Mathematical Lectures from Peking University

Michel Broué

Some Topics in Algebra

An Advanced Undergraduate Course at PKU

北京国际数学研究中心
BICMR
BEIJING INTERNATIONAL CENTER FOR MATHEMATICAL RESEARCH

Springer

Mathematical Lectures from Peking University

For further volumes:
www.springer.com/series/11574

Michel Broué

Some Topics in Algebra

An Advanced Undergraduate Course at PKU

北京国际数学研究中心
BICMR

Springer

Michel Broué
Institut Universitaire de France
Université Paris Diderot—Paris 7
Paris, France

ISSN 2197-4209 ISSN 2197-4217 (electronic)
ISBN 978-3-642-41268-4 ISBN 978-3-642-41269-1 (eBook)
DOI 10.1007/978-3-642-41269-1
Springer Heidelberg New York Dordrecht London

Mathematics Subject Classification: 11-01, 12-01, 13-01

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

Never, before I had lectured in front of second and third years students of Peking University, did I feel that strongly how much mathematics are universal, a world where human minds think alike. And never before had I enjoyed it so much.

The course I was supposed to give (an advanced undergraduate introduction to Algebra) had no specific syllabus. I decided to let it go, pushed or pulled by the student's reactions and my own feelings. It turned out to become an amazing and delightful encounter between, on one hand, ideas and discoveries of German mathematicians from the end of the XIXth and the beginning of the XXth centuries[1] revisited and taught by some French mathematicians from the XXth century[2], and, on the other hand, young brilliant Chinese students of the XXIst century.

The pleasure of these students while discovering these concepts, results, examples, has been obvious all along the course, and even sometimes expressed loudly. Moreover, the speed of their understanding and handling notions which were mostly new to them was amazing. A couple of times, at the intermission, one of them came and politely told me that he thought he had found a more elegant proof than the one I had just given—and each time he was indeed right, his proof was better, more elegant, more natural.

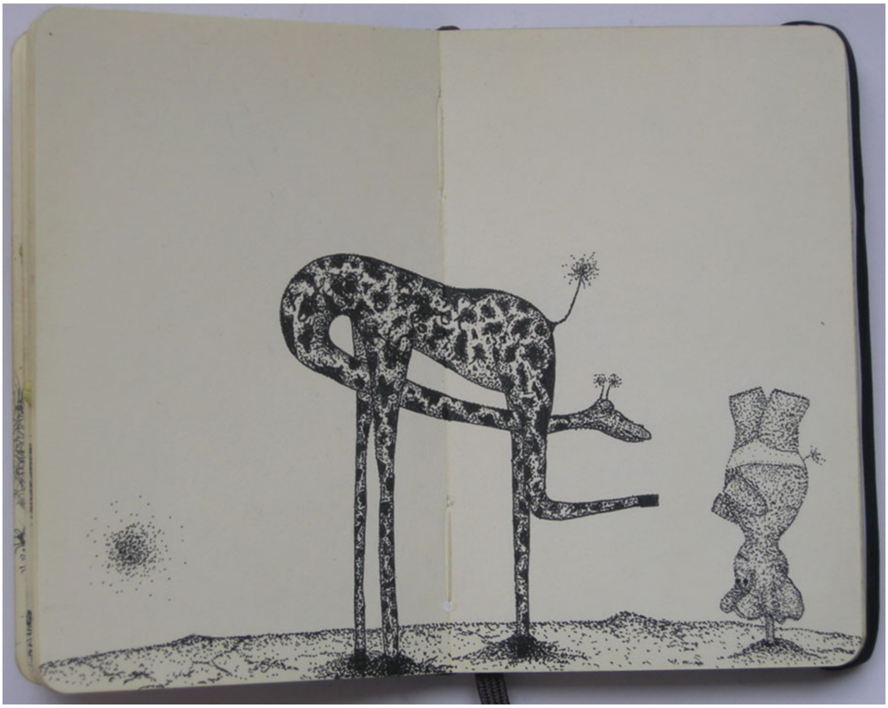
Elegant, efficient, natural, pertinent, beautiful, clever, exciting: these are words sometimes heard when a mathematician discovers a new approach, a new proof, or even a new version of an old result. Whatever country, origin, culture that mathematician may be from: what is beautiful and pertinent for a German Herr Professor of the XIXth Century is also beautiful and pertinent for a young Chinese student of 2013. Of course, universality is not the peculiarity of mathematics, it is certainly shared by most of the arts, and partly by philosophy. But the essence of the universality of mathematics is not directly connected with feelings and events of any human life, pain or joy, love or disaster, war, freedom, death or future. Besides, the

[1] Ideals were first defined by Richard Dedekind in 1876 in the third edition of his book *"Vorlesungen über Zahlentheorie"* (Lectures on Number Theory), after Ernst Kummer had introduced the concept of "ideal numbers". The notion was later expanded by David Hilbert and Emmy Noether.

[2] Like Nicolas Bourbaki.

universality of mathematics is a rule, almost a theorem: what is considered by all as good is indeed good. I do think this is one of the wonders of the world we live in.

The more elegant proofs of the students are integrated in this book, without quotation to their authors since I did not know their names. This is one of the reasons why the book is dedicated to the students of PKU.



CONVERSATION BETWEEN MATHEMATICIANS—©Anouk Grinberg

Abstract

During the Springs of 2011 and 2012, I was invited by the Beijing International Center for Mathematics Research to give an advanced undergraduate algebra course (once a week over two months each year). This is part of the Everest project of Chinese Education Ministry on first class students training.

This book has been written during and for that course. By no way does it pretend to any type of exhaustivity. It is a quick and contingent introduction to Algebra in front of an extremely pleasant and passionate audience, heterogeneous but persistent. It certainly reflects some of my own tastes, and mainly the constraints of such a short period of teaching.

A remark about the last two sections: following a well established tradition, we had planned to conclude by lecturing on the structure of finitely generated modules over principal ideal domains. But during the process of the course, after explaining that the notion of projective module is somehow more natural than the notion of free module, it became rather inevitable to replace principal ideal domains by Dedekind rings; this is less traditional in the literature—but not really more difficult.

Prerequisites

This book requires a certain familiarity with the notions of groups, rings, fields, and specially with the undergraduate knowledge of linear algebra. More specifically, let k be a commutative field. We assume the reader knows

- the definition of the ring of polynomial $k[X_1, \dots, X_n]$ in n indeterminates,
- the Euclidean division in $\mathbb{Z}$ and in $k[X]$, as well as some of the consequences, like: both these rings are principal ideal domains, hence for p a prime number and $P(X)$ an irreducible polynomial, both quotients $\mathbb{Z}/p\mathbb{Z}$ and $k[X]/(P(X))$ are fields;
- the main results of an undergraduate course on k-linear algebra;
- matrices and their determinants.

  The following identity will not be proved: let M be an $n \times n$ matrix with entries in k, let ${}^t\mathrm{Com}(M)$ denote the transpose of its matrix of cofactors, let 1_n be the identity $n \times n$ matrix; then

$$ {}^t\mathrm{Com}(M).M = \det(M).1_n. $$

We take for granted that the reader is familiar with the standard notation $\mathbb{N}$ (for "numbers")—note that by convention $\mathbb{N} = \{0, 1, 2, \dots\}$, $\mathbb{Z}$ for "Zahlen"), $\mathbb{Q}$ (for "quotients"), $\mathbb{R}$ (for "reals"), $\mathbb{C}$ (for "complexes"), as well as $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (for "finite")—see [7], p. 3.

By convention, a *field* is a *commutative* ring where all nonzero elements are invertible. A noncommutative ring where all nonzero elements are invertible is called a *division ring*.

We shall also use the following notation.

- For Ω any finite set, $|\Omega|$ will denote the number of its elements.
- For any sequence $\xi_1, \dots, \xi_n$, or any product $\xi_1 \cdots \xi_n$, and for all $j = 1, \dots, n$, we set (with obvious ad hoc convention for ξ_0 and ξ_{n+1}):

$$ (\xi_1, \dots, \widehat{\xi_j}, \dots, \xi_n) := (\xi_1, \dots, \xi_{j-1}, \xi_{j+1}, \dots, \xi_n), \quad \text{and} $$
$$ \xi_1 \cdots \widehat{\xi_j} \cdots \xi_n := \xi_1 \cdots \xi_{j-1}\xi_{j+1} \cdots \xi_n. $$

A subset (subgroup, subring, submodule, ...) Ω' of a set (group, ring, module, ...) Ω is said to be *proper* if $\Omega' \neq \Omega$.

Acknowledgements

I warmly thank Yanjun Liu, Xiong Huan, and specially Gunter Malle, for their careful and patient readings and corrections of the manuscript. My thanks go also to the students who attended the courses which motivated these notes, for their interest, their attention, their questions, their wonder for Mathematics.

Contents

1 Rings and Polynomial Algebras 1

1.1 First Definitions 1

1.1.1 Rings 1

1.1.2 Canonical Morphisms 9

1.1.3 Ideals 12

1.1.4 Algebras 15

1.1.5 Fields, Division Rings 20

1.2 Prime and Maximal Ideals, Integral Domains 36

1.2.1 Definition and First Examples 36

1.2.2 Examples in Polynomial Rings 37

1.2.3 Nilradical and Radical 39

1.2.4 Integral Domains, Fields of Fractions 42

1.3 Divisibility and Irreducible Elements 47

1.3.1 Divisors and Irreducible Elements 47

1.3.2 Euclidean Rings 49

1.3.3 GCD and LCM 51

1.3.4 Case of $\mathbb{Z}[i]$ and Application 52

1.3.5 Irreducibility Criteria in $R[X]$ 54

1.4 Polynomial Rings in Several Indeterminates 66

1.4.1 Universal Property, Substitutions 66

1.4.2 Transfer Properties 70

1.4.3 Symmetric Polynomials 71

1.4.4 Resultant and Discriminant 76

2 Modules 87

2.1 Definitions and Conventions 87

2.1.1 Definitions 87

2.1.2 Submodules 90

2.1.3 Torsion Elements, Torsion Submodule 96

2.1.4 Free and Generating Systems, Free Modules 98

2.1.5 Constructions: Direct Sums, Products, Tensor Products 102

2.1.6 Localization 110

2.2 Finitely Generated Modules 115

2.2.1 Application: Integrality over a Ring 116

2.2.2 Complement: Jacobson Rings, Hilbert's Nullstellensatz . 122

2.2.3 Noetherian Rings and Modules 127

2.2.4 Finitely Generated Free Modules 132

2.2.5 Finitely Generated Projective Modules 137

2.3 Finitely Generated Modules over Dedekind Domains 146

2.3.1 Fractional Modules, Dedekind Domains 146

2.3.2 Finitely Generated Projective Modules over Dedekind Domains 154

2.3.3 Remarkable Decompositions of Finitely Generated Torsion Modules 159

2.3.4 Adapted Pseudo-bases for Submodules of Finitely Generated Projective Modules 169

2.3.5 Applications to Abelian Groups and Endomorphisms of Vector Spaces 175

2.4 Complement on Dedekind Domains 186

2.4.1 Characterizations of Dedekind Domains 186

2.4.2 Rings of Integers of Number Fields Are Dedekind 188

Erratum to: Rings and Polynomial Algebras E1

References 195

Index 197

Chapter 1
Rings and Polynomial Algebras

1.1 First Definitions

We assume that basic notions of elementary algebra are known. Nevertheless, for the purpose of setting precisely our notation and convention, we shall repeat briefly some of the definitions.

We suggest that the reader starts by solving the following exercise.

Exercise 1.1 Let k be a (commutative) field, and let $P(X) \in k[X]$. We denote by $k[X]/(P(X))$ the quotient of $k[X]$ by the principal ideal generated by $P(X)$.

(1) The following assertions are equivalent.

  (i) The ring $k[X]/(P(X))$ is a field.
  (ii) $P(X)$ is irreducible in $k[X]$.

(2) $k[X]/(P(X))$ has dimension $\deg(P(X))$ as a k-vector space.
(3) Let $\mu_X : k[X]/(P(X)) \to k[X]/(P(X))$ be the endomorphism of that vector space induced by the multiplication by X. Then $P(X)$ is both the minimal polynomial and the characteristic polynomial of the endomorphism μ_X.

1.1.1 Rings

1.1.1.1 Definition

For us a *ring* A is

- an Abelian (additive) group, with zero element 0,
- endowed with an associative multiplication denoted $(a, a') \mapsto a \cdot a'$ (often abbreviated $(a, a') \mapsto aa'$), with a unit element denoted 1_A (usually abbreviated 1), i.e., an element such that $1_A \cdot a = a \cdot 1_A = a$ for all $a \in A$,

An erratum to this chapter is available at doi: 10.1007/978-3-642-41269-1_3.

M. Broué, *Some Topics in Algebra*, Mathematical Lectures from Peking University,
DOI 10.1007/978-3-642-41269-1_1, © Springer-Verlag Berlin Heidelberg 2014

- such that the multiplication is distributive on the addition.

Definitions 1.2

- A ring is said to be *commutative* if its multiplication is commutative.
- The ring A is said to have no zero divisor if for all $a, a' \in A \setminus \{0\}$, we have $aa' \neq 0$.
- A ring is an *integral domain* if it is nonzero, commutative, and if it has no zero divisor.

Exercises 1.3

(1) Let R be an integral domain and let $\mathrm{Mat}_n(R)$ denote the ring of $n \times n$ matrices over R. The following conditions are equivalent.

   (a) $\mathrm{Mat}_n(R)$ is commutative,
   (b) $\mathrm{Mat}_n(R)$ has no zero divisor,
   (c) $n = 1$.

(2) Let A and B be two nonzero rings. There is an obvious structure of product ring on the Cartesian product $A \times B$ (which one?). Show that the product ring has always zero divisors.
(3) For $n \in \mathbb{N}$, the ring $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is 0 or a prime number.

The set of invertible elements (or *units*) of A is the multiplicative group defined by

$$A^\times := \big\{a \in A \mid \big(\exists a' \in A\big)\big(aa' = a'a = 1\big)\big\}.$$

One says that A is a *division ring* (or a *field* if A is commutative) if $A^\times = A \setminus \{0\}$.

Exercise 1.4 Prove that there is a group isomorphism: $(A \times B)^\times \cong A^\times \times B^\times$.

1.1.1.2 Morphisms

A *ring morphism* $f : A \longrightarrow B$ is a map from A to B such that

(1) f is an additive group morphism from A to B,
(2) f is multiplicative, i.e., $f(aa') = f(a)f(a')$ for all $a, a' \in A$,
(3) $f(1_A) = 1_B$.

1.1.1.3 Subrings

A *subring* B of a ring A is a subset of A and a ring such that the natural injection $\iota : B \hookrightarrow A$ is a ring morphism.

Thus, the subrings of a ring A are all images of ring morphisms ending in A.

Examples–Definitions 1.5

- The *center* $Z(A)$ of a ring A, defined by

$$Z(A) := \big\{ z \in A \;\big|\; (\forall a \in A)(az = za) \big\},$$

  is a (commutative) subring of A.
- The intersection of subrings of A is a subring of A.

  If E is a subset of A, the intersection of all subrings of A containing E is the smallest subring of A which contains E. It is called the subring *generated by* E.

  In particular the intersection of *all* the subrings of A is a subring of A: it is the smallest subring of A. It is called the *prime subring* of A.

