequence of finitely generated R-modules. Then $0 \longrightarrow \hat{M}'_{\mathfrak{a}} \longrightarrow \hat{M}_{\mathfrak{a}} \longrightarrow \hat{M}''_{\mathfrak{a}} \longrightarrow 0$ is exact.* ⊠

Remark 3.6.39 Unlike other situations, where we can remove the noetherian assumption by taking finitely presented instead of just finitely generated modules, this result requires a finer analysis. For the (same) proof, see [1], proposition 10.12, [2], lemma 7.15 or [8] theorem 54.

Corollary 3.6.40 *Let R be a noetherian ring, $\mathfrak{a}$ an ideal. Then for any finitely generated R-module M, the map $\hat{R}_{\mathfrak{a}} \otimes_R M \to \hat{M}_{\mathfrak{a}}$ is an isomorphism.*

Proof. Every finitely generated module over a noetherian ring is finitely presented (corollary 4.1.9), so, with notation as in the proof of proposition 3.6.37, in diagram (3.19) we may replace $\varprojlim N/(N \cap \mathfrak{a}^n R^r)$ by $\hat{N}$ and γ by λ_N. Then λ_N is surjective too and, since λ_{R^n} is an isomorpism, the snake tells us that $\ker \lambda_M = 0$. □

Corollary 3.6.41 *If R is a noetherian ring and $\mathfrak{a}$ an ideal, then $\hat{\mathfrak{a}} = \mathfrak{a}\hat{R}_{\mathfrak{a}}$.*

Proof. $\mathfrak{a}$ is finitely generated by proposition 4.1.5, so we can apply corollary 3.6.40. □

Corollary 3.6.42 *If R is a noetherian ring and $\mathfrak{a}$ an ideal, then $\hat{R}_{\mathfrak{a}}$ is a flat R-algebra.*

§ 7 Exercises

Exercise 3.1 Let R be a integrally closed domain with fraction field K and $\mathfrak{p}$ a prime ideal. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in R[X]$ be an **Eisenstein polynomial** with respect to $\mathfrak{p}$, i.e. $a_i \in \mathfrak{p}$ for $i = 0, \ldots, n-1$ and $a_0 \notin \mathfrak{p}^2$.

a) Check that if $g, h \in K[X]$ are monic polynomials such that $f = g \cdot h$ then $g, h \in R[X]$. [Hint: consider a splitting field of f]

b) Show that f is irreducible.

Exercise 3.2 Let k be a field of characteristic different from 2. Show that $k[X,Y]/(X^2 + Y^2 - 1)$ is an integrally closed domain. What if the characteristic of k is 2?

Exercise 3.3 Let R be a ring, $\varphi : R \to R[X]$ the natural map.

a) Does φ have the Going Down property?

b) Let k be a field. Does $k[X] \subset k[X,Y]$ have the Going Up property? [Hint: take $\mathfrak{p}_1 = \{0\} \subset \mathfrak{p}_2 = (X)$ and $\mathfrak{q}_1 = (XY-1)$]

Exercise 3.4 Let A be a valuation ring, $L = \operatorname{Frac} A$. Let $K \subseteq L$ be a subfield and $R = A \cap K$.

a) Show that R is a valuation ring.

b) Show that if A is a discrete valuation ring, then so is R.

Exercise 3.5 Let k be a field of characteristic 2 and $k[[X]]$ the formal power series. Let $f \in k[[X]]$, $f \neq 0$ and put $K = k(X)(f^2)$, $L = k(X)(f)$, subfields of $k((X))$. Set $R = k[[X]] \cap K$ and $A = k[[X]] \cap L$.

a) Show that $[L : K] \leq 2$, with equality if f transcendental over $k(X)$.

b) Show that R and A are discrete valuation rings.

c) Show that A is the integral closure of R in L.

d) Suppose that A is finite over R. Show that $X^m A \subseteq R + Rf$ for a suitable $m \in \mathbb{N}$.

e) Write $f = \sum_{n=0}^{\infty} \alpha_n X^n \in k[[X]]$ and let $g = \sum_{n=m+1}^{\infty} \alpha_n X^n \in k[[X]]$, with m as in d). Show that $g \in A$.

f) Assume now $[L : K] = 2$, consider $X^m g \in R + Rf$ and compute the coefficient of f. Conclude that A is not finite over R.

Exercise 3.6 Let K be a field, $|\ | : K \to \mathbb{R}$ a map satisfying conditions a) and b) in definition 3.5.1 and furthermore

c'') $|x+1| \leq 1$ for all $x \in K$ such that $|x| \leq 1$

Show that $|\ |$ is a non-archimedean absolute value on K.

Exercise 3.7 Let k be a field and c a real number with $0 < c < 1$. Let $f(X), u(X), v(X) \in k[X]$ be polynomials, with f irreducible and not dividing u nor v. Define

$$\left|\frac{u(X)}{v(X)} f(X)^n\right|_f = c^{-n} \text{ (for } n \in \mathbb{Z}); \qquad \left|\frac{u(X)}{v(X)}\right|_\infty = c^{\deg v - \deg u}.$$

a) Check that $|\ |_f$ and $|\ |_\infty$ define non-archimedean absolute values on the field $k(X)$ of rational functions in the variable X.

b) Let $Y = X^{-1}$. Show that the absolute value $|\ |_\infty$ on $k(X) = k(Y)$ concides with the absolute value $|\ |_Y$ defined by the irreducible polynomial $Y \in k[Y]$.

c) Let $|\ |$ be a nontrivial absolute value on $k(X)$ such that $|a| = 1$ for each $0 \neq a \in k$. Show that $|\ |$ is equivalent to $|\ |_\infty$ or to $|\ |_f$ for some $f \in k[X]$.

Exercise 3.8 Let K be a field with an absolute value $|\ |$. Let $CS(K)$ the set of all Cauchy sequences in K and $NS(K)$ the subset of null sequences, i.e sequences $\{a_n\} \in CS(K)$ such that $\lim_{n\to\infty} |a_n| = 0$.

a) Show that every Cauchy sequence $\{a_n\}$ in K is bounded: there exists $A \in \mathbb{R}$ such that $|a_n| \leq A$ for all $n \in \mathbb{N}$.

b) Show if $\{a_n\}$ and $\{b_n\}$ are Cauchy sequences, then $\{a_n + b_n\}$ and $\{a_n b_n\}$ are a Cauchy sequences.

c) Show that $CS(K)$ is a ring and $NS(K)$ is an ideal.

d) Let $\{a_n\} \in CS(K) - NS(K)$. Show that $a_n \neq 0$ for n sufficiently large.

e) For $\{a_n\}$ as in d), construct a sequence $\{u_n\} \in CS(K)^\times$ such that $\{a_n\} - \{u_n\} \in NS(K)$.

f) Conclude that $NS(K)$ is a maximal ideal.

Exercise 3.9 Let R be a ring, $\mathfrak{a} \subset R$ an ideal and assume that R is $\mathfrak{a}$-adically complete. Let $F(X) \in R[X]$ and $x_0 \in R$ such that $F(x_0) \in \mathfrak{a}$ and $F'(x_0) \in R^\times$. Show that the sequence $x_{n+1} = x_n - \frac{F(x_n)}{F'(x_0)}$ converges to an element $x \in R$ such that $F(x) = 0$ and $x \equiv x_0 \bmod \mathfrak{a}$.

Exercise 3.10 Let R be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals such that $\mathfrak{a}^e \subseteq \mathfrak{b} \subseteq \mathfrak{a}$ for some integer $e \geq 1$. Let $\{\mathfrak{a}^n/\mathfrak{b}^n, \varphi_n)\}$ be the inverse system with φ_n induced by the inclusions $\mathfrak{a}^{n+1} \subseteq \mathfrak{a}^n$. Show that $\varprojlim \mathfrak{a}^n/\mathfrak{b}^n = 0$.

Exercise 3.11 Show that theorem 3.6.11 also holds for the trivial valuation.

Exercise 3.12 Let $F(X) = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$, where K is a complete field with a discrete valuation v. Show that if F is irreducible, $\min\{v(a_i) \mid i = 0, \ldots, n\} = \min\{v(a_0), v(a_n)\}$. [Hint: reduce to $\min\{v(a_i) \mid i = 0, \ldots, n\} = 0$, suppose $v(a_0), v(a_n) > 0$ and apply Hensel's lemma.]

Exercise 3.13 Let K be a field, complete with respect to a discrete valuation, L a finite extension of K. Show (without using theorem 3.6.11) that $|N_{L/K}(-)|^{\frac{1}{[L:K]}}$ defines an absolute value on L. [Hint: use exercises 3.6 and 3.12.]

Chapter IV

Noetherian rings and modules

§ 1 Chain conditions

Recall that a set Σ is partially ordered if it admits a reflexive and transitive relation $\leq$ such that

$$\begin{cases} x \leq y \\ y \leq x \end{cases} \quad \Longrightarrow \quad x = y.$$

Lemma 4.1.1 *Let $(\Sigma, \leq)$ be a partially ordered set. The following conditions are equivalent:*

a) Every non-empty subset $S \subseteq \Sigma$ contains a maximal element;

b) Every sequence $x_1 \leq x_2 \leq \dots$ in Σ is stationary (i.e. $\exists\, n_0 \in \mathbb{N}$ such that $x_n = x_{n+1}\ \forall\, n \geq n_0$).

Proof. Suppose that every $\varnothing \neq S \subseteq \Sigma$ contains a maximal element and let $x_1 \leq x_2 \leq \dots$ be a sequence in Σ. Put $S = \{x_n \mid \forall\, n \in \mathbb{N}\}$ and get $n_0 \in \mathbb{N}$ such that x_{n_0} is a maximal element in S. Conversely, assume every sequence in Σ is stationary and suppose $\varnothing \neq S \subseteq \Sigma$ has no maximal element. Start from any $x_1 \in S$ and construct a sequence inductively: given $x_1 \leq \cdots \leq x_n$, let $S_n = \{x \in S,\ x \gneq x_n\}$. This set is non-empty (otherwise $x_n \in S$ is maximal), so pick $x_{n+1} \in S_n$. Repeat to obtain a non-stationary sequence, a contradiction. □

Definition 4.1.2 Let R be a ring and M an R-module. Let Σ be the set of all submodules of M.

a) M is **noetherian** if $(\Sigma, \subseteq)$ satisfies the equivalent conditions of lemma 4.1.1.

b) M is **artinian** if $(\Sigma, \supseteq)$ satisfies the equivalent conditions of lemma 4.1.1.

c) R is **noetherian** if R is a noetherian R-module.

d) R is **artinian** if R is an artinian R-module.

Example 4.1.3 a) A finite-dimensional vector space over a field is both artinian and noetherian.

b) It follows easily from the elementary divisors theorem that a finitely generated module over a PID is noetherian. If it is a torsion module, it is also artinian.

c) A field is both noetherian and artinian as a ring.

d) A PID is not artinian: if $x \neq 0$ is not a unit, then $xR \supsetneq x^2R \supsetneq \cdots \supsetneq x^nR \supsetneq \ldots$

d) If k is a field, the ring $k[X_1, X_2, \ldots, X_n, \ldots]$ is neither artinian nor noetherian, as we have the chains $(X_1) \supsetneq (X_1X_2) \supsetneq (X_1X_2X_3) \supsetneq \ldots$ and $(X_1) \subsetneq (X_1, X_2) \subsetneq (X_1, X_2, X_3) \subsetneq \ldots$

Remark 4.1.4 Every artinian ring is noetherian. A proof is given in the Introduction to Ring Theory course. A self-contained proof can be found in [2], theorem 2.14.

Noetherian rings are the most useful class in Algebraic Geometry and in Number Theory. Artinian rings play a minor role. They will be characterised at the beginning of chapter VI.

Proposition 4.1.5 *Let R be a ring and M an R-module. The following conditions are equivalent:*

a) M is noetherian;

b) Every submodule $N \subseteq M$ is finitely generated.

Proof. Suppose M noetherian, $N \subseteq M$ a submodule and let Σ be the set of all finitely generated submodules of N. This set is non-empty, as it contains $\{0\}$. Let thus $N' \subseteq N$ be a maximal finitely generated submodule. For any $m \in N$, the submodule $N' + mR \subseteq N$ is finitely generated and contains N'. By maximality $N' = N' + mR$, hence $m \in N'$ for all $m \in N$ i.e. $N' = N$.
Conversely, assume that every submodule $N \subseteq M$ is finitely generated and let $M_1 \subseteq M_2 \subseteq \ldots$ be a chain of submodules of M. Put $N = \bigcup_{n=1}^{\infty} M_n$. It is a submodule because any two elements of N belong to M_n for n large enough, hence their sum is in M_n. By assumption, N is finitely generated. For some $n_0 \geq 1$ all the generators belong to M_{n_0}, hence $N = M_{n_0} = M_{n_0+1} = \ldots$ □

Corollary 4.1.6 *A PID is noetherian.*

Proof. Indeed, any ideal is generated by one element. □

Proposition 4.1.7 *Let R be a ring and $0 \to M' \xrightarrow{i} M \xrightarrow{\pi} M'' \to 0$ an exact sequence of R-modules.*

a) M is noetherian $\iff$ M' and M'' are noetherian.

b) M is artinian $\iff$ M' and M'' are artinian.

Proof. We only prove statement a), the proof of b) is similar, reversing inclusions. Suppose M is noetherian. Any submodule of M' is in M and thus finitely genereated, hence M' is noetherian. For any chain $M_1'' \subseteq M_2'' \subseteq \ldots$ in M'' we get a chain $\pi^{-1}(M_1'') \subseteq \pi^{-1}(M_2'') \subseteq \ldots$ in M. Thus $\pi^{-1}(M_n'') = \pi^{-1}(M_{n+1}'')$ for all $n \geq n_0$ for a suitable $n_0 \in \mathbb{N}$. Hence $M_n'' = \pi\left(\pi^{-1}(M_n'')\right) = \pi\left(\pi^{-1}(M_{n+1}'')\right) = M_{n+1}''$ for all $n \geq n_0$.
Suppose M' and M'' noetherian and let $M_1 \subseteq M_2 \subseteq \ldots$ be a chain of submodules in M. Then there exists $n_0', n_0'' \in \mathbb{N}$ such that $M' \cap M_n = M' \cap M_{n+1}$ for all $n \geq n_0'$ and $\pi(M_n) = \pi(M_{n+1})$ for all $n \geq n_0''$. For any $n \geq n_0 = \max\{n_0', n_0''\}$ we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' \cap M_n & \longrightarrow & M_n & \longrightarrow & \pi(M_n) & \longrightarrow & 0 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & M' \cap M_{n+1} & \longrightarrow & M_{n+1} & \longrightarrow & \pi(M_{n+1}) & \longrightarrow & 0 \end{array}$$

and by the snake lemma we conclude that $M_n = M_{n+1}$ for $n \geq n_0$. □

Corollary 4.1.8 *If $M_1, \ldots, M_n$ are noetherian (resp. artinian) modules, then $\bigoplus_{i=1}^n M_i$ is noetherian (resp. artinian).*

Proof. Induction on n using the sequence $0 \longrightarrow M_n \longrightarrow \bigoplus_{i=1}^n M_i \longrightarrow \bigoplus_{i=1}^{n-1} M_i \longrightarrow 0$. □

Corollary 4.1.9 *Let R be a noetherian ring. Every finitely generated R-module is noetherian and finitely presented.*

Proof. Choose a presentation $\pi : R^n \twoheadrightarrow M$. Since R^n is noetherian, $\ker \pi$ and M are noetherian, and $\ker \pi$ is finintely generated by proposition 4.1.5. □

Corollary 4.1.10 *Let R be a noetherian ring. Any finite R-algebra is also a noetherian ring.*

Proof. Let $I \subseteq A$ an ideal. As an R-submodule of A it is finitely generated, because A is a noetherian module. Then I is also finitely generated as an A-module. □

Corollary 4.1.11 *Let R be a noetherian integrally closed ring, K its fraction field, L a finite separable extension of K and A the integral closure of R in L. Then A is finite over R and thus noetherian.*

Proof. By corollary 3.3.14, A is a submodule of a free R-module of finite rank $[L : K]$. So it is finitely generated as an R-module and noetherian by corollary 4.1.10. □

Remark 4.1.12 Let R be an integrally closed domain, K its fraction field, L a finite extension of K and A the integral closure of R in L. In general, it is not true that A is a finitely generated R-module: see exercise 3.5 for an example in which both R and A are discrete valuation rings. A domain R whose integral closure in any finite extension of $\operatorname{Frac} R$ is a finite over R is called a **japanese ring**. Examples of japanese rings are domains of finite type over a field (corollary 4.3.8) and complete discrete valuation rings (corollary 3.6.21). More generally, a noetherian complete local ring is japanese, [8], corollary 2 to theorem 69.

Corollary 4.1.13 *Let R be a noetherian (resp. artinian) ring, $I \subset R$ an ideal. Then R/I is also noetherian (resp. artinian).*

Proof. It follows from proposition 4.1.7 that R/I is noetherian (resp. artinian) as an R-module. Therefore it is noetherian (resp. artinian) as an R/I-module. □

Remark 4.1.14 A subring of a noetherian (resp. artinian) ring is not necessarily noetherian (resp. artinian). For instance in example 4.1.3.d we have seen that $k[X_1, X_2, \ldots, X_n, \ldots]$ is neither artinian nor noetherian. Since it is a domain, it is a subring of its fraction field, and a field is both artinian and noetherian.

Proposition 4.1.15 *Let R be a noetherian ring, $S \subset R$ a multiplicative subset. Then $S^{-1}R$ is also noetherian.*

Proof. Let $J_1 \subseteq J_2 \subseteq \ldots$ be a chain of ideals in $S^{-1}R$. By proposition 2.1.10 there is a chain $I_1 \subseteq I_2 \subseteq \ldots$ in R such that $J_n = S^{-1}I_n$ for all n. Fix n_0 such that $I_n = I_{n+1}$ for all $n \geq n_0$, we get $J_n = J_{n+1}$ for all $n \geq n_0$. □

Corollary 4.1.16 *If R is a noetherian ring then $R_{\mathfrak{p}}$ is a noetherian ring for every prime $\mathfrak{p}$.*

Theorem 4.1.17 (Hilbert's Basis Theorem) *If R is a noetherian ring then $R[X]$ is also noetherian.*

Proof. Let $I \subseteq R[X]$ be an ideal and $F = \{f_\alpha\}$ an arbitrary family of generators of I. Let $J \subseteq R$ be the ideal generated by the leading coefficients of the f_α. Since R is noetherian, $J = (c_1, \ldots, c_n)$. Let $f_i = c_i X^{d_i} + g_i \in F$, with $\deg g_i < d_i$, be the generator corresponding to c_i, for $i = 1, \ldots, n$. Let $I' = (f_1, \ldots, f_n)$, set $d = \max\{d_1, \ldots, d_n\}$ and put $I'' = I \cap \bigoplus_{i=0}^{d-1} RX^i$. We shall prove that $I = I' + I''$. Since $\bigoplus_{i=0}^{d-1} RX^i$ is finitely generated, it is a noetherian R-module, so the submodule I'' is also finitely generated, say $I'' = (h_1, \ldots, h_m)$, Hence $I = (f_1, \ldots, f_n, h_1, \ldots, h_m)$ is finitely generated. Since every ideal is finitely generated, $R[X]$ is noetherian.
For every $f = cX^r + g \in I$, with $\deg g < r$, we have $c \in J$. If $r \leq d-1$ then $f \in I''$. If $r \geq d$, write $c = a_1c_1 + \cdots + a_nc_n$, with $a_i \in R$. Then $f - \sum_{i=1}^n a_i X^{r-d_i} f_i \in I$ and has degree strictly smaller than r. Repeating if necessary, we obtain the announced equality $I = I' + I''$. □

Corollary 4.1.18 *If R is a noetherian ring then $R[X_1, \ldots, X_n]$ is noetherian.*

Corollary 4.1.19 *If R is a noetherian ring then any R-algebra of finite type is noetherian and finitely presented as an R-algebra.*

Proof. Combine corollaries 4.1.19 and 4.1.13. □

Remark 4.1.20 Hilbet's basis theorem is also a crucial ingredient in the proof of the following fact: if R is a noetherian ring and $\mathfrak{a}$ an ideal, the $\mathfrak{a}$-adic completion $\hat{R}_{\mathfrak{a}}$ is a noetherian ring. See for instance [1], theorem 10.26.

§ 2 Composition series

Let R be a ring and M an R-module.

Definition 4.2.1 An R-module M is **simple** if its only submodules are 0 and M.

Notice that if $0 \neq m \in M$, then $0 \neq Rm \subseteq M$, thus if M is simple, $M = Rm$. The map $\varphi : R \to M$ defined by $\varphi(1) = m$ induces an isomorphism $M \simeq R/\mathrm{Ann}\,(m)$. Again, since M is simple, we get that $\mathrm{Ann}\,(m)$ is a maximal ideal in R.

Definition 4.2.2 Let M be an R-module. A chain $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$ of submodules is said to be of **length** n. A **composition series** or **Jordan–Hölder sequence** is a chain such that M_{i-1}/M_i is simple for $1 \leq i \leq n$.

The following result gathers some information we shall need later on. For a proof we refer to the *Introduction to Ring Theory* course. Alternatively, see [2], theorem 2.13.

Theorem 4.2.3 *Let M be an R-module.*

a) M has a composition series if and only if it is both artinian and noetherian.

b) If M has a composition series, then all composition series have the same length, called the **length** *of the module and denoted by $\ell(M)$.*

c) If M has a composition series, then any descending chain of submodules can be refined into a composition series.

d) If $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ is short exact, then $\ell(M) = \ell(M') + \ell(M'')$.

e) If M has a composition series, then $M \simeq \bigoplus_{\mathfrak{m}} M_{\mathfrak{m}}$. Only maximal ideals annihilating some quotient in some composition series appear in the sum. For a fixed maximal ideal $\mathfrak{m} \subset R$, the number of quotients M_{i-1}/M_i arising from any composition series and such that $\mathrm{Ann}\,(M_{i-1}/M_i) = \mathfrak{m}$ is equal to the length of $M_{\mathfrak{m}}$ as an $R_{\mathfrak{m}}$-module (and is the same for all series).

We shall write $\ell(M) < +\infty$ to say that M has a composition series.

§ 3 Normalisation Lemma and Nullstellensatz

In this section, k is a field and R a k-algebra of finite type.

Lemma 4.3.1 (Noether's Normalisation) *Let $R = k[X_1, \ldots, X_n]/I$. There exists an integer $d \leq n$ and an injection $k[T_1, \ldots, T_n] \subseteq k[X_1, \ldots, X_n]$ such that:*

a) $k[X_1, \ldots, X_n]$ is finite over $k[T_1, \ldots, T_n]$;

b) $I \cap k[T_1, \ldots, T_n]$ is the ideal in $k[T_1, \ldots, T_n]$ generated by $T_{d+1}, \ldots, T_n$;

c) R is finite over $k[T_1, \ldots, T_d]$.

Proof. c) follows directly from a) and b). If $n = 0$ or if $I = 0$, a) and b) are trivial. Suppose first that $I = (F)$, with $F = \sum_{\boldsymbol{\nu}} a_{\boldsymbol{\nu}} X_1^{\nu_1} \ldots X_n^{\nu_n}$. For $\mathbf{m} = (m_1, \ldots, m_{n-1}, 1) \in \mathbb{N}^n$, let $Y_i = X_i - X_n^{m_i}$, for $1 \leq i \leq n-1$. Clearly $k[X_1, \ldots, X_n] = k[Y_1, \ldots, Y_{n-1}, X_n]$. If we can find $\mathbf{m} \in \mathbb{N}^n$ such that

$$F(Y_1, \ldots, Y_{n-1}, X_n) = \alpha X_n^e + G_{e-1} X_n^{e-1} + \cdots + G_0, \quad \alpha \in k^\times,\ e \geq 1,\ G_j \in k[Y_1, \ldots, Y_{n-1}], \tag{4.1}$$

statement a) will follow by setting $T_i = Y_i$ for $1 \leq i \leq n-1$ and $T_n = F$, since (4.1) gives the integral equation $X_n^e + \alpha^{-1} G_{e-1} X_n^{e-1} + \cdots + \alpha^{-1}(G_0 - T_n) = 0$ for X_n over $k[T_1, \ldots, T_n]$. Moreover, for any $P \in I$, write $P = T_n Q$, with $Q \in k[X_1, \ldots, X_n]$. If $P \in I \cap k[T_1, \ldots, T_n]$ then $Q = \frac{P}{T_n}$ belongs to the fraction field of $k[T_1, \ldots, T_n]$ and, as an element in $k[X_1, \ldots, X_n]$, is integral over $k[T_1, \ldots, T_n]$. The latter being integrally closed, we have $Q \in k[T_1, \ldots, T_n]$, hence $I \cap k[T_1, \ldots, T_n] = T_n k[T_1, \ldots, T_n]$. That settles b).

Denote $\langle \mathbf{v}, \mathbf{w} \rangle$ the standard euclidean scalar product in $\mathbb{R}^n$. Substituting $Y_i = X_i - X_n^{m_i}$ in the monomial $a_{\boldsymbol{\nu}} X_1^{\nu_1} \dots X_n^{\nu_n}$ we get

$$\begin{aligned} a_{\boldsymbol{\nu}} X_1^{\nu_1} \dots X_n^{\nu_n} =& a_{\boldsymbol{\nu}} \left(Y_1 - X_n^{m_1}\right)^{\nu_1} \dots \left(Y_{n-1} - X_n^{m_{n-1}}\right)^{\nu_{n-1}} X_n^{\nu_n} \\ =& a_{\boldsymbol{\nu}} \left(X_n^{\langle \boldsymbol{\nu}, \mathbf{m} \rangle} + \sum_{j \lneq \langle \boldsymbol{\nu}, \mathbf{m} \rangle} H_j(Y_1, \dots, Y_{n-1}) X_n^j \right) \end{aligned} \tag{4.2}$$

By lemma 4.3.2 below, it is possible to find $\mathbf{m}$ such that the values $\langle \boldsymbol{\nu}, \mathbf{m} \rangle \in \mathbb{N}$ are all distinct for all the $\boldsymbol{\nu} \in \mathbb{N}^n$ such that $a_{\boldsymbol{\nu}} \neq 0$. Formula (4.1) now follows from (4.2) by taking $\boldsymbol{\nu}_0$ to be the unique multi-index such that $\langle \boldsymbol{\nu}_0, \mathbf{m} \rangle = \max_{a_{\boldsymbol{\nu}} \neq 0} \{ \langle \boldsymbol{\nu}, \mathbf{m} \rangle \}$ and setting $\alpha = a_{\boldsymbol{\nu}_0}$ and $e = \langle \boldsymbol{\nu}_0, \mathbf{m} \rangle$.

Now proceed by induction on n. The case $n = 1$ is settled ($k[X_1]$ is a PID). Pick any $0 \neq F \in I$. Proceeding as above, find $Y_1, \dots, Y_{n-1} \in k[X_1, \dots, X_n]$ such that $k[X_1, \dots, X_n]$ is finite over $k[Y_1, \dots, Y_{n-1}, F]$ and $Fk[X_1, \dots, X_n] \cap k[Y_1, \dots, Y_{n-1}, F] = Fk[Y_1, \dots, Y_{n-1}, F]$.
If $I \cap k[Y_1, \dots, Y_{n-1}] = 0$, put $T_i = Y_i$ for $1 \leq i \leq n-1$ and $T_n = F$ as above to get claim a) in the statement. Clearly $T_n k[T_1, \dots, T_n] \subseteq I \cap k[T_1, \dots, T_n]$. To check equality, and thus get b), localise w.r.t. $k[T_1, \dots, T_{n-1}] - \{0\}$. We have $T_n k(T_1, \dots, T_{n-1})[T_n] \subseteq I \cap k(T_1, \dots, T_{n-1})[T_n]$ and the first is a maximal ideal, so the inclusion is an equality. Hence, for any $P \in I \cap k[T_1, \dots, T_n]$ there exists $0 \neq S \in k[T_1, \dots, T_{n-1}]$ such that $SP \in T_n k[T_1, \dots, T_n]$. But $T_n k[T_1, \dots, T_n]$ is prime and S doesn't belong to it, so $P \in T_n k[T_1, \dots, T_n]$.
If, on the contrary, $I \cap k[Y_1, \dots, Y_{n-1}] \neq 0$, by inductive assumption there exist an injection $k[T_1, \dots, T_{n-1}] \subseteq k[Y_1, \dots, Y_{n-1}]$ such that $k[Y_1, \dots, Y_{n-1}]$ is finite over $k[T_1, \dots, T_{n-1}]$ and an integer $d < n-1$ such that $I \cap k[T_1, \dots, T_{n-1}]$ is the ideal in $k[T_1, \dots, T_{n-1}]$ generated by $T_{d+1}, \dots, T_{n-1}$. Put again $T_n = F$. Then $k[T_1, \dots, T_n] \subseteq k[X_1, \dots, X_n]$ is a finite injection, whence claim a). The ideal $I \cap k[T_1, \dots, T_n]$ clearly contains the ideal generated by $T_{d+1}, \dots, T_n$ and we must show that they coincide.
The ideal $T_n k[T_1, \dots, T_n]$ is the kernel of the natural projection $k[T_1, \dots, T_n] \twoheadrightarrow k[T_1, \dots, T_{n-1}]$. The inclusion $k[T_1, \dots, T_{n-1}] \subset k[T_1, \dots, T_n]$ gives a splitting, whence a decomposition

$$k[T_1, \dots, T_n] = k[T_1, \dots, T_{n-1}] \oplus T_n k[T_1, \dots, T_n]$$

as $k[T_1, \dots, T_{n-1}]$-modules. Any $P \in k[T_1, \dots, T_n]$ can be written as $P = P_0 + (P - P_0)$ for a unique $P_0 \in k[T_1, \dots, T_{n-1}]$. If $P \in I \cap k[T_1, \dots, T_n]$, since $T_n k[T_1, \dots, T_n] \subset (I \cap k[T_1, \dots, T_n])$,

$$\begin{aligned} P_0 = (P_0 - P) + P &\in (I \cap k[T_1, \dots, T_n]) \cap k[T_1, \dots, T_{n-1}] \\ &= I \cap k[T_1, \dots, T_{n-1}] \\ &= T_{d+1} k[T_1, \dots, T_{n-1}] + \dots + T_{n-1} k[T_1, \dots, T_{n-1}]. \end{aligned}$$

Finally, since $P - P_0 \in T_n k[T_1, \dots, T_n]$, we have shown that $P = P_0 + (P - P_0)$ belongs to the ideal generated by $T_{d+1}, \dots, T_n$. □

Lemma 4.3.2 *Let $N \subset \mathbb{N}^n$ be a finite set. There exists a vector $\mathbf{m} = (m_1, \dots, m_{n-1}, 1) \in \mathbb{N}^n$ such that the values $\langle \boldsymbol{\nu}, \mathbf{m} \rangle \in \mathbb{N}$ are all distinct for all the $\boldsymbol{\nu} \in N$.*

Proof. For $\boldsymbol{\nu} = (\nu_1, \dots, \nu_n) \in \mathbb{N}^n$, define $|\boldsymbol{\nu}| = \max\{\nu_i\}$, select $b > \max_{\boldsymbol{\nu} \in N} \{|\boldsymbol{\nu}|\}$ and put $\mathbf{m} = (b^{n-1}, b^{n-2}, \dots, b, 1)$. By the uniqueness of the expansion of an integer in base b, an identity

$$\langle \boldsymbol{\nu}, \mathbf{m} \rangle = \nu_1 b^{n-1} + \dots + \nu_{n-1} b + \nu_n = \nu'_1 b^{n-1} + \dots + \nu'_{n-1} b + \nu'_n = \langle \boldsymbol{\nu}', \mathbf{m} \rangle$$

with $0 \leq \nu_i, \nu'_j < b$ implies $\nu_i = \nu'_i$ for all $1 \leq i \leq n$. □

Corollary 4.3.3 *Let R be a k-algebra of finite type, $\mathfrak{m} \subset R$ a maximal ideal. Then $R/\mathfrak{m}$ is a finite extension of k*

Proof. Let $\pi : k[X_1, \ldots, X_n] \twoheadrightarrow R$ and $\widetilde{\mathfrak{m}} = \pi^{-1}(\mathfrak{m})$, a maximal ideal in $k[X_1, \ldots, X_n]$ by proposition 1.1.49. By the Normalisation lemma applied to $k[X_1, \ldots, X_n]/\widetilde{\mathfrak{m}} = R/\mathfrak{m}$, this ring is finite over $k[T_1, \ldots, T_d]$ for a suitable $d \in N$. But $R/\mathfrak{m}$ is a field, integral over the domain $k[T_1, \ldots, T_d]$. By proposition 3.2.1, the latter must be a field, which is possible only for $d = 0$. □

Corollary 4.3.4 *In a k-algebra of finite type, the Jacobson radical is equal to the nilradical.*

Proof. Recall that $\mathfrak{N}_R$ (resp. $\mathfrak{R}_R$) is the intersection of all prime (resp. maximal) ideals. Let $f \in \mathfrak{R}_R$. If f were not nilpotent, the ring $R_f = R[\frac{1}{f}]$ being still finitely generated over k and is not the zero ring, would contain a maximal ideal $\mathfrak{m}$. Let $\varphi : R \to R_f$ be the natural map and consider $k \subseteq R/\varphi^{-1}(\mathfrak{m}) \subseteq R_f/\mathfrak{m}$. Since $R_f/\mathfrak{m}$ is finite over k, it is finite over $R/\varphi^{-1}(\mathfrak{m})$. The first is a field and the latter a domain. It follows that $R/\varphi^{-1}(\mathfrak{m})$ is a field and $\varphi^{-1}(\mathfrak{m})$ is thus maximal. But $f \notin \varphi^{-1}(\mathfrak{m})$, contradicting $f \in \mathfrak{R}_R$. □

Corollary 4.3.5 (Weak Nullstellensatz) *If k is an algebraically closed field and $\mathfrak{m} \subset k[X_1, \ldots, X_n]$ is a maximal ideal, then there exists a unique $(\alpha_1, \ldots, \alpha_n) \in k^n$ such that $\mathfrak{m} = (X_1 - \alpha_1, \ldots, X_n - \alpha_n)$.*

Proof. If $\mathfrak{m}$ is maximal, $k[X_1, \ldots, X_n]/\mathfrak{m}$ is a finite field extension of the algebraically closed k. Hence $k[X_1, \ldots, X_n]/\mathfrak{m} \simeq k$. If $\alpha_i \equiv X_i \bmod \mathfrak{m}$ then $(X_1 - \alpha_1, \ldots, X_n - \alpha_n) \subseteq \mathfrak{m}$ and the first is obviously maximal, so they coincide. Uniqueness is trivial. □

Corollary 4.3.6 *Let k be algebraically closed, $I \subset k[X_1, \ldots, X_n]$ an ideal and $R = k[X_1, \ldots, X_n]/I$. There is a bijection between closed points in $\operatorname{Spec} R$ and the zero-locus of I*

$$\mathcal{Z}(I) = \{(\alpha_1, \ldots, \alpha_n) \in k^n \mid F(\alpha_1, \ldots, \alpha_n) = 0 \,\forall\, F \in I\}\,.$$

Proof. Closed points in $\operatorname{Spec} R$ are in bijection with maximal ideals in R which are in bijection with maximal ideals in $k[X_1, \ldots, X_n]$ containing I. So if $F \in I$ then

$$F \in I \subseteq \mathfrak{m} = (X_1 - \alpha_1, \ldots, X_n - \alpha_n) = \ker\left[\varepsilon : k[X_1, \ldots, X_n] \longrightarrow k\right]$$

where $\varepsilon(P) = P(\alpha_1, \ldots, \alpha_n)$. Hence $\varepsilon(F) = F(\alpha_1, \ldots, \alpha_n) = 0$. Conversely, if $\varepsilon(F) = 0$ for all $F \in I$ then $I \subseteq \ker(\varepsilon) = \mathfrak{m}$. □

Corollary 4.3.7 (Hilbert's Nullstellensatz) *Let k be algebraically closed and $I \subset k[X_1, \ldots, X_n]$ an ideal. If $F \in k[X_1, \ldots, X_n]$ satisfies $F(\alpha_1, \ldots, \alpha_n) = 0$ for all $(\alpha_1, \ldots, \alpha_n) \in \mathcal{Z}(I)$ then $F \in \sqrt{I}$.*

Proof. Let $R = k[X_1, \ldots, X_n]/I$ and denote $\overline{F}$ the class of F mod I. Then

$$\begin{aligned}
F(\alpha_1, \ldots, \alpha_n) = 0 \,\forall\, (\alpha_1, \ldots, \alpha_n) \in Z(I) \iff & \quad F \in \mathfrak{m} \quad \forall\, \mathfrak{m} \supseteq I \text{ maximal in } k[X_1, \ldots, X_n] \\
\iff & \quad \overline{F} \in \overline{\mathfrak{m}} \quad \forall\, \overline{\mathfrak{m}} \text{ maximal in } R \\
\iff & \quad \overline{F} \in \mathfrak{R}_R = \mathfrak{N}_R \quad \text{(by corollary 4.3.4)} \\
\iff & \quad F \in \sqrt{I}.
\end{aligned}$$

□

We conclude this section with another beautiful application of the Normalisation Lemma.

Corollary 4.3.8 *Let k be a field and R a k-algebra of finite type. Assume that R is a domain and let $K = \operatorname{Frac} R$. Let L be a finite extension of K and A the integral closure of R in L. Then A is a finitely generated R-module and, in particular, a k-algebra of finite type.*

Proof. By the Normalisation Lemma, R is a finitely generated module over a polynomial subalgebra $k[X_1, \ldots, X_n] \subseteq R$. Clearly, if A is a finitely generated $k[X_1, \ldots, X_n]$-module, it is finitely generated as R-module, so we may assume that $R = k[X_1, \ldots, X_n]$. Moreover, let $L \subseteq M$ be a finite field extension which is normal over K and denote by B the integral closure of A in M. Again, if B is a finitely generated R-module, so is its submodule A, since R is noetherian. So we may assume that $L = M$ is normal over K. Furthermore, let $E \subseteq L$ be the subset of elements which are fixed by every K-linear field automorphism of L. We know from Galois theory that $K \subseteq E \subseteq L$ is a tower of field extensions, the first purely inseparable and the second separable. Let C be the integral closure of K in E. We know from corollary 3.3.14 that A is finite over C, so we may assume that $L = E$ is purely inseparable over K.