(!) If A is a nonzero ring, the ring $\{0\}$ is *not* a subring of A. If A and B are nonzero rings, $A \times \{0\}$ is *not* a subring of $A \times B$.

1.1.1.4 Endomorphisms of Abelian Groups and Modules

The set of endomorphisms of an Abelian group has a natural structure of ring. Let us set our conventions.

Let M and M' be Abelian groups. We let any group morphism f act on the *left* on M, i.e., we write $f(m)$ (or fm) for the image of m under f.

- The sum of group morphisms f and f' from M into M' is defined by $(f + f')(m) := f(m) = f'(m)$, and it defines a structure of Abelian group on the set of group morphisms from M to M', denoted $\mathrm{Hom}(M, M')$.
- For M'' another Abelian group, the composition

$$\mathrm{Hom}\big(M', M''\big) \times \mathrm{Hom}\big(M, M'\big) \to \mathrm{Hom}\big(M, M''\big)$$

  is the bilinear (for the group structures) map defined by

$$(f, g) \mapsto f \cdot g \quad \text{where } (f \cdot g)(x) := f\big(g(x)\big).$$

In particular the group

$$\mathrm{End}(M) := \mathrm{Hom}(M, M)$$

inherits a natural structure of ring.

Remark 1.6 Denoting the image of m under f by $f(m)$ is a convention. It might as well be denoted by $(m)f$. But then the composition (then denoted for example $(f, g) \mapsto f \circ g$) would consist in applying first f then g), and the multiplication in $\mathrm{End}(M)$ would change. How?

Definition 1.7 Let A be a ring.

(1) A (left) A-module is a pair (M, ρ) where

- M is an Abelian group,
- $\rho : A \to \mathrm{End}(M)$ is a (ring) morphism.

We often omit the morphism ρ as we write $ax := \rho(a)(x)$ and view it as a left multiplication by A on M.

(2) A morphism $f : M \to M'$ of A-modules is a group morphism such that $f(ax) = af(x)$ for all $a \in A$ and $x \in M$.

Remark 1.8 A $\mathbb{Z}$-module is nothing but an Abelian group (see below Corollary 1.29). An ideal of $\mathbb{Z}$ (see below Sect. 1.1.3) is nothing but a subgroup.

Exercise 1.9

(1) Prove that the natural structure of $\mathbb{Z}$-module on $\mathbb{Z}/n\mathbb{Z}$ induces a ring isomorphism

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathrm{End}(\mathbb{Z}/n\mathbb{Z}), \quad m \mapsto (x \mapsto mx).$$

(2) Deduce the group isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \quad m \mapsto (x \mapsto mx).$$

Example 1.10 We may consider a ring A as a (left) module over itself, by letting A act on itself by left multiplication.

Then an endomorphism (of A-modules) $f : A \to A$ is determined by $f(1)$, since we must have $f(a) = af(1)$. This defines a bijection between the ring $\mathrm{End}(A)$ of endomorphisms of A and the ring A.

We denote by A^{op} (and call the *opposite ring* of A) the ring defined on the set A by the same additive law and by the multiplication $a \cdot b := ba$. The above bijection $\mathrm{End}(A) \xrightarrow{\sim} A$ is a ring isomorphism

$$\mathrm{End}(A) \xrightarrow{\sim} A^{\mathrm{op}}.$$

Exercise 1.11

(1) Define the notion of right module over a ring A (which we shall call *module-A*).
(2) View A as a module-A through right multiplication. What is the ring of endomorphisms of that module?

1.1.1.5 Polynomials and Power Series

Let A be a ring.

The *polynomial ring in the indeterminate X* over A, denoted $A[X]$, is the set of all formal finite sums (called *polynomials*)

$$P = a_0 + a_1X + \cdots + a_dX^d$$

while the *formal power series ring in the indeterminate* X over A denoted $A[\![X]\!]$, is the set of all formal sums (called *power series*)

$$S = a_0 + a_1 X + \cdots + a_m X^m + \cdots$$

where $a_i \in A$.

We have natural structures of rings on $A[X]$ and $A[\![X]\!]$ defined by the laws

- $(a_0 + a_1 X + \cdots + a_m X^m + \cdots) + (b_0 + b_1 X + \cdots + b_m X^m + \cdots) := a_0 + b_0 + (a_1 + b_1)X + \cdots + (a_m + b_m)X^m + \cdots$,
- $(a_0 + a_1 X + \cdots + a_m X^m + \cdots)(b_0 + b_1 X + \cdots + b_m X^m + \cdots) := a_0 b_0 + (a_1 b_0 + a_0 b_1)X + \cdots + (a_m b_0 + a_{m-1} b_1 + \cdots + a_0 b_m)X^m + \cdots$

Notice that with these laws

- X belongs to the center of $A[X]$ and of $A[\![X]\!]$,
- A is a subring of $A[X]$ and $A[X]$ is a subring of $A[\![X]\!]$.

1.1.1.6 Valuation and Degree

• The *valuation* $\mathrm{val}(P)$ of a nonzero polynomial

$$P = a_0 + a_1 X + \cdots + a_m X^m \in A[X],$$

as well as the valuation $\mathrm{val}(S)$ of a nonzero power series

$$S = a_0 + a_1 X + \cdots + a_m X^m + \cdots \in A[\![X]\!],$$

is the smallest integer i such that $a_i \neq 0$.

• The *degree* $\deg(P)$ of a nonzero polynomial

$$P = a_0 + a_1 X + \cdots + a_m X^m \in A[X]$$

is the largest integer i such that $a_i \neq 0$.

Exercise 1.12 Assume that A has no zero divisor. Let P, Q be nonzero elements of $A[X]$ and let S, T be nonzero elements of $A[\![X]\!]$. Prove that PQ and ST are nonzero and that

$$\mathrm{val}(PQ) = \mathrm{val}(P) + \mathrm{val}(Q),$$
$$\mathrm{val}(ST) = \mathrm{val}(S) + \mathrm{val}(T),$$
$$\deg(PQ) = \deg(P) + \deg(Q).$$

Exercise 1.13 Show that $Z(A[X]) = Z(A)[X]$ and $Z(A[\![X]\!]) = Z(A)[\![X]\!]$.

Exercise 1.14

(1) Show that if A has no zero divisor, then $A[X]^\times = A^\times$.

(!) **Attention** (!) This is false if A has zero divisors.

- One may for example consider the commutative ring

$$A := \left\{ \begin{pmatrix} m & n \\ 0 & m \end{pmatrix} \,\middle|\, m, n \in \mathbb{Z} \right\}$$

and $r = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$. In other words, $A = \{m1_2 + nr \mid m, n \in \mathbb{Z}\}$ and $r^2 = 0$. Then $(1 - rX)(1 + rX) = 1$ which shows that $1 - rX \in A[X]^\times$.

- One may also notice that $(1 + 2X)(1 - 2X) = 1$ in $(\mathbb{Z}/4\mathbb{Z})[X]$.

The reader may read below Proposition 1.117 to see the above examples in a more general context.

(2) Check that for any ring A, we have the following identity in $A[\![X]\!]$:

$$(1 - X)\big(1 + X + X^2 + \cdots + X^n + \cdots\big) = 1,$$

and so that $A[\![X]\!]^\times \neq A^\times$.

Remark 1.15 Power series occur in many areas in Mathematics. Their oldest occurrence is as *generating functions*: if $f : \mathbb{N} \to \mathbb{Z}$ is a function, its associated generating function is the power series $S_f(X) := \sum_{n=0}^{\infty} f(n)X^n$.

The *partition function* $p : \mathbb{N} \to \mathbb{N}$ is defined as follows: $p(0) = 1$, and for $n \in \mathbb{N}$, $n \geq 1$, $p(n)$ is the number of ways n can be expressed as a sum of positive integers. Euler proved the following identity:

$$\sum_{n=0}^{\infty} p(n)X^n = \prod_{n=1}^{\infty} \frac{1}{1 - X^n}.$$

The *Ramanujan function* τ (look for it in the literature) satisfies

$$\sum_{n=1}^{\infty} \tau(n)X^n = X \prod_{n=1}^{\infty} \big(1 - X^n\big)^{24}.$$

1.1.1.7 Euclidean Division

Notice that the following classical result is valid without any assumption about the ring A, which may be commutative or not, an integral domain or not.

Proposition 1.16 (Euclidean division by a monic polynomial) *Let $P(X)$ and $M(X)$ in $A[X]$ such that $M(X)$ is nonzero and monic. There exists a unique pair $(Q(X), N(X))$ of elements of $A[X]$ such that*

(1) $P(X) = Q(X)M(X) + N(X)$,
(2) *either* $N(X) = 0$ *or* $\deg(N(X)) < \deg(M(X))$.

Remarks 1.17

(1) We let the reader check, while reading the following proof, that in the preceding proposition as in its consequences, instead of assuming $M(X)$ *monic* me may as well assume that *the coefficient of the largest degree term of* $M(X)$ *is an invertible element of* A.
(2) Notice that in general $Q(X)M(X)$ is not necessarily equal to $M(X)Q(X)$.

Proof (1) The existence is a consequence of the well known Euclidean algorithm, as sketched below.

We may assume $P(X) \neq 0$ since for $P(X) = 0$ we can choose $Q(X) = N(X) = 0$. If $P(X) \neq 0$ we may assume (which we do from now on) that $\deg(P(X)) \geq \deg(M(X))$, since otherwise we can choose $Q(X) = 0$ and $N(X) = P(X)$. So let us assume $P(X) \neq 0$ and $P(X) = a_n X^n + \cdots + a_0$ with $a_n \neq 0$. Set $M(X) = X^m + b_{m-1}X^{m-1} + \cdots + b_0$, where $n \geq m$. Then we set $P_1(X) = P(X) - a_n X^{n-m} M(X)$ and we see that $\deg(P_1(X)) < \deg(P(X))$. We repeat the same operation as above replacing $P(X)$ by $P_1(X)$ until we get a polynomial which is zero or has degree strictly less than m.

(2) To prove the unicity, it is enough to prove that if $Q(X)M(X) + N(X) = 0$ with either $N(X) = 0$ or $\deg(N(X)) < \deg(M(X))$, then $Q(X) = N(X) = 0$.

Assume $N(X) \neq 0$. We have $Q(X)M(X) = -N(X)$, hence

$$\deg\bigl(Q(X)M(X)\bigr) = \deg\bigl(N(X)\bigr).$$

If $Q(X) \neq 0$, since $M(X)$ is monic, $Q(X)M(X) \neq 0$ and

$$\deg\bigl(Q(X)M(X)\bigr) \geq \deg\bigl(M(X)\bigr),$$

a contradiction to the hypothesis $\deg(N(X)) < \deg(M(X))$. □

For $P(X)$, $P_1(X) \in A[X]$, we say that $P_1(X)$ is a *right divisor* of $P(X)$ in $A[X]$ if there exists $Q(X) \in A[X]$ such that $P(X) = Q(X)P_1(X)$.

The following result, which shows that divisibility by a monic polynomial is an "absolute" property, is an immediate application of Proposition 1.16.

Corollary 1.18 *Let A be a subring of a ring B. Let $P(X), M(X) \in A[X]$, and assume $M(X)$ monic. The following assertions are equivalent.*

(i) *$M(X)$ is a right divisor of $P(X)$ in $A[X]$,*
(ii) *$M(X)$ is a right divisor of $P(X)$ in $B[X]$.*

In order to state (and prove) the following corollary, we make the convention that, if $P(X) = a_n X^n + \cdots + a_1 X + a_0$ and if $\nu \in A$, then $P(\nu) := a_n \nu^n + \cdots + a_1 \nu + a_0$.

(!) Note that in general $a_n \nu^n + \cdots + a_1 \nu + a_0 \neq \nu^n a_n + \cdots + \nu a_1 + a_0$.

Corollary 1.19 *Let $\lambda \in A$ and let $P(X) \in A[X]$.*

(1) *There exists a unique pair $(Q(X), \mu)$ where $Q(X) \in A[X]$ and $\mu \in A$ such that $P(X) = Q(X)(X - \lambda) + \mu$.*
(2) *Whenever $\nu \in A$ commutes with λ,*

$$P(\nu) = Q(\nu)(\nu - \lambda) + \mu.$$

(3) *We have $\mu = P(\lambda)$.*
(4) *$X - \lambda$ is a right divisor of $P(X)$ if and only if $P(\lambda) = 0$.*

Proof (1) is an immediate application of the preceding proposition.

An explicit computation of $Q(X)(X - \lambda)$ proves (2).

(3) is an immediate consequence of (1) and (2), and (4) follows from (1) and (3). □

Exercise 1.20 After having read the section on polynomial rings in several indeterminates (Chap. 1, Sect. 1.4), the reader may check the following complement to the above Corollary 1.19:

(1) Let $D_P(Y, Z) := \frac{P(Y)-P(Z)}{Y-Z}$. Then $D_P(Y, Z) \in A[Y, Z]$.
(2) If $P(X) = Q(X)(X - \lambda) + \mu$, then $Q(X) = D_P(X, \lambda)$.

Remark 1.21 The Cayley–Hamilton theorem may be proved as an application of the preceding Corollary 1.19.

Theorem 1.22 (Cayley–Hamilton) *Let R be a commutative ring, $n \geq 1$ an integer, and $M \in \mathrm{Mat}_n(R)$. Let $\Gamma_M(X) = \det(X1_n - M)$ be the characteristic polynomial of M. Then*

$$\Gamma_M(M) = 0.$$

Sketch of a Proof For $M \in \mathrm{Mat}_n(R)$, $X1_n - M \in \mathrm{Mat}_n(R)[X]$.

Recall that whenever T is a commutative ring and $N \in \mathrm{Mat}_n(T)$, if ${}^t\mathrm{Com}(N)$ denotes the transpose of the matrix whose entries are cofactors of N, then

$$\det(N)1_n = {}^t\mathrm{Com}(N).N.$$

> NOTE. The reader who does not like using the above equality for matrices with entries in a commutative ring which is not necessarily a field may first read below the section about polynomial rings in several indeterminates (Chap. 1, Sect. 1.4).

Let $\Gamma(X) := \det(X1_n - M) \in R[X]$ be the characteristic polynomial of M. Now let $\mathcal{C}_M(X) := {}^t\mathrm{Com}(X1_n - M) \in \mathrm{Mat}_n(R)[X]$. Thus

$$\Gamma(X)1_n = \mathcal{C}_M(X).(X1_n - M),$$

and that identity in $\mathrm{Mat}_n(R)[X]$ implies $\Gamma(M) = 0$ by Corollary 1.19, (3). □

Now we apply the Euclidean division to the notion of multiple roots.

Let R be a commutative ring. Let us start by the notion of *derivative* of an element of $R[X]$.

If $P(X) = a_n X^n + \cdots + a_0 \in R[X]$, its derivative is

$$P'(X) := \frac{dP}{dX} := n a_n X^{n-1} + \cdots + a_1 .$$

If $P(X), Q(X) \in R[X]$, we have

$$\begin{cases} (P+Q)'(X) = P'(X) + Q'(X), \\ (PQ)'(X) = P'(X)Q(X) + P(X)Q'(X). \end{cases}$$

We say that $\lambda \in R$ is a *multiple root* of $P(X)$ if $(X - \lambda)^2$ divides $P(X)$.

Lemma 1.23 *For $P(X) \in R[X]$ and $\lambda \in R$, the following assertions are equivalent.*

(i) *λ is a multiple root of $P(X)$.*
(ii) *$P(\lambda) = P'(\lambda) = 0$.*

Proof If $P(X) = (X - \lambda)^2 Q(X)$, then

$$P'(X) = (X - \lambda)\big((X - \lambda)Q'(X) + 2Q(X)\big),$$

thus (i)⇒(ii).

If $P(X) = (X - \lambda)Q(X)$, then $P'(X) = (X - \lambda)Q'(X) + Q(X)$. Thus if moreover $P'(\lambda) = 0$, we have $Q(\lambda) = 0$, hence $X - \lambda$ divides $Q(X)$. This proves that (ii)⇒(i). □

1.1.2 Canonical Morphisms

1.1.2.1 Prime Ring and Characteristic

The proof of the following proposition is left to the reader.

Proposition 1.24

(1) *Given a ring A, there exists one and only one ring morphism $f_A : \mathbb{Z} \to A$, and that morphism is given by the formula*

$$f_A(n) = \begin{cases} \underbrace{1_A + 1_A + \cdots + 1_A}_{n \text{ times}} & \text{if } n \geq 0, \\ -(\underbrace{1_A + 1_A + \cdots + 1_A}_{-n \text{ times}}) & \text{if } n < 0. \end{cases}$$

(2) *The image of the morphism f_A is contained in the center $Z(A)$ of A.*
(3) *The image of the morphism f_A is the prime subring of A. The prime subring is*

- *either isomorphic to the ring $\mathbb{Z}$,*
- *or isomorphic to the ring $\mathbb{Z}/n\mathbb{Z}$ for some $n > 0$.*

Definition 1.25

- If the prime subring of A is isomorphic to $\mathbb{Z}$, we say that A has *characteristic zero*.
- If the prime subring of A is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some $n > 0$, we say that A has *characteristic n*.

Exercise 1.26 Let $m \geq 2$ and $n \geq 2$ be integers. What is the characteristic of the ring $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$?

Remark 1.27 The following statement is left as an exercise to the reader:

If A has no zero divisor (so in particular if A is a division ring, or an integral domain, or a field), its characteristic is either zero or a prime number.

Exercise 1.28 Let R be a commutative ring with characteristic a prime number p. Prove that the map

$$R \to R, \qquad x \mapsto x^p,$$

is a ring endomorphism of R.

That endomorphism is called the *Frobenius endomorphism*.

In view of Definition 1.7 and the above Proposition 1.24, we get the following corollary (for more details see below Remark 2.2).

Corollary 1.29

(1) *Any Abelian group has one and only one structure of $\mathbb{Z}$-module.*
(2) *Any morphism of Abelian groups is a morphism of $\mathbb{Z}$-modules.*

1.1.2.2 Universal Property of the Polynomial Ring

Again, the proof of the following proposition is left to the reader.

Proposition 1.30

(1) *Given two rings A and B, a morphism $f : A \to B$, and an element $x \in B$ commuting with all elements of the subring $f(A)$, there is one and only one morphism $f_x : A[X] \to B$ which extends f and maps X onto x, given by the formula*

$$f_x : a_0 + a_1 X + \cdots + a_d X^d \mapsto f(a_0) + f(a_1)x + \cdots + f(a_d)x^d.$$

(2) *The image of f_x is the subring of A generated by $f(A)$ and x.*

In particular, considering the case where $B = A$ and f is the identity, given $x \in Z(A)$, there is one and only one morphism $A[X] \to A$ which sends X onto x and induces the identity on A.

That morphism, called the *evaluation morphism*, is denoted

$$P \mapsto P(x).$$

More generally, if A is a subring of B and if $f : A \to B$ is the natural injection, for $x \in B$ commuting with A, the corresponding morphism $A[X] \to B$ is again denoted

$$P \in A[X] \mapsto P(x) \in B.$$

Considering the particular case where $B = A[X]$ and $x = X$, we have

$$P = P(X),$$

a notation which we shall often use.

Assume that B is a *commutative* ring and that A is a subring of B. We see that any $P \in A[X]$ defines a map

$$B \to B, \qquad x \mapsto P(x),$$

called the *polynomial function* on B defined by P.

The following corollary results from Proposition 1.30 and from Proposition 1.24.

Corollary 1.31

(1) *Given a ring A and an element $x \in A$, there exists one and only one morphism $f_{A,x} : \mathbb{Z}[X] \to A$ such that $f_{A,x}(X) = x$.*
(2) *Its image is the subring of A generated by x.*

In view of the corollary above, we say that the ring generated by x is the polynomial ring in x with coefficients in the prime subring of A.

(!) This polynomial ring in x with coefficients in the prime subring of A is not necessarily isomorphic to the polynomial ring over the prime subring—see below.

Exercise 1.32 Let $x = \sqrt{2}$.

(1) Prove that the subring of $\mathbb{R}$ generated by $\sqrt{2}$ satisfies

$$\mathbb{Z}[\sqrt{2}] = \left\{ P(\sqrt{2}) \mid P(X) \in \mathbb{Z}[X] \right\} = \{ m + n\sqrt{2} \mid m, n \in \mathbb{Z} \}.$$

(2) Check that $\mathbb{Z}[\sqrt{2}]$ is not isomorphic to $\mathbb{Z}[X]$.
(3) Prove that the subring of $\mathbb{R}$ generated by $\mathbb{Q}$ and $\sqrt{2}$ is

$$\mathbb{Q}[\sqrt{2}] = \left\{ P(\sqrt{2}) \mid P(X) \in \mathbb{Q}[X] \right\} = \{ \mu + \nu\sqrt{2} \mid \mu, \nu \in \mathbb{Q} \}.$$

(4) Prove that if $\mu + \nu\sqrt{2} \neq 0$ ($\mu, \nu \in \mathbb{Q}$), then it is invertible in $\mathbb{Q}[\sqrt{2}]$ and its inverse is

$$\frac{\mu}{\mu^2 - 2\nu^2} - \frac{\nu}{\mu^2 - 2\nu^2}\sqrt{2}.$$

Deduce that $\mathbb{Q}[\sqrt{2}]$ is a field.

Exercise 1.33 (Decimal numbers) What is the subring of $\mathbb{Q}$ generated by $E := \{1/2, 1/5\}$? Compare with the subring of $\mathbb{Q}$ generated by $1/10$.

1.1.3 Ideals

1.1.3.1 First Definitions

A *left ideal* $\mathfrak{a}$ of a ring A is an additive subgroup of A such that for all $a \in A$ and $x \in \mathfrak{a}$ we have $ax \in \mathfrak{a}$.

A *right ideal* $\mathfrak{a}$ of a ring A is an additive subgroup of A such that for all $a \in A$ and $x \in \mathfrak{a}$ we have $xa \in \mathfrak{a}$.

A twosided ideal is a subset which is both a left and a right ideal.

For a commutative ring, the notions of left, right and twosided ideals coincide and they are then abbreviated *ideal*.

The intersection of any family of left (right, twosided) ideals is a left (right, twosided) ideal.

For E a subset of A, the intersection of all left (right, twosided) ideals containing E is the smallest left (right, twosided) ideal which contains E. It is called the left (right, twosided) *ideal generated by E*.

Examples 1.34

- The left (right, twosided) ideal generated by a singleton $\{a\}$ is denoted by Aa (aA, AaA). ((!) Describe Aa , aA, AaA.) It is called the left (right, twosided) *principal ideal* generated by a.
- Let $\mathfrak{a}$ and $\mathfrak{b}$ two left (right, twosided) ideals of A. We denote by $\mathfrak{a} + \mathfrak{b}$ the ideal generated by $\mathfrak{a} \cup \mathfrak{b}$. We have

$$\mathfrak{a} + \mathfrak{b} = \{x + y \mid x \in \mathfrak{a}, y \in \mathfrak{b}\}.$$

- If $\mathfrak{a}$ and $\mathfrak{b}$ are two twosided ideals of A, we denote by $\mathfrak{a}\mathfrak{b}$ the ideal generated by the set of products xy for $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$.

  (!) **Attention** (!) The ideal $\mathfrak{a}\mathfrak{b}$ is *not* in general the set of all products ab for $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. It is the set of all finite sums $\sum_{i \in I} x_i y_i$ of elements $x_i \in \mathfrak{a}$, $y_i \in \mathfrak{b}$.

Exercise 1.35 Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in a commutative ring R.

(1) Prove that $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subset \mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$.
(2) Deduce that if $\mathfrak{a} + \mathfrak{b} = R$, then $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$.

1.1.3.2 Ideals and Morphisms

If $f : A \to B$ is a morphism, then its kernel $\ker f$ is a twosided ideal of A.

Conversely, any twosided ideal $\mathfrak{a}$ of A is the kernel of a morphism, and even of a surjective morphism.

Indeed, there is a natural structure of ring on the group quotient $A/\mathfrak{a}$ such that the natural surjection $\pi_{\mathfrak{a}} : A \twoheadrightarrow A/\mathfrak{a}$ is a ring morphism and has kernel $\mathfrak{a}$.

Such a pair (B, f) (where B is a ring and $f : A \to B$ is a surjective morphism with kernel $\mathfrak{a}$) is *unique up to unique isomorphism* (we invite the reader to check that this is indeed a consequence of the following proposition)—hence (we invite the reader to explain this "hence") the pair $(A/\mathfrak{a}, \pi_{\mathfrak{a}})$ is *determined* by the property that $\pi_{\mathfrak{a}}$ is surjective and has kernel $\mathfrak{a}$.

Proposition 1.36 *Let $\mathfrak{a}$ be a twosided ideal of A.*

Let (B, f) be a pair where B is a ring and $f : A \twoheadrightarrow B$ is a surjective morphism with kernel $\mathfrak{a}$.

(1) *Let (C, g) be a pair where C is a ring and $g : A \to C$ is a morphism such that $\mathfrak{a} \subset \ker g$. Then there exists a unique morphism $\overline{g} : B \to C$ such that the following diagram is commutative*

$$\begin{tikzcd} & A \arrow[dl, "f"'] \arrow[dr, "g"] & \\ B \arrow[rr, "\overline{g}"] & & C. \end{tikzcd}$$

Moreover

- *$\overline{g}$ is injective if and only if $\ker g = \mathfrak{a}$,*
- *$\overline{g}$ is surjective if and only if g is surjective.*

(2) *In particular (with notation as above), if g is surjective and $\ker g = \mathfrak{a}$, then the morphism $\overline{g}$ is an isomorphism.*

The proof of the above proposition is well-known and left to the reader.

Exercise 1.37 We shall construct an isomorphism

$$\mathbb{Z}/6\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}[i\sqrt{5}]/(1 + i\sqrt{5})\mathbb{Z}[i\sqrt{5}].$$

(1) Here $\mathbb{Z}[i\sqrt{5}]$ is the subring of $\mathbb{C}$ comprised of all complex numbers $m + ni\sqrt{5}$ where $m, n \in \mathbb{Z}$.

Let $\iota : \mathbb{Z} \hookrightarrow \mathbb{Z}[i\sqrt{5}]$ be the natural injection, and let $\overline{\iota} : \mathbb{Z} \to \mathbb{Z}[i\sqrt{5}]/(1 + i\sqrt{5})\mathbb{Z}[i\sqrt{5}]$ be the composition with the natural surjection $\pi : \mathbb{Z}[i\sqrt{5}] \twoheadrightarrow \mathbb{Z}[i\sqrt{5}]/(1 + i\sqrt{5})\mathbb{Z}[i\sqrt{5}]$.

(2) The morphism $\bar{\imath}$ is onto.

HINT: Since $\pi(1+i\sqrt{5})=0$, we have $\pi(i\sqrt{5})=\pi(-1)$, hence

$$\pi(m+ni\sqrt{5})=\pi(m-n)=\bar{\imath}(m-n),$$

which shows that any element of $\mathbb{Z}[i\sqrt{5}]/(1+i\sqrt{5})\mathbb{Z}[i\sqrt{5}]$ belongs to the image of $\bar{\imath}$.

(3) We have $\ker\bar{\imath}=6\mathbb{Z}$.

HINT: $\ker\bar{\imath}$ is the set of all integers k such that $k\in(1+i\sqrt{5})\mathbb{Z}[i\sqrt{5}]$, namely such that there exist $m,n\in\mathbb{Z}$ with $k=(1+i\sqrt{5})(m+ni\sqrt{5})$, or in other words $k=(m-5n)+i(m+n)\sqrt{5}$, hence $m=-n$ and $k\in 6\mathbb{Z}$.

1.1.3.3 Chinese Lemma

Proposition 1.38 (Chinese lemma) *Let $\mathfrak{a}$ and $\mathfrak{b}$ be two twosided ideals of a ring A. We assume that*

$$\mathfrak{a}+\mathfrak{b}=A.$$

Then the diagonal morphism

$$A\to(A/\mathfrak{a})\times(A/\mathfrak{b}),\qquad x\mapsto\big(\pi_{\mathfrak{a}}(x),\pi_{\mathfrak{b}}(x)\big),$$

induces an isomorphism

$$A/(\mathfrak{a}\cap\mathfrak{b})\xrightarrow{\sim}(A/\mathfrak{a})\times(A/\mathfrak{b}).$$

Proof It is clear that the kernel of the diagonal morphism is $\mathfrak{a}\cap\mathfrak{b}$. By Proposition 1.36, it suffices to check that morphism is surjective.

Let $(\pi_{\mathfrak{a}}(x),\pi_{\mathfrak{b}}(y))$ be an arbitrary element of $(A/\mathfrak{a})\times(A/\mathfrak{b})$. By the hypothesis, there are element $a\in\mathfrak{a}$ and $b\in\mathfrak{b}$ such that $a+b=1$. Consider then the element $z:=ay+bx$. It is easy to check that $\pi_{\mathfrak{a}}(z)=\pi_{\mathfrak{a}}(x)$ and $\pi_{\mathfrak{b}}(z)=\pi_{\mathfrak{b}}(y)$, hence that $(\pi_{\mathfrak{a}}(x),\pi_{\mathfrak{b}}(y))$ is the image of z by the diagonal morphism. □

Exercise 1.39 As an application of the Chinese lemma, find an integer n such that

$$n\equiv 2\mod 7\quad\text{and}\quad n\equiv 3\mod 5.$$

Exercise 1.40 Let $\mathfrak{a}$ and $\mathfrak{b}$ be twosided ideals of A.

(1) We recall (see 1.35, (1)) that $\mathfrak{a}\mathfrak{b}\subset\mathfrak{a}\cap\mathfrak{b}$. Give an example where $\mathfrak{a}\mathfrak{b}\neq\mathfrak{a}\cap\mathfrak{b}$.

(2) Assume A commutative. We recall (see 1.35, (2)) that if $\mathfrak{a}+\mathfrak{b}=A$, then $\mathfrak{a}\mathfrak{b}=\mathfrak{a}\cap\mathfrak{b}$.

Explain why the preceding property implies the following statement:

Let m and n two natural integers which are relatively prime. Then their least common multiple equals their product mn.

Exercise 1.41 Generalize the Chinese lemma 1.38 to the situation where one has a finite number $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_s$ of twosided ideals such that $\mathfrak{a}_i + \mathfrak{a}_j = A$ whenever $i \neq j$.

Exercise 1.42 Let $n = p_1^{m_1} \cdots p_s^{m_s}$ be a natural integer, decomposed into a product of powers of pairwise distinct prime numbers.