We are now reduced to the case where L is generated over K by the q-th roots of some elements $f_1, \ldots, f_r \in K = k(X_1, \ldots, X_n)$ (where q is a power of the characteristic of k). Let k' be the finite extension of k generated by the q-th roots of the coefficients of the f_i. For the compositum extension we have $k'L \subseteq k'(Y_1, \ldots, Y_n) = L'$, where $Y_i^q = X_i$. Then $A' = k'[Y_1, \ldots, Y_n]$ is an integrally closed domain with field of fractions L' finite over R: it is thus the integral closure of R in L'. Its R-submodule A must then be finitely generated as well. □

§ 4 Exercises

Exercise 4.1 Let R be a noetherian ring. Show that every open subset $U \subseteq \operatorname{Spec} R$ is the union of a finite number of subsets of the form $\operatorname{Spec} R - \mathcal{Z}(f) = \operatorname{Spec} R_f$.

Exercise 4.2 Let R be a noetherian ring. Show that the nilradical of R is nilpotent, i.e. that $\mathfrak{N}_R^n$ is the zero ideal for some integer $n \geq 1$. Show that any ideal I contains a power of its radical: $(\sqrt{I})^n \subseteq I$ for some $n \geq 1$.

Exercise 4.3 Let R be a noetherian ring. Recall that an ideal $I \subseteq R$ is radical if $x^n \in I \Rightarrow x \in I$.

a) Let Σ be the set of all radical ideals in R which are not intersection of finitely many prime ideals. Suppose $\Sigma \neq \varnothing$ and show that it contains a maximal element I.

b) Suppose that $I \neq R$. Show that there exist $x, y \notin I$ such that $xy \in I$. Show that $I + (x) \neq R \neq I + (y)$.

c) Show that $\sqrt{I + (x)} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$ and $\sqrt{I + (y)} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ for suitable prime ideals $\mathfrak{p}_i$ and $\mathfrak{q}_j$ of R.

d) Show that $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r \cap \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$. Conclude that every radical ideal in R is the intersection of finitely many prime ideals.

e) Let J be a radical ideal, written as $J = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$ and $J = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$. Suppose $\mathfrak{p}_i \nsubseteq \mathfrak{p}_j$ and $\mathfrak{q}_i \nsubseteq \mathfrak{q}_j$ for $i \neq j$. Show that $r = s$ and that $\forall\, i\ \exists!\, j$ such that $\mathfrak{p}_i = \mathfrak{q}_j$.

Exercise 4.4 This exercise gives an alternative proof of Hilbert's Basis Theorem. Let R be a noetherian ring. For an ideal $I \subseteq R[X]$, denote $\mathfrak{a}'_d(I) \subseteq R$ the set of all leading coefficients of polynomials of degree d in I and let $\mathfrak{a}_d(I) = \mathfrak{a}'_d(I) \cup \{0\}$.

a) Show that $\mathfrak{a}_d(I)$ is an ideal for every $d \geq 0$.

b) Show that $\mathfrak{a}_d(I) \subseteq \mathfrak{a}_{d+1}(I)$.

c) Show that if $I \subseteq J$ then $\mathfrak{a}_d(I) \subseteq \mathfrak{a}_d(J)$ for all $d \geq 0$.

d) Prove, by induction on d, that if $I \subseteq J$ and $\mathfrak{a}_d(I) = \mathfrak{a}_d(J)$ for all $d \geq 0$ then $I = J$.

Let $I_0 \subseteq I_1 \subseteq \cdots \subseteq I_k \subseteq \ldots$ be a sequence of ideals in $R[X]$.

e) Show that the set $\{\mathfrak{a}_j(I_j),\, \forall i, j\}$ of ideals in R has a maximal element. Denote it $\mathfrak{a}_p(I_q)$.

f) Fix $d \geq 0$ and consider the sequence $\mathfrak{a}_d(I_0) \subseteq \mathfrak{a}_d(I_1) \subseteq \ldots$. Show that there exists an integer j_d be such that $\mathfrak{a}_d(I_j) = \mathfrak{a}_d(I_{j_d})$ for all $j \geq j_d$.

g) Put $m = \max\{j_0, \ldots, j_{p-1}, q\}$. Show that, if $d \leq p-1$, then $\mathfrak{a}_d(I_n) = \mathfrak{a}_d(I_m)$ for all $n \geq m$.

h) Use b) and c) to show that $\mathfrak{a}_p(I_q) \subseteq \mathfrak{a}_d(I_n)$, for all $d \geq p$ and $n \geq m$.

i) Conclude that $\mathfrak{a}_d(I_n) = \mathfrak{a}_d(I_m)$ for all d, provided $n \geq m$.

j) Conclude that $R[X]$ is noetherian.

Exercise 4.5 Suppose that R is a noetherian domain. Show that any nonzero ideal contains a product of nonzero prime ideals.

Exercise 4.6 Let R be a noetherian domain which is not a field. Show that R is a UFD if and only if every ideal generated by an irreducible element is prime.

Chapter V

Dedekind domains

§ 1 Discrete Valuation Rings

For the reader's convenience, we begin by recalling the:

Definition 3.4.18 *A valuation ring R with fraction field K is a* **discrete valuation ring** *(DVR for short) if $K^\times/R^\times \simeq \mathbb{Z}$. Any element $\pi \in R$ such that $v(\pi) = 1$ is called a* **uniformiser** *or uniformising parameter of R.*

Proposition 5.1.1 *Let R be a domain. The following conditions are equivalent:*

a) R is a DVR;

b) R is a local PID.

Proof. If R is a DVR, we know that it is a local ring. If $\pi \in R$ is a uniformiser, for any $0 \neq x \in R$, let $n = v(x) \in \mathbb{N}$ and $u = \frac{x}{\pi^n}$. Since $v(u) = v(x) - n = 0$, we have $u \in R^\times$ and every element can be written uniquely as $x = u\pi^n$. If $I \subset R$ is an ideal, $\{v(x) \,|\, x \in I\}$ is a subset of $\mathbb{N}$ and has thus a minimum m. Then for any $x \in I$, we can write $x = \frac{x}{\pi^m}\pi^m$ and $\frac{x}{\pi^m} \in R$ because $v\left(\frac{x}{\pi^m}\right) = v(x) - m \geq 0$. Hence $I = (\pi^m)$. Therefore R is a PID.
Conversely, let $\mathfrak{m} = (\pi) \subset R$ be the maximal ideal of a local PID. Up to a unit factor, π is the unique irreducible element in R. Thus for every $0 \neq x \in R$, we can write $x = u\pi^n$ for a unique $n \in \mathbb{N}$ and $u \in R^\times$. It is now immediate to check that

$$v : K^\times \longrightarrow \mathbb{Z}, \qquad \frac{a}{b} \longmapsto v(a) - v(b)$$

is a discrete valuation on K. □

Example 5.1.2 From the proposition above it is immediate to see that $\mathbb{Z}_{(p)}$ is a DVR for every prime number p. If k is a field, $k[X]_{(X)}$ and $k[[X]]$ are DVRs.

To prepare for another characterisation of DVRs, we need a special case of the following lemma. The general statement will be used later.

Lemma 5.1.3 *Let R be a local noetherian ring with maximal ideal $\mathfrak{m}$. Suppose that there exists $n_0 \in \mathbb{N}$ and a non-nilpotent element $\pi \in \mathfrak{m}$ such that $\mathfrak{m}^n \subseteq (\pi)$ for all $n \geq n_0$. Then $\bigcap_{n\geq 0} \mathfrak{m}^n = 0$.*

Proof. Let $\mathfrak{a} = \{x \in R \,|\, \exists\, m \in \mathbb{N}, x\pi^m = 0\}$. It is an ideal, finitely generated since R is noetherian. There is thus an integer m_0 such that $x\pi^{m_0} = 0$ for all $x \in \mathfrak{a}$.
Let now $y \in \bigcap_{n\geq 0} \mathfrak{m}^n$. In particular, for all $n \geq 0$ we have $y \in \mathfrak{m}^{n^2} \subseteq (\pi^n)$. Hence we can write $y = x_n\pi^n$ for all $n \geq n_0$ and therefore $(x_n - \pi x_{n+1})\pi^n = 0$, thus $x_n - \pi x_{n+1} \in \mathfrak{a}$. Whence an increasing sequence of ideals $\{\mathfrak{a} + (x_n)\}_n$ which must be stationary: for n sufficiently large $x_{n+1} \in \mathfrak{a} + (x_n)$. Write $x_{n+1} = a + bx_n$, for some $a \in \mathfrak{a}$. On the other hand, $x_n = \pi x_{n+1} + a'$, for some $a' \in \mathfrak{a}$. substituting, we get $(1 - b\pi)x_{n+1} \in \mathfrak{a}$. Since $\pi \in \mathfrak{m}$, then $1 - b\pi$ is a unit and $x_{n+1} \in \mathfrak{a}$ for n large enough. Taking $n \geq m_0$ and sufficiently large, we get $y = \pi^{n+1}x_{n+1} = 0$. □

Remark 5.1.4 More generally, Krull's intersection theorem states that if R is any local noetherian ring with maximal ideal $\mathfrak{m}$, then $\bigcap_{n\geq 0} \mathfrak{m}^n = 0$. The (same) proof can be found alternatively in [1], corollary 10.19, [2], corollary 5.4, [8], corollary 11.2 or [9], theorem 8.10.

Proposition 5.1.5 *Let R be a ring. The following conditions are equivalent:*

a) R is a DVR;

b) R is noetherian, local, with maximal ideal $\mathfrak{m}$ generated by a non-nilpotent element.

Proof. Recalling that a PID is noetherian, the implication a) $\Longrightarrow$ b) is clear.
For the converse, let $\pi \in R$ be a non-nilpotent element generating $\mathfrak{m}$. From lemma 5.1.3 (applied to $\mathfrak{m} = (\pi)$) we infer that for any $0 \neq x \in R$ there is an $n \in \mathbb{N}$ such that $x \in \mathfrak{m}^n$ but $x \notin \mathfrak{m}^{n+1}$. We have thus a unique expression $x = u\pi^n$, with $u = \frac{x}{\pi^n} \in R^\times$. Therefore R is a domain and, setting $n = v(x)$ and $K = \operatorname{Frac} R$, we can define a discrete valuation $v : K^\times \to \mathbb{Z}$ by the usual formula $v\left(\frac{a}{b}\right) = v(a) - v(b)$. □

This criterion allows us to generalise example 5.1.2:

Example 5.1.6 Let R be a noetherian UFD, $f \in R$ an irreducible element. The localisation of R at the ideal generated by f is a DVR. A typical case in Algebraic Geometry is the localisation of $k[X_1, \ldots, X_n]$ at an irreducible polynomial.

Example 5.1.7 Let $R = \mathbb{C}[X, Y]/(X^3 + X^2 - Y^2)$. Since $Y^2 - (X^3 + X^2) \in \mathbb{C}[X][Y]$ is Eisenstein with respect to $(X + 1) \subset \mathbb{C}[X]$, it is irreducible, hence R is a domain. As usual, write x and y for the images of X and Y in R. Since $x \notin \mathfrak{m}_1 = (x+1, y)$, we see that $\mathfrak{m}_1 R_{\mathfrak{m}_1} = (x+1, y) = (y)$, since $x + 1 = \frac{y^2}{x^2} \in (y^2)$. Hence $R_{\mathfrak{m}_1}$ is a DVR by proposition 5.1.5. On the other hand, for $\mathfrak{m}_0 = (x, y)$, we have that $\mathfrak{m}_0 R_{\mathfrak{m}_0}$ is not principal. Indeed, if $\widetilde{\mathfrak{m}}_0 = (X, Y) \subset \mathbb{C}[X, Y]_{(X,Y)}$, then $f = X^3 + X^2 - Y^2 \in \widetilde{\mathfrak{m}}_0^2$, thus $\mathfrak{m}_0/\mathfrak{m}_0^2 = (\widetilde{\mathfrak{m}}_0/(f)) \,/\, (\widetilde{\mathfrak{m}}_0^2/(f)) \cong \widetilde{\mathfrak{m}}_0/\widetilde{\mathfrak{m}}_0^2 = \mathbb{C} \cdot X \oplus \mathbb{C} \cdot Y$. But if $\mathfrak{m}_0$ were principal, by Nakayama's lemma we should have $\dim_{\mathbb{C}} \mathfrak{m}_0/\mathfrak{m}_0^2 = 1$.
This translates the fact that the plane cubic curve $X^3 + X^2 - Y^2 = 0$ has a singularity in $(0, 0)$ while $(-1, 0)$ is nonsingular.

Proposition 5.1.8 *Let R be a noetherian domain. Then R is a DVR if and only if the following two conditions hold:*

i) R is integrally closed;

ii) R has only one nonzero prime ideal.

Proof. All valuation rings are integrally closed (proposition 3.4.6) and every ideal in a DVR is principal, generated by a power of the uniformiser, so there is only one prime ideal.
Conversely, let R be a local noetherian domain with maximal ideal $\mathfrak{m}$ and fraction field K. By proposition 5.1.5, it suffices to show that $\mathfrak{m}$ is principal. Let

$$\mathfrak{m}' = \{x \in K \mid xy \in R \ \forall\, y \in \mathfrak{m}\}\,.$$

Obviously, $\mathfrak{m}'$ is an R-module and $R \subseteq \mathfrak{m}'$. Taking any $0 \neq y \in \mathfrak{m}$, the "multiplication by y" map $\mu_y : \mathfrak{m}' \to R$, given by $\mu_y(x) = yx$ injects $\mathfrak{m}'$ into R. Hence $\mathfrak{m}'$ is isomorphic to an ideal of the noetherian ring R and is thus finitely generated as R-module. Consider then the subset

$$\mathfrak{m}\mathfrak{m}' = \left\{\sum x_i y_i \in K,\ x_i \in \mathfrak{m}',\ y_i \in \mathfrak{m}\right\} \subseteq R.$$

Since $R \subseteq \mathfrak{m}'$, we have $\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{m}' \subseteq R$. Thus $\mathfrak{m}\mathfrak{m}'$ is an ideal sitting between the maximal ideal and R. One of these two inclusions must be an equality. We will establish the following facts:

Claim 1. *If $\mathfrak{m}\mathfrak{m}' = R$ then $\mathfrak{m}$ is principal.*

Claim 2. *If $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}$ and R is integrally closed, then $\mathfrak{m}' = R$.*

Claim 3. *If $\mathfrak{m}$ is the only nonzero prime ideal in R, then $\mathfrak{m}' \neq R$.*

Therefore, if we assume that our ring R satisfies coinditions i) and ii), Claims 2 and 3 tell us that $\mathfrak{m}\mathfrak{m}' \neq \mathfrak{m}$ and then Claim 1 implies that $\mathfrak{m}$ is principal and thus R is a DVR. □

Proof of Claim 1. By assumption, there are elements $x_i \in \mathfrak{m}'$, $y_i \in \mathfrak{m}$ such that $\sum_{i=1}^{r} x_i y_i = 1$. By definition $x_i y_i \in R$ for $1 \leq i \leq r$. If all $x_i y_i \in \mathfrak{m}$, we would get $1 \in \mathfrak{m}$, which is absurd. Say $u = x_1 y_1 \notin \mathfrak{m}$, hence $u \in R^\times$. Put $\pi = u^{-1} y_1 \in \mathfrak{m}$. Then $x_1 \pi = 1$. Now, for all $z \in \mathfrak{m}$ we have $z = z(x_1\pi) = (zx_1)\pi \in (\pi)$. Thus $\mathfrak{m} = (\pi)$ is principal. □

Proof of Claim 2. Suppose that $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}$ and take any $x \in \mathfrak{m}'$. Then $x\mathfrak{m} \subseteq \mathfrak{m}$. Iterating, we get $x^n\mathfrak{m} \subseteq x^{n-1}\mathfrak{m} \subseteq \cdots \subseteq x\mathfrak{m} \subseteq \mathfrak{m}$, hence $x^n \in \mathfrak{m}'$ for all $n \in \mathbb{N}$. The R-submodules $M_n = (1, x, \ldots, x^n) \subseteq \mathfrak{m}'$ build up to an increasing chain $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq M_{n+1} \subseteq \ldots$ of submodules of the finitely generated R-module $\mathfrak{m}'$. By noetherian assumption, $M_n = M_{n-1}$ for n large enough. Thus $x^n \in M_{n-1}$, i.e. $x^n = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ for suitable $a_i \in R$. Therefore any $x \in \mathfrak{m}' \subset K$ is integral over R. Since R is integrally closed, $x \in R$. □

Proof of Claim 3. Select $0 \neq y \in \mathfrak{m}$ and consider $R_y = R[\frac{1}{y}]$. Since $\mathfrak{m}$ is the only nonzero prime ideal in R, the ring R_y has no nonzero primes, hence $R_y = K$. Fix $0 \neq z \in R$ and write $\frac{1}{z} = \frac{a}{y^n}$, for suitable $a \in R$ and $n \in \mathbb{N}$. Hence $y^n = az \in (z)$. Therefore, if $y_1, \ldots, y_r$ are generators of $\mathfrak{m}$, there is an integer $n_0 \in \mathbb{N}$ such that $y_i^{n_0} \in (z)$ for $1 \leq i \leq r$. Therefore $\mathfrak{m}^n \subseteq (z)$ for all $n \geq rn_0$. Suppose furthermore that $z \in \mathfrak{m}$ and let $m_0 \in \mathbb{N}$ be the smallest nonzero integer such that $\mathfrak{m}^{m_0} \subseteq (z)$. Choose $t \in \mathfrak{m}^{m_0-1}$, $t \notin (z)$. Then $t\mathfrak{m} \subseteq (z)$, thus $\frac{t}{z} \in \mathfrak{m}'$, but $\frac{t}{z} \notin R$. □

A final characterisation of DVRs (corollary 5.2.20) will be given in the next section.

§ 2 Invertible modules, fractional ideals, divisors

Throughout this section, R is a domain, K its field of fractions.

Definition 5.2.1 *A finitely generated R-module L is* **invertible** *if for every prime ideal $\mathfrak{p}$ of R there is an isomorphism $L_\mathfrak{p} \simeq R_\mathfrak{p}$.*

In other words, L is locally free of rank 1. In particular, a free rank 1 module is invertible, e.g. any principal ideal in R.

Remark 5.2.2 It suffices to check the condition at maximal ideals: every prime $\mathfrak{p}$ is contained in a maximal ideal $\mathfrak{m}$ and $L_\mathfrak{p} = (L_\mathfrak{m})_\mathfrak{p}$.

Example 5.2.3 Let R be a DVR with maximal ideal $\mathfrak{m} = (\pi)$. Let k be a field and suppose that R is a k-algebra and that $R/\mathfrak{m} = k$. Then if $\Omega^1_{R/k}$ is a finitely generated R-module (e.g. if R is a localisation of a finitely generated k-algebra) then it is free, generated by $d\pi$, and thus is an invertible module. To prove this, it suffices to show that $\Omega^1_{R/k} = Rd\pi + \pi\Omega^1_{R/k}$ and Nakayama's lemma will imply that $\Omega^1_{R/k} = Rd\pi$. Since $R = k \oplus \mathfrak{m}$, write any $x \in R$ as $x = \alpha + y\pi$, then $dx = d(y\pi) = yd\pi + \pi dy$. The claim now follows, since $\Omega^1_{R/k}$ is generated by $\mathrm{Im}(d)$.

Example 5.2.4 Let k be a field and R a finitely generated k-algebra such that k is algebraically closed in R. Assume that $R_\mathfrak{p}$ is a DVR for every nonzero prime ideal $\mathfrak{p}$. Then $\Omega^1_{R/k}$ is an invertible R-module. If $\overline{k}$ is the algebraic closure of k, $\overline{R} = R \otimes_k \overline{k}$ is a faithfully flat R-algebra and $\Omega^1_{\overline{R}/\overline{k}} = \Omega^1_{R/k} \otimes_R \overline{R}$, so we may assume that k is algebraically closed. Under these assumptions, the residue field at every nonzero prime is equal to k and we are in the situation of example 5.2.3. We shall write $\Omega^{-1}_{R/k} = Hom_R(\Omega^1_{R/k}, R)$ for the dual module. This is consistent with proposition 5.2.6 below.

Example 5.2.5 Let $M = \sum_p \frac{1}{p}\mathbb{Z} \subset \mathbb{Q}$ (sum over all prime numbers). Using Bezout's identity, it is easy to check that M is the subgroup of all rational numbers that, in reduced form, have square-free denominator. For a fixed prime number p, clearly $\sum_{q\neq p} \frac{1}{q}\mathbb{Z} \subseteq \mathbb{Z}_{(p)}$, thus $M_{(p)} = \frac{1}{p}\mathbb{Z}_{(p)}$ is locally free of rank 1, but M is not finitely generated, so it is not an invertible module.

If L and M are invertible modules, $L \otimes_R M$ and $L^\vee = Hom_R(L, R)$ are invertible too. This follows from the canonical isomorphisms

$$(L \otimes_R M)_\mathfrak{p} \cong L_\mathfrak{p} \otimes_{R_\mathfrak{p}} M_\mathfrak{p} \quad \text{and} \quad Hom_R(L, R)_\mathfrak{p} \cong Hom_{R_\mathfrak{p}}(L_\mathfrak{p}, R_\mathfrak{p}),$$

given respectively in corollary 2.1.22 and exercise 2.1 (or proposition 1.2.84, if R is noetherian).

Proposition 5.2.6 *An R-module L is invertible if and only if the evaluation map*

$$\varepsilon : L \otimes_R L^\vee \longrightarrow R \qquad x \otimes \lambda \longmapsto \lambda(x)$$

is an isomorphism.

Proof. If L is invertible, for every prime $\mathfrak{p}$ the evaluation $\varepsilon_\mathfrak{p} : L_\mathfrak{p} \otimes_{R_\mathfrak{p}} L_\mathfrak{p}^\vee \simeq R_\mathfrak{p} \otimes_{R_\mathfrak{p}} R_\mathfrak{p} \to R_\mathfrak{p}$ is an isomorphism, so ε is an isomorphism.
Conversely, suppose that ε is an isomorphism and let $y_1, \dots, y_n \in L$ and $\lambda_1, \dots, \lambda_n \in L^\vee$ such that $\sum_{i=1}^n \lambda_i(y_i) = 1$. If $\mathfrak{p}$ is a prime and $\lambda_i(y_i) \in \mathfrak{p}$ for $i = 1, \dots, n$ then $1 \in \mathfrak{p}$, which is absurd. We may assume thus $\lambda_1(y_1) \notin \mathfrak{p}$, hence $\lambda_1(y_1)$ is a unit in $R_\mathfrak{p}$. Put $z = \lambda_1(y_1)^{-1} y_1 \in L_\mathfrak{p}$. The map $\lambda_1 : L_\mathfrak{p} \to R_\mathfrak{p}$ is surjective (since $\lambda_1(z) = 1$) and thus splits ($R_\mathfrak{p}$ being free), whence a decomposition $L_\mathfrak{p} \simeq zR_\mathfrak{p} \oplus \ker(\lambda_1)$. Similarly, viewing z as a map $L_\mathfrak{p}^\vee \to R_\mathfrak{p}$, $\lambda \mapsto \lambda(z)$, we obtain a decomposition $L_\mathfrak{p}^\vee = \lambda_1 R_\mathfrak{p} \oplus \ker(z)$. Since ε is an isomorphism, $\varepsilon_\mathfrak{p} : L_\mathfrak{p} \otimes_{R_\mathfrak{p}} L_\mathfrak{p}^\vee \to R_\mathfrak{p}$ is an isomorphism. But

$$L_\mathfrak{p} \otimes_{R_\mathfrak{p}} L_\mathfrak{p}^\vee \simeq [zR_\mathfrak{p} \otimes \lambda_1 R_\mathfrak{p}] \oplus [\ker(\lambda_1) \otimes \lambda_1 R_\mathfrak{p}] \oplus [zR_\mathfrak{p} \otimes \ker(z)] \oplus [\ker(\lambda_1) \otimes \ker(z)]$$

and $\varepsilon_\mathfrak{p}$ is already an isomorphism on the first summand, thus $\ker(\lambda_1) = \ker(z) = 0$ (because they become zero after tensorisation by a free module), hence $L_\mathfrak{p} \simeq zR_\mathfrak{p}$ (and $L_\mathfrak{p}^\vee \simeq \lambda_1 R_\mathfrak{p}$).
Moreover, let $M \subseteq L$ be the submodule generated by $y_1, \dots, y_n$ and $\iota : M \to L$ the inclusion. Since $\iota_\mathfrak{p}$ is an isomorphism for all $\mathfrak{p}$, $M = L$ so L is finitely generated. □

Definition 5.2.7 *The* **Picard group** $\mathrm{Pic}(R)$ *of R is the set of isomorphism classes of invertible modules, with $[L_1] + [L_2] = [L_1 \otimes_R L_2]$, inverse $[L]^{-1} = [L^\vee]$ and unit element $[R]$. In number theory it is usually called the* **ideal class group**.

Before we compute some Picard groups, it is better to present an intimately related class of objects, as they will make these computation much simpler.

Definition 5.2.8 *A nonzero R-submodule $I \subseteq K$ is a* **fractional ideal** *if there exists $0 \neq x \in R$ such that $xI \subseteq R$.*

Example 5.2.9 Any ideal of R is a fractional ideal. These are called **integral fractional ideals**. Any $0 \neq y \in K$ defines a fractional ideal yR. These are called **principal fractional ideals**.

Example 5.2.10 Any invertible module is isomorphic to a fractional ideal:

$$L = L \otimes_R R \hookrightarrow L \otimes_R K \cong L_\mathfrak{p} \otimes_{R_\mathfrak{p}} K \simeq R_\mathfrak{p} \otimes_{R_\mathfrak{p}} K \cong K,$$

for any choice of a prime $\mathfrak{p}$. The existence of $x \in R$ such that $xL \subseteq R$ follows from the assumption that L is finitely generated, as detailed in the following remark.

Example 5.2.11 Let R be integrally closed, L a finite separable extension of K and $A \subset L$ integral over R with L as fraction field. Recall that in definition 3.3.8 we have introduced the codifferent as the A-module $\mathfrak{D}_{A/R}^{-1} = \{x \in L \,|\, Tr_{L/K}(xy) \in R \;\forall\, y \in A\}$. It is a fractional ideal of A: let $\{y_1, \dots, y_n\}$ be a K-basis for L such that $y_i \in A$ and let $\{y_1^*, \dots, y_n^*\}$ the dual basis with respect to the trace bilinear form. For any $x = \sum_i a_i y_i^* \in \mathfrak{D}_{A/R}^{-1}$, with $a_i \in K$, we have $Tr_{L/K}(xy_j) = \sum_i a_i Tr_{L/K}(y_i^* y_j) = a_j \in R$. Thus if $z \in A$ is a common denominator of the y_i^*, we get $z\,\mathfrak{D}_{A/R}^{-1} \subseteq A$.

Remark 5.2.12 Any finitely generated R-module $I \subset K$ is a fractional ideal: a common denominator x of a finite set $y_1, \dots, y_n$ of generators of I will give $xI \subseteq R$. Conversely, if R is noetherian, any fractional ideal I is finitely generated as R-module, since xI is an ideal of R.

Example 5.2.13 If the R-module $I \subset K$ is a fractional ideal then, for any multiplicative set $S \subset R$, the $S^{-1}R$-module $S^{-1}I$ is a fractional ideal.

For I and J fractional ideals, define IJ as the set of all finite sums $\sum x_i y_i$, with $x_i \in I$ and $y_i \in J$. This is again a fractional ideal (if $aI \subseteq R$ and $bJ \subseteq R$ then $abIJ \subseteq R$). Notice that $IR = I$. If $S \subset R$ is a multiplicative set, $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$.

If I is a fractional ideal, put $I' = \{x \in K | \, xI \subseteq R\}$. This is also a fractional ideal, since $yI' \subseteq R$ for all $y \in I$. If $S \subset R$ is a multiplicative set, $S^{-1}(I') \subseteq (S^{-1}I)'$. Indeed, if $x \in K$ is such that $xy \in R$ for all $y \in I'$, then $\frac{x}{s}\frac{y}{t} \in S^{-1}R$ for all $s, t \in S$. Moreover:

Lemma 5.2.14 *If I is a finitely generated fractional ideal, then $S^{-1}(I') = (S^{-1}I)'$.*

Proof. If $y_1, \ldots, y_n$ generate I and $z \in K^\times$ is such that $zy_i = \frac{a_i}{s_i} \in S^{-1}R$ for $i = 1, \ldots, n$, taking $s = \prod s_i$ we have $szy_i \in R$ for all i and therefore $szy \in R$ for all $y \in I$. Hence $sz \in I'$, thus $z \in S^{-1}(I')$. □

Lemma 5.2.15 *For any fractional ideal I, the map $I' \to Hom_R(I, R) = I^\vee$ sending $x \in I'$ to $\mu_x : I \to R$, with $\mu_x(y) = xy$, is an isomorphism.*

Proof. This map is clearly injective (K is a domain) and R-linear. Pick a nonzero element $z \in R$ such that $zI \subseteq R$. Let $\lambda \in I^\vee$. For any $y_1, y_2 \in I'$, since $zy_i \in R$ and λ is R-linear, we have $zy_1\lambda(y_2) = \lambda(zy_1y_2) = zy_2\lambda(y_1)$. Therefore $y_1\lambda(y_2) = y_2\lambda(y_1)$. Fix y_1 and put $x = \frac{\lambda(y_1)}{y_1}$. We get $\lambda(y_2) = xy_2$ for all $y_2 \in R$, therefore $\lambda = \mu_x$. □

Definition 5.2.16 *A fractional ideal I is* **invertible** *if $II' = R$.*

Notice that if I and J are fractional ideals with $IJ = R$ then I is invertible and $J = I'$. Indeed, one has $R = IJ \subseteq II' \subseteq R$, so $II' = R$ and multiplying $IJ = R$ by I' we get $J = I'$.

Remark 5.2.17 An invertible fractional ideal is finitely generated as an R-module: since $II' = R$ there exist $y_1, \ldots, y_n \in I$ and $x_1, \ldots, x_n \in I'$ such that $1 = x_1y_1 + \cdots + x_ny_n$. Then any $y \in I$ can be written as a linear combination $y = y \cdot 1 = \sum (x_i y) y_i$ of the y_i with coefficients $x_i y$ that are in R by definition.

Example 5.2.18 Under the assumptions and notation as in example 5.2.11, let us suppose furthermore that, for every maximal ideal $\mathfrak{m} \subset R$, $A_\mathfrak{m} = R_\mathfrak{m}[X]/(f)$, with f a monic polynomial such that $f'(x) \neq 0$. From proposition 3.3.10 we know that $\mathfrak{D}^{-1}_{A/R,\mathfrak{m}} = f'(x)^{-1}A_\mathfrak{m}$. In this case the codifferent is invertible and we write $\mathfrak{D}_{A/R}$ for $(\mathfrak{D}^{-1}_{A/R})'$. Notice that, since obviously $A \subseteq \mathfrak{D}^{-1}_{A/R'}$ then $\mathfrak{D}_{A/R} \subseteq A$ is an integral ideal, called the **different ideal**.

Proposition 5.2.19 *Over a local ring, every invertible fractional ideal is principal.*

Proof. By remark 5.2.17, I is finitely generated, say by $y_1, \ldots, y_n$. We can thus repeat the argument used in the proof of Claim 1, proposition 5.1.8. Since $II' = R$, there exist $x_1, \ldots, x_n \in I'$ such that $\sum x_i y_i = 1$. If all products $x_i y_1$ belong to the maximal ideal $\mathfrak{m}$ of R, then $1 \in \mathfrak{m}$, which is absurd. We may assume $u = x_1y_1 \notin \mathfrak{m}$, thus invertible. Put $z = u^{-1}y_1$, so $x_1 z = 1$. Now for all $y \in I$ we have $y = (yx_1)z$, with $yx_1 \in R$. □

Corollary 5.2.20 *Let R be a local domain. Then R is a DVR if and only if every nonzero fractional ideal is invertible.*

Proof. If R is a DVR and π a uniformiser, every nonzero fractional ideal is of the form (π^n), for some $n \in \mathbb{Z}$, hence invertible with inverse (π^{-n}).
Conversely, if every ideal is invertible, by proposition 5.2.19 R is a PID and we conclude by proposition 5.1.1. □

Theorem 5.2.21 *Let I be a fractional ideal. The following conditions are equivalent:*

a) I is an invertible fractional ideal.

b) I is an invertible module.

c) I is a projective module.

Proof. a) ⇒ b) follows from remark 5.2.17 and proposition 5.2.19. b) ⇒ c) because I is locally free.
c) ⇒ a) Let $\varphi : F = \oplus_\alpha R e_\alpha \twoheadrightarrow I$ be a surjection from a (possibly infinitely generated) free module and $\sigma : I \to F$ a splitting. Write $\sigma(y) = \sum_\alpha \sigma_\alpha(y) e_\alpha$ and consider $\sigma_\alpha \in I^\vee$. Lemma 5.2.15 provides us with an element $x_\alpha \in I' \subset K$ such that $\sigma_\alpha(y) = x_\alpha y$ for all $y \in I$. For a given $y \neq 0$, $\sigma_\alpha(y) = 0$ for all but finitely many α's. Hence $x_\alpha \neq 0$ for only finitely many α's. Renumbering the indices if necessary, let $x_1, \ldots, x_n$ be the non-zero values and put $y_\alpha = \varphi(e_\alpha)$. For all $y \in I$ we have

$$y = \varphi(\sigma(y)) = \varphi\left(\sum_{\alpha=1}^{n} (x_\alpha y) e_\alpha\right) = \sum_{\alpha=1}^{n} (x_\alpha y) y_\alpha = y\left(\sum_{\alpha=1}^{n} x_\alpha y_\alpha\right).$$

Hence $\sum x_\alpha y_\alpha = 1 \in II'$, which is an ideal in R. Thus $II' = R$. □

Definition 5.2.22 *The group of* **Cartier divisors** $\mathrm{Div}(R)$ *is the set of all invertible fractional ideals, with the product $I_1 I_2$ defined as above, $I^{-1} = I'$ and unit element R.*

By theorem 5.2.21 we have a map (of sets) $\mathrm{Div}(R) \to \mathrm{Pic}(R)$ sending an invertible fractional ideal to its isomorphism class as invertible module. Example 5.2.10 tells us that this map is surjective.

Proposition 5.2.23 *The map $\mathrm{Div}(R) \to \mathrm{Pic}(R)$ is a group homomorphism. Specifically, for any two invertible fractional ideals the multiplication map $\mu : I \otimes J \to IJ$, given by $\mu(x \otimes y) = xy$, is an isomorphism.*

Proof. Indeed, $\mu_\mathfrak{p}$ is an isomorphism for every prime ideal $\mathfrak{p}$ in R. □

A principal fractional ideal is, as a module, isomorphic to R. If $f, g \in K^\times$, the principal ideals $I = fR$ and $J = gR$ coincide if and only if $IJ' = fg^{-1}R = R$ i.e. if and only if $f = ug$ with u a unit in R. We can thus identify the subgroup of principal fractional ideals with the image of the map $K^\times \to \mathrm{Div}(R)$ taking f to fR and we have:

Corollary 5.2.24 *The following sequence of abelian groups is exact:*

$$1 \longrightarrow R^\times \longrightarrow K^\times \longrightarrow \mathrm{Div}(R) \longrightarrow \mathrm{Pic}(R) \longrightarrow 0.$$

Proof. Exactness in $\mathrm{Div}(R)$: if $\varphi : I \to R$ is an isomorphism, let $e \in I$ such that $\varphi(e) = 1$; for any $x \in I$ we have $x = \varphi(x)e$, because $x - \varphi(x)e \in \ker \varphi = 0$. So $I = eR$.
Exactness in $K^\times$: for $x \in K^\times$, if $xR = R$ then $x = x \cdot 1 \in R$. Moreover there exists $y \in R$ such that $1 = xy \in xR$, so $x \in R^\times$. □

Corollary 5.2.25 *If R is a PID then $\mathrm{Pic}(R) = 0$.*

Proof. If I is any fractional ideal, $xI \subseteq R$ is an integral ideal for as suitable non-zero $x \in R$. Then $xI = yR$ for some $y \in R$, hence $I = \frac{y}{x}R$, i.e. every fractional ideal is principal. □

We shall see later (corollary 6.1.16) that the Picard group of a UFD is trivial. Therefore, to see an example of a ring with a non-zero Picard group we have to go beyond UFD.

Example 5.2.26 Let $I = (2, 1 + \sqrt{-5}) \subset \mathbb{Z}[\sqrt{-5}] = R$. This ring is integrally closed (it's the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-5})$) and we have seen in example 1.2.59 that I is not principal but is a projective R-module, hence an invertible ideal by theorem 5.2.21. We can also check this directly: if $\mathfrak{p}$ is any prime such that $I \nsubseteq \mathfrak{p}$ then $I_\mathfrak{p} \simeq R_\mathfrak{p}$; on the other hand, if $I \subseteq \mathfrak{p}$ then $2 = 6 - 4 = -(1 + \sqrt{-5})^2 + 2(1 + \sqrt{-5}) - 4 \in \mathfrak{p}^2$, therefore $(1 + \sqrt{-5})R_\mathfrak{p} + \mathfrak{p}I_\mathfrak{p} = I_\mathfrak{p}$ and Nakayama's lemma implies $(1 + \sqrt{-5})R_\mathfrak{p} = I_\mathfrak{p}$. Thus $\mathrm{Pic}(\mathbb{Z}[\sqrt{-5}]) \neq 0$.

Remark 5.2.27 A basic result, proven in any number theory course worth its name, is that the Picard group of the ring of integers of a number field is finite.

Definition 5.2.28 *Let I and J be fractional ideals. We say that I divides J if there exists an integral ideal $\mathfrak{a} \subseteq R$ such that $J = \mathfrak{a}I$.*

Notice that, if I divides J then $J = \mathfrak{a}I \subseteq RI = I$. Conversely, if I is an invertible fractional ideal then $I \supseteq J$ implies I divides J because $JI' \subseteq II' = R$ is an integral ideal and $J = (JI')I$.

Proposition 5.2.29 *Let $I \subseteq R$ be an integral invertible ideal. Suppose that there exists prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ of R such that $I = \mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m$. Then the $\mathfrak{p}_i$ and the $\mathfrak{q}_j$ are invertible, $n = m$ and each $\mathfrak{p}_i$ is equal to one of the $\mathfrak{q}_j$. In other words, any such factorisation is unique, up to permutation of the factors.*

Proof. Since $\mathfrak{p}_1(\mathfrak{p}_2 \cdot \mathfrak{p}_n)I' = R$, the ideal $\mathfrak{p}_1$ is invertible. Since $\mathfrak{p}_1$ divides I, we have $\mathfrak{p}_1 \supseteq I = \mathfrak{q}_1 \cdots \mathfrak{q}_m$. Since $\mathfrak{p}_1$ is prime, it contains one of the factors, say $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$. Since $\mathfrak{p}_1$ is invertible, by the remark above there exists an integral ideal $\mathfrak{a} \subseteq R$ such that $\mathfrak{q}_1 = \mathfrak{a}\mathfrak{p}_1$. Hence $\mathfrak{a}$ divides $\mathfrak{q}_1$ too, thus $\mathfrak{a} \supseteq \mathfrak{q}_1$. Going back to the factorisation $\mathfrak{q}_1 = \mathfrak{a}\mathfrak{p}_1$, since $\mathfrak{q}_1$ is also prime, either $\mathfrak{p}_1 \subseteq \mathfrak{q}_1$, and therefore $\mathfrak{p}_1 = \mathfrak{q}_1$ or $\mathfrak{a} \subseteq \mathfrak{q}_1$, and therefore $\mathfrak{a} = \mathfrak{q}_1$.
Let's show that this second case leads to a contradiction. Indeed, it means that $\mathfrak{a} = \mathfrak{q}_1 = \mathfrak{a}\mathfrak{p}_1$; since $\mathfrak{q}_1$ is invertible, we would have $\mathfrak{a}\mathfrak{p}_1\mathfrak{q}_1' = R$, so $\mathfrak{a}$ would be invertible. But then we can "simplify" $\mathfrak{a} = \mathfrak{a}\mathfrak{p}_1$ and get $\mathfrak{p}_1 = R$, contrary to our assumption. Hence $\mathfrak{a} = \mathfrak{q}_1$ is impossible, and thus $\mathfrak{p}_1 = \mathfrak{q}_1$ must hold.
Multiplying on both sides the identity $\mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m$ by $\mathfrak{p}_1'$ we get $\mathfrak{p}_2 \cdots \mathfrak{p}_n = \mathfrak{q}_2 \cdots \mathfrak{q}_m$. If $n = 1$, this means $\mathfrak{q}_2 \cdots \mathfrak{q}_m = R$, thus $R \subseteq \mathfrak{q}_j$ for $j = 2, \ldots, m$ and, since these are integral ideals, $\mathfrak{q}_j = R$ and thus $m = 1$. If $n > 1$, we can repeat the procedure. □

We can rephrase the proposition as follows. Let $Z^1_{inv}(R)$ be the free abelian group generated by all invertible integral prime ideals in R. The map $Z^1_{inv}(R) \to \mathrm{Div}(R)$, taking a prime $\mathfrak{p}$ to itself, is an injective group homomorphism. If R is noetherian, this is in fact a *split* injection. In order to discuss this, it is better to involve a larger class of primes.

Definition 5.2.30 *A prime ideal $\mathfrak{p} \subset R$ is of* **height 1** *if the only prime ideals in $R_\mathfrak{p}$ are 0 and $\mathfrak{p}R_\mathfrak{p}$.*

If R is noetherian, every invertible prime ideal $\mathfrak{p}$ is of height 1: indeed $\mathfrak{p}R_\mathfrak{p}$ is principal and thus $R_\mathfrak{p}$ is a DVR. Notice that if R is noetherian and integrally closed, then $R_\mathfrak{p}$ is a DVR for every $\mathfrak{p}$ of height 1. Still, there are height 1 primes that are not invertible:

Example 5.2.31 Let k be a field, $R = k[X,Y,Z]/(Z^2 - XY)$. The polynomial $Z^2 - XY \in k[X,Y][Z]$ is Eisenstein with respect to the ideal X, hence irreducible, so R is a domain. We leave it as an exercise to check that R is the integral closure of $k[X,Y]$ in $k(X,Y)[Z]/(Z^2-XY)$, and thus integrally closed. Denote as usual by x, y, z the images of the variables in R and let $\mathfrak{p} = (y,z)$. Since $x \notin \mathfrak{p}$, we have $y = \frac{z^2}{x} \in zR_\mathfrak{p}$ so $R_\mathfrak{p} \simeq k(X)[Z]_{(Z)}$ is a DVR and $\mathfrak{p}$ is of height 1. But if $\mathfrak{m} = (x,y,z)$, since $Z^2 - XY \in (X,Y,Z)^2$, we have $\mathfrak{m}/\mathfrak{m}^2 = kx \oplus ky \oplus kz$ and $\mathfrak{p}/(\mathfrak{p} \cap \mathfrak{m}^2) = ky \oplus kz$, so $\mathfrak{p}R_\mathfrak{m}$ can't be generated by only one element, thus $\mathfrak{p}$ is not invertible. Geometrically, $\operatorname{Spec} R$ is a cone with vertex in $\mathfrak{m}$ and $\mathcal{Z}(\mathfrak{p})$ is a line through the vertex. The fact that $\mathfrak{p}$ is not invertible translates the fact that such a line can't be obtained as the intersection of the cone with a single hypersurface.

Remark 5.2.32 If R is a UFD, any prime ideal of height 1 is principal. Indeed, if $\mathfrak{p}$ is such a prime and $0 \neq x \in \mathfrak{p}$ then for every irreducible factor y of x, the ideal (y) is prime and $0 \neq (y) \subseteq \mathfrak{p}$, hence $\mathfrak{p} = (y)$. Therefore if R has the property that $R_\mathfrak{q}$ is a UFD for every prime $\mathfrak{q}$ (a ring with this property is called **locally factorial**) then every prime ideal of height 1 is invertible. Notice that a locally factorial domain is integrally closed, by corollary 3.1.17 and example 3.1.7.

In corollary 6.1.14 we will see that in a noetherian domain every invertible ideal is contained in a prime ideal of height 1. Moreover, we have the following finiteness result:

Lemma 5.2.33 *Let $\mathfrak{a} \subseteq R$ be an ideal in a noetherian domain. Only finitely many height 1 prime ideals of R may contain $\mathfrak{a}$.*

Proof. Since $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$ and the latter is the intersection of all prime ideals containing $\mathfrak{a}$ we may assume that $\mathfrak{a}$ is radical. By exercise 4.3, every radical ideal is the intersection of finitely many non-zero prime ideals, say $\mathfrak{a} = \mathfrak{p}_1 \cap \ldots \mathfrak{p}_n$. Suppose that $\mathfrak{q} \supseteq \mathfrak{a}$ is a height 1 prime ideal. Then $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{p}_1 \cap \ldots \mathfrak{p}_n \subseteq \mathfrak{q}$. Since $\mathfrak{q}$ is prime, $\mathfrak{q} \supseteq \mathfrak{p}_i$ for some i. By definition, the only prime ideals contained in $\mathfrak{q}$ are 0 and $\mathfrak{q}$, hence $0 \neq \mathfrak{p}_i = \mathfrak{q}$. □

Definition 5.2.34 *Let R be a noetherian domain. The group of* **Weil divisors** *$Z^1(R)$ is the free abelian group generated by all height 1 prime ideals in R.*

In particular, the group $Z^1_{inv}(R)$ defined above is a subgroup of the group of Weil divisors. Remark 5.2.32 tells us that $Z^1_{inv}(R) = Z^1(R)$ if R is locally factorial.

We shall now define the map splitting the homomorphism $Z^1_{inv}(R) \to \operatorname{Div}(R)$ above under the assumption that R is integrally closed. See theorem 5.2.38 below for the definition in the general case.

Let R be an integrally closed noetherian domain, $\mathfrak{a} \subseteq R$ an invertible integral ideal and $\mathfrak{p}$ a prime ideal of height 1. Then $R_\mathfrak{p}$ is a DVR, hence $\mathfrak{a}R_\mathfrak{p} = (\pi^{v_\mathfrak{p}(\mathfrak{a})})$, where π is any uniformiser. If I is a fractional ideal and $0 \neq x \in R$ is such that $xI \subseteq R$, define $v_\mathfrak{p}(I) = v_\mathfrak{p}(xI) - v_\mathfrak{p}(x)$. It is an easy exercise to check that this does not depend on x.

Theorem 5.2.35 *Let R be an integrally closed noetherian domain. The* **cycle map**

$$\begin{array}{rcl} \mathrm{Div}(R) & \longrightarrow & Z^1(R) \\ I & \longmapsto & \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)} \end{array}$$

is a group homomorphism.

Proof. Notice first that if $\mathfrak{a} \subseteq R$ is an invertible integral ideal, if $\mathfrak{a} \nsubseteq \mathfrak{p}$ then $\mathfrak{a}R_{\mathfrak{p}} = R_{\mathfrak{p}}$. Therefore $v_{\mathfrak{p}}(\mathfrak{a}) > 0$ if and only if $\mathfrak{a} \subseteq \mathfrak{p}$. Lemma 5.2.33 ensures that the product is finite and the definition makes sense. To show that the cycle map is well defined and is a group homomorphism, we need to check that relations are preserved: if $\mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{b}_1 \cdots \mathfrak{b}_m$, the two must map to the same Weil divisor. This follows from the general properties of valuations: $v_{\mathfrak{p}}(\mathfrak{ab}) = v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b})$. □

Proposition 5.2.36 *In a locally factorial noetherian domain, every invertible fractional ideal is a product of finitely many invertible primes.*

Proof. It suffices to prove the statement for an integral invertible ideal $I \subset R$. Let $\mathfrak{p}$ be a height 1 prime ideal containing I: we shall see in corollary 6.1.14 that such a prime always exists. By remark 5.2.32, in a locally factorial domain every prime of of height 1 is invertible. As remarked right after definition 5.2.28, since $\mathfrak{p}$ is invertible $I \subseteq \mathfrak{p}$ is equivalent to saying that $\mathfrak{p}$ divides I. Thus $I = \mathfrak{p}I_1$ for some $I_1 \subseteq R$. Being a product of invertible ideals $I_1 = \mathfrak{p}'I$ is also invertible, so we can iterate. Any prime containing I_1 also contains I, so the number of primes involved is finite by lemma 5.2.33. Moreover, if $I \subseteq \mathfrak{p}_1$ then $IR_{\mathfrak{p}_1} = \mathfrak{p}_1^{n_1} R_{\mathfrak{p}_1}$, since $R_{\mathfrak{p}_1}$ is a DVR. Thus $I \nsubseteq \mathfrak{p}_1^{n_1+1}$, so a prime can only appear a finite number of times in a factorisation of I. □

In view of lemma 5.2.33 and propositions 5.2.29 and 5.2.36 we have established:

Theorem 5.2.37 *Let R be a locally factorial noetherian domain.*

a) The cycle map is an isomorphism between the groups of Cartier and Weil divisors.

b) Every invertible fractional ideal may be uniquely expressed as a finite product $\prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$, where the $\mathfrak{p}$'s are prime ideals of height 1 and $n_{\mathfrak{p}} \in \mathbb{Z}$.

Let us also define the cycle map for an arbitrary noetherian domain R. We proceed in an ad hoc manner, as a clean definition requires the notion of length which we haven't developed sufficiently. If $\mathfrak{a} \subseteq R$ an invertible integral ideal and $\mathfrak{p}$ a prime ideal of height 1, proposition 5.2.19 tells us that $\mathfrak{a}R_{\mathfrak{p}}$ is principal, say $\mathfrak{a}R_{\mathfrak{p}} = (a)$. In corollary 6.1.24, we shall see that there exists an element $\pi \in \mathfrak{p}$ such that $\mathfrak{p}^n \subseteq (\pi) \subseteq \mathfrak{p}$ for all n sufficiently large. We can thus invoke lemma 5.1.3 to conclude that $\bigcap_{n \geq 0} \mathfrak{p}^n = 0$. Therefore, there exists an integer $n \geq 0$ such that $a \in \mathfrak{p}^n R_{\mathfrak{p}}$ but $a \notin \mathfrak{p}^{n+1} R_{\mathfrak{p}}$: denote this integer by $\ell_{\mathfrak{p}}(\mathfrak{a})$. If I is an invertible fractional ideal and $0 \neq x \in R$ is such that $xI \subseteq R$, define $\ell_{\mathfrak{p}}(I) = \ell_{\mathfrak{p}}(xI) - \ell_{\mathfrak{p}}(xR)$. It can be shown, using theorem 4.2.3 and related techniques, that this definition is independent on all these choices.

Theorem 5.2.38 *Let R be a noetherian domain. The* **cycle map**

$$\begin{array}{rcl} \mathrm{Div}(R) & \longrightarrow & Z^1(R) \\ I & \longmapsto & \prod_{\mathfrak{p}} \mathfrak{p}^{\ell_{\mathfrak{p}}(I)} \end{array}$$

is a group homomorphism. ⊠

Example 5.2.39 Let k be a perfect field and $\overline{k}$ its algebraic closure. Let $F(X,Y) \in k[X,Y]$ be an irreducible polynomial and $R = k[X,Y]/(F)$. Assume that k is algebraically closed in R and that the plane curve $\mathcal{Z}(F)$ is nonsingular, i.e. for every $(x_0,y_0) \in \overline{k}^2$ such that $F(x_0,y_0) = 0$ then $\left(\frac{\partial F}{\partial X}(x_0,y_0), \frac{\partial F}{\partial Y}(x_0,y_0)\right) \neq (0,0)$.
Denote $\overline{R} = \overline{k} \otimes_k R$. Let us first check that the localisation $\overline{R}_{\mathfrak{m}}$ is a DVR for every maximal ideal $\mathfrak{m} \subset \overline{R}$. Since $\pi : \overline{k}[X,Y] \to \overline{R}$ is surjective, $\pi^{-1}(\mathfrak{m})$ is a maximal ideal in $\overline{k}[X,Y]$ and thus of the form $(X - x_0, Y - y_0)$ (weak Nullstellensatz). A linear change of variables reduces us to the case $(x_0,y_0) = (0,0)$. Then $F(X,Y) \in aX + bY + (X,Y)^2$ and by assumption $(a,b) \neq (0,0)$. If, say, $a \neq 0$ then $x \in \frac{b}{a}y + \mathfrak{m}^2$, so $\mathfrak{m}R_{\mathfrak{m}}$ is principal. Since the localisations of $\overline{R}$ at maximal ideals are all DVRs, we deduce that every nonzero prime ideal in $\overline{R}$ is maximal (take $0 \neq \mathfrak{p} \subseteq \mathfrak{m}$: since $\overline{R}_{\mathfrak{m}}$ is a DVR, $\mathfrak{p}\overline{R}_{\mathfrak{m}} = \mathfrak{m}\overline{R}_{\mathfrak{m}}$, so $\mathfrak{p} = \mathfrak{m}$).
Thus $\overline{R}$ is a **Dedekind domain**: every prime ideal is of height 1 and invertible (see definition 5.3.2 below). Let us then show that R is a Dedekind domain too. It is a domain and finitely generated over a field, thus noetherian. Every prime ideal $\mathfrak{p} \subset R$ is maximal: indeed, decompose $\overline{k} \otimes_k \mathfrak{p} = \prod_{i=1}^r \mathfrak{m}_i^{e_i}$ as a finite product in $\overline{R}$. Since $\pi^{-1}(\mathfrak{m}_i) = \widetilde{\mathfrak{m}}_i = (X - x_i, Y - y_i)$, taking $k' = k(x_1,\dots,x_r,y_1,\dots,y_r)$ (a finite extension), by the Chinese Remainder Theorem we get that $R/\mathfrak{p}$ is contained in the finite-dimensional k'-vector space $k' \otimes_k R/\mathfrak{p}R \simeq \prod_{i=1}^r k'[X,Y]/\widetilde{\mathfrak{m}}_i^{e_i}$, hence $\dim_k R/\mathfrak{p} < +\infty$. Thus $R/\mathfrak{p}$ is a domain, finite, hence integral, over a field: it is a field and therefore $\mathfrak{p}$ is maximal. To conclude that R is a Dedekind domain, we have to show that it is integrally closed. Let $z \in K = \operatorname{Frac} R$ be integral over R, then it belongs to $\overline{R}$, since the latter is integrally closed, and is in R because $\sigma(z) = z$ for every $\sigma \in \operatorname{Gal}(\overline{k}/k)$, as $z \in K$.

A divisor on R (Cartier and Weil agree in this case) is a fractional ideal $D = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$, with the $n_{\mathfrak{p}} \in \mathbb{Z}$. Geometrically this is a finite formal sum $\sum_P n_P P$ of points on the curve $\mathcal{Z}(F)$.
To a divisor D one associates the invertible module $\mathcal{L}(D) = \{f \in K \mid v_{\mathfrak{p}}(f) + n_{\mathfrak{p}} \geq 0\}$. This is nothing but the fractional ideal we denoted D'. Indeed, if $f \in \mathcal{L}(D)$ and $y \in D$ then $v_{\mathfrak{p}}(fy) \geq 0$ for all primes $\mathfrak{p}$, thus $fy \in R_{\mathfrak{p}}$ for all $\mathfrak{p}$. This is equivalent to saying $fy \in R$. Indeed, if $\frac{r}{s} \in K$ and $v_{\mathfrak{p}}(\frac{r}{s}) = v_{\mathfrak{p}}(r) - v_{\mathfrak{p}}(s) \geq 0$ for all $\mathfrak{p}$, then $(r) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(r)} \subset \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(s)} = (s)$, thus $r \in (s)$, so $r = st$ for some $t \in R$ and $\frac{r}{s} = t \in R$.
Since R is finitely generated as k-algebra, for every non-zero prime ideal $\mathfrak{p} \subset R$, the field $R/\mathfrak{p}$ is a finite extension of k. We may thus define the **degree** of a divisor

$$\deg\left(\prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}\right) = \sum_{\mathfrak{p}} n_{\mathfrak{p}} [R/\mathfrak{p} : k].$$

§ 3 Dedekind domains

Proposition 5.3.1 *Let R be a noetherian domain. The following conditions are equivalent:*

a) $R_{\mathfrak{p}}$ is a DVR for every nonzero prime ideal $\mathfrak{p} \subset R$.

b) R is integrally closed and every non-zero prime ideal is maximal.

Proof. Recall that R is integrally closed if $R_\mathfrak{p}$ is integrally closed for every prime ideal $\mathfrak{p}$. If a) holds and $\mathfrak{p}$ is a prime, let $\mathfrak{m} \supseteq \mathfrak{p}$ be a maximal ideal containing it. Then $\mathfrak{p}R_\mathfrak{m}$ is a prime in a DVR, thus either $\mathfrak{p} = 0$ or $\mathfrak{p} = \mathfrak{m}$.
Conversely, if every non-zero prime ideal $\mathfrak{p} \subset R$ is maximal, the only primes in $R_\mathfrak{p}$, being in bijection with primes in R contained in $\mathfrak{p}$, are 0 and $\mathfrak{p}R_\mathfrak{p}$. Thus $R_\mathfrak{p}$ is local, noetherian, integrally closed and has only one nonzero prime: it is a DVR by proposition 5.1.8. □

Definition 5.3.2 A **Dedekind domain** is a ring satisfying the equivalent conditions of propostion 5.3.1.

Example 5.3.3 A DVR is a Dedekind domain. More generally, a PID is a Dedekind domain. See corollary 5.3.10 below for a partial converse.

Proposition 5.3.4 *Let R be a Dedekind domain and A a noetherian integrally closed domain integral over R. Then A is also a Dedekind domain.*

Proof. If $\mathfrak{q} \subset A$ is a nonzero prime, $\mathfrak{p} = \mathfrak{q} \cap R$ is maximal; then $A/\mathfrak{q}$ is integral over the field $R/\mathfrak{p}$ and is therefore a field, so $\mathfrak{q}$ is maximal. □

Corollary 5.3.5 *Let R be a Dedekind domain, K its fraction field, L a finite separable extension of K and A the integral closure of R in L. Then A is a Dedekind domain*

Proof. Put together corollaries 4.1.11 5.3.4. □

Remark 5.3.6 The separability assumption is unnecessary, see exercise 5.4.

Example 5.3.7 The ring of integers $\mathcal{O}_K$ in a number field K is a Dedekind domain.

Example 5.3.8 $\mathbb{C}[X,Y]/(X^2+Y^2-1)$ is the integral closure of $\mathbb{C}[X]$ in $\mathbb{C}(X)[Y]/(Y^2+X^2-1)$, and is thus a Dedekind domain. On the other hand, $\mathbb{C}[X,Y]/(X^3+X^2-Y^2)$ is not a Dedekind domain, since its localisation at $\mathfrak{m}_0 = (x,y)$ is not a DVR (see example 5.1.7).

Since its localisations at every nonzero prime are PIDs, a Dedekind domain is locally factorial. Moreover, every nonzero prime ideal being maximal, it is of height 1. We can thus apply theorem 5.2.37 to conclude:

Theorem 5.3.9 *Every fractional ideal in a Dedekind domain is invertible and can be written uniquely as a product of integral powers of prime ideals.*

Corollary 5.3.10 *A semi-local Dedekind domain is a PID.*

Proof. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be all the nonzero prime ideals in R. The map $\varphi : R \to \prod_{i=1}^r R/\mathfrak{p}_i$ is surjective by the Chinese remainder theorem. Fix i and pick $x_i \in \mathfrak{p}_i$, $x_i \notin \mathfrak{p}_i^2$ (notice that $\mathfrak{p}_i \neq \mathfrak{p}_i^2$: otherwise multiplying $\mathfrak{p}_i = \mathfrak{p}_i^2$ by $\mathfrak{p}_i'$ we get $R = \mathfrak{p}_i$, absurd). Take $\pi_i \in R$ such that $\varphi(\pi_i) = (1, \dots, 1, x_i, 1, \dots, 1)$. Then $\mathfrak{p}_i | (\pi_i)$ but $\mathfrak{p}_i^2 \nmid (\pi_i)$ and $\mathfrak{p}_j \nmid (\pi_i)$ for $i \neq j$. Thus $(\pi_i) = \mathfrak{p}_i$. □

If I is a fractional ideal in a Dedekind domain, written as $I = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}$, set $v_\mathfrak{p}(I) = n_\mathfrak{p}$. The following lemma is often useful in computations.

Lemma 5.3.11 *Let I, J be fractional ideals in a Dedekind domain R and $\mathfrak{p}$ a nonzero prime ideal.*

a) $v_\mathfrak{p}(IJ) = v_\mathfrak{p}(I) + v_\mathfrak{p}(J)$.

b) $v_\mathfrak{p}(I) \geq 0 \; \forall \, \mathfrak{p} \iff I \subseteq R$.

c) $v_\mathfrak{p}(I + J) = \min\{v_\mathfrak{p}(I), v_\mathfrak{p}(J)\}$.

d) $v_\mathfrak{p}(I \cap J) = \max\{v_\mathfrak{p}(I), v_\mathfrak{p}(J)\}$.

Proof. The first two are obvious. Since $I, J \subseteq I + J$, we have $v_\mathfrak{p}(I + J) \leq \min\{v_\mathfrak{p}(I), v_\mathfrak{p}(J)\}$. On the other hand, for every fractional ideal H containing both I and J, from $H \supseteq I + J$ it follows that $v_\mathfrak{p}(H) \leq v_\mathfrak{p}(I + J)$. Therefore, from

$$I + J = \mathfrak{p}^{v_\mathfrak{p}(I+J)} \prod_{\mathfrak{q} \neq \mathfrak{p}} \mathfrak{q}^{n_\mathfrak{q}} \subseteq \mathfrak{p}^{\min\{v_\mathfrak{p}(I), v_\mathfrak{p}(J)\}} \prod_{\mathfrak{q} \neq \mathfrak{p}} \mathfrak{q}^{n_\mathfrak{q}}$$

we get $\min\{v_\mathfrak{p}(I), v_\mathfrak{p}(J)\} \leq v_\mathfrak{p}(I + J)$.
Since $I, J \supseteq I \cap J$, we have $v_\mathfrak{p}(I \cap J) \geq \max\{v_\mathfrak{p}(I), v_\mathfrak{p}(J)\}$. On the other hand, for every fractional ideal H contained both I and J, since $H \subseteq I \cap J$ it follows that $v_\mathfrak{p}(H) \geq v_\mathfrak{p}(I \cap J)$, hence from

$$I \cap J = \mathfrak{p}^{v_\mathfrak{p}(I \cap J)} \prod_{\mathfrak{q} \neq \mathfrak{p}} \mathfrak{q}^{n_\mathfrak{q}} \supseteq \mathfrak{p}^{\max\{v_\mathfrak{p}(I), v_\mathfrak{p}(J)\}} \prod_{\mathfrak{q} \neq \mathfrak{p}} \mathfrak{q}^{n_\mathfrak{q}}$$

we get $\max\{v_\mathfrak{p}(I), v_\mathfrak{p}(J)\} \geq v_\mathfrak{p}(I \cap J)$. □

Let now R be a Dedekind domain, K its fraction field, L be a finite extension of K and A the integral closure of R in K. We will assume that A is noetherian and then, as seen in proposition 5.3.4, A is again Dedekind. In corollary 5.3.5, we have shown that this is indeed the case if L/K is separable, but it is true in general by exercise 5.4. Beware that if L/K is not separable, A is not necessarily a finitely generated R-module: exercise 3.5 provides a counterexample with both R and A discrete valuation rings..

Let $\mathfrak{p} \subset R$ be a nonzero prime and $\mathfrak{p}A = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$ the decomposition of the ideal $\mathfrak{p}A$, with $\mathfrak{q}_i$ primes in A. Notice that $\mathfrak{q}_i \cap R$ is a prime ideal containing the maximal ideal $\mathfrak{p}$. Thus $\mathfrak{q}_i \cap R = \mathfrak{p}$ for $1 \leq i \leq r$.

Definition 5.3.12 The exponent $e_i = e(\mathfrak{q}_i/\mathfrak{p}) = v_{\mathfrak{q}_i}(\mathfrak{p}A)$ is called the **ramification index** of $\mathfrak{q}_i$ over $\mathfrak{p}$. The number $f_i = f(\mathfrak{q}_i/\mathfrak{p}) = [A/\mathfrak{q}_i : R/\mathfrak{p}]$ is the **residue** (or **inertia**) **degree** of $\mathfrak{q}_i$ over $\mathfrak{p}$.

The residue degree is a finite number in view of the following result.

Lemma 5.3.13 *Let $\mathfrak{a} \subset A$ be an ideal such that $\mathfrak{a} \cap R = \mathfrak{p}$. Then $\dim_{R/\mathfrak{p}}(A/\mathfrak{a}) \leq [L : K]$.*

Proof. Since $A_\mathfrak{p}/\mathfrak{a}_\mathfrak{p} \cong A/\mathfrak{a}$, we may localise in $\mathfrak{p}$ and thus assume that R is a DVR, with maximal ideal $\mathfrak{p} = (\pi)$. Let $x_1, \ldots, x_r$ be elements in A such that the classes $\overline{x}_i \in A/\mathfrak{a}$ are $R/\mathfrak{p}$-linearly independent. The claim follows if we show that $x_1, \ldots, x_r$ are K-linearly independent. Indeed, if $\sum \alpha_i x_i = 0$ and some $\alpha_i \neq 0$, taking $m = \min\{v_\mathfrak{p}(\alpha_i)\}$ and multiplying by π^{-m} we may assume that all the $\alpha_i \in R$ and that at least one of the coefficients is in $R - \mathfrak{p}$. Reducing modulo $\mathfrak{p}$, we obtain an $R/\mathfrak{p}$-linear combination of the $\overline{x}_i$ with some nonzero coefficients, a contradiction. □

Theorem 5.3.14 *Let $R \subseteq A$ be an extension of Dedekind domains, A the integral closure of R in the finite extension L of $K = \operatorname{Frac} R$. Let $\mathfrak{p} \subset R$ be a nonzero prime, $\mathfrak{p}A = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$. Then*

a) $\sum_{i=1}^{r} e_i f_i = \dim_{R/\mathfrak{p}} A/\mathfrak{p}A \leq [L : K]$.

b) If $A_\mathfrak{p}$ is finite over $R_\mathfrak{p}$ (e.g. if L/K is separable or if $R_\mathfrak{p}$ is complete), then $\sum_{i=1}^{r} e_i f_i = [L : K]$.

Proof. The inequality in a) is given in lemma 5.3.13. For the first equality, by the Chinese remainder theorem $A/\mathfrak{p}A \cong \bigoplus_{i=1}^{r} A/\mathfrak{q}_i^{e_i}$. From the sequence

$$\mathfrak{q}_i^{e_i} \subsetneq \mathfrak{q}_i^{e_i-1} \subsetneq \cdots \subsetneq \mathfrak{q}_i \subsetneq A$$

we obtain an isomorphism $A/\mathfrak{q}_i^{e_i} \simeq \bigoplus_{j=0}^{e_i-1} \mathfrak{q}_i^j/\mathfrak{q}_i^{j+1}$ as $R/\mathfrak{p}$-vector spaces. If τ is a uniformiser of $A_{\mathfrak{q}_i}$ then $\mathfrak{q}_i^j A_{\mathfrak{q}_i} = (\tau^j)$, hence $\dim_{A/\mathfrak{q}_i} \mathfrak{q}_i^j/\mathfrak{q}_i^{j+1} = 1$ and therefore $\dim_{R/\mathfrak{p}} \mathfrak{q}_i^j/\mathfrak{q}_i^{j+1} = f_i$.
Assume now that $A_\mathfrak{p}$ is finitely generated as an $R_\mathfrak{p}$ module. Since the latter is a PID we can apply the elementary divisors theorem. Since A is a domain, so is $A_\mathfrak{p}$, which is then torsion free and thus free. Its rank can be computed as $\operatorname{rk} A_\mathfrak{p} = \dim_K(A_\mathfrak{p} \otimes_{R_\mathfrak{p}} K) = [L : K]$, but also $\operatorname{rk} A_\mathfrak{p} = \dim_{R/\mathfrak{p}}(A_\mathfrak{p} \otimes_{R_\mathfrak{p}} R/\mathfrak{p}) = \dim_{R/\mathfrak{p}}(A/\mathfrak{p}A)$. □

Remark 5.3.15 Fixing a prime $\mathfrak{q}$ above $\mathfrak{p} = \mathfrak{q} \cap R$, the valuations give a commutative diagram

$$\begin{array}{ccc} K^\times & \xrightarrow{v_\mathfrak{p}} & \mathbb{Z} \\ {\scriptstyle\iota}\downarrow & & \downarrow{\scriptstyle e} \\ L^\times & \xrightarrow{v_\mathfrak{q}} & \mathbb{Z} \end{array}$$

where $\iota : K \subseteq L$ is the inclusion and the vertical arrow to the right is multiplication by the ramification index $e = e(\mathfrak{q}/\mathfrak{p})$. Indeed, if $\pi \in \mathfrak{p}R_\mathfrak{p}$ is a uniformiser, since $\mathfrak{p}A_\mathfrak{q} = \mathfrak{q}^e A_\mathfrak{q}$, we have $v_\mathfrak{q}(\pi) = e$ and then $v_\mathfrak{q}(x) = e v_\mathfrak{p}(x)$ for all $x \in K^*$.

Definition 5.3.16 Let R be a Dedekind domain, K its fraction field, L/K a finite separable extension and A the integral closure of R in L. Let $0 \neq \mathfrak{p} \subset R$ be a prime, $\mathfrak{p}A = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$. We say that

a) L/K is **unramified** at $\mathfrak{q}_i$ if $e_i = 1$ and $A/\mathfrak{q}_i$ is separable over $R/\mathfrak{p}$.

b) L/K is **totally ramified** above $\mathfrak{p}$ if $e_1 = [L : K]$.

c) $\mathfrak{p}$ is **inert** in L if $f_1 = [L : K]$.

d) $\mathfrak{p}$ **splits completely** in L if $r = [L : K]$.

In order to investigate the behaviour of a nonzero prime $\mathfrak{p} \subset R$ in a a finite separable extension, an extremely useful tool is the technique of completion, as it allows one to assume that there is only one prime above $\mathfrak{p}$. Indeed, by theorem 3.6.11, the integral closure of a complete DVR in a finite extension of its fraction field is also a complete DVR. Notice by the way that we only need the uniqueness part in this case, as we know that a prime above $\mathfrak{p}$ exists. By proposition 3.6.10, the extension is automatically complete. Moreover, if L/K is also normal, we may replace the Galois group by a smaller, and much simpler, subgroup (see remark 5.3.19).

Proposition 5.3.17 *Let R be a Dedekind domain, K its fraction field, L/K a finite extension and A the integral closure of R in L. Let $0 \neq \mathfrak{p} \subset R$ be a prime ideal, $\mathfrak{p}A = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$ its decomposition, $f_i = f(\mathfrak{q}_i/\mathfrak{p})$ the inertia degrees. Let $\hat{K}$ (resp. $\hat{L}_i$) be the completion of K (resp. L) with respect to $v_\mathfrak{p}$ (resp. $v_{\mathfrak{q}_i}$). Let $\hat{R}$ and $\hat{A}_i$ be the valuation rings, $\hat{\mathfrak{p}} \subset \hat{R}$ and $\hat{\mathfrak{q}}_i \subset \hat{A}_i$ their maximal ideals. Then*

a) $\hat{R}$ (resp. $\hat{A}_i$) is the completion of $R_\mathfrak{p}$ (resp. $A_{\mathfrak{q}_i}$); $\hat{\mathfrak{p}} = \mathfrak{p}\hat{R}$ and $\hat{\mathfrak{q}}_i = \mathfrak{q}_i\hat{A}_i$;

b) $e_i(\hat{\mathfrak{q}}_i/\hat{\mathfrak{p}}) = e_i$ and $f_i(\hat{\mathfrak{q}}_i/\hat{\mathfrak{p}}) = f_i$;

c) $\hat{L}_i$ is an extension of $\hat{K}$ of degree $e_i f_i$;

d) The natural map $\varphi : \hat{R} \otimes_R A \to \prod_{i=1}^{r} \hat{A}_i$ is injective and induces $\hat{K} \otimes_K L \cong \prod_{i=1}^{r} \hat{L}_i$. Moreover φ is an isomorphism if A is finite over R.

Proof. a) the first part follows immediately from the definitions, for the second notice that by lemma 3.6.15 the maximal ideal of $\hat{R}$ (resp $\hat{A}_i$) is generated by a uniformizer of $R_\mathfrak{p}$ (resp. $A_{\mathfrak{q}_i}$).
b) The equality of the ramification indices follows from what we just said about uniformizers. By proposition 3.6.16 and corollary 2.1.13, $\hat{R}/\hat{\mathfrak{p}} = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} = R/\mathfrak{p}$ and similarly $\hat{A}_i/\hat{\mathfrak{q}}_i = A/\mathfrak{q}_i$, hence $f_i(\hat{\mathfrak{q}}_i/\hat{\mathfrak{p}}) = f_i$.
c) follows from b) and theorem 5.3.14.
d) The second claim follows from the first, which gives an injection between $\hat{K}$-vector spaces of the same dimension. For every $i \neq j$ and $n_i, n_j \in \mathbb{N}$, the ideals $\mathfrak{q}_i^{n_i}$ and $\mathfrak{q}_j^{n_j}$ are coprime: indeed, if $\mathfrak{q}_i^{n_i} + \mathfrak{q}_j^{n_j} \neq A$, there is a maximal ideal $\mathfrak{m} \subset A$ containing it, which implies $\mathfrak{q}_i^{n_i} \subseteq \mathfrak{m}$ and $\mathfrak{q}_j^{n_j} \subseteq \mathfrak{m}$, whence $\mathfrak{q}_i = \mathfrak{m} = \mathfrak{q}_j$. For every $n \geq 1$, by the Chinese Remainder Theorem, we have an exact sequence

$$0 \longrightarrow \prod_{i=1}^{r} \mathfrak{q}_i^n / \prod_{i=1}^{r} \mathfrak{q}_i^{ne_i} \longrightarrow A/\prod_{i=1}^{r} \mathfrak{q}_i^{ne_i} \longrightarrow \prod_{i=1}^{r} A/\mathfrak{q}_i^n \longrightarrow 0. \tag{5.1}$$

Notice that $A/\prod_{i=1}^{r} \mathfrak{q}_i^{ne_i} = R/\mathfrak{p}^n \otimes_R A$ (just tensor $0 \longrightarrow \mathfrak{p}^n \longrightarrow R \longrightarrow R/\mathfrak{p}^n \longrightarrow 0$ by A). The sequences (5.1) build up to an exact sequence of inverse systems, so by proposition 3.6.35 we get an exact sequence

$$0 \longrightarrow \varprojlim \left(\prod_{i=1}^{r} \mathfrak{q}_i^n / \prod_{i=1}^{r} \mathfrak{q}_i^{ne_i}\right) \longrightarrow \hat{R} \otimes_R A \longrightarrow \prod_{i=1}^{r} \hat{A}_i.$$

A priori we do not get a zero on the right as the maps for the left hand side system are not surjective. By exercise 3.10, we have $\varprojlim \left(\prod_{i=1}^{r} \mathfrak{q}_i^n / \prod_{i=1}^{r} \mathfrak{q}_i^{ne_i}\right) = 0$, hence $\hat{R} \otimes_R A \to \prod_{i=1}^{r} \hat{A}_i$ is an injection of $\hat{R}$-modules. Let C be its cokernel. Tensoring $0 \longrightarrow \hat{R} \otimes_R A \longrightarrow \prod_{i=1}^{r} \hat{A}_i \longrightarrow C \longrightarrow 0$ by $R/\mathfrak{p}$ we get the isomorphism $A/\mathfrak{p}A \simeq \prod_{i=1}^{r} A/\mathfrak{q}_i^{e_i}$, hence $C/\mathfrak{p}C = 0$. Assuming finiteness of A over R, we can apply Nakayama's lemma to conclude that $C = 0$. □

Remark 5.3.18 One can also prove the second claim in d) using a little functional analysis: L is dense in $\hat{L}_i$ so $\hat{K} \otimes_K L \to \prod_{i=1}^{r} \hat{L}_i$ has a dense image. It is a linear continuous map between Banach $\hat{K}$-algebras, so its image is closed, hence the map surjective. Both sides have the same finite dimension, so the map is an isomorphism.