Construct a ring isomorphism

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{m_s}\mathbb{Z}.$$

1.1.4 Algebras

1.1.4.1 Definitions

The notion of R-algebra defined below is a generalization of the notion of ring (see below Example 1.45, (1)). *What we call* "algebra" *is what is usually called* "associative algebra".

Definition 1.43 Let R be a *commutative* ring. An R-algebra is a pair (A, μ) where

- A is a ring,
- $\mu : R \to Z(A)$ is a ring morphism.

Remarks 1.44

(1) We shall often omit the morphism μ and write λa instead of $\mu(\lambda)a$ for $\lambda \in R$ and $a \in A$.
(2) If R is a field (denoted k), then the morphism μ is injective and k is identified with a subring of $Z(A)$.
(3) Since $Z(A)$ is a subring of the ring of endomorphisms of A as an Abelian group, we see in particular that an R-algebra has a natural structure of R-module (thus in the case where R is a field k, a k-algebra is in particular a vector space over k).

    The reader may check that an R-algebra A is both a ring and an R-module such that

$$\lambda(ab) = (\lambda a)b = a(\lambda b) \quad \text{for all } \lambda \in R \text{ and } a, b \in A.$$

Examples 1.45

(1) Any ring is (in a unique way—why?) a $\mathbb{Z}$-algebra.
(2) If R is a commutative ring,

    - $\mathrm{Mat}_n(R)$ is an R-algebra,
    - $R[X]$ and $R[\![X]\!]$ are R-algebras.

(3) If A is an R-algebra, any subring of A which contains the image of R is naturally an R-algebra (a *subalgebra* of A).
(4) Any ring A is naturally a $Z(A)$-algebra.
(5) If K is a subfield of the field L, then L is naturally a K-algebra.

1.1.4.2 Morphisms

Definition 1.46 Let R be a *commutative* ring and let A and B be R-algebras. An *algebra morphism* $f : A \to B$ is a ring morphism which is R-linear, i.e., such that for all $\lambda \in R$ and $a \in A$ we have $f(\lambda a) = \lambda f(a)$.

Lemma 1.47 *Let $f : A \to B$ be a morphism of R-algebras.*

(1) *The image $f(A)$ of f is an R-subalgebra of B,*
(2) *the kernel* $\ker f$ *is a two sided ideal stable under multiplication by elements of R, and the quotient $A/\ker f$ is an R-algebra isomorphic to $f(A)$.*

The next results are straightforward generalizations of statements in Propositions 1.24 and 1.30.

Proposition 1.48

(1) *Given an R-algebra A, there exists one and only one R-algebra morphism $f_A : R \to A$.*
(2) *Given an R-algebra morphism $f : A \to B$ and an element $x \in B$ which commutes with all the elements of the R-algebra $f(A)$, there exists one and only one R-algebra morphism*

$$f_x : A[X] \to B \quad \textit{such that} \quad f : X \mapsto x.$$

The following definition—an immediate consequence of the fact that $k[X]$ is a principal ideal domain—may be viewed as the analog of the notion of characteristic of a ring (see Definition 1.25).

Definition 1.49 Let k be a field, let A be a k-algebra, and let $x \in A$. Let $k[x]$ denote the k-subalgebra generated by x, i.e., the image of the unique k-algebra morphism $k[X] \to A$ which sends X onto x.

(1) Either for all nonzero $P(X) \in k[X]$ we have $P(x) \neq 0$, and the algebra $k[x]$ is an infinite dimensional k-vector space—then we say that x is *transcendental* over k,
(2) or there is a (unique) monic (nonzero) element $M(X) \in k[X]$ such that the set of $P(X) \in k[X]$ with $P(x) = 0$ is the principal ideal $M(X)k[X]$, and the algebra $k[x]$ is isomorphic to $k[X]/(M(X))$, hence is a k-vector space of dimension $\deg M(X)$—then we say that x is *algebraic* over k, and we call $M(X)$ the *minimal polynomial of x* over k.

Assume the k-algebra A has no zero divisor. Then for $x \in A$ the ring $k[x]$ is an integral domain. It follows that if x is algebraic, its minimal polynomial $M(X)$ is *irreducible*. The next proposition is then immediate.

Proposition 1.50 *Let k be a field, let A be a k-algebra which is an integral domain, and let $x \in A$. Then*

- *either x is algebraic over k, and $k[x]$ is a field,*
- *or x is transcendental over k, and $k[x]$ is not a field (it is then isomorphic to the polynomial algebra $k[X]$).*

Example 1.51 Let us consider the case where $k = \mathbb{Q}$ and $A = \mathbb{C}$.

- The elements $i\sqrt{5}$, $(1+i)\sqrt{2}/2$, and $(1+\sqrt{5})/2$ are algebraic over $\mathbb{Q}$, with minimal polynomial respectively X^2+5, X^4+1, X^2-X-1.
- The element
$$\pi = 4\left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} + \cdots\right)$$
is transcendental over $\mathbb{Q}$ (look in the literature…).

1.1.4.3 Roots of Unity, Cyclotomic Polynomials

Let $\boldsymbol{\mu}(\mathbb{C})$ be the group of all roots of unity in $\mathbb{C}$. For $r \in \mathbb{Q}$ a rational number, we set $\zeta(r) := \exp(2i\pi r)$ so that the map

$$\mathbb{Q} \to \boldsymbol{\mu}(\mathbb{C}), \qquad r \mapsto \zeta(r),$$

induces an isomorphism from the additive group $\mathbb{Q}/\mathbb{Z}$ onto the multiplicative group $\boldsymbol{\mu}(\mathbb{C})$.

If $n \geq 1$ is a natural integer, we set

$$\boldsymbol{\mu}_n := \{\zeta \in \boldsymbol{\mu} \mid \zeta^n = 1\}.$$

Then

$$\boldsymbol{\mu}_n = \{\zeta(m/n) \mid 0 \leq m \leq n-1\},$$

and the map

$$\mathbb{Z} \to \boldsymbol{\mu}_n, \qquad m \mapsto \zeta(m/n),$$

induces an isomorphism from the additive group $\mathbb{Z}/n\mathbb{Z}$ onto the multiplicative group $\boldsymbol{\mu}_n$.

Whenever d divides n, there is a unique subgroup of order d in the additive group $\mathbb{Z}/n\mathbb{Z}$ (resp. the multiplicative group $\boldsymbol{\mu}_n$); moreover, that subgroup is cyclic hence isomorphic to $\mathbb{Z}/d\mathbb{Z}$ (resp. to $\boldsymbol{\mu}_d$).

Let us denote by $\boldsymbol{\mu}_n^0$ the set of all elements of $\boldsymbol{\mu}_n$ with order exactly n. From what precedes it follows that

$$\boldsymbol{\mu}_n = \bigsqcup_{d|n} \boldsymbol{\mu}_d^0. \tag{1.1}$$

Let us recall that the Euler function φ is defined by

$$\begin{aligned}\varphi(n) :&= \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| = \left|\boldsymbol{\mu}_n^0\right| \\ &= \left|\left\{m \;\middle|\; (1 \le m \le n-1)(m \text{ and } n \text{ are relatively prime})\right\}\right|,\end{aligned}$$

and so by (1.1)

$$n = \sum_{d|n} \varphi(d).$$

The next definition and properties of the cyclotomic polynomial are due to Gauß.

Definition 1.52 The n-th cyclotomic polynomial is

$$\Phi_n(X) := \prod_{\zeta \in \boldsymbol{\mu}_n^0} (X - \zeta).$$

Proposition 1.53 *For each integer* $n \ge 1$,

(1) $\Phi_n(X)$ *is monic and* $\deg \Phi_n(X) = \varphi(n)$,
(2) $X^n - 1 = \prod_{d|n} \Phi_d(X)$,
(3) $\Phi_n(X) \in \mathbb{Z}[X]$.

Proof (1) is obvious, and (2) follows immediately from (1.1). Let us prove (3) by induction on n.

We have $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$. Assume that $n > 1$ and that $\Phi_m(X) \in \mathbb{Z}[X]$ for all $m < n$, hence that $\prod_{\substack{d|n \\ d<n}} \Phi_d(X) \in \mathbb{Z}[X]$. By (2) above we see then that $\Phi_n(X)$ is

the quotient of the division of $X^n - 1$ by an integral monic polynomial, hence that $\Phi_n(X) \in \mathbb{Z}[X]$ by Corollary 1.18. □

Examples 1.54

$$\begin{array}{ll}
\Phi_2(X) = X+1 & \Phi_3(X) = X^2+X+1 \\
\Phi_4(X) = X^2+1 & \Phi_5(X) = X^4+X^3+X^2+X+1 \\
\Phi_6(X) = X^2-X+1 & \Phi_7(X) = X^6+X^5+X^4+X^3+X^2+X+1 \\
\Phi_8(X) = X^4+1 & \Phi_9(X) = X^6+X^3+1\ldots
\end{array}$$

The following proposition may be useful to compute some cyclotomic polynomials. Its proof is left as an exercise to the reader.

Exercise 1.55 Prove the following:

Proposition 1.56

(1) *If p is a prime number, then $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$.*
(2) *Changing X into $-X$:*

$$\Phi_n(-X) = \Phi_{2n}(X) \quad \textit{for } n \textit{ odd and } n > 1,$$
$$\Phi_n(-X) = \Phi_n(X) \quad \textit{for } n \textit{ divisible by } 4.$$

(3) *For p a prime number*

$$\begin{cases} \Phi_n\big(X^p\big) = \Phi_n(X)\Phi_{pn}(X) & \textit{if } p \nmid n, \\ \Phi_n\big(X^p\big) = \Phi_{pn}(X) & \textit{if } p \mid n. \end{cases}$$

Exercise 1.57 For $m, n \in \mathbb{N}$, let us set $m = m_n m_{n'}$, where $m_{n'}$ is prime to n, and all the prime numbers which divide m_n are divisors of n. Prove that

$$\Phi_n\big(X^m\big) = \prod_{d \mid m_{n'}} \Phi_{d m_n n}(X)\,.$$

Exercise 1.58 (The values of Φ_d and Φ_e at integers are almost relatively prime) Let $d, e \in \mathbb{N}$, $d \neq e$. Set $d \vee e := \operatorname{lcm}(d, e)$ and $d \wedge e := \gcd(d, e)$.

Let $q \in \mathbb{N}$, and let ℓ be a number which divides both $\Phi_d(q)$ and $\Phi_e(q)$.

(1) From the derivative of the formula $X^{d\vee e} - 1 = \prod_{m \mid d\vee e} \Phi_m(X)$, deduce that there exist $U_{d,e}(X), U_{e,d}(X) \in \mathbb{Z}[X]$ such that

$$U_{d,e}(X)\Phi_d(X) + U_{e,d}(X)\Phi_e(X) = (d \vee e)X^{(d\vee e)-1},$$

hence that ℓ divides $(d \vee e)q^{(d\vee e)-1}$.

(2) Show that there exist $V_d(X), V_e(X) \in \mathbb{Z}[X]$ such that

$$X^{d\wedge e} - 1 = V_d(X)\big(X^d - 1\big) + V_e(X)\big(X^e - 1\big),$$

and deduce that ℓ divides $q^{d\wedge e} - 1$.

(3) Prove that ℓ divides both $d \vee e$ and $q^{d\wedge e} - 1$.

The proof of the following theorem, which shows that $\Phi_n(X)$ is the minimal polynomial of each root of unity of order n, will be given later (see Theorem 1.171).

Theorem 1.59 *For all $n \geq 1$, $\Phi_n(X)$ is irreducible in $\mathbb{Q}[X]$.*

1.1.5 Fields, Division Rings

1.1.5.1 Finite Subgroups of the Multiplicative Group of a Field

Using basic properties of finite cyclic groups, we shall prove the following property.

Proposition 1.60 *Any finite subgroup of the multiplicative group of a field is cyclic.*

Proof Let k be a field, and let G be a finite subgroup of $k^\times$. Assume that G has order $|G| = n$.

For all divisor d of n, let us denote by G_d the set of elements of G of order d. We shall prove that for all $d \mid n$ we have $|G_d| = \varphi(d)$, hence in particular $G_n \neq \emptyset$ and G is cyclic.

Assume $G_d \neq \emptyset$. If $g \in G_d$, the cyclic group $\langle g \rangle$ (of order d) generated by g consists of elements $x \in k$ which satisfy $x^d = 1$. Since the polynomial $X^d - 1$ has at most d roots in (the *commutative* field) k, the elements of $\langle g \rangle$ consist of *all* the roots of $X^d - 1$, so any other element of G_d, being a root of $X^d - 1$, belongs to $\langle g \rangle$. This shows that $|G_d| = \varphi(d)$. In conclusion, we have proved that either $G_d = \emptyset$ or $|G_d| = \varphi(d)$.

But we have $|G| = n = \sum_{d|n} |G_d|$. Since we know that $n = \sum_{d|n} \varphi(d)$, it follows that for all $d \mid n$ we have $|G_d| = \varphi(d)$. □

Example 1.61 If p is a prime number, the group $\mathbb{F}_p^\times$ is cyclic of order $p - 1$.

⚠ This is an existence statement, which does not indicate how to find in practice a generator (i.e., an element of order $p - 1$) of $\mathbb{F}_p^\times$ (*"primitive root problem"*). In fact, this is very hard.

Exercises 1.62

(1) Find all the generators of $\mathbb{F}_{17}^\times$.

Hint: *Notice that* $2^4 = 16\ldots$

(2) Prove that $X^3 - 1$ has exactly 6 zeros in the ring $\mathbb{Z}/91\mathbb{Z}$.

> HINT: *Notice that $\mathbb{Z}/91\mathbb{Z}$ is the product of two fields, hence that the multiplicative group $(\mathbb{Z}/91\mathbb{Z})^\times$ is the product of two cyclic groups.*

Corollary 1.63 *If p is an odd prime, -1 is a square in $\mathbb{F}_p$ if and only if $p \equiv 1 \bmod 4$.*

Proof The (multiplicative) group $\mathbb{F}_p^\times$ is a cyclic group of even order $p - 1$.

Lemma 1.64 *Let G be a cyclic group of order $2n$. Then an element $g \in G$ is a square if and only if $g^n = 1$.*

Proof of Lemma 1.64 If $g = h^2$ for some $h \in G$, then $g^n = h^{2n} = 1$.

Let g_0 be a generator of G, and set $g = g_0^m$. Then if $g^n = 1$, we see that $g_0^{mn} = 1$, so $2n \mid mn$, so $m = 2m'$ and $g = (g_0^{m'})^2$ is a square. □

Thus -1 is a square in $\mathbb{F}_p^\times$ if and only if $(-1)^{(p-1)/2} = 1$, i.e., if and only if $p \equiv 1 \bmod 4$. □

In number theory, the Dirichlet prime number theorem states that for any two positive coprime integers a and t, there are infinitely many primes of the form $a + mt$, where $m \geq 0$. As an application of Lemma 1.64, we shall give now an elementary proof of a particular case of Dirichlet's prime number theorem.

Corollary 1.65 *There are infinitely many primes of the form $4m + 1$.*

Proof We must prove that, given any integer $N > 0$, there is a prime number p such that $p > N$ and $p \equiv 1 \bmod 4$.