Remark 5.3.19 With notation and assumptions as in proposition 5.3.17, suppose furthermore that L/K is a Galois extension. The subset $D(\mathfrak{q}_i) = \{g \in \mathrm{Gal}(L/K) |\, g(x) \in \mathfrak{q}_i \ \forall\, x \in \mathfrak{q}_i\}$ is easily seen to be a subgroup, called the *decomposition group of* $\mathfrak{q}_i$. One can then show that $\hat{L}_i/\hat{K}$ is a

Galois extension with $\mathrm{Gal}(\hat{L}_i/\hat{K}) = D(\mathfrak{q}_i)$: see [3] theorem III.1.2 or [17], corollaire II.4. Such decomposition groups are either cyclic or (if $\mathrm{char}(R/\mathfrak{p}) = p > 0$) semi-direct product of a cyclic group of order prime to p by a p-group: see [17], corollaire IV.2 and corollaire IV.4 respectively.

Proposition 5.3.20 *Let R be a Dedekind domain, K its fraction field, L/K a finite separable extension and A the integral closure of R in L. Let $0 \neq \mathfrak{p} \subset R$ be a prime. The following are equivalent:*

a) L/K is unramified at every prime $\mathfrak{q} \subset A$ above $\mathfrak{p}$.

b) The discriminant $\mathfrak{d}_{A/R} \nsubseteq \mathfrak{p}$.

Proof. Without loss of generality, we may assume that R is a DVR. Since $e(\mathfrak{q}/\mathfrak{p}) = e(\hat{\mathfrak{q}}/\hat{\mathfrak{p}})$ for every prime $\mathfrak{q}$ above $\mathfrak{p}$ and $\hat{R}/\hat{\mathfrak{p}} = R/\mathfrak{p}$, we may replace R by $\hat{R}$ and A by its completion at $\mathfrak{q}$. Then A is also a complete DVR, free of rank $n = [L : K]$ as an R-module and $\mathfrak{q}$ is the unique prime above $\mathfrak{p}$. Choose $x_1, \ldots, x_n \in A$ such that $\{\overline{x}_1, \ldots, \overline{x}_n\}$ is an $R/\mathfrak{p}$-basis of $A/\mathfrak{p}A$. Then $\{x_1, \ldots, x_n\}$ is an R-basis for A: they are generators by corollary 1.2.41 and they are K-linearly independent, as seen in the proof of lemma 5.3.13. Put $d = \Delta(x_1, \ldots, x_n) = \det(\mathrm{Tr}(x_i x_j) \in R$ and let $\overline{d} = \overline{\Delta(x_1, \ldots, x_n)} = \det(\mathrm{Tr}(\overline{x}_i \overline{x}_j) \in R/\mathfrak{p}$. Recall that $\mathfrak{d}_{A/R} = dR$. Write $\mathfrak{p}A = \mathfrak{q}^e$. Then $\mathfrak{q}$ is unramified if and only if $A/\mathfrak{q}^e$ is a field (i.e. $e = 1$), separable over $R/\mathfrak{p}$. In particular, the bilinear form $\mathrm{Tr} : A/\mathfrak{q} \times A/\mathfrak{q} \to R/\mathfrak{p}$ is non-degenerate, i.e. $\overline{d} \neq 0$, hence $d \notin \mathfrak{p}$.
Conversely, if $\overline{d} \neq 0$, lemma 5.3.21 below implies that $A/\mathfrak{q}^e$ has no nilpotents and thus $e = 1$. Therefore $A/\mathfrak{p}$ is a field, separable over $R/\mathfrak{p}$ since $\overline{d} \neq 0$. □

Lemma 5.3.21 *Let k be a field and B a finite k-algebra. If $\mathfrak{d}_{B/k} \neq 0$ then B is reduced (i.e. $\mathfrak{N}_B = 0$).*

Proof. Let $0 \neq x \in \mathfrak{N}_B$. Let $\{x_1 = x, x_2, \ldots, x_n\}$ be a k-basis of B. We can use it to compute the discriminant. Since $x_1 = x$ is nilpotent, $x_1 x_j$ is nilpotent for $1 \leq j \leq n$. Since the trace of any nilpotent endomorphism is 0, the first row of the matrix $(\mathrm{Tr}(x_i x_j))$ is the zero vector, hence $\mathfrak{d}_{B/k} = \Delta(x_1, \ldots, x_n) = \det(\mathrm{Tr}(x_i x_j)) = 0$, a contradiction. □

The next result is very useful for computations, both in Number Theory and Algebraic Geometry, where the residue fields are perfect (finite in the first case, algebraically closed in the second).

Proposition 5.3.22 *Let R be a DVR with maximal ideal $\mathfrak{p}$ and fraction field K. Let L/K be a finite separable extension and A the integral closure of R in L. Suppose that A is a DVR, with maximal ideal $\mathfrak{q}$. Assume that $A/\mathfrak{q}$ is separable over $R/\mathfrak{p}$. There exists an element $x \in A$ such that $\{1, x, \ldots, x^{n-1}\}$ is a basis for A over R.*

Proof. Let e and f be the ramification index and residue degree, with $n = [L : K] = ef$ by proposition 5.3.14. By Abel's theorem, $A/\mathfrak{q} \simeq R/\mathfrak{p}(\overline{x}) = R/\mathfrak{p}[X]/\overline{F}(X)$, for suitable $\overline{x} \in A/\mathfrak{q}$ and $\overline{F}(X) \in R/\mathfrak{p}[X]$ monic. Choose $y \in A$ such that $y \equiv \overline{x} \bmod \mathfrak{q}$ and $F(X) \in R[X]$ monic lifting $\overline{F}(X)$. Denoting $w = v_{\mathfrak{q}}$ the valuation on A, we have $w(F(y)) \geq 1$. If $w(F(y)) = 1$, put $x = y$. Otherwise, take $h \in \mathfrak{q}$ with $w(h) = 1$ and put $x = y + h$. We have $F(x) = F(y) + hF'(y) + h^2 a$ for some $a \in A$ and $w(F'(y)) = 0$ because $\overline{F}(X)$ is separable. Since w is non-archimedean and $w(F(y) + h^2 a) \geq \min\{w(F(y)), w(h^2 a)\} \geq 2$ we get

$$w(F(x)) = \min\left\{w\left(hF'(y)\right), w\left(F(y) + h^2 a\right)\right\} = w(hF'(y)) = 1.$$

Choose $\tau = F(x)$ as a uniformiser for A and let $\mathcal{B} = \{\tau^i x^j,\, 0 \leq i \leq e-1, 0 \leq j \leq f-1\}$. It suffices to show that $\mathcal{B}$ is a basis for A over R, because then $R[x] \subseteq A$ contains a basis (recall $\tau^i = F(x)^i$), so $R[x] = A$. Since $|\mathcal{B}| = n$, it suffices to show that its elements are generators (they will be independent over K and thus over R). Since $\mathfrak{p}A = (\tau^e)$, by Nakayama's lemma it suffices to show that $\mathcal{B}$ generates $A/\mathfrak{p}A = A/(\tau^e)$. By induction, it suffices to show that if $\mathcal{B}$ generates $A/(\tau^m)$ then it generates $A/(\tau^{m+1})$, for $m < e$. This follows from the sequence

$$0 \longrightarrow \tau^m A/\tau^{m+1}A \longrightarrow A/\tau^{m+1}A \longrightarrow A/\tau^m A \longrightarrow 0$$

since $\tau^m A/\tau^{m+1}A \simeq (A/\tau A)\,\tau^m = (A/\mathfrak{q})\,\tau^m$. □

Corollary 5.3.23 *Let R be a Dedekind domain, K its fraction field, L/K a finite separable extension and A the integral closure of R in L. Let $0 \neq \mathfrak{p} \subset R$ be a prime and $\mathfrak{q} \subset A$ a prime above $\mathfrak{p}$. Assume that $A/\mathfrak{q}$ is separable over $R/\mathfrak{p}$. Then L/K is unramified at $\mathfrak{q}$ if and only if the different $\mathfrak{D}_{A/R} \nsubseteq \mathfrak{q}$.*

Proof. As in the proof of proposition 5.3.20, we may replace R and A by their completions at $\mathfrak{p}$ and $\mathfrak{q}$ respectively. Then, by proposition 5.3.22 we may write $A = R[x]$ with x root of a monic $F(X) \in R[X]$. From proposition 3.3.10, we get $\mathfrak{D}_{A/R} = (F'(x))$ and by corollary 3.3.11 we have $\mathfrak{d}_{A/R} = \left(N_{L/K}(F'(x))\right)$. Clearly $v_{\mathfrak{q}}\left(F'(x)\right) > 0$ if and only if $v_{\mathfrak{p}}\left(N_{L/K}(F'(x)\right) > 0$. We can now apply proposition 5.3.20. □

Remark 5.3.24 In corollary 5.3.23, the condition on the separability of the residue extension can in fact be removed, see corollary 5.4.12 below.

Corollary 5.3.25 *Let R be a Dedekind domain, K its fraction field, L/K a finite separable extension and A the integral closure of R in L. Assume that $A/\mathfrak{q}$ is a separable extension of $R/\mathfrak{q} \cap R$ for every prime ideal ideal $\mathfrak{q} \subseteq A$. Then $\mathfrak{D}_{A/R} = \mathrm{Ann}_A(\Omega^1_{A/R})$.*

Proof. $\mathfrak{D}_{A/R}$ and $\mathrm{Ann}\,(\Omega^1_{A/R})$ are ideals in the Dedekind domain A. To show they are equal, we need to check that they have the same factorisation. To compute the exponent of a prime $\mathfrak{q} \subset A$, we may replace A by its completion at $\mathfrak{q}$ (and R by its completion at $\mathfrak{q} \cap R$). We can now apply proposition 5.3.22 and write $A = R[x]$ with x root of a monic polynomial $f(X) \in R[X]$. Then $A = R[x]$, $\mathfrak{D}_{A/R} = (f'(x))$ and $\Omega^1_{A/R} = Adx/f'(x)Adx$. □

Example 5.3.26 With notation as in example 5.2.39, let $K \subseteq L$ be a finite separable extension of $K = \mathrm{Frac}\, R$ and A the integral closure of R in L. Assume furthermore that k is algebraically closed in A as well. The formula $\sum_{\mathfrak{q}|\mathfrak{p}} e(\mathfrak{q})f(\mathfrak{q}) = [L:K]$ tells us that if D is a divisor on R then $\deg(A \otimes_R D) = [L:K]\deg(D)$.

Consider now the first fundamental sequence of differentials:

$$A \otimes_R \Omega^1_{R/k} \xrightarrow{v} \Omega^1_{A/k} \longrightarrow \Omega^1_{A/R} \longrightarrow 0. \tag{5.2}$$

By example 5.2.4, $\Omega^1_{R/k}$ and $\Omega^1_{A/k}$ are invertible modules. Since L is finite separable over K, we have $\Omega^1_{L/K} = 0$. The map $id_L \otimes v : L \otimes_K \Omega^1_{K/k} \to \Omega^1_{L/k}$ is a surjection between 1-dimensional vector spaces, hence an isomorphism. Therefore $\ker v$ is a torsion A-module, hence $\ker v = 0$

since A is a domain. We can thus complete sequence (5.2) by a zero on the left. $\Omega^1_{A/k}$ being an invertible A-module, we obtain a new sequence

$$0 \longrightarrow \Omega^{-1}_{A/k} \otimes_R \Omega^1_{R/k} \longrightarrow A \longrightarrow \Omega^{-1}_{A/k} \otimes_A \Omega^1_{A/R} \longrightarrow 0.$$

Hence $\Omega^{-1}_{A/k} \otimes_R \Omega^1_{R/k}$ is an ideal in A, the annihilator of the torsion module $\Omega^{-1}_{A/k} \otimes_A \Omega^1_{A/R}$. Let us now remark that $\mathrm{Ann}\,(M) = \mathrm{Ann}\,(\Lambda \otimes_A M)$ for any A-module M and invertible A-module Λ: indeed, if $am = 0$ for all $m \in M$ then $a(x \otimes m) = x \otimes am = x \otimes 0 = 0$ hence $\mathrm{Ann}\,(M) \subseteq \mathrm{Ann}\,(\Lambda \otimes M)$. For the same reason $\mathrm{Ann}\,(\Lambda \otimes M) \subseteq \mathrm{Ann}\,(\Lambda^\vee \otimes \Lambda \otimes M) = \mathrm{Ann}\,(M)$. Hence, by corollary 5.3.25,

$$\Omega^{-1}_{A/k} \otimes_R \Omega^1_{R/k} = \mathrm{Ann}\,(\Omega^1_{A/R}) = \mathfrak{D}_{A/R}. \tag{5.3}$$

We now use some input from algebraic geometry. Realise $\Omega^1_{R/k}$ as a fractional ideal (example 5.2.10) and pick any $\omega \in K^\times$ in it: the set $\{f \in K : v(f\omega) \geq 0 \ \forall v \text{ valuation of } K\}$ is a finite-dimensional k-vector space. Its dimension g_K is called the **genus** of K. The degree of the left-hand side of (5.3) can be computed by means of the Riemann-Roch formula: it is $2g_L - 2 - [L : K](2g_K - 2) - \delta_\infty$, where δ_∞ is a contribution from the points at infinity (in algebraic terms: the valuations on L whose valuation ring does not contain A). If we assume that $K \subset L$ is unramified at infinity (i.e. $\delta_\infty = 0$), taking degrees in (5.3) we obtain the famous **Riemann–Hurwitz formula**

$$2g_L - 2 = [L : K](2g_K - 2) + \deg \mathfrak{D}_{A/R}.$$

§ 4 Modules over Dedekind domains

Throughout this section, R is a Dedekind domain, K its fraction field. We begin the discussion with finitely generated projective R-modules.

Lemma 5.4.1 *Let M be a finitely generated projective R-module. There exist ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ of R such that $M \simeq \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$.*

Proof. Choose an embedding $M \subseteq R^n$ and compose with the projection onto the first factor to get $\varphi : M \to R^n \to R$. Put $\mathfrak{a}_1 = \mathrm{Im}(\varphi)$, an ideal in R. Since ideals in Dedekind domains are locally principal, they are locally free hence projective, as R-modules. Choose a splitting of φ and write $M = \mathfrak{a}_1 \oplus \ker(\varphi)$. Proceed by induction on the rank. □

Lemma 5.4.2 *Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ and $\mathfrak{b}_1, \ldots, \mathfrak{b}_s$ be ideals of R. Then $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r \simeq \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_s$ if and only if $r = s$ and $\mathfrak{a}_1 \cdots \mathfrak{a}_r \simeq \mathfrak{b}_1 \cdots \mathfrak{b}_s$.*

Proof. Let $\varphi : \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r \simeq \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_s$. Clearly $r = s$ as this is the rank of these locally module. Recall that $Hom_R(\mathfrak{a}_i, R) \simeq \{x \in K \,|\, x\mathfrak{a}_i \subseteq R\}$. Let $q_{ij} \in K$ be the element corresponding to $\mathfrak{a}_i \hookrightarrow \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r \simeq \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_r \twoheadrightarrow \mathfrak{b}_j$. Thus, if $Q = (q_{ij}) \in \mathrm{GL}_r(K)$ and $\varphi(a_1, \ldots, a_r) = (b_1, \ldots, b_r)$ then $b_i = \sum_{j=1}^r q_{ij} a_j$. Therefore for each $(a_1, \ldots, a_r) \in \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$ we have $\det(Q) a_1 \cdots a_r = \det\left(Q \,\mathrm{diag}(a_1, \ldots, a_r)\right) \in \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_r$.

Thus $\det(Q)\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r \subseteq \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_r$. Symetrically $\det(Q)^{-1}\mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_r \subseteq \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$ therefore $\det(Q)\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r = \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_r$. The map $a \mapsto \frac{a}{\det(Q)}$ is thus an isomorphism $\mathfrak{a}_1 \cdots \mathfrak{a}_r \to \mathfrak{b}_1 \cdots \mathfrak{b}_r$.

To establish the converse, it suffices to show that $\mathfrak{a} \oplus \mathfrak{b} \simeq R \oplus \mathfrak{ab}$ for any two ideals $\mathfrak{a}, \mathfrak{b} \subseteq R$. This is easy if $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, in view of the exact sequence

$$0 \longrightarrow \mathfrak{a} \cap \mathfrak{b} \longrightarrow \mathfrak{a} \oplus \mathfrak{b} \xrightarrow{\delta} R \longrightarrow 0 \tag{5.4}$$

where $\delta(a, b) = a - b$ is surjective because $\mathfrak{a} + \mathfrak{b} = R$. Since for coprime ideals $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$, we just have to take a splitting of the sequence (5.4).
Let's now show we can always reduce to this case. Fix $0 \neq a \in \mathfrak{a}$ and write $aR = \mathfrak{ac}$ for some ideal $\mathfrak{c} \subseteq R$. Consider the prime factorisations $\mathfrak{cb} = \prod_{i=1}^m \mathfrak{p}_i^{d_i} \subseteq \prod_{i=1}^m \mathfrak{p}_i^{e_i} = \mathfrak{c}$ with $0 \leq e_i \leq d_i$ for $i = 1, \ldots, m$. Choose $\pi_i \in R$ uniformiser of $\mathfrak{p}_i R_{\mathfrak{p}_i}$ and use the Chinese remainder theorem to find $c \in R$ such that $c \equiv \pi_i^{e_i} \bmod \mathfrak{p}_i^{e_i+1}$ for $i = 1, \ldots, m$. Localising at all primes, one checks that $cR + \mathfrak{bc} \subseteq \mathfrak{c}$ is an equality: indeed $cR_{\mathfrak{p}_i} = \mathfrak{c}R_{\mathfrak{p}_i}$ and $\mathfrak{bc}R_{\mathfrak{q}} = \mathfrak{c}R_{\mathfrak{q}} = R_{\mathfrak{q}}$ for $\mathfrak{q} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$.

Multiplying by $\mathfrak{a}$ the equation $\mathfrak{c} = cR + \mathfrak{cb}$ and substituting $aR = \mathfrak{ac}$ we get $aR = c\mathfrak{a} + a\mathfrak{b}$. Dividing now by a we get $R = \frac{c}{a}\mathfrak{a} + \mathfrak{b}$ in K. Hence $\mathfrak{a}_1 = \frac{c}{a}\mathfrak{a} \subseteq R$ is an ideal coprime with $\mathfrak{b}$ and $x \mapsto \frac{c}{a}x$ is an isomorphism $\mathfrak{a} \to \mathfrak{a}_1$ as R-modules. □

Corollary 5.4.3 *For any finitely generated projective module M of rank r there exists an ideal $\mathfrak{a} \subseteq R$ such that $M \simeq R^{r-1} \oplus \mathfrak{a}$.*

Proof. Put together lemmas 5.4.1 and 5.4.2 and write $M \simeq \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r \simeq R^{r-1} \oplus \mathfrak{a}_1 \cdots \mathfrak{a}_r$. □

Let now M be an arbitrary finitely generated R-module. Since R is a domain, the subset of torsion elements $M_{\text{tors}} = \{m \in M \,|\, \exists\, 0 \neq x \in R,\ xm = 0\}$ is a submodule (lemma 1.2.19). Consider then the exact sequence

$$0 \longrightarrow M_{\text{tors}} \longrightarrow M \longrightarrow M/M_{\text{tors}} \longrightarrow 0 \tag{5.5}$$

Lemma 5.4.4 *M/M_{tors} is a projective R-module and $M \simeq M_{\text{tors}} \oplus M/M_{\text{tors}}$.*

Proof. The second statement follows from the first by taking any splitting of (5.5). The module M/M_{tors} is torsion-free: if $\overline{m} \in M/M_{\text{tors}}$ and $x \neq 0$ such that $x\overline{m}$. Choose any $m \in M$ projecting to $\overline{m}$, then $xm \in M_{\text{tors}}$. Taking $y \neq 0$ such that $yxm = 0$, se see that $m \in M_{\text{tors}}$, thus $\overline{m} = 0$. For every prime $\mathfrak{p} \subseteq R$, as a torsion free finitely generated module over a PID, $(M/M_{\text{tors}})_{\mathfrak{p}}$ is free, hence M/M_{tors} is projective. □

If M is a torsion module, $\operatorname{Ann}(m) \subseteq R$ is a nonzero ideal for all $m \in M$; taking generators $m_1, \ldots, m_n$ of M we see that $\operatorname{Ann}(M) = \bigcap_{i=1}^r \operatorname{Ann}(m_i)$ is a non-zero ideal. Hence M is an $R/\operatorname{Ann}(M)$-module and as such it has finite length.

Definition 5.4.5 The **Grothendieck group** $K_0(R)$ is the quotient of the free abelian group on all finitely generated R-modules modulo the subgroup generated by the elements $M - M' - M''$ for each short exact sequence $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$.

Notice that if $M \simeq N$ then $[M] = [N]$ in $K_0(R)$ (consider $0 \longrightarrow M \longrightarrow N \longrightarrow 0 \longrightarrow 0$), so we could have used isomorphism classes of modules as generators of $K_0(R)$.

By lemma 5.4.4, for each finitely generated R-module $[M] = [M_{\text{tors}}] + [M/M_{\text{tors}}]$, with M/M_{tors} projective, hence isomorphic to a module of $R^{r-1} \oplus \mathfrak{a}$ for some $\mathfrak{a} \subseteq R$ by corollary 5.4.3. Because of the exact sequence $0 \longrightarrow \mathfrak{a} \longrightarrow R \longrightarrow R/\mathfrak{a} \longrightarrow 0$, we have $[\mathfrak{a}] = [R] - [R/\mathfrak{a}]$. Therefore $[M/M_{\text{tors}}] = (r-1)[R] + [\mathfrak{a}] = r[R] - [R/\mathfrak{a}]$ in $K_0(R)$. We can thus say that $K_0(R)$ is generated by $[R]$ and the isomorphism classes of torsion modules.

We can now define a map $\chi : K_0(R) \longrightarrow \mathbb{Z} \oplus \text{Pic}(R)$ by setting $\chi([R]) = (1, 0)$ and

$$\chi(M) = \left(0, \sum_{\mathfrak{p}} \ell_{\mathfrak{p}}(M)\,[\mathfrak{p}]\right)$$

for each torsion R-module, where $\ell_{\mathfrak{p}}(M)$ is the lenght of the $R_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$. Notice that by the preceding remarks $\chi\left(\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r\right) = (r, -[\mathfrak{a}_1 \cdots \mathfrak{a}_r])$. From Jordan-Hölder theory (theorem 4.2.3) we now obtain:

Theorem 5.4.6 *$\chi : K_0(R) \longrightarrow \mathbb{Z} \oplus \text{Pic}(R)$ is a group isomorphism.*

Example 5.4.7 Let $\eta : R^n \to R^n$ be an endomorphism with $\det(\eta) \neq 0$. Then $\eta_{\mathfrak{p}}$ is an isomorphism for every prime $\mathfrak{p} \subset R$ such that $\det(\eta) \notin \mathfrak{p}$, hence $\text{coker}(\eta)$ is a torsion R-module. Then $\chi(\text{coker}(\eta)) = (0, [\det(\eta)R])$. This is clear if $n = 1$. Localising at all primes, the general case follows by induction from the elementary divisors theorem.

We now wish to investigate functoriality. Let $K \subseteq L$ be a finite separable extension and A the integral closure of R in L. For Picard groups, there are two natural maps associated with this situation, which it suffices to give on prime ideals

$$\begin{array}{rcl} i : \text{Pic}(R) & \longrightarrow & \text{Pic}(A); \\ [\mathfrak{p}] & \longmapsto & [\mathfrak{p}A] \end{array} \qquad \begin{array}{rcl} N : \text{Pic}(A) & \longrightarrow & \text{Pic}(R) \\ [\mathfrak{q}] & \longmapsto & [\mathfrak{q} \cap R]^{f(\mathfrak{q})} \end{array}$$

where as usual $f(\mathfrak{q}) = [A/\mathfrak{q} : R/\mathfrak{q} \cap R]$. In view of the formula $\sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q})e(\mathfrak{q}) = [L : K]$ we have $N(i(\mathfrak{a})) = \mathfrak{a}^{[L:K]}$ for every ideal $\mathfrak{a} \subseteq R$ (and thus for every invertible module).

On Grothendieck groups there are two maps as well

$$\begin{array}{rcl} \varphi^* : K_0(R) & \longrightarrow & K_0(A); \\ M & \longmapsto & A \otimes_R M \end{array} \qquad \begin{array}{rcl} \varphi_* : K_0(A) & \longrightarrow & K_0(R) \\ M & \longmapsto & \varphi_*(M) \end{array}$$

where $\varphi : R \to A$ is the inclusion map and $\varphi_*(M)$ is the A-module M seen as an R-module.

The isomorphisms $\chi_R : K_0(R) \longrightarrow \mathbb{Z} \oplus \text{Pic}(R)$ and $\chi_A : K_0(A) \longrightarrow \mathbb{Z} \oplus \text{Pic}(A)$ of theorem 5.4.6 are compatible with the above maps.

Proposition 5.4.8 *For finitely generated torsion modules $P \in \mathbf{Mod}_R$ and $Q \in \mathbf{Mod}_A$*

$$\chi_R(\varphi_*(Q)) = (0, N(\chi_A(Q)))\,; \qquad \chi_A(\varphi^*(P)) = (0, i(\chi_R(P)))\,.$$

Proof. By additivity, it suffices to treat only the cases $P = R/\mathfrak{p}$ and $Q = A/\mathfrak{q}$, for $\mathfrak{p} \subseteq A$ and $\mathfrak{q} \subseteq A$ prime ideals. If $\mathfrak{q} \subseteq A$ is prime and $\mathfrak{p} = \mathfrak{q} \cap R$ then by definition $\ell_{\mathfrak{p}}(A/\mathfrak{q}) = f(\mathfrak{q})$ so $\chi_R(\varphi_*(A/\mathfrak{q})) = N(\mathfrak{q})$. Since we assumed $K \subseteq L$ separable, A is a locally free R module, hence flat. Thus the multiplication map $A \otimes_R \mathfrak{p} \to \mathfrak{p}A$ is an isomorphism and tensoring by A the sequence $0 \longrightarrow \mathfrak{p} \longrightarrow R \longrightarrow R/\mathfrak{p} \longrightarrow 0$ we get $0 \longrightarrow \mathfrak{p}A \longrightarrow A \longrightarrow \varphi^*(R/\mathfrak{p}) \longrightarrow 0$ hence $\varphi^*(R/\mathfrak{p}) = A/\mathfrak{p}A$ and thus $\chi_A(\varphi^*(R/\mathfrak{p})) = (0, i([\mathfrak{p}]))$. □

Corollary 5.4.9 *For any $a \in A$ we have $N(aA) = N_{L/K}(a)R$.*

Proof. Let $\mu_a : A \to A$ be the multiplication map. By definition $N_{L/K}(a) = \det(\mu_a)$ and $N(aA) = \chi_R(A/aA) = \operatorname{coker}(\mu_a)$. We can conclude by example 5.4.7. □

Theorem 5.4.8 only describes the functoriality for torsion modules. To get the complete picture, we should also understand what happens to free modules. Since $A \otimes_R R \cong A$, clearly $\chi_A(\varphi^*(R)) = (1, 0)$. On the other hand, A is a locally free R module of rank $[L : K]$, thus the first component of $\chi_R(\varphi_*(A))$ is $[L : K]$. But, unless R is a DVR, A is not necessarily a free R-module, so the second component is more complicated.
A is free if the discriminant ideal $\mathfrak{d}_{A/R} = R$: for any $x_1, \dots, x_n \in A$ with $\Delta(x_1, \dots, x_n) \in R^\times$, the composite map $\bigoplus_{i=1}^n Rx_i \hookrightarrow A \hookrightarrow \bigoplus_{i=1}^n Rx_i^*$ (where $\{x_1^*, \dots, x_n^*\}$ is the dual basis with respect to the trace bilinear form) is an isomorphism because its matrix $(\mathrm{Tr}_{L/K}(x_i x_j)$ is invertible.
By exercise 5.8, if there exists $\alpha \in A$ such that $v_{\mathfrak{p}}(\Delta(\alpha)) = v_{\mathfrak{p}}(\Delta(1, \alpha, \dots, \alpha^{n-1})) \leq 1$ for each prime $\mathfrak{p} \subseteq R$, then $A = R[\alpha]$ is free. But even this is not a necessary condition: if $\zeta = \exp \frac{2\pi i}{p^n} \in \mathbb{C}$ the ring of integers of $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$ but $\Delta(\zeta) = \pm p^{p^{n-1}(np-n-1)}$.

Remark 5.4.10 If L is a Galois extension with $\mathrm{Gal}(L/K) = G$ a much more delicate question is to establish whether A is a free $R[G]$-module. This means that A has an integral normal basis, i.e. a basis of the form $\{g(\alpha)\}_{g \in G}$ for some $\alpha \in A$. Again this is possible when $\mathfrak{d}_{A/R} = R$. Emmy Noether has shown that if A is a DVR, it has an integral normal basis if and only if $K \subseteq L$ is *tamely ramified* i.e., in the notation of exercise 5.7, $w(\mathfrak{D}_{A/R}) = e - 1$ (i.e. minimum).

Recall that the codifferent of $R \subseteq A$ is the A-module $\mathfrak{D}_{A/R}^{-1} = \{x \in L \,|\, \mathrm{Tr}_{L/K}(xy) \in R \;\forall\, y \in A\}$, a fractional ideal of A. Clearly, $A \subseteq \mathfrak{D}_{A/R}^{-1}$, so $\mathfrak{D}_{A/R}^{-1}/A$ is a torsion module. As noticed in corollary 5.3.25, we have $\mathrm{Ann}\,(\mathfrak{D}_{A/R}^{-1}/A) = \mathrm{Ann}\,(A/\mathfrak{D}_{A/R}) = \mathfrak{D}_{A/R}$, thus

$$\chi_A\left(\mathfrak{D}_{A/R}^{-1}/A\right) = \left(0, [\mathfrak{D}_{A/R}]\right). \tag{5.6}$$

On the other hand, to compute $\chi_R(\varphi_*(\mathfrak{D}_{A/R}^{-1}/A))$ we may localise at primes $\mathfrak{p} \subseteq R$ and so assume that A is a free R-module, with basis $\{x_1, \dots, x_n\}$. The dual basis $\{x_1^*, \dots, x_n^*\}$ with respect to the trace bilinear form is then a basis of $\mathfrak{D}_{A/R}^{-1}$. The inclusion $\eta : R^n \simeq A \hookrightarrow \mathfrak{D}_{A/R}^{-1} \simeq R^n$ is given on bases by $\eta(x_i) = \sum_{j=1}^n \mathrm{Tr}_{L/K}(x_i x_j) x_j^*$, hence by example 5.4.7 we have

$$\chi_R\left(\varphi_*(\mathfrak{D}_{A/R}^{-1}/A)\right) = \left(0, [\det(\mathrm{Tr}_{L/K}(x_i x_j)R]\right) = \left(0, [\mathfrak{d}_{A/R}]\right) \tag{5.7}$$

where $\mathfrak{d}_{A/R}$ is the discriminant.

Corollary 5.4.11 $\mathfrak{d}_{A/R} = N(\mathfrak{D}_{A/R})$.

Proof. Combine (5.6), (5.7) and proposition 5.4.8. □

Corollary 5.4.12 *Let R be a Dedekind domain, K its fraction field, L/K a finite separable extension and A the integral closure of R in L. Then L/K is unramified at a prime $\mathfrak{q} \subset A$ if and only if $\mathfrak{D}_{A/R} \nsubseteq \mathfrak{q}$.*

Proof. By proposition 5.3.17, we may replace A and R by their completions at $\mathfrak{q}$ and $\mathfrak{p} = \mathfrak{q} \cap R$ respectively. Then $\mathfrak{D}_{A/R} \subseteq \mathfrak{q}$ if and only if $\mathfrak{d}_{A/R} = N(\mathfrak{D}_{A/R}) \subseteq N(\mathfrak{q}) \subseteq \mathfrak{q} \cap R = \mathfrak{p}$ and we know from proposition 5.3.20 that $\mathfrak{p}$ is unramified if and only if $\mathfrak{d}_{A/R} \nsubseteq \mathfrak{p}$. □

§ 5 Exercises

Exercise 5.1 Let R be a DVR, $v : K^\times \to \mathbb{Z}$ the valuation. Show that if $a_1 + \cdots + a_r = 0$ in R then $\exists\, 1 \leq i < j \leq r$ such that $v(a_i) = v(a_j)$.

Exercise 5.2 Let R be a domain which is not a field.

a) Show that $R = \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$ (intersection of all localisations at all maximal ideals).

b) Let $\mathfrak{b} \subseteq \mathfrak{a} \subseteq R$ be ideals. Show that if $\mathfrak{b}R_{\mathfrak{m}} = \mathfrak{a}R_{\mathfrak{m}}$ for all maximal ideals, then $\mathfrak{a} = \mathfrak{b}$.

Suppose from now on that $R_{\mathfrak{m}}$ is a DVR for each maximal ideal $\mathfrak{m} \subset R$.

c) Use a) to show that R is integrally closed.

d) Let $\mathfrak{a} \subset R$ an ideal, $0 \neq a \in \mathfrak{a}$. Suppose that a is contained in only finitely many prime ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ of R. Write $\mathfrak{a}R_{\mathfrak{m}_i} = \frac{a_i}{s} R_{\mathfrak{m}_i}$, with $a_i \in \mathfrak{a}$, $s \notin \mathfrak{m}_i$ for all i. Show that $\mathfrak{a}$ is generated by $a, a_1, \ldots, a_r$.

e) Let R be a domain which is not a field. Show that the following conditions are equivalent:

   i) R is a Dedekind domain.

   ii) $R_{\mathfrak{m}}$ is a DVR for each maximal ideal $\mathfrak{m} \subset R$ and each $0 \neq a \in R$ is contained in only finitely many prime ideals of R.

Exercise 5.3 Let R be a Dedekind domain of characteristic $p > 0$, $K = \operatorname{Frac} R$, $K \subseteq L$ a finite purely inseparable field extension, A the integral closure of R in L. Let $q = p^m$ such that $x^q \in K$ for all $x \in L$.

a) Show that $A = \{x \in L \mid x^q \in R\}$.

b) Let $0 \neq \mathfrak{q} \subset A$ be a prime ideal, $\mathfrak{p} = \mathfrak{q} \cap R$. Show that $\mathfrak{q} = \{x \in L \mid x^q \in \mathfrak{p}\}$.

c) Show that $\operatorname{Spec} A \to \operatorname{Spec} R$ is bijective.

d) Show that each $0 \neq a \in A$ is contained in only finitely many prime ideals of A.

e) Let $\mathfrak{q} \neq 0$ be a prime ideal in A, $\mathfrak{p} = \mathfrak{q} \cap R$ and $S = R - \mathfrak{p}$. Show that $S^{-1}A = A_{\mathfrak{q}}$.

f) Let π be a uniformiser of $\mathfrak{p}R_{\mathfrak{p}}$. For every $y \in \mathfrak{q}A_{\mathfrak{q}}$, write $y^q = u\pi^n$, where $u \in R_{\mathfrak{p}}^\times$. Choose $y \in \mathfrak{q}A_{\mathfrak{q}}$ such that n is minimal. Show that $\mathfrak{q}A_{\mathfrak{q}}$ is principal, generated by y.

g) Conclude that $A_{\mathfrak{q}}$ is a DVR.

h) Show that A is noetherian. [Hint: let $I \subset A$ be an ideal, $0 \neq a \in I$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ the primes containing a; choose $x_i \in I$ such that $I_{\mathfrak{q}_i} = x_i A_{\mathfrak{q}_i}$ and show that $I = (a, x_1, \ldots, x_r)$.]

i) Show that A is a Dedekind domain.

Exercise 5.4 Let R be a Dedekind domain, $K = \operatorname{Frac} R$, $K \subseteq L$ a finite field extension, A the integral closure of R in L. Use exercise 5.3 to show that A is a Dedekind domain.

Exercise 5.5 Let R be a Dedekind domain, $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ distinct prime ideals and denote $v_i = v_{\mathfrak{p}_i}$ the associated discrete valuation on K. Let $x_1, \ldots, x_r \in K$ and $n_1, \ldots, n_r \in \mathbb{Z}$. We want to show that the system of inequalities

$$v_i(x - x_i) \geq n_i \quad i = 1, \ldots, r; \qquad v_{\mathfrak{q}}(x) \geq 0 \quad \forall \mathfrak{q} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$$

always has a solution $x \in K$ (approximation lemma).

a) Show that if the system has a solution for all $(x_1, \ldots, x_r) \in R^r$ then it has a solution for all $(x_1, \ldots, x_r) \in K^r$. From now on, assume $(x_1, \ldots, x_r) \in R^r$.

b) Show that if the system has a solution for all $(n_1, \ldots, n_r) \in \mathbb{N}^r$ then it has a solution for all $(n_1, \ldots, n_r) \in \mathbb{Z}^r$.

c) Show that it suffices to solve the system for the vectors $(0 \ldots, 0, x_i, 0, \ldots, 0)$.

d) Show that the system with $(x_1, 0, \ldots, 0)$ has a solution $x \in R$. [Hint: consider the ideal $\mathfrak{p}_1^{n_1} + \mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_r^{n_r}$]

Exercise 5.6 Show that a semi-local Dedekind domain is a PID. [Hint: approximation lemma]

Exercise 5.7 Let R be a DVR, $K = \operatorname{Frac} R$, L a finite separable extension of K of degree e and A the integral closure of R in L. We assume that A is a DVR and that if $\mathfrak{q} \subset A$ is the maximal ideal, $\mathfrak{p} = \mathfrak{q} \cap R$ then $\mathfrak{p}A = \mathfrak{q}^e$ (i.e. the extension is totally ramified). Let $x \in \mathfrak{q}$ be a uniformiser.

a) Let $w = v_{\mathfrak{q}}$ be the valuation of A. Show that $w(t) \equiv 0 \bmod e \; \forall \, t \in R$.

b) Let $f \in K[X]$ be the characteristic polynomial of $\mu_x : L \to L$, $\mu_x(y) = xy$. Show that $f \in R[X]$.

c) Show that f is an Eisenstein polynomial and that $A = R[X]/(f)$.

d) Compute the different $\mathfrak{D}_{A/R}$.

e) Show that $e - 1 \leq w(\mathfrak{D}_{A/R}) \leq e - 1 + w(e)$, with $w\left(\mathfrak{D}_{A/R}\right) = e - 1$ if and only if $w(e) = 0$.

Exercise 5.8 Let R be a Dedekind domain, $K = \operatorname{Frac} R$, L a finite separable extension of K of degree n and A the integral closure of R in L. Let $\alpha \in A$ be such that $L = K(\alpha)$ and $\Delta(\alpha) = \Delta(1, \alpha, \ldots, \alpha^{n-1})$. If $\mathfrak{p}$ is a nonzero prime ideal in R and $\{x_1, \ldots, x_n\}$ is a basis of $A_{\mathfrak{p}}$ over $R_{\mathfrak{p}}$, write $\alpha^{i-1} = \sum_j m_{ij} x_j$, put $M = (m_{ij}) \in \mathrm{GL}_n(K)$ (with $m_{ij} \in R_{\mathfrak{p}}$) and let $d = \det M$.

a) Show that $\Delta(\alpha) = d^2 \Delta(x_1, \ldots, x_n)$.

b) Show that $d \cdot y \in R_{\mathfrak{p}}[\alpha]$ for all $y \in A_{\mathfrak{p}}$.

c) Show that $\Delta(\alpha) \cdot y \in R_{\mathfrak{p}}[\alpha]$ for all $y \in A_{\mathfrak{p}}$.

d) Show that $\Delta(\alpha)A \subseteq R[\alpha]$.

e) Show that if $\Delta(\alpha) \notin \mathfrak{p}^2$ then $A_{\mathfrak{p}} = R_{\mathfrak{p}}[\alpha]$.

Chapter VI

Dimension theory

§ 1 Height and dimension

Definition 6.1.1 *The (Krull)* **dimension** *of a ring R is the supremum of the lengths of chains of prime ideals in R:*

$$\dim R = \sup \{n \mid \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n,\ \mathfrak{p}_i \in \operatorname{Spec} R\}\,.$$

The **height** *of a prime ideal $\mathfrak{p} \subset R$ is* $\operatorname{ht} \mathfrak{p} = \dim R_{\mathfrak{p}}$.

Hence $\operatorname{ht} \mathfrak{p}$ is the supremum of the lengths of chains of prime ideals contained in $\mathfrak{p}$.

Remark 6.1.2 If $\mathfrak{p} \subseteq \mathfrak{q}$ are prime ideals with $\operatorname{ht} \mathfrak{p} = \operatorname{ht} \mathfrak{q} = h < +\infty$ then $\mathfrak{p} = \mathfrak{q}$. Indeed, take $\mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_h$, then the first inclusion in $\mathfrak{q} \supseteq \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_h$ can't be strict, otherwise $\operatorname{ht} \mathfrak{q} > h$.

Remark 6.1.3 For any prime ideal $\mathfrak{p} \subset R$ we have $\dim R/\mathfrak{p} + \operatorname{ht} \mathfrak{p} \leq \dim R$. This is immediate from the bijections between primes in $R/\mathfrak{p}$ and primes in R containing $\mathfrak{p}$ and that between primes in R contained in $\mathfrak{p}$ and primes in $R_{\mathfrak{p}}$.

Example 6.1.4 A field is of dimension zero. A Dedekind domain is of dimension 1, since every nonzero prime ideal is maximal.

We shall see later (theorem 6.1.28) that if R is a noetherian ring of dimension $d < +\infty$ then $\dim R[X] = d + 1$. In particular, if k is a field, $\dim k[X_1, \ldots, X_n] = n$, as we should expect from any reasonable notion of dimension, as $\operatorname{Spec} k[X_1, \ldots, X_n] = \mathbb{A}^n_k$ is the affine n-dimensional space. We shall also prove that finitely generated algebras over fields have finite dimension.

A noetherian ring may have infinite dimension (exercise 6.3), but we shall see in corollary 6.1.20 that the dimension of a *local* noetherian ring is always finite.

We begin our investigation with rings of dimension zero, i.e. in which every prime is maximal.

Proposition 6.1.5 *An artinian domain is a field. In an artinian ring, every prime ideal is maximal.*

Proof. Let R be an artinian domain. Let $0 \neq x \in R$ and consider the chain

$$(x) \supseteq (x^2) \supseteq \cdots \supseteq (x^n) \supseteq \dots$$

By the artinian assumption, $(x^n) = (x^{n+1}) = \dots$ for n large enough. Then $x^n = yx^{n+1}$ for a suitable $y \in R$, hence $(1 - yx)x^n = 0$. Since R is a domain, we have $xy = 1$ so $x \in R^\times$.
If R is any artinian ring and $\mathfrak{p}$ is prime, $R/\mathfrak{p}$ is again artinian and is a domain, thus a field, hence $\mathfrak{p}$ is maximal. □

A remarked, proposition 6.1.5 means that an artinian ring has dimension zero. In fact the converse holds for noetherian rings. We first need the following characterisation:

Lemma 6.1.6 *Let R be a ring, $\mathfrak{m}_1, \dots, \mathfrak{m}_r \subset R$ (not necessarily distinct) maximal ideals such that $\mathfrak{m}_1 \cdots \mathfrak{m}_r = 0$. Then R is noetherian if and only if it is artinian.*

Proof. Each quotient $\mathfrak{m}_1 \cdots \mathfrak{m}_{i-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_i$ in the chain $R \supseteq \mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \cdots \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_r = 0$. is an $R/\mathfrak{m}_i$-vector space, so each of these quotients satisfies the ascending chain condition if and only if it satisfies the descending chain condition. The result now follows by *dévissage* i.e. by considering the exact sequences

$$0 \longrightarrow \mathfrak{m}_1 \cdots \mathfrak{m}_{i-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_i \longrightarrow R/\mathfrak{m}_1 \cdots \mathfrak{m}_i \longrightarrow R/\mathfrak{m}_1 \cdots \mathfrak{m}_{i-1} \longrightarrow 0$$

and remembering that the middle term of a short exact sequence satisfies a chain condition if and only if the first and last term have the same property (proposition 4.1.7). □

Corollary 6.1.7 *A noetherian ring of dimension zero is artinian.*

Proof. If $\dim R = 0$, every prime ideal is maximal, hence the Jacobson and nilradical of R coincide. If R is noetherian, by exercise 4.3 $\sqrt{0} = \mathfrak{N}_R = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$ is the intersection of finitely many maximal ideals. Moreover, by exercise 4.2 the nilradical noetherian of ring is nilpotent. Therefore $\mathfrak{m}_1^n \cdots \mathfrak{m}_r^n \subseteq (\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r)^n = \mathfrak{N}_R^n = 0$ for a suitable $n > 0$ and applying lemma 6.1.6 we conclude that R is artinian. □

Remark 6.1.8 In fact a ring R is artinian if and only if it is noetherian of dimension zero. To prove it, in view of proposition 6.1.5 we only need to know that every artinian ring is noetherian, see remark 4.1.4.

By definition, a prime ideal of height 0 is a **minimal** prime. Let us investigate these first.

Lemma 6.1.9 *Any ring $R \neq 0$ contains minimal prime ideals.*

Proof. Let Σ be the set of all prime ideals in R, partially ordered by $\mathfrak{p} \leq \mathfrak{q} \iff \mathfrak{p} \supseteq \mathfrak{q}$. The claim will follow from Zorn's lemma once we show that any chain $\mathfrak{p}_1 \leq \mathfrak{p}_2 \leq \dots$ (i.e. $\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \dots$) has an upper bound in Σ. The obvious candidate is $\bigcap_n \mathfrak{p}_n$: let us show that it is indeed a prime ideal. Let $xy \in \bigcap_n \mathfrak{p}_n$ and suppose $x \notin \bigcap_n \mathfrak{p}_n$. So there exists $n_0 \in \mathbb{N}$ such that $x \notin \mathfrak{p}_n$ for all $n \geq n_0$. Since $xy \in \mathfrak{p}_n$ for all $n \in \mathbb{N}$ and the $\mathfrak{p}_n$ are primes, this means $y \in \mathfrak{p}_n$ for all $n \geq n_0$. Moreover $y \in \mathfrak{p}_{n_0} \subseteq \mathfrak{p}_{n_0-1} \subseteq \cdots \subseteq \mathfrak{p}_1$, so $y \in \bigcap_{n\in\mathbb{N}} \mathfrak{p}_n$. □

Corollary 6.1.10 *Any prime ideal contains a minimal prime.*

Proof. Apply the lemma to $R_{\mathfrak{p}}$. □

Corollary 6.1.11 *A noetherian ring has a finite number of minimal prime ideals. The nilradical of a noetherian ring is the intersection of all the prime ideals of height 0.*

Proof. By exercise 4.3,

$$\sqrt{0} = \mathfrak{N}_R = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r \tag{6.1}$$

is the intersection of finitely many prime ideals. If $\mathfrak{q}$ is any prime ideal, $\mathfrak{N}_R \subseteq \mathfrak{q}$, hence $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r \subseteq \mathfrak{q}$ and thus $\mathfrak{p}_i \subseteq \mathfrak{q}$ for some $1 \leq i \leq r$. If $\mathfrak{q}$ is minimal, this must be an equality. Thus every prime of height 0 appears (6.1). Suppose one of the primes in (6.1), say $\mathfrak{p}_1$, is not minimal: by corollary 6.1.10 it contains a minimal prime, i.e. a prime in the set $\{\mathfrak{p}_2, \ldots, \mathfrak{p}_r\}$. Hence $\mathfrak{N}_R = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_r = \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_r$ and we can remove $\mathfrak{p}_1$. □

Theorem 6.1.12 (Krull's Hauptidealsatz) *Let R be a noetherian ring, $x \in R$, not invertible. If $\mathfrak{p} \subset R$ is a prime ideal, minimal among those containing x, then* $\operatorname{ht} \mathfrak{p} \leq 1$.

Proof. Let $\mathfrak{p}$ be a prime, minimal among those containing x and let $\mathfrak{p} \supsetneq \mathfrak{q}_1 \supseteq \mathfrak{q}_0$ be primes contained in $\mathfrak{p}$. By minimality of $\mathfrak{p}$, $x \notin \mathfrak{q}_1$. We want to show that $\mathfrak{q}_1 = \mathfrak{q}_0$. Since we are only interested in primes between $\mathfrak{p}$ and $\mathfrak{q}_0$, we may replace R by $R_{\mathfrak{p}}/\mathfrak{q}_0 R_{\mathfrak{p}}$. We may thus assume that R is a local domain with maximal ideal $\mathfrak{p}$, with $x \in \mathfrak{p}$ not contained in any other prime ideal and we want to show that if $\mathfrak{q} \subsetneq \mathfrak{p}$ is a prime ideal then $\mathfrak{q} = 0$. The ring R/xR is noetherian and its only prime ideal, $\mathfrak{p}/xR$, is minimal by assumption: it is thus an artinian ring by corollary 6.1.7. Consider, for all $n \in \mathbb{N}$, the *symbolic powers*

$$\mathfrak{q}^{(n)} = \{y \in R \mid \exists\, z \notin \mathfrak{q} \text{ such that } yz \in \mathfrak{q}^n\}\,.$$

$\mathfrak{q}^{(n)}$ is an ideal: it is obviously closed under multiplication by elements in R and if $y_1, y_2 \in \mathfrak{q}^{(n)}$ and $z_1, z_2 \notin \mathfrak{q}$ satisfy $z_i y_i \in \mathfrak{q}^n$ then $z_1 z_2 (y_1 + y_2) \in \mathfrak{q}^n$ and $z_1 z_2 \notin \mathfrak{q}$ because $\mathfrak{q}$ is prime. Clearly $\mathfrak{q}^n \subseteq \mathfrak{q}^{(n)}$. Moreover $\mathfrak{q}^{(n)} \supseteq \mathfrak{q}^{(n+1)}$, so we have a descending chain of ideals, whence a descending chain $\ldots \mathfrak{q}^{(n)} + xR \supseteq \mathfrak{q}^{(n+1)} + xR \ldots$. Since R/xR is artinian, $\mathfrak{q}^{(n)} + xR = \mathfrak{q}^{(n+1)} + xR$ for n sufficiently large. This in turn implies that

$$\mathfrak{q}^{(n)} = x\mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)}. \tag{6.2}$$

Indeed, trivially $\mathfrak{q}^{(n)} \supseteq x\mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)}$ and for any $y \in \mathfrak{q}^{(n)}$ we have $y = rx + q$ for some $r \in R$ and $q \in \mathfrak{q}^{(n+1)} \subseteq \mathfrak{q}^{(n)}$. So $rx \in \mathfrak{q}^{(n)}$ and, by definition, there exists $z \notin \mathfrak{q}$ such that $rxz \in \mathfrak{q}^n \subseteq \mathfrak{q}^{(n)}$. But $x, z \notin \mathfrak{q}$ and the latter is prime, thus $xz \notin \mathfrak{q}$. Hence $r \in \mathfrak{q}^{(n)}$, which proves (6.2).

From (6.2), by Nakayama's lemma we deduce that $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$. Let now $S = R - \mathfrak{q}$. Clearly $S^{-1}\mathfrak{q}^{(n)} = \left(S^{-1}\mathfrak{q}\right)^n$ and $S^{-1}\mathfrak{q}^{(n+1)} = \left(S^{-1}\mathfrak{q}\right)^{n+1}$. Therefore $\left(S^{-1}\mathfrak{q}\right)^n = \left(S^{-1}\mathfrak{q}\right)^{n+1}$. Since $S^{-1}\mathfrak{q}$ is the maximal ideal of the local ring $S^{-1}R = R_{\mathfrak{q}}$, Nakayama again implies $\left(S^{-1}\mathfrak{q}\right)^n = 0$. But R is a domain, hence $S^{-1}\mathfrak{q} = 0$ and therefore $\mathfrak{q} = 0$. □

The Principal Ideal's Theorem's name is justified by the following application:

Corollary 6.1.13 *Let R be a noetherian domain. We suppose that R is not a field. Then R is a UFD if and only if every prime ideal of height 1 is principal.*

Proof. If R is a UFD and $\mathfrak{p}$ is a prime of height 1, choose any $0 \neq x \in \mathfrak{p}$. At least one irreducible factor y of x belongs to $\mathfrak{p}$. Then $0 \subsetneq (y) \subseteq \mathfrak{p}$: since (y) is prime and $\operatorname{ht}\mathfrak{p} = 1$, it follows $\mathfrak{p} = (y)$.

Conversely, suppose that every prime of height 1 is principal. Let $0 \neq x \in R$, $x \notin R^\times$. Suppose that x can't be written as a finite product of irreducibles. Let $\mathfrak{p}$ be a minimal prime containing x. Then $\operatorname{ht}\mathfrak{p} \leq 1$ by theorem 6.1.12, but 0 is the only prime of height 0 in a domain, thus $\operatorname{ht}\mathfrak{p} = 1$. By assumption, $\mathfrak{p} = (y_1)$, hence $x = x_1 y_1$ for a suitable $x_1 \in R$. We have $x_1 \neq 0$ (since $x \neq 0$) and $x_1 \notin R^\times$ otherwise x would be irreducible, because associated to the irreducible element y_1. Moreover x_1 can't be written as a finite product of irreducibles, because otherwise the same would hold for x, contrary to our assumptions. So x_1 has the same properties as x and $(x) \subsetneq (x_1)$. We can repeat the process to get an infinite ascending chain $(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \dots$ contradicting the assumption that R is noetherian. □

Corollary 6.1.14 *Let R be a noetherian domain, $I \subset R$ an integral invertible ideal. Then $I \subseteq \mathfrak{p}$ for some prime ideal $\mathfrak{p} \subset R$ of height 1.*

Proof. Let $\pi : R \to R/I$ and $\mathfrak{q} \subset R/I$ a minimal prime ideal. Then $\mathfrak{p} = \pi^{-1}(\mathfrak{q})$ is minimal among primes containing I. By assumption, $IR_\mathfrak{p} = (x)$ for some $x \in R_\mathfrak{p}$. Therefore $\mathfrak{p}R_\mathfrak{p}$ is minimal among the primes in $R_\mathfrak{p}$ containing x: by the Principal Ideal theorem, $\operatorname{ht}\mathfrak{p}R_\mathfrak{p} = \operatorname{ht}\mathfrak{p} \leq 1$, and in fact $\operatorname{ht}\mathfrak{p} = 1$ since R is a domain. □

Remark 6.1.15 In the course of the proof, we have also reproved lemma 5.2.33 for invertible ideals: an invertible ideal in a noetherian domain is contained in only finitely many height 1 primes: they are in bijection with the minimal primes in R/I.

Corollary 6.1.16 *If R is a noetherian UFD, then $\operatorname{Pic}(R) = 0$.*

Proof. The Picard group is generated by the invertible prime ideals and every invertible prime is of height 1, thus principal, hence free as an R-module. □

We now prepare for a generalisation of theorem 6.1.12.

Lemma 6.1.17 *Let R be a noetherian ring, $\mathfrak{p} \subset R$ a prime ideal and $x \in \mathfrak{p}$. For any chain of primes $\mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n$ descending from $\mathfrak{p}$, there exists a chain of primes $\mathfrak{p} = \mathfrak{q}_0 \supsetneq \mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_n$ such that $x \in \mathfrak{q}_{n-1}$.*

Proof. Suppose $x \in \mathfrak{p}_{i-1}$ but $x \notin \mathfrak{p}_i$ for some $i < n$. In the domain $R/\mathfrak{p}_{i+1}$ we have the chain of primes $\mathfrak{p}_{i-1}/\mathfrak{p}_{i+1} \supsetneq \mathfrak{p}_i/\mathfrak{p}_{i+1} \supsetneq 0$ of length 2, so theorem 6.1.12 implies that $\mathfrak{p}_{i-1}/\mathfrak{p}_{i+1}$ is not minimal among the primes in $R/\mathfrak{p}_{i+1}$ containing x mod $\mathfrak{p}_{i+1}$. Hence $\mathfrak{p}_{i-1}$ is not minimal among the primes in R containing $x + \mathfrak{p}_{i+1}$: there is then a prime $\mathfrak{q}_i$ such that $x \in \mathfrak{q}_i$ and $\mathfrak{p}_{i-1} \supsetneq \mathfrak{q}_i \supseteq x + \mathfrak{p}_{i+1} \supsetneq \mathfrak{p}_{i+1}$. Replace $\mathfrak{p}_i$ by $\mathfrak{q}_i$ in the sequence to get a chain such that $x \in \mathfrak{q}_i$. We can repeat this process if necessary until we get a chain as required. □

Corollary 6.1.18 *Let R be a local noetherian ring and $x \notin R^\times$. Then $\dim(R/xR) \geq \dim R - 1$.*

Proof. Let $\mathfrak{m} \subset R$ be the maximal ideal. Necessarily $x \in \mathfrak{m}$. By lemma 6.1.17, for any chain of length n descending from $\mathfrak{m}$ there is a chain $\mathfrak{m} = \mathfrak{q}_0 \supsetneq \mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_n$ with $x \in \mathfrak{q}_{n-1}$, whence a chain $\mathfrak{m}/xR \supsetneq \mathfrak{q}_1/xR \supsetneq \cdots \supsetneq \mathfrak{q}_{n-1}/xR$ of length $n-1$ in R/xR. □

Theorem 6.1.19 *Let R be a noetherian ring, $I \subsetneq R$ an ideal generated by n elements $x_1, \dots, x_n$. If $\mathfrak{p}$ is a prime ideal of R, minimal among those containing I, then $\operatorname{ht} \mathfrak{p} \leq n$.*

Proof. For $n = 1$, this is theorem 6.1.12. Assume that the statement holds for all ideals generated by at most $n-1$ elements and let $\mathfrak{p}$ be a prime ideal containing I. Choose an integer $k \leq \operatorname{ht} \mathfrak{p}$ and a chain $\mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_k$. By lemma 6.1.17, we may assume that $x_1 \in \mathfrak{p}_{k-1}$. Denoting by h the height in R/x_1R of the prime ideal $\mathfrak{p}/x_1R$ we have $h \geq k-1$ (because of the bijection between primes in R and primes in R/x_1R, the $\mathfrak{p}_i/x_1R$ are all distinct for $0 \leq i \leq k-1$). If $\mathfrak{p}$ is minimal among the primes of R containing I, then $\mathfrak{p}/x_1R$ is minimal among the primes of R/x_1R containing I/x_1R and, by inductive assumption, $h \leq n-1$. Hence $k-1 \leq h \leq n-1$ and thus $k \leq n$. Therefore any strictly decreasing chain of prime ideals descending from $\mathfrak{p}$ has length at most n. This means precisely that $\operatorname{ht} \mathfrak{p} \leq n$. □

Corollary 6.1.20 *In a noetherian ring, the height of any prime ideal is finite. The dimension of any local noetherian ring is finite.*

Proof. A prime ideal $\mathfrak{p}$ in a noetherian ring is finitely generated and obviously minimal among the primes containing $\mathfrak{p}$, so has finite height by theorem 6.1.19. The second statement is a rephrasement of the first, since $\dim R_{\mathfrak{p}} = \operatorname{ht} \mathfrak{p}$. □

Corollary 6.1.21 *Let R be a local noetherian ring, $\mathfrak{m}$ its maximal ideal and k its residue field. Then $\dim R \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$.*

Proof. By Nakayama's lemma, $\mathfrak{m}$ can be generated by $\dim_k \mathfrak{m}/\mathfrak{m}^2$ elements, and an ideal is clearly minimal among those containing its generators. □

Theorem 6.1.19 admits a converse, proposition 6.1.23 below. Its proof requires a useful trick.

Lemma 6.1.22 (prime avoidance) *Let R be a ring, $I \subseteq R$ an ideal and $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_s$ be ideals with $\mathfrak{a}_2, \dots, \mathfrak{a}_s$ primes. If $I \subseteq \bigcup_{j=1}^s \mathfrak{a}_j$, then I is contained in one of the $\mathfrak{a}_j$.*

Proof. The claim is trivial if $s = 1$. By induction, assume that the claim holds for unions of at most $s-1$ ideals, suppose $I \nsubseteq \bigcup_{j \neq i}^s \mathfrak{a}_j$, for $1 \leq i \leq s$ and let's derive a contradiction. Let thus $x_i \in I \cap \mathfrak{a}_i$ such that $x_i \notin \mathfrak{a}_j \ \forall\ j \neq i$. Then $x_s + x_1 \cdots x_{s-1} \in I$, but is neither in $\mathfrak{a}_s$ (because $x_1, \dots, x_{s-1} \notin \mathfrak{a}_s$ and $\mathfrak{a}_s$ is prime), nor in any of the $\mathfrak{a}_1, \dots, \mathfrak{a}_{s-1}$, because $x_s \notin \mathfrak{a}_j$ for all $j \leq s-1$. This contradicts the assumption $I \subseteq \bigcup_{j=1}^s \mathfrak{a}_j$. Hence I is contained in a union of $s-1$ of these ideals and we can conclude by induction. □

Proposition 6.1.23 *Let R be a noetherian ring and $\mathfrak{p} \subset R$ a prime ideal of height h. There exist $x_1, \dots, x_h \in R$ such that $\mathfrak{p}$ is one of the minimal primes containing $x_1, \dots, x_h$.*

Proof. An ideal of height 0 is a minimal prime of R, which we can view as a minimal prime containing the empty set. By induction on $k \leq h$, we want to construct a sequence $x_1, \dots, x_k \in \mathfrak{p}$ such that every minimal prime ideal containing $x_1, \dots, x_k$ has height k. For $k = h$ we end up with primes in $\mathfrak{p}$, minimal among those containing a sequence of h elements and with the same height as $\mathfrak{p}$, so by remark 6.1.2 they all coincide with $\mathfrak{p}$.
For $0 \leq k < h$, let $x_1, \dots, x_k \in \mathfrak{p}$, write $\mathfrak{a} = (x_1, \dots, x_k)$ and let $\mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_s$ be the minimal prime ideals containing $x_1, \dots, x_k$: there is a finite number of them, since they are in bijection

with the minimal primes of $R/\mathfrak{a}$, and we can apply corollary 6.1.11. We assume that $\operatorname{ht}\mathfrak{q}_j = k$ for all j. Applying lemma 6.1.22, we see that $\mathfrak{p} \nsubseteq \bigcup_{j=1}^{s} \mathfrak{q}_j$, otherwise $\mathfrak{p} \subseteq \mathfrak{q}_j$ for some j, which is impossible since $\operatorname{ht}\mathfrak{p} > \operatorname{ht}\mathfrak{q}_j$. Therefore, we may select $x_{k+1} \in \mathfrak{p}$ but $x_{k+1} \notin \mathfrak{q}_i$ for $1 \leq i \leq s$. Now if $\mathfrak{r}$ is any minimal prime ideal containing $x_1, \ldots, x_k, x_{k+1}$, then $\operatorname{ht}\mathfrak{r} \leq k+1$ by theorem 6.1.19. On the other hand, $\mathfrak{r}$ contains one of the $\mathfrak{q}_j$, because

$$\mathfrak{r}/\mathfrak{a} \supseteq \mathfrak{N}_{R/\mathfrak{a}} = (\mathfrak{q}_1/\mathfrak{a}) \cap \cdots \cap (\mathfrak{q}_s/\mathfrak{a}) \supseteq (\mathfrak{q}_1/\mathfrak{a}) \cdots (\mathfrak{q}_s/\mathfrak{a})$$

and $\mathfrak{r}/\mathfrak{a}$, being prime in $R/\mathfrak{a}$, contains one of the factors. Thus $\operatorname{ht}\mathfrak{r} = k+1$, by remark 6.1.2. □

Corollary 6.1.24 *The dimension of a local noetherian ring with maximal ideal $\mathfrak{m}$ is the smallest number $d \in \mathbb{N}$ such that there exist $x_1, \ldots, x_d \in \mathfrak{m}$ and $n_0 \in \mathbb{N}$ such that*

$$\mathfrak{m}^n \subseteq (x_1, \ldots, x_d) \subseteq \mathfrak{m} \qquad \forall\, n \geq n_0.$$

Proof. If $x_1, \ldots, x_d$ and n are as in the statement, $\mathfrak{m}^n \subseteq \mathfrak{p}$ for any prime $\mathfrak{p}$ containing the x_i, hence $\mathfrak{m} \subseteq \mathfrak{p}$ and $\mathfrak{p} = \mathfrak{m}$ by maximality of $\mathfrak{m}$. Thus $\mathfrak{m}$ is minimal among ideals containing $x_1, \ldots, x_d$, hence $\operatorname{ht}\mathfrak{m} \leq d$ by theorem 6.1.19. On the other hand, by proposition 6.1.23, for $h = \operatorname{ht}\mathfrak{m} = \dim R$ we may find $x_1, \ldots, x_h \in \mathfrak{m}$ such that $\mathfrak{m}$ is minimal among the primes containing $x_1, \ldots, x_h$. Consider $\mathfrak{a} = (x_1, \ldots, x_h)$. The minimality property of $\mathfrak{m}$ implies that $\mathfrak{m}/\mathfrak{a}$ is the only prime in $R/\mathfrak{a}$. Thus $\mathfrak{m}/\mathfrak{a} = \mathfrak{N}_{R/\mathfrak{a}}$ and, since $R/\mathfrak{a}$ is noetherian, its nilradical is nilpotent. Therefore $(\mathfrak{m}/\mathfrak{a})^n = 0$ for some $n \in \mathbb{N}$, hence $\mathfrak{m}^n \subseteq \mathfrak{a} = (x_1, \ldots, x_h) \subseteq \mathfrak{m}$. □

Example 6.1.25 Let k be a field. Recall from example 5.2.31 that in $R = k[X,Y,Z]/(Z^2 - XY)$ the prime ideal $\mathfrak{p} = (y, z)$ is of height 1 but not principal. If $\mathfrak{q} \subset R$ is any prime such that $y \in \mathfrak{q}$ then $z \in \mathfrak{q}$, because $z^2 = xy \in \mathfrak{q}$ and $\mathfrak{q}$ is prime. Thus $\mathfrak{p}$ is minimal among prime ideals containing y and $\mathfrak{p}^2 = (y^2, yz, z^2) = (y^2, yz, xy) \subset (y)$.

The following result expresses semi-continuity for the dimension of the fibres of a morphism and highlights one of the fundamental properties of flat morphisms: continuous variation of the fibres.

Theorem 6.1.26 *Let $\varphi : R \to A$ be a morphism of noetherian rings, $\mathfrak{q} \subset A$ a prime ideal and $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$. Then*

$$\dim A_{\mathfrak{q}} \leq \dim R_{\mathfrak{p}} + \dim\left(A_{\mathfrak{q}} \otimes_R R/\mathfrak{p}\right)$$

with equality if $\varphi : R \to A$ satisfies the Going Down property.

Proof. Let $d = \dim R_{\mathfrak{p}}$ and h the dimension of $A_{\mathfrak{q}} \otimes_{R_{\mathfrak{p}}} R/\mathfrak{p} = A/\mathfrak{p}A$. By proposition 6.1.23, there exist $x_1, \ldots, x_d \in \mathfrak{p}$ such that $\mathfrak{p}^n \subseteq (x_1, \ldots, x_d) \subseteq \mathfrak{p}$ and $y_1, \ldots, y_h \in \mathfrak{q}A_{\mathfrak{q}}$ such that $\mathfrak{q}^m A_{\mathfrak{q}} \subseteq (y_1, \ldots, y_h) + \mathfrak{p}A_{\mathfrak{q}}$ for $m, n \in \mathbb{N}$ sufficiently large. Therefore

$$\mathfrak{q}^{nm} A_{\mathfrak{q}} \subseteq ((y_1, \ldots, y_h) + \mathfrak{p}A_{\mathfrak{q}})^n \subseteq (y_1, \ldots, y_h) + \mathfrak{p}^n A_{\mathfrak{q}} \subseteq (x_1, \ldots, x_d, y_1, \ldots, y_h) A_{\mathfrak{q}} \subseteq \mathfrak{q}A_{\mathfrak{q}}$$

hence $\mathfrak{q}$ is a minimal prime containing $x_1, \ldots, x_d, y_1, \ldots, y_h$, thus $\dim A_{\mathfrak{q}} = \operatorname{ht}\mathfrak{q} \leq d + h$ by theorem 6.1.19.
Now suppose that $\varphi : R \to A$ satisfies the Going Down property. By definition, there is a chain of primes $\mathfrak{q} = \mathfrak{q}_0 \supsetneq \cdots \supsetneq \mathfrak{q}_h$ such that $\mathfrak{p}A \subseteq \mathfrak{q}_h$. Since $\mathfrak{p} \subseteq \varphi^{-1}(\mathfrak{q}_h) \subseteq \varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$ we have

$\varphi^{-1}(\mathfrak{q}_i) = \mathfrak{p}$ for $0 \leq i \leq h$. Since $d = \dim R_{\mathfrak{p}} = \operatorname{ht} \mathfrak{p}$, there is a chain of primes $\mathfrak{p} = \mathfrak{p}_0 \supsetneq \cdots \supsetneq \mathfrak{p}_d$ in R. By the going down property, there is a chain of primes $\mathfrak{q}_h = \mathfrak{r}_0 \supsetneq \cdots \supsetneq \mathfrak{r}_d$ in A such that $\varphi^{-1}(\mathfrak{r}_i) = \mathfrak{p}_i$. Whence a chain $\mathfrak{q} = \mathfrak{q}_0 \supsetneq \cdots \supsetneq \mathfrak{q}_h = \mathfrak{r}_0 \supsetneq \cdots \supsetneq \mathfrak{r}_d$ of length $d + h$ in $A_{\mathfrak{q}}$. Thus $\dim A_{\mathfrak{q}} \geq d + h$. We conclude that $\dim A_{\mathfrak{q}} = d + h$. □

Corollary 6.1.27 *Let R be a local noetherian ring and $\hat{R}$ its completion. Then $\dim R = \dim \hat{R}$.*

Proof. Follows from corollary 3.6.42 and remark 4.1.20. ⊠

Theorem 6.1.28 *If R is a noetherian ring, then $\dim R[X] = \dim R + 1$.*

Proof. If $I \subset R$ is any ideal, reducing mod I the coefficients yields a surjective homomorphism $R[X] \to (R/I)[X]$ whose kernel is clearly $IR[X]$. In particular, if I is prime, R/I is a domain and so is $(R/I)[X]$, hence $IR[X]$ is prime. Then $IR[X] + (X) \supsetneq IR[X]$ is also a prime, since $R[X]/(IR[X] + (X)) \cong (R/I)[X]/(X) \cong R/I$. If $I \subsetneq J \subseteq R$ are arbitrary ideals, supposing $IR[X] = JR[X]$ we would have that any $y \in J$ could be written $y = a_0 + a_1X + \cdots + a_nX^n$ with $a_i \in I$, thus $(-y + a_0) + a_1X + \cdots + a_nX^n = 0$ in $R[X]$, hence $y = a_0 \in I$, contradicting $J \nsubseteq I$. These computations show that any chain of primes $\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n$ in R gives rise to a chain $\mathfrak{p}_0R[X] + (X) \supsetneq \mathfrak{p}_0R[X] \supsetneq \mathfrak{p}_1R[X] \supsetneq \cdots \supsetneq \mathfrak{p}_nR[X]$ in $R[X]$. Therefore $\dim R[X] \geq \dim R + 1$.

Let $\mathfrak{p} \subset R$ be a prime ideal and $\mathfrak{q} \subset R[X]$ be a prime ideal, maximal among those containing $\mathfrak{p}R[X]$ and such that $\mathfrak{q} \cap R = \mathfrak{p}$. We shall prove that

$$\dim R[X]_{\mathfrak{q}} = \dim R_{\mathfrak{p}} + 1. \tag{6.3}$$

Granting this, for any prime $\mathfrak{r} \subset R[X]$, put $\mathfrak{p} = \mathfrak{r} \cap R$ and let $\mathfrak{q} \supseteq \mathfrak{r}$ be a prime ideal, maximal among those containing $\mathfrak{p}R[X]$ and such that $\mathfrak{q} \cap R = \mathfrak{p}$. From (6.3) we get

$$\operatorname{ht} \mathfrak{r} \leq \operatorname{ht} \mathfrak{q} = \dim R[X]_{\mathfrak{q}} \leq \dim R_{\mathfrak{p}} + 1 \leq \dim R + 1.$$

Therefore if the dimension of R is finite, so is that of $R[X]$ and, choosing $\mathfrak{r}$ such that $\operatorname{ht} \mathfrak{r} = \dim R[X]$, we conclude that $\dim R[X] = \dim R + 1$.
If R is a field, $\dim R = 0$ and $R[X]$ is a Dedekind domain, so (6.3) follows from example 6.1.4. In the general case, we may replace R by $R_{\mathfrak{p}}$ and assume that $\mathfrak{p}$ is maximal in R, with residue field $k = R/\mathfrak{p}$. As above, if $\mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_d$ is a chain in R, with $d = \dim R$, we get the chain $\mathfrak{q} \supseteq \mathfrak{p}R[X] \supsetneq \mathfrak{p}_1R[X] \supsetneq \cdots \supsetneq \mathfrak{p}_dR[X]$ in $R[X]$ and $\mathfrak{q} \neq \mathfrak{p}R[X]$ because the latter is not maximal among those containing $\mathfrak{p}R[X]$ and such that $\mathfrak{q} \cap R = \mathfrak{p}$ (it is contained in $\mathfrak{p}R[X] + (X)$). Thus $\dim R[X]_{\mathfrak{q}} \geq \dim R_{\mathfrak{p}} + 1$. On the other hand, from theorem 6.1.26 we get

$$\dim R[X]_{\mathfrak{q}} \leq \dim R_{\mathfrak{p}} + \dim (R[X]_{\mathfrak{q}} \otimes_R k) = \dim R_{\mathfrak{p}} + \dim k[X] = \dim R_{\mathfrak{p}} + 1.$$ □

Corollary 6.1.29 *If k is a field, $\dim k[X_1, \ldots, X_n] = n$.*

Example 6.1.30 Let k be a field. For $h \leq n$, let $\mathfrak{p} = (X_1, \ldots, X_h) \subset R = k[X_1, \ldots, X_n]$. Then $R/\mathfrak{p} = k[X_{h+1}, \ldots, X_n]$ and $R_{\mathfrak{p}} = k(X_{h+1}, \ldots, X_n)[X_1, \ldots, X_h]$. Hence $\operatorname{ht} \mathfrak{p} = h$ and $\dim R/\mathfrak{p} = n - h$. In particular, the inequality in remark 6.1.3 is sharp. We shall generalise this in proposition 6.1.35 below.