Indeed, choose a prime divisor p of $(N!)^2 + 1$. It is clear that $p > N$, and since $N!$ is a square root of -1 in $\mathbb{F}_p$, we see by Lemma 1.64 that $p \equiv 1 \bmod 4$. □

1.1.5.2 Algebraic Extensions

Notation 1.66 If k is a subfield of a field K,

- we say that K is an *extension of* k, or that K/k is a *field extension*,
- K is naturally a k-algebra, and we denote by $[K : k]$ the dimension of K as a k-vector space.
- If $[K : k]$ is finite, we say that K/k is a *finite extension* . If not, we say that the extension is infinite.

The proof of the next result is an easy exercise, left to the reader.

Lemma 1.67 *Let $K \subset L \subset M$ be a tower of field extensions.*

(1) *Let $(l_i)_{i\in I}$ be a basis of L as a K-vector space, and let $(m_j)_{j\in J}$ be a basis of M as an L-vector space. Then $(l_i m_j)_{(i,j)\in I\times J}$ is a basis of M as a K-vector space.*

(2) *In particular*

$$[M:K]=[M:L][L:K].$$

Notice that the equality in the above assertion (2) holds also if one of the extensions is infinite.

Notation 1.68 Let k be a subfield of a field K, and let $x\in K$. We denote by $k(x)$ the *smallest subfield of K containing k and x.*

Recall from Definition 1.49 that, given a subfield k of a field K, an element $x\in K$ is algebraic over k if one of the equivalent conditions is satisfied:

(i) there exists $P(X)\in k[X]$, $P(X)\neq 0$ such that $P(x)=0$,
(ii) $k[x]$ is a field,
(iii) $[k(x):k]<\infty$,

and in that case we have $k(x)=k[x]$.

A consequence of Lemma 1.67 is the following useful result.

Lemma 1.69 *Let K/k be an extension, and $x_1,\dots,x_n\in K$. Let $k(x_1,\dots,x_n)$ denote the subfield of K generated by k and $x_1,\dots,x_n$. The following assertions are equivalent.*

(i) *$x_1,\dots,x_n$ are algebraic over k,*
(ii) *$[k(x_1,\dots,x_n):k]$ is finite.*

Proof (i)⇒(ii). For all $j=1,\dots,n-1$, x_{j+1} is algebraic over $k(x_1,\dots,x_j)$ since it is algebraic over k, which is equivalent to

$$\big[k(x_1,\dots,x_{j+1}):k(x_1,\dots,x_j)\big]<\infty.$$

By Lemma 1.67,

$$\big[k(x_1,\dots,x_n):k\big]=\big[k(x_1,\dots,x_n):k(x_1,\dots,x_{n-1})\big]\cdots\big[k(x_1):k\big],$$

and so $[k(x_1,\dots,x_n):k]<\infty$.

(ii)⇒(i). For all $j=1,\dots,n-1$, $k(x_j)\subset k(x_1,\dots,x_n)$, hence $[k(x_j):k]$ is finite and x_j is algebraic over k. □

We say that a field K is *algebraically closed* if every non constant polynomial with coefficients in K has a root in K.

We assume that the reader knows at least one algebraically closed field: the field $\mathbb{C}$ of complex numbers.

Theorem 1.70 *Let K be an extension of k.*

(1) *The set $K_{\mathrm{alg}/k}$ of elements of K which are algebraic over k is a subfield of K*
(2) *If K is algebraically closed, the field $K_{\mathrm{alg}/k}$ is algebraically closed.*

Proof (1) It suffices to prove that if x and y are algebraic over k, so are $x+y$ and xy. Thus it suffices to prove that all the elements of $k(x,y)$ are algebraic over k. This follows from Lemma 1.69.

Remark 1.71 For a constructive proof of the fact that $x+y$ and xy are algebraic, the reader may have a look at Exercise 1.234 below.

(2) Let $P(X) = a_n X^n + \cdots + a_0 \in K_{\mathrm{alg}/k}[X]$. By assumption, there exists $x \in K$ such that $P(x) = 0$. We shall prove that $x \in K_{\mathrm{alg}/k}$.

By definition, x is algebraic over $k(a_n, \dots, a_0)$, hence

$$\big[k(a_n, \dots, a_0, x) : k(a_n, \dots, a_0)\big] < \infty.$$

Since (by Lemma 1.69) $[[k(a_n, \dots, a_0)] : k] < \infty$, it follows from Lemma 1.67 that $[k(a_n, \dots, a_0, x) : k] < \infty$, which implies $[k(x) : k] < \infty$ and x is algebraic over k. □

Corollary 1.72 *The field $\overline{\mathbb{Q}}$ of all complex numbers which are algebraic over $\mathbb{Q}$ is an algebraically closed field.*

Notice that, since e and π are transcendental numbers (see for example [6], Appendix 1), the field $\overline{\mathbb{Q}}$ is a proper subfield of $\mathbb{C}$.

As an exercise, the reader may use a countability argument to give another proof of the fact that $\overline{\mathbb{Q}} \neq \mathbb{C}$.

1.1.5.3 Extending Fields to Split Polynomials

- Let K be an extension of k, and let x be an element of K which is algebraic over k, so that $k[x] = k(x)$. Let $P(X)$ be its minimal polynomial over k, i.e., the monic generator of the kernel of the natural map $k[X] \to K,\ X \mapsto x$. Then that map induces an isomorphism $k[X]/(P(X)) \xrightarrow{\sim} k[x]$ and $P(X)$ is irreducible.
- Now let $P(X)$ be an irreducible element of $k[X]$. The injection $k \hookrightarrow k[X]$ induces an injection $k \hookrightarrow k[X]/(P(X))$, hence a structure of k-algebra on the field $k_P := k[X]/(P(X))$, showing that k_P is an extension of k.

Let x be the image of X in k_P. We have

(1) $k_P = k[x] = k(x)$,
(2) $P(x) = 0$,
(3) $[k_P : k] = \deg P(X)$.

In other words, we have constructed an extension of k which is *a field generated over k by a root of $P(X)$.*

The existence of such a field is a result of Kronecker:

Proposition 1.73 *Let $P(X)$ be an irreducible element of $k[X]$. Let K_1 and K_2 be extensions of k. Assume that, for $i = 1, 2$,*

- *$P(X)$ has a root x_i in K_i,*
- *$K_i = k(x_i)$.*

Then there is a unique isomorphism from K_1 to K_2

$$\begin{tikzcd}
K_1 \arrow[rr, "\sim"] & & K_2 \\
& k \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

which sends x_1 onto x_2 and induces the identity on k.

Proof Indeed, using the above situation, for $i = 1, 2$ there is a unique isomorphism from $k(x)$ onto $k(x_i)$ which sends x onto x_i and induces the identity on k. □

(!) **Attention** (!) Thus two extensions of k generated by a root of $P(X)$ are isomorphic (both are isomorphic to k_P). But (since such an extension may contains *several* roots of $P(X)$), in general there are several isomorphisms of k-algebras between such fields, and this is precisely the starting point of Galois theory. For example, the identity and the complex conjugation are two different automorphisms of $\mathbb{C} = \mathbb{R}[i]$, field generated over $\mathbb{R}$ by a root of $X^2 + 1$.

(!) **Attention** (!) Let $P(X) \in k[X]$ be irreducible. Assume that K is an extension of k in which $P(X)$ has roots x and y. These roots generate subfields $k(x) = k[x]$

and $k(y) = k[y]$ of K which are isomorphic (by Proposition 1.73 above). But these subfields may be *distinct*.

Consider for example the case $k = \mathbb{Q}$, $P(X) = X^3 - 2$ and $K = \mathbb{C}$. The roots of $P(X)$ in $\mathbb{C}$ are $\{\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}\}$ where $\zeta_3 = \exp(2i\pi/3)$. Then we have (prove it!)

$$\mathbb{Q}\big(\sqrt[3]{2}\big) \cap \mathbb{Q}\big(\zeta_3\sqrt[3]{2}\big) = \mathbb{Q}.$$

Actually, if $x_j = \zeta_3^j\sqrt[3]{2}$ ($j = 0$, 1 or 2) is one of the three roots of $P(X)$, the decomposition of $P(X)$ into a product of irreducible factors over $\mathbb{Q}(x_j)$ is

$$P(X) = (X - x_j)\big(X^2 + x_j X + x_j^2\big).$$

Now consider an element $P(X) \in k[X]$ (not necessarily irreducible). We shall build an extension K of k in which $P(X)$ splits into degree one factors and which is minimal for that property. We will then prove that two such extensions are isomorphic.

Let us argue by induction on $\deg(P)$.

- If $\deg(P) = 1$, we may choose $K = k$.
- Assume $\deg(P) \geq 2$.

Let $Q(X)$ be an irreducible divisor of $P(X)$ in $k[X]$. By what precedes, we know that there exists a field $k_1 = k(x)$ where x is a root of $Q(X)$. Thus there exists $P_1(X) \in k_1[X]$ such that $P(X) = (X - x)P_1(X)$.

Applying the induction hypothesis to the pair $(k_1, P_1(X))$, we see that there exists an extension K of k_1 over which $P_1(X)$ splits into degree one factors. Thus $P(X)$ splits as well into degree one factors over K.

Notice that the subfield of K generated by all the roots of $P(X)$ satisfies the following definition.

Definition 1.74 For $P(X)$ a nonzero element of degree n of $k[X]$, we call *splitting field* of $P(X)$ over k an extension K of k with the following property: there exist $x_1, \ldots, x_n \in K$ such that

(1) $P(X) = \lambda(X - x_1)\cdots(X - x_n)$ for some $\lambda \in k^\times$,
(2) $K = k(x_1, \ldots, x_n)$.

Notice that, given an extension L of k over which $P(X)$ splits into degree one factors, there is a unique subfield of L which is a splitting field of $P(X)$ (namely, the subfield of K generated over k by all the roots of $P(X)$).

For example, let $k = \mathbb{Q}$, $P(X) = X^3 - 2$, $L = \mathbb{C}$. The unique subfield of $\mathbb{C}$ which is a splitting field of $P(X)$ is

$$\mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}\big) = \mathbb{Q}\big(\zeta_3, \sqrt[3]{2}\big).$$

Proposition 1.75 *A splitting field K of $P(X)$ over k has finite degree over k.*

Indeed, it is an immediate consequence of Lemma 1.69.

Theorem 1.76 *Let $P(X) = a_n X^n + \cdots + a_0 \in k[X]$, and let K be a splitting field of $P(X)$. Let $\widetilde{k}$ be a field and let $\phi : k \xrightarrow{\sim} \widetilde{k}$ be a field isomorphism. We set $\widetilde{P}(X) := \phi(P(X)) := \phi(a_n)X^n + \cdots + \phi(a_0)$.*

Let L be an extension of $\widetilde{k}$ in which $\widetilde{P}(X)$ splits into degree one factors.

(1) *There exists at least one morphism $\Phi : K \to L$*

$$\begin{tikzcd} K \arrow[r, "\Phi"] & L \\ k \arrow[u] \arrow[r, "\phi"] & \widetilde{k} \arrow[u] \end{tikzcd}$$

which extends ϕ.

(2) *Such a morphism Φ induces a bijection (preserving multiplicities) between the family of roots of $P(X)$ in K and the family of roots of $\widetilde{P}(X)$ in L.*

Corollary 1.77 *For $P(X) \in k[X]$, let K and L be splitting fields of $P(X)$ over k. Then there exists an isomorphism*

$$\begin{tikzcd} K \arrow[rr, "\simeq"] & & L \\ & k \arrow[ul] \arrow[ur] & \end{tikzcd}$$

from K onto L which induces the identity on k.

Proof of Theorem 1.76 We use induction on the degree $[K : k]$.

Notice that both assertions are immediate if $[K : k] = 1$, since in that case we may choose $\Phi = \phi$.

Now assume $[K : k] > 1$. Thus there exists a root x of $P(X)$ in K which does not belong to k. Let $M(X)$ be its minimal polynomial over k. We have $k(x) \cong k[X]/(M(X))$ and $\deg M(X) = [k(x) : k] > 1$. Then the polynomial $\widetilde{M}(X) := \phi(M(X))$ (a divisor of $\widetilde{P}(X)$) is irreducible in $\widetilde{k}[X]$, and if y denotes one of its roots in L we have $\widetilde{k}(y) \cong \widetilde{k}[X]/(\widetilde{M}(X))$.

It follows (from Proposition 1.73, slightly reformulated—how?) that the isomorphism ϕ may be extended to an isomorphism $\psi : k(x) \xrightarrow{\sim} \widetilde{k}(y)$:

$$\begin{tikzcd}
K & L \\
k(x) \arrow[u] \arrow[r, "\psi"] & \widetilde{k}(y) \arrow[u] \\
k \arrow[u] \arrow[r, "\phi"] & \widetilde{k} \arrow[u]
\end{tikzcd}$$

Now replacing (k, ϕ) by $(k(x), \psi)$ and applying the induction hypothesis and Proposition 1.75 proves the theorem. □

Proof of Corollary 1.77 By Theorem 1.76, there exists at least one morphism $\Phi : K \to L$ which induces the identity on k, and one morphism $\Psi : L \to K$ which induces the identity on k. Both Φ and Ψ are injective (as all morphisms between fields!), and k-linear maps. Since $[K : k]$ and $[L : k]$ are finite (see Proposition 1.75), the injectivity of Φ (resp. of Ψ) implies $[K : k] \leq [L : k]$ (resp. $[K : k] \leq [L : k]$), hence $[K : k] = [L : k]$, proving that both Φ and Ψ are isomorphisms. □

The following proposition is a useful characterization of extensions which are the splitting field of some polynomial.

It may be viewed as a *trade-union like* property: *"one root out, all out!"*

Proposition 1.78 *Let K be a finite extension of k. The following assertions are equivalent.*

(i) *There exists $P(X) \in k[X]$ such that K is the splitting field of $P(X)$ over k.*
(ii) *Whenever $Q(X)$ is an irreducible element of $k[X]$ which has at least one root in K, then $Q(X)$ splits into a product of degree one factors over K.*

Proof (i)⇒(ii).

This follows from the following more general lemma.

Lemma 1.79 *Let K be a splitting field for $P(X)$ over k. Let $Q(X)$ be an irreducible element of $k[X]$. Let x and y be roots of $Q(X)$ in suitable extensions of K. Then*

$$\big[K(x) : K\big] = \big[K(y) : K\big].$$

Proof of Lemma 1.79 By Proposition 1.73, we know that there exists an isomorphism $k(x) \xrightarrow{\sim} k(y)$ which restricts trivially to k. Since $K(x)$ and $K(y)$ are splitting fields of $P(X)$ respectively over $k(x)$ and $k(y)$, it follows from Theorem 1.76 that such an isomorphism can be extended to an isomorphism $K(x) \xrightarrow{\sim} K(y)$:

$$\begin{tikzcd}
K(x) \arrow[rr, "\sim"] \arrow[dd, dash] \arrow[dr, dash] & & K(y) \arrow[dd, dash] \arrow[dl, dash] \\
& K \arrow[dd, dash] & \\
k(x) \arrow[rr] \arrow[dr, dash] & & k(y) \arrow[dl, dash] \\
& k &
\end{tikzcd}$$

Since $K(x)$ and $K(y)$ are isomorphic as k-vector spaces, we have $[K(x) : k] = [K(y) : k]$. Since $[K(x) : k] = [K(x) : K][K : k]$ and $[K(y) : k] = [K(y) : K][K : k]$, it follows that $[K(x) : K] = [K(y) : K]$. □

(ii)⇒(i). Assume that $K = k(x_1, \ldots, x_n)$. For all $j = 1, \ldots, n$, denote by $M_j(X)$ the minimal polynomial of x_j over k. Then obviously K is the splitting field of $M_1(X) \cdots M_n(X)$ over k. □

Definition 1.80 An extension K of k satisfying the properties stated in the preceding Proposition 1.78 is called *a normal extension.*

1.1.5.4 Finite Fields

The next omnibus theorem gives a complete description of finite fields. It shows in particular that there is a bijection between isomorphism classes of finite fields and powers of prime numbers.

Theorem 1.81

(1) *Existence and unicity of finite fields.*

  (a) *Let $\mathbb{F}$ be a finite field with q elements. Then there exist a prime number p and an integer $n \geq 1$ such that $q = p^n$.*
  (b) *Reciprocally, let q be a power of a prime. Then there exists a field with q elements.*
  (c) *Two fields with q elements are isomorphic.*

(2) *Description of finite fields.*
Let $q = p^n$ be a power of a prime and let $\mathbb{F}$ be a field with q elements.

  (a) *The prime subring of $\mathbb{F}$ is $\mathbb{F}_p$ and $[\mathbb{F} : \mathbb{F}_p] = n$.*
  (b) *$\mathbb{F}$ is a splitting field of $X^q - X$ over $\mathbb{F}_p$.*

(c) *There is a bijection between the set of divisors of n and the set of subfields of $\mathbb{F}$ defined by*

$$d \mapsto \mathbb{F}_{p^d} := \left\{ x \in \mathbb{F} \mid x^{p^d} = x \right\},$$

and $\mathbb{F}_{p^d}$ has p^d elements.

(d) *The group* $\mathrm{Aut}(\mathbb{F})$ *of all automorphisms of $\mathbb{F}$ is cyclic of order n, generated by the Frobenius morphism $F : x \mapsto x^p$.*

(e) *The map, from the set of subgroups of* $\mathrm{Aut}(\mathbb{F})$ *to the set of subfields of* $\mathbb{F}$, *which associates to a subgroup H the set* $\mathrm{Fix}^H(\mathbb{F})$ *of elements of $\mathbb{F}$ fixed by H, is an inclusion reversing bijection. Moreover,* $[\mathbb{F} : \mathrm{Fix}^H(\mathbb{F})] = |H|$.

(!) It follows from the above theorem that if $\mathbb{F}$ and $\mathbb{F}'$ are two fields with p^n elements, there is an isomorphism $\mathbb{F} \xrightarrow{\sim} \mathbb{F}'$. But the same theorem shows also that such an isomorphism is in general not unique: there are n such isomorphisms. So, unless $n = 1$, one cannot speak of *the* field with p^n-elements.

Nevertheless, it is customary to denote by $\mathbb{F}_q$ a field with q elements. It is defined up to non unique isomorphisms. . . .

Proof • Let $\mathbb{F}$ be a field with q elements.

Since the prime subring of $\mathbb{F}$ (see Proposition 1.24) cannot be $\mathbb{Z}$ (since $\mathbb{Z}$ is infinite!), it is $\mathbb{F}_p$ for some prime number p. This establishes assertion (2)(a).

Thus $\mathbb{F}$ has a natural structure of $\mathbb{F}_p$-vector space, and it is finite dimensional (since it is finite!). If $n := [\mathbb{F} : \mathbb{F}_p]$ is the dimension of that vector space, it follows that, as vector spaces, $\mathbb{F} \cong \mathbb{F}_p^n$, hence $q = p^n$. This is assertion (1)(a).

The multiplicative group $\mathbb{F}^\times$ is of order $q - 1$, which implies that for all $x \in \mathbb{F}^\times$, $x^{q-1} = 1$. Hence

$$\forall x \in \mathbb{F}, \quad x^q - x = 0.$$

Thus all elements of $\mathbb{F}$ are roots of the polynomial $X^q - X$. Since that polynomial has degree q, it has at most q roots, which shows that $X^q - X$ splits into a product of degree one factors over $\mathbb{F}$—actually,

$$X^q - X = \prod_{\lambda \in \mathbb{F}} (X - \lambda),$$

and this shows indeed that $\mathbb{F}$ is a splitting field of $X^q - X$ over $\mathbb{F}_p$. This is (2)(b).

Since two splitting fields of $X^q - X$ are isomorphic (see Corollary 1.77), that establishes as well assertion (1)(c).

• Now let q be a power of a prime number p. Let us call $\mathbb{F}$ a splitting field of $X^q - X$ over $\mathbb{F}_p$. All roots of $X^q - X$ (in $\mathbb{F}$) are distinct; indeed, the derivative of $X^q - X$ is the constant polynomial -1, which proves that $X^q - X$ has no multiple root. Moreover, it is immediate to check (see Exercise 1.28) that the *set of q roots of* $X^q - X$ in $\mathbb{F}$ is a subfield of $\mathbb{F}$, hence is equal to $\mathbb{F}$. That shows that $\mathbb{F}$ has q elements, and establishes assertion (1)(b).

• Let $\mathbb{F}$ be a field with q elements, where $q = p^n$.

Let $\mathbb{F}'$ be a subfield of $\mathbb{F}$. Since $\mathbb{F}_p$ is the prime subring of $\mathbb{F}$, we have $\mathbb{F}_p \subset \mathbb{F}' \subset \mathbb{F}$. This shows that $\mathbb{F}'$ has p^d elements for some integer $d \geq 1$. But $\mathbb{F}$ is an $\mathbb{F}'$-vector space, of finite dimension, say m, which implies that $q = (p^d)^m$, hence $n = dm$.

Since $\mathbb{F}'$ has p^d elements, the same argument as above shows that $\mathbb{F}'$ is comprised of all the roots of $X^{p^d} - X$ (a subset of the roots of $X^{p^n} - X$ since $d \mid n$). Hence there is only one subfield of $\mathbb{F}$ with p^d elements.

Reciprocally, given a divisor d of n, the set of roots of $X^{p^d} - X$ in $\mathbb{F}$ is a subfield, with p^d elements, of $\mathbb{F}$. This establishes assertion (2)(c).

• The Frobenius endomorphism $F : \mathbb{F} \to \mathbb{F}$, $x \mapsto x^p$, induces the identity on $\mathbb{F}_p$, and it is injective. Hence, since $\mathbb{F}$ is finite, it is an automorphism. Since, for all $x \in \mathbb{F}$, $F^n(x) = x^q$, F^n is the identity on $\mathbb{F}$ hence the order of F divides n. Moreover, the multiplicative group $\mathbb{F}^\times$ is cyclic (see Proposition 1.60), so there exists $x_0 \in \mathbb{F}$ of order $q - 1$, hence $F^d(x_0) \neq x_0$ if $d \mid n$ and $d < n$, which shows that F has indeed order n. In particular, the cyclic group $\langle F \rangle$ generated by F is a subgroup of order n of $\mathrm{Aut}(\mathbb{F})$.

• In order to prove (2)(d), it suffices to prove that $\mathrm{Aut}(\mathbb{F})$ has at most order n.

Since x_0 generates $\mathbb{F}^\times$ as a group, it generates a fortiori $\mathbb{F}$ as a field. Hence $\mathbb{F} = \mathbb{F}_p[x_0]$. In particular, the minimal polynomial $M(X)$ of x_0 over $\mathbb{F}_p$ has degree n, hence it has at most n roots in $\mathbb{F}$ (actually it has exactly n roots: why?). Now an automorphism σ of $\mathbb{F}$ must send the root x_0 of $M(X)$ onto a root of $M(X)$ and it is determined by that root, which proves that $\mathrm{Aut}(\mathbb{F})$ has at most n elements, and establishes (2)(d).

Assume that $n = de$. The (unique) subgroup of order e of $\mathrm{Aut}(\mathbb{F}) = \langle F \rangle$ is generated by F^d, and the set of fixed points under that subgroup is $\{x \in \mathbb{F} \mid x^{p^d} = x\}$, i.e., the (unique) subfield of p^d elements. That establishes assertion (2)(e). □

1.1.5.5 Quaternions

Here we give examples of (noncommutative) division rings, which allow us to check that the conclusion of Proposition 1.60 is false in the noncommutative case.

For $z \in \mathbb{C}$, we denote by z^* its complex conjugate, and we set $|z|^2 := zz^*$.

We say that a subring R of $\mathbb{C}$ is stable under complex conjugation if for all $z \in R$, we have $z^* \in R$.

Exercise 1.82 Give an example of a subfield of $\mathbb{C}$ which is *not* stable under complex conjugation.

HINT: *Consider for example the field* $\mathbb{Q}[\zeta_3 \sqrt[3]{2}]$, *where* $\zeta_3 := \exp(2i\pi/3)$.

Definition 1.83 Let R be a subring of $\mathbb{C}$ which is stable under complex conjugation.

(1) We call *ring of quaternions over* R and we denote by $\mathbb{H}(R)$ the subset of $\mathrm{Mat}_2(R)$ defined as

$$\mathbb{H}(R) := \left\{ q(\alpha, \beta) := \begin{pmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{pmatrix} \,\middle|\, \alpha, \beta \in R \right\}.$$

(2) For $q(\alpha, \beta) = \left(\begin{smallmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{smallmatrix}\right) \in \mathbb{H}(R)$, we set

$$q(\alpha, \beta)^* := q\big(\alpha^*, -\beta\big) = \begin{pmatrix} \alpha^* & -\beta \\ \beta^* & \alpha \end{pmatrix},$$

and, for $q := q(\alpha, \beta)$,

$$N(q) := qq^*.$$

Lemma 1.84

(1) $\mathbb{H}(R)$ *is a subring of* $\mathrm{Mat}_2(\mathbb{C})$.
(2) $\mathbb{H}(R)$ *is commutative if and only if* $R \subseteq \mathbb{R}$.
(3) $\mathbb{H}(R)$ *has a natural structure of* $(R \cap \mathbb{R})$*-algebra*.

Proof (1) results from the formula

$$q(\alpha_1, \beta_1)q(\alpha_2, \beta_2) = q\big(\alpha_1\alpha_2 - \beta_1\beta_2^*, \alpha_1\beta_2 + \beta_1\alpha_2^*\big). \tag{Q}$$

(2) results from formula (Q), and from the particular cases

$$q(0, 1)q(0, z) = q\big(-z^*, 0\big), \qquad q(0, z)q(0, 1) = q(-z, 0).$$

(3) Formula (Q) implies that, for $\lambda \in R \cap \mathbb{R}$,

$$q(\lambda, 0)q(\alpha, \beta) = q(\alpha, \beta)q(\lambda, 0) = q(\lambda\alpha, \lambda\beta). \qquad \square$$

Exercise 1.85 What are $\mathbb{H}(\mathbb{R})$, $\mathbb{H}(\mathbb{Q})$?

The following properties are straightforward.
Here we identify the subring $R1_2$ of $\mathbb{H}(R)$ with R.

Lemma 1.86

(1) *For* $q := \left(\begin{smallmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{smallmatrix}\right) \in \mathbb{H}(R)$ *we have*

$$N(q) = |\alpha|^2 + |\beta|^2.$$

(2) *For* $q, q' \in \mathbb{H}(R)$, *we have*

$$\begin{aligned} \big(qq'\big)^* &= q'^* q^* \\ N\big(qq'\big) &= N(q)N\big(q'\big). \end{aligned}$$

Proposition 1.87

(1) *An element* $q \in \mathbb{H}(R)$ *is invertible if and only if* $N(q) \in R^\times$, *in which case its inverse is* $\frac{q^*}{N(q)}$.

(2) *Let* K *be a subfield of* $\mathbb{C}$, *which is stable under complex conjugation. Then every nonzero element of* $\mathbb{H}(K)$ *is invertible, so*

- *for* $K \subset \mathbb{R}$, $\mathbb{H}(K)$ *is a field,*
- *for* $K \not\subset \mathbb{R}$, $\mathbb{H}(K)$ *is a (non-commutative) division* $(K \cap \mathbb{R})$*-algebra.*

Proof (1) Let $q \in \mathbb{H}(R)$.

If $qq' = 1$, then $N(q)N(q') = 1$ hence $N(q) \in R^\times$.

Reciprocally, if $N(q) \in R^\times$, we have $q\frac{q^*}{N(q)} = 1$, hence q is invertible and its inverse is $\frac{q^*}{N(q)}$.

(2) Since clearly $(q = 0) \Leftrightarrow (N(q) = 0)$, we see that any nonzero element of $\mathbb{H}(K)$ is invertible. □

Remarks 1.88

(1) In 1877, Georg Frobenius proved the following result:

Theorem 1.89 *There are three non isomorphic finite dimensional division* $\mathbb{R}$*-algebras, namely* $\mathbb{R}$, $\mathbb{C}$, *and* $\mathbb{H}(\mathbb{C})$.

(2) in 1905, Joseph Wedderburn proved the following result:

Theorem 1.90 *Any finite division algebra is commutative* (*hence a field*).

1.1.5.6 The Quaternion Group

Let us define the following four elements of $\mathbb{H}(\mathbb{Q}[i])$:

$$\mathbf{1} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \mathbf{i} := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad \mathbf{j} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \mathbf{k} := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Exercise 1.91

(1) Check that

$$\mathbf{ij} = \mathbf{k}, \qquad \mathbf{jk} = \mathbf{i}, \qquad \mathbf{ki} = \mathbf{j},$$
$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}.$$

(2) Deduce that $G := \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ is a noncommutative finite subgroup of order 8 of the multiplicative group of the division algebra $\mathbb{H}(\mathbb{Q}[i])$.

More Exercises on Sect. 1.1

Exercise 1.92 The Möbius function $\mu : \mathbb{N} \to \mathbb{Z}$ is defined recursively by the formulae

$$\begin{cases} \mu(1) = 1 \\ \sum_{d|n} \mu(d) = 0 \quad \text{for } n \geq 2. \end{cases}$$

Let G be an Abelian additive group. For $f : \mathbb{N} \to G$ any map, we define

$$\hat{f}(n) := \sum_{d|n} f(d).$$

(1) Prove that $f(n) = \sum_{d|n} \mu(d)\widehat{f}(n/d)$.

(2) Prove that

$$\mu(n) = \begin{cases} 1 & \text{for } n = 1, \\ 0 & \text{if } n \text{ is divisible by a square,} \\ (-1)^m & \text{if } n \text{ is the product of } m \text{ distinct prime numbers.} \end{cases}$$

(3) Prove that

$$\Phi_n(X) = \prod_{d|n} \left(X^{n/d} - 1\right)^{\mu(d)} \quad \text{and} \quad \varphi(n) = \sum_{d|n} \mu(d)n/d.$$

(4) We recall that $\boldsymbol{\mu}_n^0$ denotes the set of elements of $\mathbb{C}^\times$ of order n. Prove that

$$\sum_{\zeta \in \boldsymbol{\mu}_n^0} \zeta = \mu(n).$$

(5) Prove that

$$\sum_{n=1}^{\infty} \mu(n) \frac{X^n}{1 - X^n} = X.$$

Exercise 1.93 Let R be a commutative ring, and let $P(X) \in R[X]$. Prove that $P(X) - X$ divides $P(P(X)) - X$.

Exercise 1.94 What is the last digit (to the right) of the integer 17^{2006} written in decimal notation?

Exercise 1.95 Let k be the subring of $\mathrm{Mat}_2(\mathbb{F}_5)$ defined by

$$k = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{F}_5 \right\}$$

Prove that k is a field.