Example 6.1.31 Theorem 6.1.28 says that $\dim \mathbb{Z}[X] = \dim \mathbb{Z} + 1 = 2$. This may come as a surprise, given that $\operatorname{Spec} \mathbb{Z}[X] = \mathbb{A}^1_{\mathbb{Z}}$ is the affine *line* over $\mathbb{Z}$. Let us check its points. Being a domain, the only minimal prime in $\mathbb{Z}[X]$ is 0. Its residue field is $\operatorname{Frac} \mathbb{Z}[X] = \mathbb{Q}(X)$. If $0 \neq \mathfrak{p} \subset \mathbb{Z}[X]$, then $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. Notice that $p\mathbb{Z}[X] \subseteq \mathfrak{p}$ is a prime ideal, since $\mathbb{Z}[X]/p\mathbb{Z}[X]$ is equal to $\mathbb{F}_p[X]$ (if p is a prime number) or $\mathbb{Z}[X]$ (if $p = 0$). If $\operatorname{ht} \mathfrak{p} = 1$ and p is a prime, necessarily $0 \subsetneq p\mathbb{Z}[X] = \mathfrak{p}$, while for $p = 0$, since $\mathfrak{p} \cap (\mathbb{Z} - \{0\}) = \varnothing$, we have $\mathfrak{p} \subset \mathbb{Q}[X]$, generated by an irreducible polynomial. If $\operatorname{ht} \mathfrak{p} = 2$, since $\dim \mathbb{Q}[X] = 1$, necessarily $\mathfrak{p}$ contains a prime number $p > 0$. Then $0 \subsetneq p\mathbb{Z}[X] \subsetneq \mathfrak{p} = (p, F(X))$, where $F(X) \in \mathbb{Z}[X]$ is an irreducible polynomial such that $F \bmod p\mathbb{Z}[X]$ generates the (maximal) ideal $\mathfrak{p}/p\mathbb{Z}[X] \subset \mathbb{F}_p[X]$. These are all the closed points of $\mathbb{A}^1_{\mathbb{Z}}$. The best way to picture this is shown in figure 6.1. One should regard $\mathbb{A}^1_{\mathbb{Z}}$ as an (affine) **arithmetic surface**, fibered over $\operatorname{Spec} \mathbb{Z}$ (the inclusion $\mathbb{Z} \subset \mathbb{Z}[X]$ corresponding to the projection $\operatorname{Spec} \mathbb{A}^1_{\mathbb{Z}} \to \operatorname{Spec} \mathbb{Z}$). Above each prime number $p \in \mathbb{Z}$ lies the affine line $\mathbb{A}^1_{\mathbb{F}_p} = \operatorname{Spec} \mathbb{F}_p[X] \hookrightarrow \mathbb{A}^1_{\mathbb{Z}}$ (corresponding to $\mathbb{Z}[X] \twoheadrightarrow \mathbb{F}_p[X]$) and similarly $\mathbb{A}^1_{\mathbb{Q}} \hookrightarrow \mathbb{A}^1_{\mathbb{Z}}$ (corresponding to $\mathbb{Z}[X] \subset \mathbb{Q}[X]$) lies above $0 \in \mathbb{Z}$. Points corresponding to primes of height ≤ 1 shown as squiggles. These include all the points on the "generic fibre" $\mathbb{A}^1_{\mathbb{Q}}$: taking their closure gives rise to the horizontal curves. The minimal prime 0 doesn't contain any proper ideal in $\mathbb{Z}[X]$ and so belongs to every open set. It is thus called the "generic point".
Notice that the way the closure of the point $(f(X)) \subset \mathbb{Q}[X]$ meets the fibre $\mathbb{A}^1_{\mathbb{F}_p}$ is prescribed by the splitting of the prime p in the field extension $\mathbb{Q} \subseteq \mathbb{Q}[X]/(f(X))$. There can be one or more points, defined over $\mathbb{F}_p$ or some finite extension, and ramification is shown as tangency between the horizontal curve and the vertical fibre.

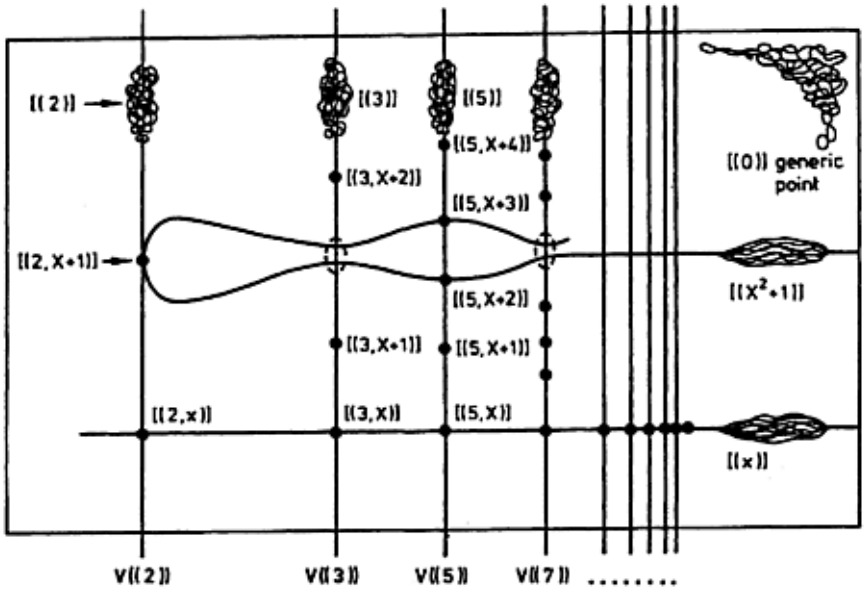


Figure 6.1: The affine line $\mathbb{A}^1_{\mathbb{Z}}$ (taken from [12]).

Now that we have some examples of finite-dimensional rings, we can get more by means of the following result.

Proposition 6.1.32 *Let $R \subset A$ be rings, with A integral over R. Then $\dim R = \dim A$ (and in particular, one is finite if and only if the other is finite). If $\mathfrak{q} \subset A$ is a prime and $\mathfrak{p} = \mathfrak{q} \cap R$, then $\operatorname{ht} \mathfrak{p} = \operatorname{ht} \mathfrak{q}$.*

Proof. If $\dim R = d$, there exists a chain $\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_d$ of primes in R. By Going Up there is a chain $\mathfrak{q}_0 \supsetneq \mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_d$ in A with $\mathfrak{q}_i \cap R = \mathfrak{p}_i$, thus $\dim A \geq \dim R$. Moreover, if $\mathfrak{q}_i \supseteq \widetilde{\mathfrak{q}} \supseteq \mathfrak{q}_{i+1}$ then $\mathfrak{p}_i \supseteq \widetilde{\mathfrak{q}} \cap R \supseteq \mathfrak{p}_{i+1}$ and, since there are no primes between $\mathfrak{p}_{i+1}$ and $\mathfrak{p}_i$, either $\widetilde{\mathfrak{q}} \cap R = \mathfrak{p}_{i+1}$ or $\widetilde{\mathfrak{q}} \cap R = \mathfrak{p}_i$, which, by corollary 3.2.3, implies either $\widetilde{\mathfrak{q}} = \mathfrak{q}_{i+1}$ or $\widetilde{\mathfrak{q}} = \mathfrak{q}_i$. Hence the sequence $\{\mathfrak{q}_i\}$ can't be refined, thus $\dim A = \dim R$.
Conversely, taking a chain of length $\dim A$ in A and intersecting with R we get $\dim R \geq \dim A$, and such a chain in R can't be refined because otherwise we would get a chain of length strictly bigger than $\dim A$ in A. Therefore $\dim R = \dim A$. □

Corollary 6.1.33 *If R is an algebra of finite type over a field, then $\dim R < +\infty$.*

Proof. By Noether's Normalisation lemma 4.3.1, R is integral over a subalgebra $k[Y_1, \ldots, Y_d]$. Combining corollary 6.1.29 and proposition 6.1.32 we conclude $\dim R = d$. □

Corollary 6.1.34 *If R is a domain, of finite type over a field k and $K = \operatorname{Frac} R$ then $\dim R$ equals the transcendence degree of K over k.*

Proof. The transcendence degree of $k(X_1, \ldots, X_n)$ over k is $n = \dim k[X_1, \ldots, X_n]$. The general case follows from the Normalisation lemma as in the proof of corollary 6.1.33. □

Proposition 6.1.35 *If R is a domain, of finite type over a field, $\dim R/\mathfrak{p} + \operatorname{ht} \mathfrak{p} = \dim R$ for any prime $\mathfrak{p} \subset R$.*

Proof. Let $R = k[X_1, \ldots, X_n]/I$ (where I is prime since R is a domain) and $\mathfrak{q} \supseteq I$ the prime ideal in $k[X_1, \ldots, X_n]$ such that $\mathfrak{q}/I = \mathfrak{p}$. We shall prove that there exist integers $e \leq d \leq n$ and an injection $k[Z_1, \ldots, Z_n] \subseteq k[X_1, \ldots, X_n]$ such that:

a) $k[X_1, \ldots, X_n]$ is finite over $k[Z_1, \ldots, Z_n]$;

b) $I \cap k[Z_1, \ldots, Z_n] = (Z_{d+1}, \ldots, Z_n)$;

c) $\mathfrak{q} \cap k[Z_1, \ldots, Z_n] = (Z_{e+1}, \ldots, Z_n)$.

It follows immediately that R is finite over $k[Z_1, \ldots, Z_d]$, hence $\dim R = d$, by corollary 6.1.29 and propostion 6.1.32; that $R/\mathfrak{p}$ is finite over $k[Z_1, \ldots, Z_e]$, thus $\dim R/\mathfrak{p} = e$, for the same reasons; and that $\mathfrak{p} \cap k[Z_1, \ldots, Z_d] \cong (\mathfrak{q} \cap k[Z_1, \ldots, Z_n]) / (I \cap k[Z_1, \ldots, Z_n])$ is the ideal in $k[Z_1, \ldots, Z_d]$ generated by $Z_{e+1}, \ldots, Z_d$. Example 6.1.30 now tells us $\operatorname{ht}(\mathfrak{p} \cap k[Z_1, \ldots, Z_d]) = d - e$ and by propostion 6.1.32 this is also the height of $\mathfrak{p}$, since R is finite over $k[Z_1, \ldots, Z_d]$. Therefore $\operatorname{ht} \mathfrak{p} = d - e = \dim R - \dim R/\mathfrak{p}$ as contended.
By the Normalisation lemma, there exists a finite injection $A = k[T_1, \ldots, T_n] \subseteq k[X_1, \ldots, X_n]$ and an integer $d \leq n$ such that

i) R is finite over $k[T_1, \ldots, T_d]$;

ii) $I \cap A = T_{d+1}A + \cdots + T_nA$.

We can also apply the Normalisation lemma to $k[T_1,\dots,T_d]/(\mathfrak{q}\cap k[T_1,\dots,T_d])$: there exists a finite injection $B=k[Z_1,\dots,Z_d]\subseteq k[T_1,\dots,T_d]$ and an integer $e\leq d$ such that

iii) $k[T_1,\dots,T_d]/(\mathfrak{q}\cap k[T_1,\dots,T_d])$ is finite over $k[Z_1,\dots,Z_e]$;

iv) $(\mathfrak{q}\cap k[T_1,\dots,T_d])\cap B=Z_{e+1}B+\cdots+Z_dB$.

Put $Z_i=T_i$ for $d+1\leq i\leq n$. Clearly $C=k[Z_1,\dots,Z_n]\subseteq A=k[T_1,\dots,T_n]\subseteq k[X_1,\dots,X_n]$ is a finite injection. This establishes a). Moreover

$$I\cap C=(I\cap A)\cap C=(T_{d+1}A+\cdots+T_nA)\cap C\subseteq T_{d+1}C+\cdots+T_nC=Z_{d+1}C+\cdots+Z_nC.$$

This inclusion is an equality by remark 6.1.2 because both ideals have the same height: by example 6.1.30, in A we have $\operatorname{ht}(T_{d+1},\dots,T_n)=n-d$, and this is also the height of $(I\cap A)\cap C$ by proposition 6.1.32, since A is integral over C. Again example 6.1.30 yields $\operatorname{ht}(Z_{d+1},\dots,Z_n)=n-d$ in C. This proves b).
Notice that $I\cap C=(Z_{d+1},\dots,Z_n)$ is the kernel of the natural projection $C\twoheadrightarrow B$. The inclusion $B\subset C$ gives a splitting, whence a decomposition $C=B\oplus(I\cap C)$ (as B-modules). Thus any $F\in C$ can be written as $F=F_0+(F-F_0)$ for a unique $F_0\in B$. Since $I\subseteq\mathfrak{q}$, for all $F\in C$ we have $F-F_0\in I\cap C\subseteq\mathfrak{q}\cap C$. Thus $F\in\mathfrak{q}\cap C$ if and only if

$$F_0\in(\mathfrak{q}\cap C)\cap B=(\mathfrak{q}\cap A)\cap B=Z_{e+1}B+\cdots+Z_dB\subseteq Z_{e+1}C+\cdots+Z_dC.$$

Therefore $\mathfrak{q}\cap C=Z_{e+1}C+\cdots+Z_nC$. This settles c) and concludes the proof. □

We conclude with an important structure theorem for the image of a morphism between the spectra of noetherian rings.

Definition 6.1.36 A subset of a topological space is **locally closed** if it is the intersection of an open subset with a closed subset. A finite union of locally closed subsets is called a **constructible** subset.

Theorem 6.1.37 (Chevalley) *Let R be a noetherian ring, A an R-algebra of finite type, $\varphi:R\to A$ the natural map. The image of $\varphi^\sharp:\operatorname{Spec}A\to\operatorname{Spec}R$ is a constructible set.*

Proof. We prove the theorem under the assumption that $\dim R<+\infty$, for the general case we refer to exercise 6.5. Let $\mathfrak{p}_1,\dots,\mathfrak{p}_n$ be the minimal primes of R. Since every prime contains a minimal prime, $\operatorname{Spec}R=\mathcal{Z}(\mathfrak{p}_1)\cup\cdots\cup\mathcal{Z}(\mathfrak{p}_n)$ is a union of finitely many closed subsets $\mathcal{Z}(\mathfrak{p}_i)=\operatorname{Spec}R/\mathfrak{p}_i$. From the proof of proposition 1.1.75 we get $(\varphi^\sharp)^{-1}((\mathcal{Z}(\mathfrak{p}_i))=\mathcal{Z}(\varphi(\mathfrak{p}_i)A)=\operatorname{Spec}A/\varphi(\mathfrak{p}_i)A$. Since a finite union of constructible sets is constructible, we may replace R by $R/\mathfrak{p}_i$ and A by $A/\varphi(\mathfrak{p}_i)A$. In particular, we may assume that R is a domain.
We proceed by induction on $\dim R$. If $\dim R=0$, the claim is trivial, as R is now a field and $\varphi^{-1}(\mathfrak{q})=0$ for any prime $\mathfrak{q}\subset A$, so $\operatorname{im}\varphi^\sharp=\operatorname{Spec}R$. For $\dim R=d>0$, let us compute $\overline{\operatorname{im}\varphi^\sharp}$, the closure of the image. As a closed subset, $\overline{\operatorname{im}\varphi^\sharp}=\mathcal{Z}(J)$, where J is the smallest ideal contained in every prime of the form $\varphi^{-1}(\mathfrak{q})$ for $\mathfrak{q}\subset A$ i.e.

$$J=\bigcap_{\mathfrak{q}\in\operatorname{Spec}A}\varphi^{-1}(\mathfrak{q})=\varphi^{-1}\left(\bigcap_{\mathfrak{q}\in\operatorname{Spec}A}\mathfrak{q}\right)=\varphi^{-1}\left(\mathfrak{N}_A\right).$$

If $\overline{\operatorname{im}\varphi^\sharp} \subsetneq \operatorname{Spec} R$, then $J \neq 0 = \mathfrak{N}_R$ and φ factors as $R \to R/J \to A$. Since $\dim R/J \leq d-1$ (any chain of primes in R/J lifts to a chain in R which can be extended by sticking the zero ideal at the bottom), we conclude by induction. If, on the contrary, $\overline{\operatorname{im}\varphi^\sharp} = \operatorname{Spec} R$ then

$$\ker\varphi = \varphi^{-1}(0) \subseteq \varphi^{-1}(\mathfrak{N}_A) = J = \mathfrak{N}_R = 0$$

so φ is injective: we may apply corollary 3.2.7 to conclude that $\operatorname{im}\varphi$ contains a non-empty open subset $U \subseteq \operatorname{Spec} R$. If $U = \operatorname{Spec} R$, we are done. Otherwise, write $Z = \operatorname{Spec} R - U$. There exists then an ideal $0 \neq I \subseteq R$ such that $Z = \mathcal{Z}(I) = \operatorname{Spec} R/I$. As above, $(\varphi^\sharp)^{-1}((\mathcal{Z}(I)) = \mathcal{Z}(\varphi(I)A) = \operatorname{Spec} A/\varphi(I)A$ and the image of $\varphi^\sharp$ is the disjoint union of U and $\operatorname{im}\overline{\varphi}^\sharp$, where $\overline{\varphi} : R/I \to A/\varphi(I)A$. Again, $\dim R/I \lneq \dim R$, since $I \neq 0$, and we conclude by induction. □

Corollary 6.1.38 *Let R be a noetherian ring, A an R-algebra of finite type, $\varphi : R \to A$ the natural map. If φ has the Going Down property, then $\varphi^\sharp : \operatorname{Spec} A \to \operatorname{Spec} R$ is an open map.*

Proof. Let $U = \operatorname{Spec} A - \mathcal{Z}(J)$ be an open subset. Since A is noetherian, $J = (f_1, \ldots, f_m)$ is finitely generated. Thus $U = \operatorname{Spec} A - (\bigcap_{i=1}^m \mathcal{Z}(f_i)) = \bigcup_{i=1}^m (\operatorname{Spec} A - \mathcal{Z}(f_i))$. Therefore, to show that $\varphi^\sharp(U)$ is an open subset, it suffices to do so for U of the form $\operatorname{Spec} A - \mathcal{Z}(f) = \operatorname{Spec} A_f$. Replacing A by $A_f = A[X]/(Xf-1)$, we are reduced to show that the image of $\varphi^\sharp$ is open. By Chevalley's theorem, $\operatorname{im}\varphi^\sharp$ is a constructible subset. Since φ has the Going Down property, for every $\mathfrak{p} \in \operatorname{im}\varphi^\sharp$ any $\mathfrak{p}' \subseteq \mathfrak{p}$ is also in the image. We conclude by lemma 6.1.39 below. □

Lemma 6.1.39 *A constructible subset $S \subseteq \operatorname{Spec} R$ is an open subset if and only if for every $\mathfrak{p} \in S$ all the primes $\mathfrak{p}' \subseteq \mathfrak{p}$ belong to S.*

Proof. We may assume that $S = U \cap T$ is the intersection of an open subset U and a closed subset T. It suffices to show that T is also open. Write $\operatorname{Spec} R = \mathcal{Z}(\mathfrak{p}_1) \cup \cdots \cup \mathcal{Z}(\mathfrak{p}_n)$ as the union of the closures of the minimal primes of R. The intersection $T \cap \mathcal{Z}(\mathfrak{p}_i)$ is either empty or equal to $\mathcal{Z}(\mathfrak{p}_i)$: if there is a $\mathfrak{q} \in T \cap \mathcal{Z}(\mathfrak{p}_i)$ then $\mathfrak{q} \supseteq \mathfrak{p}_i$, so by hypothesis $\mathfrak{p}_i \in U \cap T \subseteq T$, hence the closure $\overline{\{\mathfrak{p}_i\}} = \mathcal{Z}(\mathfrak{p}_i)$ is contained in the closed set T. Possibly renumbering the minimal primes, we have $T = \mathcal{Z}(\mathfrak{p}_1) \cup \cdots \cup \mathcal{Z}(\mathfrak{p}_m)$ and $T \cap \mathcal{Z}(\mathfrak{p}_i) = \varnothing$ for $m < i \leq n$. Therefore T is the complement in $\operatorname{Spec} R$ of the closed set $\bigcup_{i=m+1}^n \mathcal{Z}(\mathfrak{p}_i)$, and thus open.
Conversely, if S is open $\operatorname{Spec} R - S = \mathcal{Z}(I)$ for a suitable ideal $I \subset R$. Thus $\mathfrak{p} \in S$ iff $\mathfrak{p} \notin \mathcal{Z}(I)$ i.e. $I \nsubseteq \mathfrak{p}$. Therefore any prime $\mathfrak{p}' \subseteq \mathfrak{p}$ cannot contain I, i.e. $\mathfrak{p}' \notin \mathcal{Z}(I)$ so $\mathfrak{p}' \in S$. □

§ 2 Regular rings

Let R be a local noetherian ring, $\mathfrak{m}$ its maximal ideal and k its residue field. Recall that, by corollary 6.1.21, $\dim R \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$.

Definition 6.2.1 Let R be a local noetherian ring, $\mathfrak{m}$ its maximal ideal and k its residue field. We say that a noetherian ring R is **regular** if $\dim R = \dim_k \mathfrak{m}/\mathfrak{m}^2$. We say that a ring R is regular if $R_\mathfrak{p}$ is a regular local ring for every prime ideal $\mathfrak{p}$.

If $(R, \mathfrak{m})$ is a local k-algebra such that $R/\mathfrak{m} = k$, in remark 1.3.17 we have defined its tangent space as the dual vector space to $\mathfrak{m}/\mathfrak{m}^2$. Therefore R is regular if it has the same dimension as its tangent space.

Example 6.2.2 $\mathbb{Z}[X]$ is a regular ring. Indeed, from example 6.1.31, we know that its ideals of height 1 are principal and those of height 2 are generated by two elements.

Proposition 6.2.3 *Let R be a local noetherian ring with maximal ideal $\mathfrak{m}$.*

a) If $\dim R = 0$ then R is regular if and only if R is a field;

b) If $\dim R = 1$ then R is regular if and only if R is a DVR.

Proof. Clearly, a field is regular. Conversely, if R is regular of dimension zero then $\mathfrak{m} = \mathfrak{m}^2$, so by Nakayama $\mathfrak{m} = 0$ and thus R is a field.
A DVR is regular, since it is 1-dimensional and, if π is a uniformiser, $\mathfrak{m}/\mathfrak{m}^2 = (\pi)/(\pi^2)$ is also 1-dimensional. Conversely, if R is regular $\dim \mathfrak{m}/\mathfrak{m}^2 = 1$, so $\mathfrak{m}$ is principal, generated by any element in $\mathfrak{m} \setminus \mathfrak{m}^2$. Then R is a DVR by proposition 5.1.5, and the next result which ensures that the generator is not nilpotent. □

Proposition 6.2.4 *A regular noetherian local ring is a domain.*

Proof. Let $\mathfrak{m} \subset R$ be the maximal ideal and $d = \dim R$. The proof is by induction on $d = \dim R$. By proposition 6.2.3.a, we may assume $d \geq 1$.
Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the minimal prime ideals of R (there are finitely many of them, by corollary 6.1.11). By lemma 6.1.22, if $\mathfrak{m}$ were contained in the union of $\mathfrak{m}^2$ and the $\mathfrak{p}_i$'s, then either $\mathfrak{m} \subseteq \mathfrak{m}^2$, which is impossible because $\dim \mathfrak{m}/\mathfrak{m}^2 = d > 0$, or $\mathfrak{m} \subseteq \mathfrak{p}_i$ for some i, which is impossible because $\operatorname{ht} \mathfrak{m} = d > 0 = \operatorname{ht} \mathfrak{p}_i$. Therefore, there is an element $x \in \mathfrak{m}$ not contained in $\mathfrak{m}^2$ or any of the minimal primes.
Let $\pi : R \to \overline{R} = R/xR$ and $\overline{\mathfrak{m}} = \mathfrak{m}/xR$. Notice that $c = \dim \overline{R} < \dim R$: take a chain $\overline{\mathfrak{m}} \supsetneq \overline{\mathfrak{q}}_1 \supsetneq \cdots \supsetneq \overline{\mathfrak{q}}_c$ in $\overline{R}$, set $\mathfrak{q}_i = \pi^{-1}(\overline{\mathfrak{q}}_i)$ and get a chain $\mathfrak{m} \supsetneq \mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_c$. Since $x \in \mathfrak{q}_c$, we have $\operatorname{ht} \mathfrak{q}_c > 0$ and we can nest more primes inside $\mathfrak{q}_c$. On the other hand $\dim \overline{R} \geq \dim R - 1$, by corollary 6.1.18. Thus $\dim \overline{R} = d - 1$. From the exact sequence of $k = R/\mathfrak{m}$-vector spaces

$$0 \longrightarrow (xR + \mathfrak{m}^2)/\mathfrak{m}^2 \longrightarrow \mathfrak{m}/\mathfrak{m}^2 \longrightarrow \mathfrak{m}/(\mathfrak{m}^2 + xR) \cong \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 \longrightarrow 0$$

we deduce that $d - 1 = \dim \overline{R} \leq \dim_k \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 < \dim \mathfrak{m}/\mathfrak{m}^2 = d$. Thus the first is an equality and $\overline{R}$ is regular, of dimension $d - 1$, thus a domain by inductive assumption. Therefore xR is a prime ideal. By construction, it is not minimal, so it contains properly one of the minimal primes. Say $\mathfrak{p}_1 \subsetneq xR$. If $y \in \mathfrak{p}_1$, then $y = ax$ for some $a \in R$. Since $x \notin \mathfrak{p}_1$, then $a \in \mathfrak{p}_1$. Thus $\mathfrak{p}_1 \subseteq x\mathfrak{p}_1$. Hence $\mathfrak{p}_1 = x\mathfrak{p}_1 \subseteq \mathfrak{m}\mathfrak{p}_1 \subseteq \mathfrak{p}_1$. Therefore $\mathfrak{m}\mathfrak{p}_1 = \mathfrak{p}_1$ and by Nakayama we conclude $\mathfrak{p}_1 = 0$. So 0 is a minimal prime, i.e. R is a domain. □

The following theorem is a fundamental result on regular local rings. The proof ([18], chap. IV, proposition 23; see also [2] corollary 19.14, [8] corollary 18 G) is based on Serre's characterisation of regularity in terms of homological algebra.

Theorem 6.2.5 *If R is a regular local ring then $R_\mathfrak{p}$ is regular for every prime ideal $\mathfrak{p} \subset R$.* ⊠

Theorem 6.2.6 (Auslander-Buchsbaum) *A regular local ring is factorial.*

Remark 6.2.7 Thus: PID $\Longrightarrow$ regular $\Longrightarrow$ locally factorial $\Longrightarrow$ integrally closed $\Longrightarrow$ domain.

Example 6.2.8 Let k be a field, $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n) \in k^n$ and $\widetilde{\mathfrak{m}} = (X_1 - \alpha_1, \dots, X_n - \alpha_n) \in k[X_1, \dots, X_n]$. Define a k-linear map

$$\begin{aligned} \vartheta : k[X_1, \dots, X_n] &\longrightarrow k^n \\ P &\longmapsto \left(\tfrac{\partial P}{\partial X_1}(\boldsymbol{\alpha}), \dots, \tfrac{\partial P}{\partial X_n}(\boldsymbol{\alpha})\right). \end{aligned}$$

Clearly $\vartheta(X_i - \alpha_i) = \mathbf{e}_i$. By Leibnitz rule $\frac{\partial PQ}{\partial X_j} = P\frac{\partial Q}{\partial X_j} + Q\frac{\partial P}{\partial X_j}$, thus $\vartheta(\widetilde{\mathfrak{m}}^2) = 0$. Hence $\vartheta : \widetilde{\mathfrak{m}}/\widetilde{\mathfrak{m}}^2 \simeq k^n$. Therefore $k[X_1, \dots, X_n]$ is regular at $\widetilde{\mathfrak{m}}$ (hence, by weak Nullstellensatz, at all closed points, if k algebraically closed).
Let now $I = (F_1, \dots, F_m)$ and $R = k[X_1, \dots, X_n]/I$. Assume that $F_j(\boldsymbol{\alpha}) = 0$ for $\leq j \leq m$, so $I \subseteq \widetilde{\mathfrak{m}}$ and let $\mathfrak{m} = \widetilde{\mathfrak{m}}/I$ be the corresponding maximal ideal in R. In example 1.3.5 we have computed $\Omega^1_{R/k} \simeq R^n/\operatorname{Im} J^t$, where $J = \left(\frac{\partial F_i}{\partial X_j}\right)$ is the jacobian matrix. Hence, from corollary 1.3.16 we deduce $\dim_k \mathfrak{m}/\mathfrak{m}^2 = n - \operatorname{rk} J(\boldsymbol{\alpha})$. It is easy to obtain the same result directly: clearly $\dim_k \vartheta(I) = \operatorname{rk} J(\boldsymbol{\alpha})$, therefore

$$\dim_k \left((I + \widetilde{\mathfrak{m}}^2)/\widetilde{\mathfrak{m}}^2\right) = \dim_k \vartheta(I) = \operatorname{rk} J(\boldsymbol{\alpha}). \tag{6.4}$$

On the other hand, since $\mathfrak{m}^2 = (\widetilde{\mathfrak{m}}/I)^2 = \widetilde{\mathfrak{m}}^2/(I + \widetilde{\mathfrak{m}}^2)$, we have

$$\mathfrak{m}/\mathfrak{m}^2 = (\widetilde{\mathfrak{m}}/I)/\left(\widetilde{\mathfrak{m}}^2/(I + \widetilde{\mathfrak{m}}^2)\right) \cong \widetilde{\mathfrak{m}}/(I + \widetilde{\mathfrak{m}}^2). \tag{6.5}$$

We have an exact sequence of k-vector spaces

$$0 \longrightarrow (I + \widetilde{\mathfrak{m}}^2)/\widetilde{\mathfrak{m}}^2 \longrightarrow \widetilde{\mathfrak{m}}/\widetilde{\mathfrak{m}}^2 \longrightarrow \widetilde{\mathfrak{m}}/(I + \widetilde{\mathfrak{m}}^2) \longrightarrow 0$$

from which, by (6.4) and (6.5), we conclude that $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = n - \operatorname{rk} J(\boldsymbol{\alpha})$.
Therefore $\dim R_{\mathfrak{m}} \leq \dim_k \mathfrak{m}/\mathfrak{m}^2 = n - \operatorname{rk} J(\boldsymbol{\alpha})$ and by definition R is regular at $\mathfrak{m}$ if and only if this is an equality. Moreover, the set of points $\boldsymbol{\alpha} \in \mathbb{A}^n(k)$ at which $\operatorname{rk} J(\boldsymbol{\alpha}) \leq n - \dim R$ is Zariski closed (vanishing locus of all the minors of size $\leq n - \dim R$). Thus the set of singular (i.e. non-regular) points in $\mathcal{Z}(I)$ is Zariski closed.
A priori, the singular locus could be the whole of $\mathcal{Z}(I)$ (example: $R = k[X]/(X^2)$). In the case $m \leq n$, a simple sufficient condition for a point to be regular is to impose that $\operatorname{rk} J(\boldsymbol{\alpha}) = n - m$. This fits nicely with the theory of differentiable manifolds.

Assume now that I is a prime ideal, i.e. that R is a domain (in geometric language, $\mathcal{Z}(I)$ is a variety). Then, by corollary 6.1.34, $d = \dim R$ equals the transcendence degree of $K = \operatorname{Frac} R$ over k. Assume furthermore that also $\dim_K \Omega^1_{K/k} = d$. Then $\Omega^1_{K/k} = K \otimes_R \Omega^1_{R/k} \simeq K^n/\operatorname{Im} J^t$. There is thus an $(n-d) \times (n-d)$ minor M of the matrix J such that $\det M \neq 0$. Therefore, for every $\mathfrak{m}$ such that $\det M \notin \mathfrak{m}$, we have $\operatorname{rk} J(\boldsymbol{\alpha}) \geq n - d$ and thus $d = \dim R_{\mathfrak{m}} \leq n - \operatorname{rk} J(\boldsymbol{\alpha}) \leq d$, so all these are regular points.

The assumption that $\dim_K \Omega^1_{K/k}$ is equal to the trascendence degree of K/k is satisfied if k is perfect, see [8], §27. If the characteristic of k is 0, we can check this directly, using the Normalisation lemma: K is a finite extension of $k(T_1, \dots, T_d)$. We know that $\Omega^1_{k(T_1,\dots,T_d)/k} = k(T_1, \dots, T_d) \otimes_{k[T_1,\dots,T_d]} \Omega^1_{k[T_1,\dots,T_d]/k}$ is a vector space of dimension d. If K is separable over $k(T_1, \dots, T_d) \subseteq K$, by corollary 1.3.12, $\Omega^1_{K/k} \cong K \otimes_{k(T_1,\dots,T_d)} \Omega^1_{k(T_1,\dots,T_d)/k}$, hence $\dim_K \Omega^1_{K/k} = d$.

§ 3 Exercises

Exercise 6.1 Let R be a ring. Show that $\operatorname{Spec} R$ can be written as a union $\bigcup_i Z_i$ of irreducible subsets such that $Z_j \not\subseteq Z_i$ if $i \neq j$, called the irreducible components of $\operatorname{Spec} R$. [Hint: consider the subsets $\mathcal{Z}(\mathfrak{p})$ defined by the minimal primes of R.]

Exercise 6.2 Let R be an integrally closed noetherian domain and $\mathfrak{q} \subset R$ a prime ideal. Recall that we defined the n-th symbolic power $\mathfrak{q}^{(n)} = \{y \in R \mid \exists\, z \notin \mathfrak{q} \text{ and } yz \in \mathfrak{q}^n\}$. Suppose that $\operatorname{ht} \mathfrak{q} = 1$ and let v be the discrete valuation of $R_{\mathfrak{q}}$. Show that $\mathfrak{q}^{(n)} = \{x \in R \mid v(x) \geq n\}$.

Exercise 6.3 Let k be a field, $R = k[X_{i,j}]_{i\geq 1;\ 1\leq j\leq i}$. Let $\mathfrak{p}_i = (X_{i,1}, \ldots, X_{i,i})$ and $S = R - \bigcup_{i=1}^{\infty} \mathfrak{p}_i$. Put $A = S^{-1}R$. This ring has been studied in exercise 2.2. Show that A is noetherian and $\dim A = +\infty$.

Exercise 6.4 Let X be a topological space and $S \subseteq X$ a subset. Say that S satisfies $(\star)$ if for every irreducible closed subset $T \subseteq X$ such that $S \cap T$ is dense in T then $S \cap T$ contains a non-empty open subset of T. Let R be a noetherian ring.

a) Show that if $S \subseteq \operatorname{Spec} R$ is constructible then S satisfies $(\star)$. [Hint: for T irreducible closed, show that $S \cap T$ is constructible; compute the closure of $S \cap T$ and use exercise 1.19.]

Conversely, let $S \subseteq \operatorname{Spec} R$ be a subset satisfying $(\star)$. We'll show that S is constructible. Since $\varnothing$ is constructible, assume $S \neq \varnothing$ and that for every $S' \subset S$ such that S' satisfying $(\star)$ and whose closure $\overline{S'}$ is properly contained in the closure $\overline{S}$, then S' is constructible.

b) Write $\overline{S} = Z_1 \cup Z_2 \cup \cdots \cup Z_r$ as the union of its irreducible components. Show that $S \cap Z_1$ is dense in Z_1. Conclude that there exists a closed subset $Z_1' \subsetneq Z_1$ such that $Z_1 - Z_1' \subseteq S$.

c) Put $Y = Z_1' \cup Z_2 \cup \cdots \cup Z_r$ and notice that $S = (Z_1 - Z_1') \cup (S \cap Y)$. Show that $Z_1 - Z_1'$ is locally closed in $\operatorname{Spec} R$ and that $S \cap Y$ satisfies $(\star)$.

d) Show that $S \cap Y$ is constructible and conclude that S is constructible too.

Exercise 6.5 Use the characterisation of constructible sets in exercise 6.4 to prove Chevalley's theorem without the assumption $\dim R < +\infty$.

Exercise 6.6 Let A be a noetherian ring, $S \subseteq \operatorname{Spec} A$ a constructible subset. Then there exists an A-algebra of finite type $\psi : A \to B$ such that $S = \operatorname{im} \psi^\sharp$. [Hint: do first the case $S = [\operatorname{Spec} A - \mathcal{Z}(f)] \cap Z$, for $f \in A$ and Z a closed subset.]

Exercise 6.7 Use exercise 6.6 to prove the following form of Chevalley's theorem: let R be a noetherian ring and A an R-algebra of finite type, $\varphi : R \to A$ the natural map. Then $\varphi^\sharp$ maps constructible subsets of $\operatorname{Spec} A$ to constructible subsets of $\operatorname{Spec} R$.

Exercise 6.8 Let p be a prime number. Show that $\mathfrak{p} = (pX - 1) \subset \mathbb{Z}[X]$ is a prime ideal with $\operatorname{ht} \mathfrak{p} = 1$. Can you place it in figure 6.1? How would you draw its closure?

Exercise 6.9 Show that every prime of height 1 in $\mathbb{Z}[X]$ is contained in infinitely many primes of height 2. Let R be Dedekind domain: is it true that every prime of height 1 in $R[X]$ is contained in a prime of height 2?

Appendix I

Categories and functors

Definition A.1 A **category** $\mathfrak{C}$ is the datum of a collection $\mathrm{Ob}(\mathfrak{C})$ of objects and for any two objects X, Y a set $Hom_{\mathfrak{C}}(X, Y)$ whose elements are called morphisms. Furthermore, for any three objects X, Y, Z there is an associative (i.e. $h \circ (g \circ f) = (h \circ g) \circ f$) composition rule

$$\begin{array}{rl} Hom_{\mathfrak{C}}(X,Y) \times Hom_{\mathfrak{C}}(Y,Z) & \longrightarrow Hom_{\mathfrak{C}}(X,Z) \\ (f,g) & \longmapsto g \circ f. \end{array}$$

Finally, attached to every object X there is a distinguished element $id_X \in Hom_{\mathfrak{C}}(X, X)$ such that $id_Y \circ g = g$ and $f \circ id_X = f$, for any $f \in Hom_{\mathfrak{C}}(X, Y)$ and $g \in Hom_{\mathfrak{C}}(Y, X)$.