Exercise 1.96 Let k be a field, and let $x := \left(\begin{smallmatrix} 1 & -2 \\ 1 & -1 \end{smallmatrix}\right) \in \mathrm{Mat}_2(k)$.

(1) Prove that for $k = \mathbb{Q}$ or $k = \mathbb{F}_3$, the k-subalgebra $k[x]$ of $\mathrm{Mat}_2(k)$ generated by x is a field.
(2) Prove that for $k = \mathbb{C}$ or $k = \mathbb{F}_5$, the k-subalgebra $k[x]$ of $\mathrm{Mat}_2(k)$ generated by x is not an integral domain.

Exercise 1.97

(1) Let $\sigma : \mathbb{R} \to \mathbb{R}$ be a field automorphism of $\mathbb{R}$. Check that σ sends $\mathbb{R}^+$ onto $\mathbb{R}^+$.
(2) Let K be a subfield of $\mathbb{R}$, and let $\sigma : K \to K$ a field automorphism of K. Does σ send $K^+ := K \cap \mathbb{R}^+$ onto K^+?

Exercise 1.98 We consider the following five rings:

$$\mathbb{C}[X]/\big(X^2 + X + 1\big), \qquad \mathbb{R}[X]/\big(X^2 + X + 1\big), \qquad \mathbb{Q}[X]/\big(X^2 + X + 1\big),$$
$$\mathbb{F}_2[X]/\big(X^2 + X + 1\big), \qquad \mathbb{F}_5[X]/\big(X^2 + X + 1\big).$$

Which of these rings are integral domains? Which are fields? Describe the structure of those which are not integral domains.

Exercise 1.99 Let $R := \mathcal{C}^0([0, 1], \mathbb{R})$ be the ring of continuous functions from $[0, 1]$ to $\mathbb{R}$ (endowed with the pointwise addition and multiplication).

(1) Is the ring R an integral domain?
(2) Exhibit a maximal ideal in R.

Exercise 1.100 Let $R := \mathbb{F}_2[X]/(X^6 - 1)$.

(1) Describe all the ideals of R.
(2) How many maximal ideals are there in R?

Exercise 1.101 Let p be a prime number. For any integer n prime to p, the *Legendre symbol* is defined as

$$\left(\frac{n}{p}\right) := \begin{cases} +1 & \text{if } n \text{ is a square in } \mathbb{F}_p, \\ -1 & \text{if } n \text{ is not a square in } \mathbb{F}_p. \end{cases}$$

- Let us denote by $\sigma_n = \mathbb{F}_p \to \mathbb{F}_p$ the permutation of $\mathbb{F}_p$ induced by the multiplication by n, so that $\sigma_n \in \mathfrak{S}(\mathbb{F}_p)$, the symmetric group of the set $\mathbb{F}_p$.
- Let us denote by $\operatorname{sgn} : \mathfrak{S}(\mathbb{F}_p) \to \{\pm 1\}$ the morphism "signature".

Prove that $\operatorname{sgn}(\sigma_n) = (\frac{n}{p})$.

Exercise 1.102 Let $P(X) = X^4 + 1$.

(1) Compute the decomposition of $P(X)$ into a product of degree 2 factors over $\mathbb{R}$.
(2) Prove that $P(X)$ is irreducible over $\mathbb{Q}$.
(3) Compute the decomposition of $P(X)$ into a product of degree 2 factors over $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(i)$.
(4) Prove that if p is an odd prime number, at least one of the following properties holds:

   (a) -1 is a square in $\mathbb{F}_p$,
   (b) 2 is a square in $\mathbb{F}_p$,
   (c) -2 is a square in $\mathbb{F}_p$.

(5) Deduce from (3) and (4) that $P(X)$ is *reducible* in $\mathbb{F}_p[X]$ for any prime number p.
(6) Write decompositions of $P(X)$ over $\mathbb{F}_3[X]$, $\mathbb{F}_5[X]$, $\mathbb{F}_7[X]$.
(7) Here is a hint for yet another proof of (5):

   - for p odd, notice that $p^2 \equiv 1 \bmod 8$;
   - deduce that a splitting extension of $P(X)$ over $\mathbb{F}_p$ has degree at most 2 over $\mathbb{F}_p$;
   - deduce that $P(X)$ is reducible over $\mathbb{F}_p[X]$.

Exercise 1.103 Let $\mathbb{F}_q$ be a finite field with q elements. For any integer $n \geq 1$, let us denote by $\operatorname{Irr}_n \mathbb{F}_q[X]$ the set of irreducible monic polynomials over $\mathbb{F}_q$ of degree n.

(1) Prove that

$$X^{q^n} - X = \prod_{d|n} \prod_{P(X) \in \mathrm{Irr}_d \mathbb{F}_q[X]} P(X).$$

(2) We denote by $I_n(q)$ the number of irreducible monic polynomials over $\mathbb{F}_q$ of degree n. Prove that

$$q^n = \sum_{d|n} d I_d(q).$$

(3) If μ denotes the Möbius function (see Exercise 1.92), prove that

$$I_d(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

Exercise 1.104 Let $n \geq 1$ be an integer. We recall that $\zeta_n = \exp(2i\pi/n)$.

(1) Prove that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\cos(2\pi/n))] \leq 2$.
(2) Prove that $\mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\cos(2\pi/n))$.
(3) Prove that for $n \geq 3$, $[\mathbb{Q}(\cos(2\pi/n)) : \mathbb{Q}] = \varphi(n)/2$.
(4) For which values of n is $\cos(2\pi/n)$ a rational number?

1.2 Prime and Maximal Ideals, Integral Domains

1.2.1 Definition and First Examples

From now on, R denotes a commutative ring.

Definitions 1.105

- An ideal $\mathfrak{p}$ of R is said to be *prime* if the quotient ring $R/\mathfrak{p}$ is an integral domain.
  We denote by $\mathrm{Spec}(R)$ and call *spectrum* of R the set of all prime ideals of R.
- An ideal $\mathfrak{m}$ of R is said to be *maximal* if the quotient ring $R/\mathfrak{m}$ is a field.
  We denote by $\mathrm{Spec}_{\max}(R)$ and call *maximal spectrum* of R the set of all maximal ideals of R.

Examples 1.106

- Any maximal ideal is prime, hence $\mathrm{Spec}_{\max}(R) \subseteq \mathrm{Spec}(R)$.
- All prime ideals but the trivial ideal $\{0\}$ are maximal in both $\mathbb{Z}$ and $k[X]$ (where k is a field)—and more generally if R is a principal ideal domain.
- The principal ideal $(1 + i\sqrt{5})\mathbb{Z}[i\sqrt{5}]$ is not a prime ideal in $\mathbb{Z}[i\sqrt{5}]$ (see Exercise 1.37).

- $2\mathbb{Z}[X]$ is prime but not maximal in $\mathbb{Z}[X]$.

  Indeed, the unique morphism $\mathbb{Z} \to \mathbb{F}_2$ induces the unique morphism between polynomial rings $\mathbb{Z}[X] \to \mathbb{F}_2[X]$ which sends X onto X. The kernel of that morphism is $2\mathbb{Z}[X]$, which establishes the isomorphism $\mathbb{Z}[X]/2\mathbb{Z}[X] \xrightarrow{\sim} \mathbb{F}_2[X]$. That last ring is an integral domain but not a field.

The following characterization of prime ideals is an immediate application of the definition.

Lemma 1.107 *A proper ideal of R is prime if and only if, for all $\lambda, \mu \in R$ such that $\lambda \notin \mathfrak{p}$ and $\mu \notin \mathfrak{p}$, we have $\lambda\mu \notin \mathfrak{p}$.*

The following characterization of maximal ideals justifies their name.

Lemma 1.108 *A proper ideal $\mathfrak{m}$ of R is maximal if and only if, whenever $\mathfrak{a}$ is a proper ideal of R which contains $\mathfrak{m}$, then $\mathfrak{a} = \mathfrak{m}$.*

Proof Indeed, the property described in the above lemma is equivalent to saying that the ring $R/\mathfrak{m}$ has no proper ideal but the trivial one, i.e., that $R/\mathfrak{m}$ is a field. □

We leave to the reader the following important property, whose proof relies on Zorn's Lemma.

Proposition 1.109 *Given any proper ideal $\mathfrak{a}$ of R, there exists a maximal ideal $\mathfrak{m}$ of R which contains $\mathfrak{a}$.*

1.2.2 Examples in Polynomial Rings

1.2.2.1 Generalities

Let $\mathfrak{a}$ be an ideal of R. We denote by $\mathfrak{a}R[X]$ the ideal of $R[X]$ generated by $\mathfrak{a}$. It is immediate to check that

$$\mathfrak{a}R[X] = \left\{a_0 + a_1X + \cdots + a_dX^d \;\middle|\; a_j \in \mathfrak{a}\right\}.$$

The canonical morphism $R \twoheadrightarrow R/\mathfrak{a}$ induces a unique morphism

$$R[X] \twoheadrightarrow (R/\mathfrak{a})[X] \tag{1.2}$$

which sends the indeterminate X onto the indeterminate X. The kernel of that morphism is $\mathfrak{a}R[X]$, which establishes the isomorphism

$$R[X]/\mathfrak{a}R[X] \xrightarrow{\sim} (R/\mathfrak{a})[X]. \tag{1.3}$$

Lemma 1.110

(1) *If* $\mathfrak{p}$ *is a prime ideal of* R, *then* $\mathfrak{p}R[X]$ *is a prime ideal of* $R[X]$.
(2) *If* $\mathfrak{P}$ *is a prime ideal of* $R[X]$, *then* $\mathfrak{P} \cap R$ *is a prime ideal of* R.

Proof (1) results from the preceding isomorphism and from the fact that a polynomial ring over an integral domain is again an integral domain (see Exercise 1.12).

(2) Let $\mathfrak{A}$ be an ideal of $R[X]$. The canonical morphism $\pi_{\mathfrak{A}} : R[X] \twoheadrightarrow R[X]/\mathfrak{A}$ sends R onto a ring isomorphic to $R/R \cap \mathfrak{A}$ and X onto an element x. In particular $R/R \cap \mathfrak{A}$ is isomorphic to a subring of $R[X]/\mathfrak{A}$, and the image of $\pi_{\mathfrak{A}}$ is isomorphic to $(R/R \cap \mathfrak{A})[x]$, an image of $(R/R \cap \mathfrak{A})[X]$.

In particular, if $\mathfrak{P}$ is prime, then $R/R \cap \mathfrak{P}$ is an integral domain, as a subring of the integral domain $R[X]/\mathfrak{P}$. □

Exercise 1.111 Let R be a commutative ring. Prove that $R[X]$ is a principal ideal domain if and only if R is a field.

HINT: *If* $R[X]$ *is a principal ideal domain, note that the ideal generated by* X *is maximal.*

1.2.2.2 Example of Maximal Ideals of $\mathbb{Z}[X]$

Proposition 1.112 *Let* p *be a prime number, let* $P(X) \in \mathbb{Z}[X]$ *be such that its image* $\overline{P}(X) \in \mathbb{F}_p[X]$ *is irreducible. Then the ideal* $p\mathbb{Z}[X] + P(X)\mathbb{Z}[X]$ *of* $\mathbb{Z}[X]$ *generated by* p *and* $P(X)$ *is maximal.*

Proof of Proposition 1.112 We shall use the following lemma.

Lemma 1.113 *Let* $\mathfrak{a}$ *and* $\mathfrak{b}$ *be two ideals of* R, *let* $\pi_{\mathfrak{a}} : R \twoheadrightarrow R/\mathfrak{a}$ *and* $\pi_{\mathfrak{b}} : R \twoheadrightarrow R/\mathfrak{b}$ *be the corresponding canonical morphisms.*

(1) *We have* $\pi_{\mathfrak{a}}(\mathfrak{b}) = (\mathfrak{a} + \mathfrak{b})/\mathfrak{a}$ *and* $\pi_{\mathfrak{b}}(\mathfrak{a}) = (\mathfrak{a} + \mathfrak{b})/\mathfrak{b}$.
(2) *The morphisms* $\pi_{\mathfrak{a}}$ *and* $\pi_{\mathfrak{b}}$ *induce isomorphisms*

$$R/(\mathfrak{a}+\mathfrak{b}) \xrightarrow{\sim} (R/\mathfrak{a})/\pi_{\mathfrak{a}}(\mathfrak{b}) \quad \textit{and} \quad R/(\mathfrak{a}+\mathfrak{b}) \xrightarrow{\sim} (R/\mathfrak{b})/\pi_{\mathfrak{b}}(\mathfrak{a})$$

Proof Lemma 1.113 (1) is left to the reader. (2) results from the fact that the kernel of the natural composed surjective morphism $R \to R/\mathfrak{a} \to (R/\mathfrak{a})/\pi_{\mathfrak{a}}(\mathfrak{b})$ is the inverse image of $\pi_{\mathfrak{a}}(\mathfrak{b})$ in R, namely $\mathfrak{a} + \mathfrak{b}$ by (1). □

Applying the preceding lemma to the particular case where $R = \mathbb{Z}[X]$, $\mathfrak{a} = p\mathbb{Z}[X]$ and $\mathfrak{b} = P(X)\mathbb{Z}[X]$, we see that we have the natural isomorphism

$$\mathbb{Z}[X]/\big(p\mathbb{Z}[X] + P(X)\mathbb{Z}[X]\big) \xrightarrow{\sim} \mathbb{F}_p[X]/\big(\overline{P}(X)\big),$$

which shows that the quotient ring $\mathbb{Z}[X]/(p\mathbb{Z}[X] + P(X)\mathbb{Z}[X])$ is indeed a field. □

Remark 1.114 We shall prove later on (see Theorem–Definition 2.92 and Theorem 2.95) that all the maximal ideals of $\mathbb{Z}[X]$ are of that preceding type.

Exercise 1.115 Let k be a field. Give an example of a maximal ideal in the ring of polynomials in two (commuting) indeterminates $k[X, Y]$.

HINT: *View $k[X, Y]$ as $k[Y][X]$ and use the fact that $k[Y]$, as $\mathbb{Z}$, is a principal ideal domain.*

1.2.3 Nilradical and Radical

1.2.3.1 Definition and Characterizations

Definition 1.116

- The *radical of R*, denoted $\operatorname{Rad}(R)$, is the intersection of all maximal ideals of R, i.e.,
$$\operatorname{Rad}(R) = \bigcap_{\mathfrak{m} \in \operatorname{Spec}_{\max}(R)} \mathfrak{m}.$$
- The *nilradical of R*, denoted $\operatorname{Nil}\operatorname{Rad}(R)$, is the intersection of all prime ideals of R, i.e.,
$$\operatorname{Nil}\operatorname{Rad}(R) = \bigcap_{\mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p}.$$

Thus we have
$$\operatorname{Nil}\operatorname{Rad}(R) \subseteq \operatorname{Rad}(R).$$

Proposition 1.117

(1) $\operatorname{Rad}(R) = \{r \in R \mid (\forall x \in R)(1 - rx \in R^\times)\}$.
(2) $\operatorname{Nil}\operatorname{Rad}(R) = \{r \in R \mid 1 - rX \in R[X]^\times\}$.

Proof We shall use the following lemma.