Example A.2 The category **Sets** (objects are sets, morphisms are maps). The category **Top** (objects are topological spaces, morphisms are continuous maps). The category **Groups** (resp. **Rings**) (objects are groups (resp. rings), morphisms are homomorphisms). For any ring R, the category $\mathbf{Mod}_R$ of R-modules (see definition 1.2.2).

Example A.3 If $\mathfrak{C}$ is a category, the **opposite** category $\mathfrak{C}^{\mathrm{op}}$ is obtained from $\mathfrak{C}$ by "reversing the arrows" i.e $\mathrm{Ob}(\mathfrak{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathfrak{C})$ and $Hom_{\mathfrak{C}^{\mathrm{op}}}(X, Y) = Hom_{\mathfrak{C}}(Y, X)$ for any two objects X, Y.

Definition A.4 If $\mathfrak{C}$ and $\mathfrak{D}$ are categories, a **functor** $F : \mathfrak{C} \to \mathfrak{D}$ is the datum of an object (resp. morphism) $F(X)$ in $\mathfrak{D}$ (resp. $F(f) \in Hom_{\mathfrak{D}}(F(X), F(Y))$ for every object X in $\mathfrak{C}$ (resp. every $f \in Hom_{\mathfrak{C}}(X, Y)$) such that $F(g \circ f) = F(g) \circ F(f)$ and $F(id_X) = id_{F(X)}$.
A functor $F : \mathfrak{C} \to \mathfrak{D}$ is called **faithful** (resp. **full**, resp. **fully faithful**) if the map

$$\begin{array}{rl} Hom_{\mathfrak{C}}(X,Y) & \longrightarrow Hom_{\mathfrak{D}}(F(X),F(Y)) \\ f & \longmapsto F(f) \end{array}$$

is injective (resp. surjective, resp. bijective) for al pair of objects X, Y in $\mathfrak{C}$.

Example A.5 The forgetful functor $\mathbf{Top} \to \mathbf{Sets}$ sends a topological space to its underlying set. Similarly, there are forgetful functors $\mathbf{Rings} \to \mathbf{Groups} \to \mathbf{Sets}$. Forgetful functors are faithful.

Example A.6 Any object T of a category $\mathfrak{C}$ defines a functor $\boldsymbol{h}_T : \mathfrak{C} \to \mathbf{Sets}$ defined by $\boldsymbol{h}_T(X) = Hom_{\mathfrak{C}}(T, X)$ for any object X in $\mathfrak{C}$; if $f : X \to Y$ is a morphism in $\mathfrak{C}$ then

$$\begin{array}{rl} \boldsymbol{h}_T(f) : Hom_{\mathfrak{C}}(T,X) & \longrightarrow Hom_{\mathfrak{C}}(T,Y). \\ g & \longmapsto f \circ g \end{array} \tag{A.1}$$

Viewing T as an object in $\mathfrak{C}^{\mathrm{op}}$, it also defines a contravariant functor $Hom_{\mathfrak{C}}(-,T) : \mathfrak{C}^{\mathrm{op}} \to \mathbf{Sets}$.

Example A.7 If R is a ring, any R-module M defines functors $Hom_R(M,-) : \mathbf{Mod}_R \to \mathbf{Mod}_R$ and $Hom_R(-,M) : \mathbf{Mod}_R^{\mathrm{op}} \to \mathbf{Mod}_R$: see example 1.2.7.

Example A.8 Any ring homomorphism $\varphi : R \to A$ defines a functor $\varphi_* : \mathbf{Mod}_A \to \mathbf{Mod}_R$ where $\varphi_*(M)$ is M seen as an R-module: see example 1.2.8. The tensor product $N \mapsto A \otimes_R N$ defines a functor $\mathbf{Mod}_R \to \mathbf{Mod}_A$.

Example A.9 Let R be a ring and $\mathbf{Free}_R$ be the category whose objects are free R-modules, with linear maps as morphisms. The inclusion functor $\mathbf{Free}_R \to \mathbf{Mod}_R$ is a fully faithful functor. If $I \subset R$ is an ideal, the rule $M \mapsto (R/I) \otimes_R M$ is a full functor $\mathbf{Free}_R \to \mathbf{Free}_{R/I}$.

Example A.10 Proposition 1.1.75 tells us that $\mathrm{Spec} : \mathbf{Rings}^{\mathrm{op}} \to \mathbf{Top}$ is a functor. It is not faithful: the complex conjugation $\sigma : \mathbb{C} \to \mathbb{C}$ is a ring homomorphism, $\sigma \neq id$ yet obviously $\sigma^\sharp = id^\sharp$ since $\mathrm{Spec}\,\mathbb{C}$ is just a point. The functor Spec is not full: if p is a prime number, from proposition 1.1.17 we easily see that $\pi : \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ induces an homeomorphism $\pi^\sharp : \mathrm{Spec}\,\mathbb{Z}/p\mathbb{Z} \to \mathrm{Spec}\,\mathbb{Z}/p^2\mathbb{Z}$. But $(\pi^\sharp)^{-1} : \mathrm{Spec}\,\mathbb{Z}/p^2\mathbb{Z} \to \mathrm{Spec}\,\mathbb{Z}/p\mathbb{Z}$ is not induced by some $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z}$, as there are no such maps which are ring homomorphism.

Definition A.11 Let $E : \mathfrak{C} \to \mathfrak{D}$ and $F : \mathfrak{C} \to \mathfrak{D}$ be two functors. A **natural transformation** or **morphism** $\tau : E \to F$ is the datum of a morphism $\tau_X : E(X) \to F(X)$ in $\mathfrak{D}$ for every object X in $\mathfrak{C}$, such that for every morphism $f : X \to Y$ in $\mathfrak{C}$ there is a commutative diagram in $\mathfrak{D}$

$$\begin{array}{ccc} E(X) & \xrightarrow{\tau_X} & F(X) \\ {\scriptstyle E(f)}\downarrow & & \downarrow{\scriptstyle F(f)} \\ E(Y) & \xrightarrow{\tau_Y} & F(Y). \end{array} \tag{A.2}$$

τ is called a **natural isomorphism** (written $\tau : E \cong F$) if τ_X is an isomorphism for all X in $\mathfrak{C}$.

Definition A.12 A functor $F : \mathfrak{C} \to \mathfrak{D}$ is an **equivalence of categories** if there exists a functor $E : \mathfrak{D} \to \mathfrak{C}$ and natural isomorphisms $E \circ F \cong id_{\mathfrak{C}}$ and $F \circ E \cong id_{\mathfrak{D}}$.

Notice that an equivalence is necessarily a fully faithful functor. An interesting example of an equivalence is given in theorem 2.2.13.

Proposition A.13 *Let $F : \mathfrak{C} \to \mathbf{Sets}$ be a functor and T an object in $\mathfrak{C}$. There is a canonical bijection between $F(T)$ and the set of all natural transformations $\tau : \boldsymbol{h}_T \to F$ sending $u \in F(T)$ to the "evaluation" morphism τ_u whose value at an object X of $\mathfrak{C}$ is*

$$\begin{array}{rcl} \tau_{u,X} : Hom_{\mathfrak{C}}(T,X) & \longrightarrow & F(X). \\ f & \longmapsto & F(f)(u) \end{array} \tag{A.3}$$

The inverse map takes a natural transformation $\tau : \boldsymbol{h}_T \to F$ to the element $u_\tau = \tau_T(id_T) \in F(T)$.

Proof. F being a functor, τ_u is a natural transformation: diagram (A.2) boils down to the condition $F(g) \circ F(f) = F(g \circ f)$. Let's check the composition of the two maps. For $v \in F(T)$,

$$u_{\tau_v} = \tau_{v,T}(id_T) = F(id_T)(v) = id_{F(T)}(v) = v.$$

Conversely, if $\sigma : \boldsymbol{h}_T \to F$ is a natural transformation, for any morphism $f : T \to X$ in $\mathfrak{C}$, then

$$\begin{array}{lll} \tau_{u_\sigma,X}(f) & = F(f)\left(\sigma_T(id_T)\right) & \\ & = \sigma_X\left(\boldsymbol{h}_T(f)(id_T)\right) & \text{by (A.2)} \\ & = \sigma_X(f \circ id_T) & \text{by (A.1)} \\ & = \sigma_X(f). & \end{array}$$

Hence $\tau_{u_\sigma} = \sigma$. Therefore the maps $u \mapsto \tau_u$ and $\tau \mapsto u_\tau$ are inverse to each other. □

Applying the proposition to the functor $F = \boldsymbol{h}_{T'}$, we get

Corollary A.14 *For any two objects T, T' in $\mathfrak{C}$, the map $u \mapsto \tau_u$ is a canonical bijection between $Hom_{\mathfrak{C}}(T', T)$ and the set of all natural transformations $\tau : \boldsymbol{h}_T \to \boldsymbol{h}_{T'}$. Moreover $u : T' \to T$ is an isomorphism in $\mathfrak{C}$ if and only if $\tau_u : \boldsymbol{h}_T \to \boldsymbol{h}_{T'}$ is a natural isomorphism.*

Proof. Only the second claim needs to be justified. If $u : T' \to T$ is an isomorphism then for every object X of $\mathfrak{C}$ and $f : T \to X$, we have $\tau_{u,X}(f) = \boldsymbol{h}_T(f)(u) = f \circ u$, so

$$\begin{array}{rcl} \tau_{u,X} : Hom_{\mathfrak{C}}(T, X) & \longrightarrow & Hom_{\mathfrak{C}}(T', X). \\ f & \longmapsto & f \circ u \end{array} \tag{A.4}$$

is a bijection (with inverse $g \mapsto g \circ u^{-1}$). Conversely, suppose $\tau : \boldsymbol{h}_T \to \boldsymbol{h}_{T'}$ is a natural isomorphism and let $u_\tau = \tau_T(id_T) \in Hom_{\mathfrak{C}}(T', T)$. From proposition A.13, we know that $\tau = \tau_{u_\tau}$, hence for every X the map (A.4), with $u = u_\tau$, is bijective: taking $X = T'$, there exists $v : T \to T'$ such that $v \circ u_\tau = id_{T'}$. Consider the associated transformation $\tau_v : \boldsymbol{h}_{T'} \to \boldsymbol{h}_T$ and

$$\begin{array}{ccccc} Hom_{\mathfrak{C}}(T', Y) & \xrightarrow{\tau_{v,Y}} & Hom_{\mathfrak{C}}(T, Y) & \xrightarrow{\tau_Y} & Hom_{\mathfrak{C}}(T', Y). \\ g & \longmapsto & g \circ v & f & \longmapsto & f \circ u_\tau \end{array}$$

For all Y of $\mathfrak{C}$, the composition of these two maps is the identity (since $v \circ u_\tau = id_{T'}$) and τ_Y is bijective by assumption. Therefore $\tau_{v,Y}$ is a bijection too: taking $Y = T$, we get $w : T \to T'$ such that $w \circ v = id_T$. Since $w = w \circ (v \circ u_\tau) = (w \circ v) \circ u_\tau = u_\tau$, we conclude that u_τ is invertible. □

Definition A.15 A functor $F : \mathfrak{C} \to \mathbf{Sets}$ is **representable** if there exists an object T of $\mathfrak{C}$ and a natural isomorphism $\tau : \boldsymbol{h}_T \to F$.

It follows from corollary A.14 that an object T representing a given functor $F : \mathfrak{C} \to \mathbf{Sets}$ is unique up to unique isomorphism: if $\tau : \boldsymbol{h}_T \to F$ and $\tau' : \boldsymbol{h}_{T'} \to F$ are natural isomorphism, the natural isomorphism $(\tau')^{-1} \circ \tau : \boldsymbol{h}_T \to \boldsymbol{h}_{T'}$ determines a unique isomorphism $T' \xrightarrow{\sim} T$ in $\mathfrak{C}$.

Remark A.16 According to proposition A.13, a natural isomorphism $\tau : \boldsymbol{h}_T \to F$ is equivalent to the datum of a **universal element** $u_\tau \in F(T)$. Notice that, since $\tau = \tau_{u_\tau}$ is a natural

isomorphism, for every object X of $\mathfrak{C}$, the map (A.3) is bijective. This translates into the following **universal property**: for every object X in $\mathfrak{C}$ and every $x \in F(X)$, there exists a unique morphism $\xi : T \to X$ in $\mathfrak{C}$ such that

$$F(\xi)(u_\tau) = x. \tag{A.5}$$

The universal property implies that u_τ is unique up to unique isomorphism. Viceversa, again by proposition A.13, the pair (T, u_τ) determines the natural isomorphism $\tau : \boldsymbol{h}_T \to F$. We then say that (T, u_τ) **represents** F.

Example A.17 If R is a ring and M, N are R-modules, $\mathrm{Bil}_R(M \times N, -) : \mathbf{Mod}_R \to \mathbf{Mod}_R$ is represented by the tensor product $M \otimes_R N$: see theorem 1.2.61. The universal element is the bilinear map $b : M \times N \to M \otimes_R N$ given by $b(x, y) = x \otimes y$.

Example A.18 If R is a ring and A an R-algebra, the functor $\mathrm{Der}_R(A, -) : \mathbf{Mod}_A \to \mathbf{Mod}_A$ is represented by the module of differentials $(\Omega^1_{A/R}, d_{A/R})$: see proposition 1.3.2.

The language of representable functors is widely used in Algebraic Geometry. It allows to transport to arbitrary categories (e.g. varieties, or schemes) familiar notions from set (group, ring,...) theory.

Example A.19 An inverse system in a category $\mathfrak{C}$ is a collection $\{(X_i, \varphi_{i,j})\}_{i \in I}$ of objects of $\mathfrak{C}$ indexed by a directed set and morphisms $\varphi_{i,j} : X_j \to X_i$ for every $i \leq j$ in I such that $\varphi_{i,j} \circ \varphi_{j,k} = \varphi_{i,k}$ for every $i \leq j \leq k$. For any object Y of $\mathfrak{C}$, this gives rise to an inverse system of sets $\{(Hom_{\mathfrak{C}}(Y, X_i), \phi_{i,j})\}_{i \in I}$, where $\phi_{i,j}(f) = \varphi_{i,j} \circ f$. Inverse limits in $\mathbf{Sets}$ are defined as in definition 3.6.24. Then we say that the **inverse limit exists in** $\mathfrak{C}$ if the functor

$$\begin{array}{rcl} \mathfrak{C}^{\mathrm{op}} & \longrightarrow & \mathbf{Sets} \\ Y & \longmapsto & \varprojlim Hom_{\mathfrak{C}}(Y, X_i) \end{array}$$

is representable, and we call the representing object $\varprojlim X_i$.

Appendix II

Solutions to selected exercises

§ 1 Chapter I

Exercise 1.7. Let $\mathfrak{a} = \bigcup_{i=1}^{\infty} \mathfrak{a}_i$. It is an ideal, by the argument used in the proof of corollary 1.1.51. Let $x \in \mathfrak{a}$ be a generator. By construction, $x \in \mathfrak{a}_n$ for some $n \in \mathbb{N}$. For any $m \geq n$, let x_m be a generator of $\mathfrak{a}_m$. On the one hand $x|x_m$, because $x \in \mathfrak{a}_n \subseteq \mathfrak{a}_m$; on the other $x_m|x$, because $\mathfrak{a}_m \subseteq \mathfrak{a}$. Therefore x and x_m are associates, and $\mathfrak{a} = \mathfrak{a}_m$ for all $m \geq n$.

Exercise 1.8. a) We transform $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \rightsquigarrow \begin{pmatrix} a & 0 \\ ar & d \end{pmatrix} \rightsquigarrow \begin{pmatrix} a & 0 \\ ar+ds & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 1 & d \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & d \\ a & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & d \\ 0 & -ad \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & d \\ 0 & ad \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & ad \end{pmatrix}$.

b) We compute $\det \begin{pmatrix} x & y \\ \frac{c}{e_1} & -\frac{a}{e_1} \end{pmatrix} = \frac{1}{e_1}(-ax - cy) = -1$.

c) Multiplying we get $S_1 A = \begin{pmatrix} x & y \\ \frac{c}{e_1} & -\frac{a}{e_1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ax+cy & bx+dy \\ 0 & \frac{bc-ad}{e_1} \end{pmatrix} = \begin{pmatrix} e_1 & bx+dy \\ 0 & \frac{bc-ad}{e_1} \end{pmatrix}$.

d) Applying step c) to $(S_1 A)^t$ we find $T_2^t \in GL_2(R)$ such that $T_2^t (S_1 A)^t = \begin{pmatrix} e_2 & * \\ 0 & * \end{pmatrix}$, with $e_2 = \gcd(e_1, bx+dy)$. Its transpose $S_1 A T_2$ has thus the desired shape.

e)+f) Starting from A, from c) we get $S_1 \in \mathrm{GL}_2(R)$ such that $S_1 A = \begin{pmatrix} e_1 & b_1 \\ 0 & d_1 \end{pmatrix}$. If $b_1 = e_1 m_1$, then $\begin{pmatrix} e_1 & e_1 m_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} 1 & -m_1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} e_1 & 0 \\ 0 & d_1 \end{pmatrix}$ and we are done. Otherwise, take $e_2 = \gcd(e_1, b_1)$ (notice that $(e_1) \subsetneq (e_2)$) and as in d) find $T_2 \in \mathrm{GL}_2(R)$ such that $S_1 A T_2 = \begin{pmatrix} e_2 & 0 \\ c_2 & d_2 \end{pmatrix}$. If $c_2 = e_2 m_2$ then $\begin{pmatrix} 1 & 0 \\ -m_2 & 1 \end{pmatrix} \begin{pmatrix} e_2 & 0 \\ e_2 m_2 & d_2 \end{pmatrix} = \begin{pmatrix} e_2 & 0 \\ 0 & d_2 \end{pmatrix}$ and we are done. Otherwise, take $e_3 = \gcd(e_2, c_2)$ (hence $(e_1) \subsetneq (e_2) \subsetneq (e_3)$) and repeat step c). Iterating, either the process terminates and we get that SAT is of the desired form for suitable $S, T \in \mathrm{GL}_2(R)$ or we produce an infinite increasing sequence $(e_1) \subsetneq \cdots \subsetneq (e_n) \subsetneq (e_{n+1}) \subsetneq \ldots$. But the latter option is impossible by exercise 1.7.

g) First apply f) to transform A into the diagonal matrix with entries e, g. Set $h = \gcd(e, g)$ and write $h = er + gs$. We conclude by a variation on the process in a):

$$\begin{pmatrix} e & 0 \\ 0 & g \end{pmatrix} \rightsquigarrow \begin{pmatrix} e & 0 \\ er & g \end{pmatrix} \rightsquigarrow \begin{pmatrix} e & 0 \\ er+gs & g \end{pmatrix} = \begin{pmatrix} e & 0 \\ h & g \end{pmatrix} \rightsquigarrow \begin{pmatrix} h & g \\ e & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} h & g \\ 0 & -\frac{e}{h}g \end{pmatrix} \rightsquigarrow \begin{pmatrix} h & 0 \\ 0 & -\frac{e}{h}g \end{pmatrix}.$$

h) From $6 = \gcd(84, 66)$ and $6 = 84 \cdot 4 - 66 \cdot 5$ we get $\begin{pmatrix} 4 & -5 \\ 11 & -14 \end{pmatrix} \begin{pmatrix} 84 & 18 & 141 \\ 66 & 12 & 108 \end{pmatrix} = \begin{pmatrix} 6 & 12 & 24 \\ 0 & 30 & 39 \end{pmatrix}$. Moreover $\begin{pmatrix} 6 & 12 & 24 \\ 0 & 30 & 39 \end{pmatrix} \begin{pmatrix} 1 & -2 & -4 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 0 & 0 \\ 0 & 30 & 39 \end{pmatrix}$. Now $3 = -6 \cdot 6 + 39$ so, as in g),

$$\begin{pmatrix} 6 & 0 & 0 \\ 0 & 30 & 39 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 6 & 0 & 0 \\ -36 & 30 & 39 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 6 & 0 & 0 \\ 3 & 30 & 39 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 30 & 39 \\ 6 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 30 & 39 \\ 0 & -60 & -78 \end{pmatrix}.$$

Now we do step d) again: $\begin{pmatrix} 3 & 30 & 39 \\ 0 & -60 & -78 \end{pmatrix} \begin{pmatrix} 1 & -10 & -13 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & -60 & -78 \end{pmatrix}$. We clean up the last row by repeating the step in d): $\gcd(60, 78) = 6$ and $6 = 4 \cdot 60 - 3 \cdot 78$, so

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & -60 & -78 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -4 & 13 \\ 0 & 3 & -10 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix}.$$

i) Permuting rows and columns of A, we may assume that $a_{1,1} \neq 0$. We generalise steps c) and d): let $e_1 = \gcd(a_{1,1}, a_{2,1}, \ldots, a_{m,1})$ and write $e_1 = a_{1,1}x + a_{2,1}y$. Then it is easy to check that

$$S_1 = \begin{pmatrix} x & y & 0 & \ldots & 0 \\ -\frac{a_{2,1}}{e_1} & \frac{a_{2,1}}{e_1} & 0 & \ldots & 0 \\ -\frac{a_{3,1}}{e_1} & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ -\frac{a_{m,1}}{e_1} & 0 & 0 & \ldots & 1 \end{pmatrix} \in \mathrm{GL}_m(R)$$

and that $S_1 A$ has the desired shape.
j) As in e), applying step i) to $(S_1 A)^t$ we find $T_2 \in \mathrm{GL}_n(R)$ such that $S_1 A T_2$ has the desired shape.
k)+l) The proof in f)+g) carries over verbatim to establish k). We conclude by induction.

Exercise 1.10. If $\pi_1 : R[X_1, \ldots, X_n] \to A_1$ and $\pi_2 : R[Y_1, \ldots, Y_m] \to A_2$ are two presentations, define $\pi : R[X_1, \ldots, X_n, Y_1, \ldots, Y_m] \to A_1 \times A_2$ by $\pi(X_i) = (\pi_1(X_i), 0)$ and $\pi(Y_j) = (0, \pi_2(Y_j))$.

Exercise 1.12. The ideals $\mathfrak{m}_i$ are maximal because $A/\mathfrak{m}_i \cong k[X]/\overline{g}_i$ is a field. Let $\mathfrak{n} \subsetneq A$ be a maximal ideal. Necessarily $\mathfrak{m}A \subseteq \mathfrak{n}$, since otherwise $\mathfrak{n} + \mathfrak{m}A = A$ and, A being a finitely generated R-module, Nakayama's lemma would imply $\mathfrak{n} = A$. Then $\mathfrak{n}/\mathfrak{m}A$ is a prime ideal in $A/\mathfrak{m}A = k[X]/\overline{f}$, and these are precisely the ideals generated by the $\overline{g}_i$'s. Thus $\mathfrak{n}$ contains one of the $\mathfrak{m}_i$'s, and they are equal by maximality.

Exercise 1.15. Tensoring the exact sequence

$$0 \longrightarrow I \cap J \longrightarrow R \longrightarrow R/I \oplus R/J \longrightarrow 0$$

by the flat R-algebra A gives rise to the exact sequence

$$0 \longrightarrow \varphi(I \cap J)A \longrightarrow A \longrightarrow A/\varphi(I) \oplus A/\varphi(J) \longrightarrow 0$$

from which the concluson is immediate.

Exercise 1.16. It is elementary to check that $g \mapsto [m \mapsto g(m \otimes 1)]$ is a B-linear map. If $g(m \otimes 1) = 0$ for all $m \in M$ then $g(m \otimes b) = bg(m \otimes 1) = 0$ for all $b \in B$ and $m \in M$, hence $g = 0$, so the map is injective. To an A-linear $f : M \to N$ we may associate the map

$$\begin{aligned} h : M \times B &\longrightarrow N \\ (m, b) &\longmapsto bf(m) \end{aligned}$$

which is immediately seen to be A-bilinear, whence a B-linear $g : M \otimes_A B \to N$ by the universal property. By construction, $g(m \otimes 1) = f(m)$, so the map $Hom_B(M \otimes_A B, N) \to Hom_A(M, N)$ is surjective.

Exercise 1.18. Since the projections $\pi_i : R_1 \times R_2 \to R_i$ are ring homomorphisms, we have the natural continuous map $h : \operatorname{Spec} R_1 \coprod \operatorname{Spec} R_2 \to \operatorname{Spec}(R_1 \times R_2)$ whose restriction to $\operatorname{Spec} R_i$ is $\pi_i^\sharp$. Explicitely, if $\mathfrak{p}_i \subset R_i$ is a prime ideal, then $h(\mathfrak{p}_1) = \mathfrak{p}_1 \times R_2$ and $h(\mathfrak{p}_2) = R_1 \times \mathfrak{p}_2$. The map h is clearly injective. To prove surjectivity, consider the elements $e_1 = (1, 0)$ and $e_2 = (0, 1)$: they are orthogonal idempotents:

$$e_i^2 = e_i; \qquad e_1 e_2 = 0; \qquad e_1 + e_2 = 1.$$

Let $\mathfrak{q} \subset R$ be a prime ideal. If $e_1 \notin \mathfrak{q}$ then $e_2 \in \mathfrak{q}$ because $e_1 e_2 = 0 \in \mathfrak{q}$. On the other hand, if $e_1 \in \mathfrak{q}$ then $e_2 \notin \mathfrak{q}$ because otherwise $1 = e_1 + e_2 \in \mathfrak{q}$ and we assume $\mathfrak{q} \neq R_1 \times R_2$. Thus precisely one of these two elements belongs to $\mathfrak{q}$. Say $e_2 \in \mathfrak{q}$ and let

$$\mathfrak{p} = \pi_1(\mathfrak{q}) = \{x \in R_1 \,|\, \exists y \in R_2,\ (x, y) \in \mathfrak{q}\}\,.$$

This is clearly an ideal in R_1. Even better, it is a prime ideal: if $x, x' \in R_1$ are such that there exists $z \in R_2$ with $(xx', z) \in \mathfrak{q}$ then, because $(xx', z) = (x, 1)(x', z) \in \mathfrak{q}$, either $(x, 1) \in \mathfrak{q}$ or $(x', z) \in \mathfrak{q}$, so either x or x' is in $\mathfrak{p}$.
I claim $\mathfrak{q} = h(\mathfrak{p}) = \pi_1^\sharp(\mathfrak{p}) = \pi_1^{-1}(\pi_1(\mathfrak{q}))$. Trivially $\mathfrak{q} \subseteq \pi_1^{-1}(\pi_1(\mathfrak{q}))$. If $x \in \mathfrak{p}$, take $y \in R_2$ such that $(x, y) \in \mathfrak{q}$. For any $t \in R_2$, we have $(0, t) = (1, t)e_2 \in \mathfrak{q}$ because $e_2 \in \mathfrak{q}$. So for every $u \in R_2$ we have $(x, u) = (x, y) + (0, u - y) \in \mathfrak{q}$ for all $x \in \mathfrak{p}$ and all $u \in R_2$. This means precisely that $\pi_1^{-1}(\pi_1(\mathfrak{q})) \subseteq \mathfrak{q}$.

Exercise 1.19. The closure $Z_1 = \overline{U \cap Z}$ is a closed subset of Z. Let $T = X - U$, a closed subset of X, and put $Z_2 = T \cap Z$, also closed. Then $Z = Z_1 \cup Z_2$ and by irreducibility either $Z = Z_1$ or $Z = Z_2$. But Z contains at least one point $x \in U \cap Z \subseteq Z_1$ such that $x \notin Z_2$. Therefore $Z = Z_1$ as contended.

Any closed subset of $\operatorname{Spec} R$ can be expressed as $Z = \mathcal{Z}(I)$ with $I = \bigcap_{\mathfrak{p} \in Z} \mathfrak{p}$. Suppose $f, g \in R \backslash I$ but $fg \in I$. Then $Z \subsetneq \mathcal{Z}(f)$ and $Z \subsetneq \mathcal{Z}(g)$ but $Z \subseteq \mathcal{Z}(f) \cup \mathcal{Z}(g) = \mathcal{Z}(fg)$. Whence an expression of $Z = (Z \cap \mathcal{Z}(f)) \cup (Z \cap \mathcal{Z}(g))$ as the union of two proper closed subsets, a contradiction.

Conversely, let $\mathfrak{p}$ be a prime. If $\mathcal{Z}(\mathfrak{p}) = \mathcal{Z}(I) \cup \mathcal{Z}(J) = \mathcal{Z}(IJ)$, then $IJ \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is prime, this implies either $I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$.

Exercise 1.20. The closure of the image of $\varphi^\sharp$ is

$$\overline{\operatorname{Im}\varphi^\sharp} = \mathcal{Z}(I) \quad \text{with} \quad I = \bigcap_{\mathfrak{q}\in\operatorname{Spec} A} \varphi^{-1}(\mathfrak{q}) = \varphi^{-1}\Big(\bigcap_{\mathfrak{q}\in\operatorname{Spec} A} \mathfrak{q}\Big) = \varphi^{-1}\left(\mathfrak{N}_A\right).$$

Hence $\overline{\operatorname{Im}\varphi^\sharp} = \operatorname{Spec} R = \mathcal{Z}(\mathfrak{N}_R)$ implies $\ker\varphi = \varphi^{-1}(0) \subseteq \varphi^{-1}\left(\mathfrak{N}_A\right) \subseteq \mathfrak{N}_R$.
Conversely, suppose $\ker\varphi \subseteq \mathfrak{N}_R$. For $x \in R$, to say $\varphi(x) \in \mathfrak{N}_A$ means $\varphi(x)^n = \varphi(x^n) = 0$ for some $n \geq 1$. Hence $x^n \in \ker\varphi \subseteq \mathfrak{N}_R$, thus $x \in \mathfrak{N}_R$. Therefore $\varphi^{-1}\left(\mathfrak{N}_A\right) \subseteq \mathfrak{N}_R$, hence $\operatorname{Spec} R = \mathcal{Z}(\mathfrak{N}_A) \subseteq \overline{\operatorname{Im}\varphi^\sharp} \subseteq \operatorname{Spec} R$.

Exercise 1.22. We leave to the reader to check that the map $f \mapsto f \circ \pi$ is A-linear. It is injective because π is surjective: if $f(\pi(x)) = 0$ for all $x \in J$, necessarily for all $\bar{x} = \pi(x) \in J/J^2$ we have $f(\bar{x}) = 0$, so $f = 0$. If $g : J \to N$ is A-linear, for $x, y \in J$ we have $g(xy) = xg(y) = 0$ because N is an A/J-module. It follows immediately that $J^2 \subseteq \ker g$, hence g factors through J/J^2 and thus $Hom_B(J/J^2, N) \to Hom_A(J, N)$ is surjective.

§ 2 Chapter II

Exercise 2.1. To say $\frac{1}{s}S^{-1}f(\frac{m}{t}) = \frac{f(m)}{st} = 0$ for every $\frac{m}{t} \in S^{-1}M$ means that there exists a $u \in S$ such that $uf(m) = 0$ for every $m \in M$, i.e. that $(f, s) \sim (0, s)$. Hence ϑ is injective.
Let $m_1, \ldots, m_r$ be generators for M. Il $\lambda : S^{-1}M \to S^{-1}N$ is an $S^{-1}R$-linear map, consider $\lambda(\frac{m_i}{1}) = \frac{n_i}{s_i}$ and take $s = s_1 \cdots s_r$. For every $m \in M$, writing $m = x_1m_1 + \cdots + x_rm_r$ with $x_i \in R$ we see that

$$s\lambda(\frac{m}{1}) = \sum_{i=1}^{r} x_i \frac{s}{s_i}\frac{n_i}{1} \in \operatorname{im}\left[N \hookrightarrow S^{-1}N\right].$$

Hence, composing the natural map $M \to S^{-1}M$ with $s\lambda$ defines an R-linear map $f : M \to N$ such that $\lambda = \frac{1}{s}S^{-1}f$. Therefore ϑ is surjective.

Exercise 2.2. If $f, g \in S$, i.e. $f, g \notin \mathfrak{p}_i$ for all i, then $fg \notin \mathfrak{p}_i$ for all i because the $\mathfrak{p}_i$ are prime. Therefore S is multiplicative.
a) Straightforward from the definitions. Notice that $A_{S^{-1}\mathfrak{p}_i} = R_{\mathfrak{p}_i}$. b) Any $f \in R$ is a polynomial, hence involves only finitely many variables.

c) By proposition 2.2.2, it suffices to check that $\operatorname{Spec}\varphi : \coprod_{i=1}^{\infty} \operatorname{Spec} R_{\mathfrak{p}_i} \to \operatorname{Spec} A$ is surjective. Since R is a domain, $A \to A_{S^{-1}\mathfrak{p}_i} = R_{\mathfrak{p}_i}$ is injective and the inverse image of the zero ideal is the zero ideal. By proposition 2.1.10, the prime ideals of A are in bijection with the primes $\mathfrak{q} \subset R$ such that $\mathfrak{q} \cap (R - \bigcup_{i=1}^{\infty} \mathfrak{p}_i) = \varnothing$ i.e. $\mathfrak{q} \subseteq \bigcup_{i=1}^{\infty} \mathfrak{p}_i$. If $0 \neq \mathfrak{q} \subseteq \bigcup_{i=1}^{\infty} \mathfrak{p}_i$, it follows from c) that $\mathfrak{q}$ is contained in only finitely many of the $\mathfrak{p}_i$. By lemma 6.1.22, we conclude that $\mathfrak{q} \subseteq \mathfrak{p}_i$ for some i. By proposition 2.1.10 again, $\mathfrak{q}$ is in the image of $\operatorname{Spec} R_{\mathfrak{p}_i} \to \operatorname{Spec} A$.

d) Taking $0 \neq y \in I$, we have that $\frac{y}{1} \in IA_{S^{-1}\mathfrak{p}_i}$ is a unit in $A_{S^{-1}\mathfrak{p}_i}$ for almost all i.

e) Consider the exact sequence $0 \to J \to I \to I/J \to 0$ and tensor it by $\prod_{i=1}^{\infty} R_{\mathfrak{p}_i}$: since φ is fully faithful, it suffices to show that the inclusion $JA_{S^{-1}\mathfrak{p}_i} \subseteq IA_{S^{-1}\mathfrak{p}_i}$ is an equality for all i.

For $i \geq n$, we have $JA_{S^{-1}\mathfrak{p}_i} = IA_{S^{-1}\mathfrak{p}_i} = A_{S^{-1}\mathfrak{p}_i}$, because $\frac{y}{1}$ is a unit. For $i \leq n$, the subideal $JA_{S^{-1}\mathfrak{p}_i}$ contains the generators $\frac{x_{i,1}}{s_{i,1}}, \ldots, \frac{x_{i,r_i}}{s_{i,r_i}}$ of $IA_{S^{-1}\mathfrak{p}_i}$, and thus they coincide.

§ 3 Chapter III

Exercise 3.1. a) The roots of f (in a splitting field) are integral over R, hence so are the roots of g and h. The coefficients of g and h are algebraic expressions in the roots, so they are integral over R. They are also in K hence, since R is integrally closed, in R.
b) Let $f = g \cdot h$ a factorisation in $K[X]$, and therefore in $R[X]$ by a), with g and h monic. Let $\overline{f}$, $\overline{g}$ and $\overline{h}$ be the reduction of these polynomials in $R/\mathfrak{p}[X]$. Since f is Eisenstein, $\overline{f} = X^n$. Hence $\overline{g} = X^m$ and $\overline{h} = X^{n-m}$, for some $0 \leq m < n$. Therefore

$$g = X^m + b_{m-1}X^{n-1} + \cdots + b_1X + b_0; \quad h = X^{n-m} + c_{n-m-1}X^{n-1} + \cdots + c_1X + c_0; \quad b_i, c_j \in \mathfrak{p}.$$

If $m > 0$, one gets $a_0 = b_0c_0 \in \mathfrak{p}^2$, a contradiction.

Exercise 3.2. $R = k[X]$ is a PID, hence an integrally closed domain. The polynomial $Y^2 + X^2 - 1 \in R[Y]$ is Eisenstein with respect to $\mathfrak{p} = (X - 1)$. By exercise 3.1 it is irreducible, hence $A = k[X, Y]/(X^2 + Y^2 - 1) = R[Y]/(Y^2 + X^2 - 1)$ is a domain. Let $K = k(X) = \operatorname{Frac} R$ and $L = K[Y]/(Y^2 + X^2 - 1) = \operatorname{Frac} A$. We'll show that A is the integral closure of R in L. Write y for the image of Y in A and let $z = f + yg \in L = K \oplus yK$ be integral over R. Clearly z is a solution to the integral equation

$$Z^2 - 2fZ + \left(f^2 + (X^2 - 1)g^2\right) = 0.$$

Thus $-2f \in R$, hence $f \in R$ and $(X^2 - 1)g^2 \in R$, therefore $X \pm 1$ divides g^2. Since $X \pm 1$ is irreducible, it must divide g. Therefore $g \in R$ and $z \in A$.
If the characteristic of k is 2, then $(X^2 + Y^2 - 1) = (X + Y - 1)^2$. Writing $T = X + Y - 1$, we get $A = R[T]/T^2$, which is not even a domain.

Exercise 3.3. $R[X]$ is a free R-module, so φ is flat and therefore has the Going Down property (corollary 3.2.12).
Clearly $\mathfrak{q}_1 \cap k[X] = 0 = \mathfrak{p}_1$, since $XY - 1$ is of degree 1 in Y and no nonzero multiple can have degree 0. Any ideal containing $\mathfrak{q}_1$ and lying over $\mathfrak{p}_2$ must contain the polynomials $XY - 1$ and X, is thus the whole ring because it contains $(-1)(XY - 1) + Y(X) = 1$. So the Going Down property does not hold.

Exercise 3.4. If $x \in K^\times$ either $x \in A \cap K = R$ or $x^{-1} \in A \cap K = R$. Hence R is a valuation ring. If $x \in K^\times$ is also in $A^\times$ then $x^{-1} \in A \cap K = R$ so $x \in R^\times$. Hence $K^\times/R^\times$ injects into $L^\times/A^\times \simeq \mathbb{Z}$ and is thus cyclic of infinite order, so isomorphic to $\mathbb{Z}$.

Exercise 3.5. Clearly $L \simeq K[T]/(T^2 - f)$ so $[L : K] \leq 2$. Clearly, if f is not algebraic over K, then $f^2 \notin K$ so $[L : K] > 1$.
It follows from exercise 3.4 that R and A as valuation subrings of the discrete valuation ring $k[[X]]$ are discrete valuation rings.

For any $\lambda = \phi + \psi f \in L$, with $\phi, \psi \in K$, we have $\lambda^2 = \phi^2 + \psi^2 f^2$ (since the characteristic is 2), thus $\lambda^2 \in K$. If moreover $\lambda \in A$, then $\lambda^2 \in A \cap K = R$, so A is integral over R. It is integrally closed, so it must be the integral closure of R in L.
Suppose that A is generated by $y_1, \dots, y_r$ as an R-module and let $y_i = g_i + h_i f$, with $g_i, h_i \in K$. So g_i, h_i are Laurent power series in X and thus $X^{n_i} g_i, X^{m_j} h_j \in k[[X]]$ for suitable $n_i, m_j \in \mathbb{N}$. Therefore, taking $m = \max\{n_i, m_j,\ 1 \le i, j \le r\}$ (this is where we use that A is a finitely generated R-module), we get $X^m y_i \in k[[X]] \cap K = R$ for $i = 1, \dots, r$, hence for any element $a = \rho_1 y_1 + \dots + \rho_r y_r \in A$ we have $X^m a = \sum_{i=1}^r \rho_i X^m y_i \in R + Rf$.
Let $p = \sum_{n=0}^m \alpha_n X^n \in k[X]$. Then $g = X^{-m-1}(f - p) \in K(X)(f) = L$. Since $g \in k[[X]]$ by definition, $g \in k[[X]] \cap L = A$.
If $[L : K] = 2$, every element in L can be written uniquely as $\phi + \psi f$, with $\phi, \psi \in K$. By construction, $X^m g = -X^{-1} p + X^{-1} f$. This should be in $R + Rf$ but $X^{-1} \notin k[[X]]$, so $X^{-1} \notin R$. We have found a contradiction, so A can't be finitely generated as an R-module.

Exercise 3.6. We just have to check condition c') in definition 3.5.1. Let $x, y \in K$ and. say, $|x| \le |y|$. Then $y = 0$ implies $x = 0$ and $|0 + 0| = |0|$. If $y \neq 0$ then $|\frac{x}{y}| \le 1$, hence

$$|x + y| = |y| \left| \frac{x}{y} + 1 \right| \le |y| = \max\{|x|, |y|\}.$$

Exercise 3.8. a) By definition, there exists an $N_1 \in \mathbb{N}$ such that $|a_n - a_m| < 1$ for all $n, m \ge N_1$. Then $|a_n| = |a_n - a_{N_1} + a_{N_1}| \le 1 + |a_{N_1}|$ for all $n \ge N_1$. Take then $A = \max\{|a_0|, \dots, |a_{N_1 - 1}|, |a_{N_1}| + 1\}$.
b) Let $\{a_n\}, \{b_n\} \in CS(K)$. For every $\varepsilon > 0$ let $N_\varepsilon \in \mathbb{N}$ such that $|a_n - a_m| < \varepsilon$ and $|b_n - b_m| < \varepsilon$ for all $n, m \ge N_\varepsilon$. Then

$$|a_n + b_n - a_m - b_m| \le |a_n - a_m| + |b_n - b_m| < \varepsilon \qquad \forall\, n, m \ge N_{\frac{\varepsilon}{2}};$$

$$|a_n b_n - a_m b_m| = |a_n b_n - a_m b_n + a_m b_n - a_m b_m \le |a_n - a_m| B + |b_n - b_m| A < \varepsilon \quad \forall\, n, m \ge N_{\frac{\varepsilon}{2M}}$$

where $|a_n| \le A$, $|b_n| \le B$ for all $n \in \mathbb{N}$ and $M = \max\{A, B\}$.
c) It follows easily from b) that $CS(K)$ is a ring, with unit the constant sequence $\{1, 1, \dots\}$. On $CS(K)$ we define a relation $\{a_n\} \sim \{b_n\}$ if $\lim_{n \to \infty} |a_n - b_n| = 0$. This is clearly reflexive and symmetric. Let $\{a_n\} \sim \{b_n\} \sim \{c_n\}$. For every $\varepsilon > 0$ let $N_\varepsilon \in \mathbb{N}$ such that $|a_n - b_n| < \varepsilon$ and $|b_n - c_n| < \varepsilon$ for all $n \ge N_\varepsilon$. Then

$$|a_n - c_n| = |a_n - b_n + b_n - c_n| \le |a_n - b_n| + |b_n - c_n| < \varepsilon \qquad \forall\, n, m \ge N_{\frac{\varepsilon}{2}}$$

so $\sim$ is also transitive. Therefore the subset $NS(K)$ of null sequences $\{a_n\} \in CS(K)$ such that $\lim_{n \to \infty} |a_n| = 0$ is an ideal.
d) Let $\{a_n\} \in CS(K) - NS(K)$: there exists $\varepsilon > 0$ such that for all $N \in \mathbb{N}$ there exists an $n \ge N$ with $|a_n| > \varepsilon$. For this choice of ε, fix $N_{\frac{\varepsilon}{2}}$ such that $|a_n - a_m| < \frac{\varepsilon}{2}$ for all $n, m \ge N_{\frac{\varepsilon}{2}}$ and select $m \ge N_{\frac{\varepsilon}{2}}$ such that $|a_m| > \varepsilon$. Then for all $n \ge N_{\frac{\varepsilon}{2}}$ we have

$$\varepsilon < |a_m| = |a_m - a_n + a_n| \le |a_n - a_m| + |a_n| < \frac{\varepsilon}{2} + |a_n|$$

hence $|a_n| > \frac{\varepsilon}{2} > 0$.

e) With notation as in d), define two sequences $\{u_n\}$ and $\{v_n\}$ by setting

$$u_n = \begin{cases} a_n & \text{if } |a_n| > \frac{\varepsilon}{2} \\ \frac{\varepsilon}{2} & \text{if } |a_n| \leq \frac{\varepsilon}{2} \end{cases}; \qquad v_n = \frac{1}{u_n}.$$

The sequence $\{u_n\}$ is Cauchy, because it coincides with $\{a_n\}$ at least for $n \geq N_{\frac{\varepsilon}{2}}$. Moreover for every $\delta > 0$ we have

$$|v_n - v_m| = \frac{|u_n - u_m|}{|u_n u_m|} \leq \frac{4}{\varepsilon^2}|u_n - u_m| < \delta$$

for all $n, m \geq N_{\frac{\delta\varepsilon^2}{4}}$. Thus $\{v_n\} \in CS(K)$, hence $\{u_n\}$ is a unit. By construction, the sequence $\{a_n\} - \{u_n\} \in NS(K)$.
f) It follows from d) and e) that for any $\{a_n\} \in CS(K) - NS(K)$ we have $(\{a_n\}, NS(K)) = CS(K)$. Therefore $NS(K)$ is a maximal ideal in $CS(K)$.

Exercise 3.10. By definition, $(\dots, x_n, \dots) \in \varprojlim \mathfrak{a}^n/\mathfrak{b}^n$ means $x_n \equiv x_{n+1} \equiv \cdots \equiv x_{n+m} \bmod \mathfrak{b}^n$ for all m. Taking $m = (e-1)n$ we get $x_n \equiv x_{en} = 0$ because $x_{en} \in \mathfrak{a}^{en} \subseteq \mathfrak{b}^n$.

Exercise 3.12. Let $\pi \in R$ such that $v(\pi) = 1$. If $m = \min\{v(a_i) \mid i = 0, \dots, n\}$, then $\pi^{-m}F \in R[X]$ and at least one of its coefficients is a unit. Let $r \leq n$ be the largest integer such that $v(a_i) = 0$. If $r < n$ and $v(a_0) > 0$, let $g = \overline{a}_0 + \cdots + \overline{a}_r X^r$ and $h = 1$. Then $F(X) \equiv gh \bmod \mathfrak{m}$. Applying Hensel's lemma, we get that F is reducible, which is a contradiction.

Exercise 3.13. By exercise 3.6, it suffices to show that for any $x \in L$ such that $|N_{L/K}(x)| \leq 1$ then $|N_{L/K}(x+1)| \leq 1$. Let $F(X) = a_0 + \cdots + a_{n-1}X^{n-1} + X^n$ be the minimal polynomial of x over K. Then $N_{L/K}(x) = \pm a_0^{\frac{n}{[L:K]}}$ so $|a_0| \leq 1$. The minimal polynomial of $x+1$ is $F(X-1)$, so

$$N_{L/K}(x+1) = \pm\left(F(-1)\right)^{\frac{n}{[L:K]}} = \pm\left(a_0 - a_1 + \cdots + (-1)^{n-1}a_{n-1} + (-1)^n\right)^{\frac{n}{[L:K]}}$$

and $|a_0 - a_1 + \cdots + (-1)^{n-1}a_{n-1} + (-1)^n| \leq \max\{|a_i| \, i = 0, \dots, n\} = \max\{|a_0|, 1\} = 1$ where for the one but last equality we have used exercise 3.12. This method in fact suffices to prove that $|N_{L/K}(-)|^{\frac{1}{[L:K]}}$ defines an absolute value on a finite extension of any complete field with respect to a non-archimedean absolute value, not only a discrete one. The only missing ingredient is a suitable generalisation of Hensel's lemma. For a proof, see B. Dwork, G. Gerotto and F. Sullivan, *An introduction to G-functions*, Annals of Mathematics Studies No. 133, Princeton University Press, 1994, theorem 5.1.

§ 4 Chapter IV

Exercise 4.1. Let $Z = \operatorname{Spec} R - U$. It is a closed subset, so $Z = \mathcal{Z}(I)$ for a suitable ideal $I \subset R$. Since R is noetherian, $I = (f_1, \dots, f_m)$ is finitely generated. Thus $U = \operatorname{Spec} R - (\bigcap_{i=1}^m \mathcal{Z}(f_i)) = \bigcup_{i=1}^m (\operatorname{Spec} R - \mathcal{Z}(f_i))$.

Exercise 4.3. Since R is noetherian, any chain in Σ is stationary. By Zorn's Lemma, Σ has maximal elements. Let I be such a maximal element and suppose $I \neq R$. Since I can't be

written as the intersection of finitely many prime ideals, it is not prime itself: pick $x, y \in R$, $x, y \notin I$ with $xy \in I$. If $I + (x) = R$, there would be a $z \in I$ and $a \in R$ such that $1 = z + ax$. Then $y = 1 \cdot y = zy + axy \in I$, which is a contradiction. Therefore $I + (x)$ and $I + (y)$ are proper ideals strictly bigger than I. Hence $\sqrt{I + (x)}$ and $\sqrt{I + (y)}$ are proper radical ideals strictly bigger than I and thus not in Σ: we can write them as intersection of finitely many prime ideals.
Clearly $I \subseteq \sqrt{I + (x)} \cap \sqrt{I + (y)} \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r \cap \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$. If $t \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r \cap \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ then $t^n \in I + (x)$ and $t^m \in I + (y)$ for suitable $n, m \in \mathbb{N}$. Therefore

$$t^{n+m} \in (I + (x))\,(I + (y)) \subseteq I + (xy) = I.$$

Since I is radical, this implies $t \in I$. We conclude that $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r \cap \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$, which is a contradiction.
Suppose $J = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$. Fix $j \in \{1, \ldots, s\}$. Then $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r = J \subseteq \mathfrak{q}_j$. Since $\mathfrak{q}_j$ is prime, it contains at least one of the $\mathfrak{p}_i$, hence $r \leq s$. Symmetrically, every $\mathfrak{p}_i$ contains one of the $\mathfrak{q}_j$, thus $r = s$ and from the assumption $\mathfrak{p}_i \nsubseteq \mathfrak{p}_j$ and $\mathfrak{q}_i \nsubseteq \mathfrak{q}_j$ for $i \neq j$ we conclude also that the decomposition is unique.

§ 5 Chapter V

Exercise 5.1 Without loss of generality, we may assume $v(a_1) = \min_{1 \leq i \leq r} v(a_i)$ and, multiplying by a_1^{-1}, that $a_1 = 1$. If $v(a_i) > 0$ for $i \geq 2$, then $1 + (a_2 + \cdots + a_r) \in 1 + \mathfrak{q} \subset A^\times$, while we asumed $1 + a_2 + \cdots + a_r = 0$. Thus $v(a_i) = v(a_1)$ for some $i \geq 2$.

Exercise 5.3. If $x \in L$ satisfies an equation $x^q - a_0 = 0$ with $a_0 \in R$, it is integral over R, hence $x \in A$. Conversely, for every $x \in A$ we have $x^q \in A \cap K$: since R is integrally closed, $x^q \in R$.
If $x \in \mathfrak{q}$ then $x^q \in \mathfrak{q} \cap K = \mathfrak{p}$. Conversely, if $x^q \in \mathfrak{p} \subseteq R$, then $x \in A$ by what we have just seen. Moreover $x^q \in \mathfrak{p} \subseteq \mathfrak{q}$ implies $x \in \mathfrak{q}$, because $\mathfrak{q}$ is prime.
It follows from b) that the map $\mathfrak{q} \mapsto \mathfrak{q} \cap R$ is injective. It is surjective by proposition 3.2.4.
If $0 \neq a \in A$ then $0 \neq a^q \in R$. Decomposing (a^q) as a product of prime ideals in R we see that a^q is contained in finitely many of these, and they correspond to finitely many prime ideals in A containing a.
The inclusion $S^{-1}A \subseteq A_\mathfrak{q}$ is obvious. If $\frac{b}{a} \in A_\mathfrak{q}$, with $a \notin \mathfrak{q}$, then $\frac{b}{a} = \frac{a^{q-1}b}{a^q}$. Now $a^q \in R$ and $a^q \notin \mathfrak{p}$, therefore $a^q \in S$.
Fix $y \in \mathfrak{q}A_\mathfrak{q}$, with $y^q = u\pi^n$, $u \in R_\mathfrak{p}^\times$ and n minimal. For $x \in \mathfrak{q}A_\mathfrak{q}$, write $x^q = v\pi^m$, with $v \in R_\mathfrak{p}^\times$. Set $z = xy^{-1} \in L$. Then $z^q = vu^{-1}\pi^{m-n} \in R_\mathfrak{p}$, since $m \geq n$ by assumption. Therefore z belongs to the integral closure of $R_\mathfrak{p}$, which by corollary 3.1.16 is $S^{-1}A = A_\mathfrak{q}$. Thus $x = yz \in yA_\mathfrak{q}$ and therefore $\mathfrak{q}A_\mathfrak{q} = yA_\mathfrak{q}$.
Any ideal $I \subset A_\mathfrak{q}$ is contained in $\mathfrak{q}A_\mathfrak{q}$. If $\{x_\alpha\}$ generate I, writing $x_\alpha = u_\alpha y^{n_\alpha}$ we see immediately that I id generated by y^m for $m = \min_\alpha\{n_\alpha\}$. So $A_\mathfrak{q}$ is a local PID and thus a DVR by proposition 5.1.1.
Let $I \subset A$ is an ideal, $0 \neq a \in I$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ the finitely many primes containing a. Since the $A_{\mathfrak{q}_i}$ are DVRs, we know that $I_{\mathfrak{q}_i} = x_i A_{\mathfrak{q}_i}$, for a suitable $x_i \in A_{\mathfrak{q}_i}$. Replacing x_i by a multiple (by an element in $A - \mathfrak{q}_i$), we may assume that $x_i \in I$. Let $J = (a, x_1, \ldots, x_r)$. We have

$J \subseteq I$ (because every generator of J is in I). We have $x_i A_{\mathfrak{q}_i} \subseteq J_{\mathfrak{q}_i} \subseteq I_{\mathfrak{q}_i} = x_i A_{\mathfrak{q}_i}$, hence $J_{\mathfrak{q}_i} = I_{\mathfrak{q}_i}$ for $i = 1, \dots, r$. On the other hand, if $\mathfrak{m} \subset A$ is a maximal ideal, $\mathfrak{m} \notin \{\mathfrak{q}_1, \dots, \mathfrak{q}_r\}$, by assumption $a \notin \mathfrak{m}$ so $J_{\mathfrak{m}} = I_{\mathfrak{m}} = A_{\mathfrak{m}}$. Therefore $(I/J)_{\mathfrak{m}} = 0$ for every maximal ideal $\mathfrak{m} \subset A$. By proposition 2.1.24, we conclude that $I = J$. Thus every ideal in A is finitely generated, hence A is noetherian.
A is a noetherian domain and $A_{\mathfrak{q}}$ is a DVR for every prime: it follows from proposition 5.3.1 that it is a Dedekind domain.

Exercise 5.4. Let K' be the largest intermediate extension $K \subseteq K' \subseteq L$ which is separable over K and R' the integral closure of R in K'. By corollary 5.3.5, R' is a Dedekind domain and by corollary 3.1.14 A is the integral closure of R' in L. We may thus assume that $K \subseteq L$ is purely inseparable and conclude by exercise 5.3.

Exercise 5.7. Let π be a uniformiser for $\mathfrak{p}$. Every element in R can be written as $t = u\pi^n$ for some $u \in R^\times$ and $n \in \mathbb{N}$. Since π generates $\mathfrak{q}^e$, we have $w(\pi) = e$ and $w(u) = 0$ for every $u \in R^\times \subseteq A^\times$, hence $w(t) = ne$.
By corollary 3.3.15, A is a free R-module of finite rank $e = [L : K]$ and $\mu_x : A \to A$ is R-linear: in an R-basis of A the matrix of μ_x has coefficients in R.
Since $\mu_x^e(A) \subseteq \mathfrak{p}A$, the reduction of μ_x mod $\mathfrak{p}$ is nilpotent. The characteristic polynomial of μ_x is thus congruent to X^e mod $\mathfrak{p}$. Its constant term is by definition $N_{L/K}(x)$ and by corollary 5.4.9 this element is a uniformiser of $\mathfrak{p}$. The map $R[X] \to A$ sending X to x defines an injection $A' = R[X]/(f(X)) \subseteq A$. Since $f(X) \equiv X^e$ mod $\mathfrak{p}$, exercise 1.12 implies that A' is a local ring with maximal ideal $\mathfrak{q}' = (\mathfrak{p}, x)$. Writing $f(X) = X^e + a_{e-1}X^{e-1} + \cdots + a_0$, since $f(x) = 0$, we have $-a_0 = x^e + a_{e-1}x^{e-1} + \cdots + a_1 x$. Recalling that $a_0 = N_{L/K}(x)$ is a uniformiser of $\mathfrak{p}$, we conclude that $\mathfrak{p}A' \subseteq (x)$, hence $\mathfrak{q}' = (x)$. From proposition 5.1.5 we then get that A' is a DVR. But $A' \subseteq A$ and $\operatorname{Frac} A' = \operatorname{Frac} A = L$, hence $A' = A$.
From proposition 3.3.10 we get that $\mathfrak{D}_{A/R}$ is generated by

$$f'(x) = ex^{e-1} + (e-1)a_{e-1}x^{e-2} + \cdots + a_1.$$

By a) we get that $w(a_i) \equiv 0$ mod e and also $w(n) \equiv 0$ mod e for every integer n, since the map $\mathbb{Z} \to A$ factors through R. Therefore $w\left((e-i)a_i x^{e-i-1}\right) \equiv -i - 1$ mod e. Since all the terms in $f'(x)$ have different valuations, we get

$$w\left(f'(x)\right) = \min_{0 \le i \le e-1} w\left((e-i)a_i x^{e-i-1}\right).$$

We have $w\left(ex^{e-1}\right) = w(e) + e - 1$ and $w\left((e-i)a_i x^{e-i-1}\right) \geq w(a_i) \geq e$ for $1 \leq i \leq e-1$, thus $e - 1 \leq w\left(f'(x)\right) \leq e - 1 + w(e)$ and $w\left(f'(x)\right) = e - 1$ if and only if $w(e) = 0$.

Exercise 5.8. The relation $\Delta(\alpha) = d^2\Delta(x_1, \dots, x_n)$ has already been established in formula (3.3). Let then $C = (c_{ij})$ be the cofactor matrix, so $c_{ij} \in R_{\mathfrak{p}}$. For any $y \in A_{\mathfrak{p}}$, we can write $y = \sum_{i=1}^n a_i x_i$ with $a_i \in R_{\mathfrak{p}}$ and, since $M^{-1} = d^{-1}C$,

$$dy = d\sum_{i=1}^n a_i x_i = d\sum_{i=1}^n a_i \sum_{j=0}^{n-1} d^{-1}c_{ij}\alpha^j = \sum_{j=0}^{n-1}\left(\sum_{i=1}^n a_i c_{ij}\right)\alpha^j \in R_{\mathfrak{p}}[\alpha].$$

Since $\Delta(x_1, \dots, x_n) \in R_{\mathfrak{p}}$, we see immediately that $\Delta(\alpha)y = \left(d\Delta(x_1, \dots, x_n)\right) dy \in R_{\mathfrak{p}}[\alpha]$.

Consider now the composite map of R-modules $\phi : A \xrightarrow{\mu_{\Delta(\alpha)}} A \longrightarrow A/R[\alpha]$, where the first map is multiplication by $\Delta(\alpha)$ and second is the projection and let $Q = \operatorname{im}\phi$. We have just shown that $\phi_{\mathfrak{p}}$ is the zero map for all $\mathfrak{p}$, hence $Q_{\mathfrak{p}} = 0$ for all maximal ideals in R. From proposition 2.1.24 we conclude that $Q = 0$, i.e. $\phi = 0$ and thus $\Delta(\alpha)A \subseteq R[\alpha]$.

Let $\mu_d : A_{\mathfrak{p}} \to A_{\mathfrak{p}}$ be the multiplication by d. We have established in b) that $\operatorname{im}\mu_d \subseteq R_{\mathfrak{p}}[\alpha]$. If $d \in \mathfrak{p}R_{\mathfrak{p}}$, then $v_{\mathfrak{p}}(\Delta(\alpha)) \geq 2$ by a). Therefore, if $\Delta(\alpha) \notin \mathfrak{p}^2$ then $d \notin \mathfrak{p}R_{\mathfrak{p}}$, hence d is a unit in $R_{\mathfrak{p}}$, so μ_d is an isomorphim. We are done: $R_{\mathfrak{p}}[\alpha] \subseteq A_{\mathfrak{p}} = \operatorname{im}\mu_d \subseteq R_{\mathfrak{p}}[\alpha]$.

§ 6 Chapter VI

Exercise 6.1. Let $\{\mathfrak{p}_i\}_i$ be all the minimal primes of R and put $Z_i = \mathcal{Z}(\mathfrak{p}_i)$. By exercise 1.19.a, the Z_i are irreducible subsets and, since every prime contains a minimal prime, $\operatorname{Spec} R = \bigcup_i Z_i$. If $\mathcal{Z}(\mathfrak{p}_j) \subseteq \mathcal{Z}(\mathfrak{p}_i)$, then $\mathfrak{p}_j \supseteq \mathfrak{p}_i$ and by minimality $\mathfrak{p}_j = \mathfrak{p}_i$.

Exercise 6.3. In view of exercise 2.2a), from corollary 6.1.29 we have $\dim A_{S^{-1}\mathfrak{p}_i} = \dim R_{\mathfrak{p}_i} = i$. Hence $\dim A = +\infty$. A is noetherian, since, by exercise 2.2e), every ideal is finitely generated.

Exercise 6.4. If S is constructible, for any irreducible closed subset $T \subseteq \operatorname{Spec} R$, expressing S as a union of locally closed subsets and intersecting with T we may write $S \cap T = \bigcup_{i=1}^{n}(U_i \cap Z_i)$ with the U_i open and the Z_i closed. Without loss of generality, we may assume that the Z_i are irreducible and that $U_i \cap Z_i \neq \varnothing$. Then the closure $\overline{U_i \cap Z_i}$ equals Z_i by exercise 1.19.a, hence $\overline{S \cap T} = \bigcup_{i=1}^{r} Z_i$. Therefore if $S \cap T$ is dense in T then $\bigcup_{i=1}^{r} Z_i = \overline{S \cap T} = T$. Since T is irreducible, $T = Z_i$ for some i. Then $U_i \cap Z_i$ is an open subset of $T = Z_i$ contained in S.

Clearly $\overline{Z_1 \cap S} \subseteq Z_1$. On the other hand, if W is a closed subset containing $Z_1 \cap S$, then $W \cup Z_2 \cup \cdots \cup Z_r$ is a closed subset containing S, therefore $(W \cup Z_2 \cup \cdots \cup Z_r) \supseteq \overline{S} \supseteq Z_1$ and thus $Z_1 = (W \cup Z_2 \cup \cdots \cup Z_r) \cap Z_1 = (W \cap Z_1) \cup (Z_2 \cap Z_1) \cup \cdots \cup (Z_r \cap Z_1)$. Since Z_1 is irreducible, either $W \cap Z_1 = Z_1$, which means $Z_1 \subseteq W$ or, for some $i \geq 2$, $Z_i \cap Z_1 = Z_1$, which means $Z_1 \subseteq Z_i$, forbidden by the definition of irreducible component. Hence Z_1 is contained in every closed subset W containing $Z_1 \cap S$ and is thus contained in $\overline{Z_1 \cap S}$. Therefore $\overline{Z_1 \cap S} = Z_1$. By assumption, S satisfies $(\star)$ and so a non-empty open subset $Z_1 - Z_1'$ in Z_1 must be contained in $S \cap Z_1 \subset S$.

Clearly $Z_1 - Z_1' = Z_1 \cap (\operatorname{Spec} R - Z_1')$, so it is locally closed. Let $T \subseteq \operatorname{Spec} R$ be an irreducible closed subset and assume that $\overline{S \cap Y \cap T} = T$. Since Y is closed and contains $S \cap Y \cap T$, then $T \subseteq Y$, so $S \cap Y \cap T = S \cap T$. By assumption, S satisfies $(\star)$ and so a non-empty open subset of T must be contained in $S \cap T = S \cap Y \cap T$. Therefore $S \cap Y$ satisfies $(\star)$ too.

We have seen that $S' = S \cap Y$ satisfies $(\star)$. Moreover its closure $\overline{S \cap Y}$ is contained in Y which is properly contained in $\overline{S}$. By our working hypothesis, $S \cap Y$ is constructible. Therefore $S = (Z_1 - Z_1') \cup (S \cap Y)$ is the union of constructible subsets and thus constructible.

Exercise 6.5. We have a noetherian ring R and an R-algebra of finite type $\varphi : R \to A$. We want to show that $\operatorname{im}\varphi^\sharp$ satisfies condition $(\star)$ of exercise 6.4. Let $T \subseteq \operatorname{Spec} R$ be an irreducible closed subset and assume that $T \cap \operatorname{im}\varphi^\sharp$ is dense in T. By exercise 1.19.b, $T = \mathcal{Z}(\mathfrak{p})$ for some prime $\mathfrak{p} \subset R$. The map φ induces $\overline{\varphi} : R/\mathfrak{p} \to A/\varphi(\mathfrak{p})A$. As seen in the proof of Chevalley's theorem, $\overline{\varphi}^\sharp$

identifies with the restriction of $\varphi^\sharp$ to $(\varphi^\sharp)^{-1}(T) = (\varphi^\sharp)^{-1}((\mathcal{Z}(\mathfrak{p})) = \mathcal{Z}(\varphi(\mathfrak{p})A) = \operatorname{Spec} A/\varphi(\mathfrak{p}_i)A$. Thus, by assumption, $\operatorname{im}\overline{\varphi}^\sharp$ is dense. By exercise 1.20, we have $\ker\overline{\varphi} \subseteq \mathfrak{N}_{R/\mathfrak{p}} = 0$ (as $R/\mathfrak{p}$ is a domain). Again we may apply corollary 3.2.7 to conclude that $\operatorname{im}\overline{\varphi}^\sharp = \operatorname{im}\varphi^\sharp \cap T$ contains a non-empty open subset of T. This is precisely condition $(\star)$ for $\operatorname{im}\varphi^\sharp$.

Exercise 6.6. If $S = \operatorname{Spec} A_f \cap \mathcal{Z}(I)$, the A-algebra $B = (A/I)_f = A[X]/J$, with $J = (Xf-1) + IA[X]$ is a finitely generated A-algebra. The points of $\operatorname{Spec} B$ are in bijection with the prime ideals $\mathfrak{q} \subset A$ such that $I \subseteq \mathfrak{q}$ and $f \notin \mathfrak{q}$ i.e. with the points of S.
Let $S = \bigcup_{i=1}^m (U_i \cap Z_i) \subseteq \operatorname{Spec} A$ be a constructible subset, with the U_i open and the Z_i closed. In view of exercise 4.1, there is no loss of generality in assuming that $U_i = \operatorname{Spec} A - \mathcal{Z}(f_i) = \operatorname{Spec} A_{f_i}$ for a suitable $f_i \in A$. We have shown above that there exist finitely generated A-algebras $\psi_i : A \to B_i$ such that $\operatorname{im}\psi_i^\sharp = U_i \cap Z_i$. The A-algebra $B = \prod_{i=1}^m B_i$ is again of finite type by exercise 1.10 and $\operatorname{Spec}\left(\prod_{i=1}^m B_i\right) = \coprod_{i=1}^m \operatorname{Spec} B_i$ by exercise 1.18, so its image in $\operatorname{Spec} A$ is equal to S.

Exercise 6.7. Let $S \subseteq \operatorname{Spec} A$ be a constructible subset. By exercise 6.6 we can find an A-algebra of finite type $\psi : A \to B$ such that $S = \operatorname{im}\psi^\sharp$. Hence B is also an R-algebra of finite type and the claim follows from theorem 6.1.37 applied to the R-algebra B.

Exercise 6.8. The polynomial $pX - 1$ is irreducible (it is of degree 1), so $\mathfrak{p}$ is a prime. It is principal, so is of height 1. Clearly $\mathfrak{p} \cap \mathbb{Z} = \{0\}$, so $\mathfrak{p}$ represents a point on $\mathbb{A}^1_{\mathbb{Q}}$. Let $\ell \in \mathbb{N}$ be a prime number. If $\ell \neq p$ then $(pX-1, \ell)$ is a maximal ideal in $\mathbb{Z}[X]$: if $m \in \mathbb{Z}$ is such that $pm \equiv 1 \bmod \ell$, then $\mathbb{Z}[X]/(pX-1,\ell) \cong \mathbb{F}_\ell[X]/(X-m) \cong \mathbb{F}_\ell$. The closure of $\mathfrak{p}$ intersects the line $\mathbb{A}^1_{\mathbb{F}_\ell}$ at the point $X = m$. On the other hand, if $\ell = p$ then $(-1)(pX-1) + X(p) = 1$, so $(pX-1, p) = \mathbb{Z}[X]$: the closure of $\mathfrak{p}$ doesn't meet the line $\mathbb{A}^1_{\mathbb{F}_p}$. The horizontal curve $\mathcal{Z}(\mathfrak{p})$ "goes to infinity" at p.

Exercise 6.9. From example 6.1.31 we know that there are two types of primes of height 1 in $\mathbb{Z}[X]$. Those of the form $p\mathbb{Z}[X]$ for some prime number p can obviously be embedded in the maximal ideals $(p, F(X))$, where $F(X) \in \mathbb{Z}[Z]$ is any polynomial whose reduction mod p is irreducible. On the other hand we have the height 1 primes generated by an irreducible polynomial $F(X) \in \mathbb{Z}[X]$. There are infinitely many prime numbers $p \in \mathbb{Z}$ such that the reduction of $F(X)$ mod p is not a constant polynomial; for all such primes, $(F(X))$ is not coprime with $p\mathbb{Z}[X]$, so $(p, F(X)) \subsetneq \mathbb{Z}[X]$, hence $(p, F(X))$ is contained in some maximal ideal $\mathfrak{m}$ and $(F(X)) \subsetneq (p, F(X)) \subseteq \mathfrak{m}$.
If R is a DVR with uniformiser π then $R\left[\frac{1}{p}\right] = R[X]/(\pi X - 1) = \operatorname{Frac} R$. So $(\pi X - 1)$ is a maximal ideal and is of height 1 because it is principal.

Glossary of notations

$\mathrm{Ann}\,(M)$, annihilator 13
$Bil_R(M \times N, P)$, bilinear maps 21
$\mathrm{coker} f$, cokernel of a linear map 13
$\Delta_{A/R}(x_1, \ldots, x_n)$, discriminant of a basis 62
$\mathfrak{d}_{A/R}$, discriminant ideal 63
$\mathfrak{D}^{-1}_{A/R}$, codifferent 63
$\mathfrak{D}_{A/R}$, different ideal 100
$\deg(D)$, degree of a divisor 105
$\mathrm{Der}_R(A, M)$, module of derivations 26
$\dim(R)$, (Krull) dimension of a ring 119
$\mathrm{Div}(R)$, group of Cartier divisors 101
$Ext^1_R(Q, N)$, module extension 34
$\mathbb{F}_q$, field with q elements 4
$\mathrm{Frac}\, R$, fraction field of a domain 38
$\boldsymbol{h}_T$, representable functor 133
$Hom_R(M, N)$, module homomorphisms 12
$\sqrt{I}$, radical of an ideal 11
$I \cap J$, intersection of ideals 8
IJ, product of ideals 8
$I + J$, sum of ideals 8
$\mathrm{ht}\,\mathfrak{p}$, height of a prime 119
$k[\varepsilon]$, ring of dual numbers 30
$k((X))$, Laurent power series 38
$k(X_1, \ldots, X_n)$, rational functions 38
$\ell(M)$, length of a module 89
$\varprojlim G_i$ inverse limit 78
$K_0(R)$, Grothendieck group 113
M_f module of fractions 40
$M_\mathfrak{p}$ localisation at a prime ideal 40
M_{tors} torsion elements 13
$M_1 \cap M_2$, intesection of submodules 14
$M_1 + M_2$, sum of submodules 14
$M_1 \oplus M_2$, direct sum 14
$M \otimes_R N$, tensor product 22
$(M : N)$, index of two submodules 13
$\mathbf{Mod}_R$ category of R-modules 12
$\mathfrak{N}_R$, nilradical 4
$N_{A/R}(x)$, norm of an element 61
$\mathcal{O}_K$, integers in a number field 54
$\mathrm{Pic}(R)$, Picard group of a ring 99
$\mathbb{Q}_p$, p-adic numbers 73
$\mathfrak{R}_R$, Jacobson radical 7
$R^\times$ units in a ring 3
$\hat{R}_\mathfrak{a}$ $\mathfrak{a}$-adic completion 79
$R\left[\frac{1}{f}\right]$, R_f ring of fractions 38
$R_\mathfrak{p}$ localisation at a prime ideal 37
$R[[X]]$ formal power series 14
$S^{-1}M$, module of fractions 40
$S^{-1}R$, ring of fractions 37
$\mathrm{Spec}\, R$, spectrum of a ring 10
$\mathrm{Tr}_{A/R}(x)$, trace of an element 61
(x), xR, principal ideal 3
$|x|$, absolute value 68
$\mathbb{Z}_{(p)}$, localisation of $\mathbb{Z}$ at p 38
$\mathbb{Z}_p$, p-adic integers 73
$\mathcal{Z}(I)$, zero locus of an ideal 10
$Z^1(R)$, group of Weil divisors 103
$Z^1_{inv}(R)$, invertible Weil divisors 102
$\Omega^1_{A/R}$, module of differentials 26

Index

Bibliography

[1] ATIYAH, M AND MACDONALD, I., *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[2] EISENBUD, D., *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics, No. 150, Springer-Verlag, 1994.

[3] JANUSZ, G., *Algebraic Number Fields*, Graduate Studies in Mathematics, No. 7, AMS, 1996.

[4] HARTSHORNE, R., *Algebraic Geometry*, Graduate Texts in Mathematics, No. 52, Springer-Verlag, 1977.

[5] LIU, Q., *Algebraic geometry and Arithmetic Surfaces*, Oxford Graduate Texts in Mathematics, No. 6, Oxford University Press, 2002.

[6] LORENZINI, D., *An Invitation to Arithmetic Geometry*, Graduate Studies in Mathematics, No. 9, AMS, 1996.

[7] MALLIAVIN, M.-P., *Algèbre Commutative, Applications en Géométrie et Théorie des Nombres*, Masson 1985.

[8] MATSUMURA, H., *Commutative Algebra*, W.A. Benjamin, 1970.

[9] MATSUMURA, H., *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, 1986.

[10] MILNE, J.S., *Étale cohomology*, Princeton Mathematical Series No 33, Princeton University Press, 1970.

[11] MILNOR, J., *Introduction to Algebraic K-Theory*, Princeton University Press, 1971.

[12] MUMFORD, D., *The Red Book of Varieties and Schemes*, Lecture Notes in Mathematics, No. 1358, Springer-Verlag, 1988.

[13] NAGATA, M., *Local Rings*, Interscience, New York, 1962.

[14] RAMERO, L., *Grimoire d'Algèbre Commutative*, Les Presses Insoumises, 2014. Available at `http://math.univ-lille1.fr/~ramero/CoursAG.pdf`.

[15] RAYNAUD, M., *Anneaux Locaux Henséliens*, Lecture Notes in Mathematics, No. 169, Springer-Verlag, 1970.

[16] SAMUEL, P., *Théorie Algébrique des Nombres*, Hermann, Paris 1967.

[17] SERRE, J.-P., *Corps Locaux*, Hermann, Paris, 1962.

[18] SERRE, J.-P., *Algèbre locale. Multiplicités*, Lecture Notes in Mathematics, No. 11, Springer-Verlag, 1965.

[19] WEIBEL, C., *An introduction to Homological Algebra*, Cambridge Studies in Advanced Mathematics 38, Cambridge University Press, 1994.