Lemma 1.118 *The set of nonunits of R coincide with the union of all maximal ideals, i.e.,*
$$R \setminus R^\times = \bigcup_{\mathfrak{m} \in \operatorname{Spec}_{\max}(R)} \mathfrak{m}, \quad \textit{or equivalently} \quad R = R^\times \sqcup \Bigg(\bigcup_{\mathfrak{m} \in \operatorname{Spec}_{\max}(R)} \mathfrak{m} \Bigg)$$

Proof of Lemma 1.118 If $u \in R^\times$, then u cannot belong to a proper ideal of R, so $u \notin \bigcup_{\mathfrak{m} \in \operatorname{Spec}_{\max}(R)} \mathfrak{m}$.

If $a \notin R^\times$, then the ideal generated by a is proper, which implies by Proposition 1.109 that a belongs to a maximal ideal. □

Let us now turn to the proof of Proposition 1.117.

Proof of (1).

- If $r \in \operatorname{Rad}(R)$, then for all $x \in R$ and for all maximal ideals $\mathfrak{m}$ we have $rx \in \mathfrak{m}$, hence $1 - rx \notin \mathfrak{m}$. By Lemma 1.118, this implies that $1 - rx \in R^\times$.
- If $r \notin \operatorname{Rad}(R)$ there exists a maximal ideal $\mathfrak{m}$ such that $r \notin \mathfrak{m}$. Since $R/\mathfrak{m}$ is a field, there exists $x \in R$ such that $rx \equiv 1 \bmod \mathfrak{m}$, i.e., $1 - rx \in \mathfrak{m}$ and so $1 - rx \notin R^\times$.

Proof of (2).

It is a consequence of the following more precise result.

Lemma 1.119 *Let $r \in R$. The following assertions are equivalent.*

(i) *r is nilpotent.*
(ii) $r \in \operatorname{Nil}\operatorname{Rad}(R)$.
(iii) $1 - rX \in R[X]^\times$.

Proof of Lemma 1.119 (i)⇒(ii). Assume r is nilpotent. Then for all prime ideals $\mathfrak{p}$, it results from Lemma 1.107 that $r \in \mathfrak{p}$.

(ii)⇒(iii). Assume $r \in \operatorname{Nil}\operatorname{Rad}(R)$. Then it follows from Lemma 1.110, (2), that $r \in \operatorname{Rad}(R[X])$. So by the first assertion of Proposition 1.117 that we proved above, we see that $1 - rX \in R[X]^\times$.

(iii)⇒(i). Assume that there exist $a_0, a_1, \dots, a_m \in R$ such that

$$(1 - rX)\big(a_0 + a_1X + \cdots + a_mX^m\big) = 1.$$

An immediate computation gives

$$a_0 = 1, \qquad a_1 = r, \qquad a_m = r^m \quad \text{and} \quad r^{m+1} = 0. \qquad \square$$

$\square$

1.2.3.2 Local Rings

Definition 1.120 A (commutative) ring R is said to be *local* if it has only one maximal ideal.

Proposition 1.121 *Let R be a commutative ring. The following assertions are equivalent*:

(i) *R is a local ring.*
(ii) $\operatorname{Rad}(R) = R \setminus R^\times$.
(iii) *$R \setminus R^\times$ is an ideal.*
(iv) *$R/\operatorname{Rad}(R)$ is a field.*

Proof (i)⇒(ii) follows immediately from Lemma 1.118.

(ii)⇒(iii) is obvious.

(iii)⇒(iv). If $R \setminus R^\times$ is an ideal, it is the unique maximal ideal (by Lemma 1.118). Hence we have $\mathrm{Rad}(R) = R \setminus R^\times$, and $\mathrm{Rad}(R)$ is maximal, which implies (iv).

(iv)⇒(i). If (iv) holds, $\mathrm{Rad}(R)$ is maximal, hence it is the unique maximal ideal. □

Examples 1.122

- A field is a local ring.
- Let p be a prime number. We define the subring $\mathbb{Z}_{(p)}$ of $\mathbb{Q}$ by

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \;\middle|\; (a, b \in \mathbb{Z})(p \nmid b) \right\}.$$

  Then $\mathbb{Z}_{(p)}$ is a local ring, whose unique maximal ideal is $p\mathbb{Z}_{(p)}$.
- Let k be a field. Then $k[\![X]\!]$ is a local ring with unique maximal ideal $Xk[\![X]\!]$.

  Indeed, it suffices to check that any element of $k[\![X]\!]$ which does not belong to the ideal generated by X is invertible. Such an element can be written $a_0(1 - XS(X))$ where $a_0 \in k$ ($a_0 \neq 0$) and $S(X) \in k[\![X]\!]$. That element has an inverse which can be computed as

$$a_0^{-1}\big(1 + XS(X) + X^2S(X)^2 + \cdots + X^mS(X)^m + \cdots\big).$$

We shall see below (see Examples 1.132) other examples of local rings.

1.2.3.3 Finite Dimensional Algebras over a Field

Let k be a field.

Notation 1.123 For A a k-algebra, we denote by $[A : k]$ *the dimension of A as a k-vector space.*

Proposition 1.124 *Let R be, either a finite commutative ring, or a finite dimensional commutative k-algebra.*

(1) *Every prime ideal of R is maximal.*
(2) *There is a finite number of prime (maximal) ideals in R.*
(3) *Let* $\mathrm{Spec}(R) = \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s\}$. *For all $i \leq s$, let us set $k_i := R/\mathfrak{p}_i$. Then the diagonal map induces an isomorphism*

$$R/\mathrm{Rad}(R) \xrightarrow{\sim} k_1 \times k_2 \times \cdots \times k_s.$$

Proof We give the proof in the case where R is a finite dimensional k-algebra, the finite case being analogous (and simpler).

(1) will result from the following lemma, applied to the algebra $R/\mathfrak{p}$ for $\mathfrak{p} \in \mathrm{Spec}(R)$.

Lemma 1.125 *A finite dimensional* (*not necessarily commutative*) *k–algebra A which has no zero divisor is a division algebra.*

Proof Let $a \in A, a \neq 0$. The k-linear endomorphism of the k-vector space A defined by $x \mapsto ax$ is injective since its kernel is $\{0\}$. Hence it is surjective, and a has a right inverse. A similar argument shows that a has a left inverse, so a is invertible. □

(2) Let us choose m distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m$ of R. Since each $\mathfrak{p}_i$ is maximal, for $i \neq j$ we have $\mathfrak{p}_i + \mathfrak{p}_j = R$. By the Chinese lemma (see Proposition 1.38, and also Exercise 1.41) we know that the diagonal morphism defines an algebra isomorphism

$$R/(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m) \xrightarrow{\sim} (R/\mathfrak{p}_1) \times \cdots \times (R/\mathfrak{p}_m).$$

Since each $R/\mathfrak{p}_i$ is a k-algebra, it follows that

$$[R:k] \geq \big[R/(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m) : k\big] = \sum_{i=1}^{m} [R/\mathfrak{p}_i : k] \geq m.$$

(3) This is a particular case of what is proved above. □

Remark 1.126 (The noncommutative case) Let A be a finite dimensional (not necessarily commutative) k-algebra.

- One can define the radical $\mathrm{Rad}(A)$ of A as the intersection of all maximal left ideals, which is equal to the intersection of all maximal right ideals.
- One can prove that $\mathrm{Rad}(A)$ is a twosided ideal of A, and that there exist a finite number of division k-algebras $D_1, \ldots, D_s$, and integers $n_1, \ldots, n_s$ such that

$$A/\,\mathrm{Rad}(A) \xrightarrow{\sim} \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_s}(D_s)$$

(see for example [6], Chap. XVII).

1.2.4 Integral Domains, Fields of Fractions

1.2.4.1 Construction of Field of Fractions

If R is a subring of a field K, the subfield F of K generated by R (i.e., the intersection of all subfields of K containing R) is clearly

$$F = \left\{ \frac{a}{b} \,\middle|\, (a \in R)\big(b \in R \setminus \{0\}\big) \right\}.$$

The field F is isomorphic to the field $\mathrm{Frac}(R)$, called *field of fractions of R* defined as follows.

- $\mathrm{Frac}(R) := (R \times R \setminus \{0\})/\sim$, where $\sim$ is the equivalence relation defined by

$$(a,b) \sim (c,d) \quad \Leftrightarrow \quad (ad = bc).$$

- Addition and multiplication are defined (here we denote by $\mathrm{cl}(a,b)$ the equivalence class of $(a,b) \in R \times R \setminus \{0\})$ by

$$\mathrm{cl}(a,b) + \mathrm{cl}(c,d) := \mathrm{cl}(ad + bc, bd),$$
$$\mathrm{cl}(a,b)\,\mathrm{cl}(c,d) := \mathrm{cl}(ac, bd).$$

Now if R is *any* integral domain—which is not a priori contained in a field—, we can build "abstractly" (using only R) the field $\mathrm{Frac}(R)$ as above.

This shows in particular that *any integral domain may be embedded as a subring into a field.*

Examples 1.127

- In some countries, the field $\mathbb{Q}$ is defined (in high school, or in college) as $\mathrm{Frac}(\mathbb{Z})$.
- If k is a field, the field of fractions of $k[X]$ is called the *field of rational fractions in X* and denoted by $k(X)$.

  ⚠ The field $k(X)$ is usually called the *field of rational functions in X*. We prefer here the French terminology (*"corps des fractions rationnelles"*) since, properly speaking, the elements of $k(X)$ are not "functions".

1.2.4.2 Universal Property of the Field of Fractions

We leave the proof of the following characterization to the reader.

Proposition 1.128 *Let R be an integral domain.*

(1) *The natural morphism $\iota : R \to \mathrm{Frac}(R)$ is injective.*

(2) *Let $\sigma : R \hookrightarrow K$ be an injective morphism from R into a field K. Then there is a unique (injective) morphism $\tilde{\sigma} : \mathrm{Frac}(R) \hookrightarrow K$ such that the following diagram is commutative:*

$$\begin{tikzcd} R \arrow[rr, hook, "\iota"] \arrow[dr, hook, "\sigma"] & & \mathrm{Frac}(R) \arrow[dl, hook', "\tilde{\sigma}"'] \\ & K & \end{tikzcd}$$

(3) *If R is contained in a field K, there is one and only one isomorphism from the smallest subfield of K containing R onto $\mathrm{Frac}(R)$, which is the identity on R.*

Examples 1.129

- If R is an integral domain with field of fractions F, the field of fractions of $R[X]$ is $F(X)$.

  Typical argument: Indeed, the field $F(X)$ contains $R[X]$, hence contains its field of fractions. Reciprocally, the field of fractions of $R[X]$ contains R, hence contains the field of fractions of R, namely F; so it contains $F[X]$, hence it contains its field of fractions $F(X)$.
- The field of fractions of $\mathbb{Z}[\sqrt{2}]$ is $\mathbb{Q}[\sqrt{2}]$.
- If the complex number x is transcendental over $\mathbb{Q}$, the field of fractions of $\mathbb{Q}[x]$ is isomorphic to $\mathbb{Q}(X)$.
- Let K be a field. Its *prime subfield* (i.e., its smallest subfield) is the field of fractions of its prime subring. Hence that prime subfield is
  - $\mathbb{F}_p$ if K has characteristic p (for p a prime number),
  - $\mathbb{Q}$ if K has characteristic zero.

Exercise 1.130 Let k be a field and let $u \in k(X)$, $u \notin k$. Prove that the map $X \mapsto u$ induces a k-algebra isomorphism

$$k(X) \xrightarrow{\sim} k(u).$$

1.2.4.3 Localizations

Let R be an integral domain with field of fractions F.

Let S be a nonempty subset of $R \setminus \{0\}$ which is closed under multiplication. We denote by S^{-1} the subset of F defined by

$$S^{-1} := \left\{ \frac{1}{s} \,\middle|\, s \in S \right\}.$$

Notation 1.131 The subring $R[S^{-1}]$ of F generated by R and S^{-1} (in other words, the R-subalgebra of F generated by S^{-1}) is called the localization of R by S and is often denoted $S^{-1}R$. Thus

$$S^{-1}R = \left\{ \frac{a}{s} \,\middle|\, s \in S,\, a \in R \right\}.$$

Notice that $1 = \frac{s}{s}$ for $s \in S$.

Examples 1.132

- Let p be a prime number. The set $S_p := \mathbb{Z} \setminus p\mathbb{Z}$ is stable under multiplication. We have $\mathbb{Z}_{(p)} = S_p^{-1}\mathbb{Z}$, where we recall that

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

- Let k be a field, and let $P(X)$ be an irreducible element of $k[X]$. The set $S_{P(X)} := k[X] \setminus P(X)k[X]$ is stable under multiplication, and we set $k[X]_{P(X)} := S_{P(X)}^{-1}k[X]$, i.e.,

$$k[X]_{(P(X))} = \left\{ \frac{a(X)}{b(X)} \;\middle|\; \big(a(X), b(X) \in k[X]\big)\big(P(X) \nmid b(X)\big) \right\}.$$

- Let $R[\![X]\!]$ be the ring of formal power series over R. The ring of *formal Laurent series* over R is the ring

$$R\big((X)\big) := R[\![X]\!]\left[\frac{1}{X}\right],$$

the localization of $R[\![X]\!]$ at $S = \{X^n \mid n \geq 0\}$.

The reader may check that $\mathbb{Z}_{(p)}$, $k[X]_{(P(X))}$, and $k[\![X]\!]$ are local principal ideal domains.

The following lemma describes ideals of localized rings.

Lemma 1.133 *Let R be an integral domain and let $S \subset R \setminus \{0\}$ be nonempty and multiplicatively stable. For $\mathfrak{a}$ an ideal of R, we set*

$$S^{-1}\mathfrak{a} := \left\{ \frac{a}{s} \;\middle|\; (a \in \mathfrak{a})(s \in S) \right\}.$$

(1) *If $\mathfrak{a}$ is an ideal of R, $S^{-1}\mathfrak{a}$ is an ideal of $S^{-1}R$. It is proper if and only if $\mathfrak{a} \cap S = \emptyset$.*
(2) *For each ideal $\mathfrak{A}$ of $S^{-1}R$, there exists an ideal $\mathfrak{a}$ of R such that $\mathfrak{A} = S^{-1}\mathfrak{a}$.*

Proof The proof of (1) is immediate. Let us prove (2).

Let $\mathfrak{A}$ be an ideal of $S^{-1}R$. Let $\mathfrak{a} := \mathfrak{A} \cap R$. Then $\mathfrak{a}$ is an ideal of R, and since $\mathfrak{a} \subset \mathfrak{A}$, we have $S^{-1}\mathfrak{a} \subset \mathfrak{A}$. Conversely if $\frac{a}{s} \in \mathfrak{A}$, then $s\frac{a}{s} = a \in \mathfrak{A}$, hence $a \in \mathfrak{a}$. □

Proposition 1.134 *Let R be an integral domain and let $\mathfrak{p}$ be a prime ideal of R. The set $S_\mathfrak{p} := R \setminus \mathfrak{p}$ is closed under multiplication (see 1.107), and we set $R_\mathfrak{p} := S_\mathfrak{p}^{-1}R$, i.e.,*

$$R_\mathfrak{p} = \left\{ \frac{a}{b} \;\middle|\; (a, b \in R)(b \notin \mathfrak{p}) \right\}.$$

(1) *Every ideal of $R_\mathfrak{p}$ is of the form $R_\mathfrak{p}\mathfrak{a}$ where $\mathfrak{a}$ is an ideal of R.*
(2) *$R_\mathfrak{p}\mathfrak{a} \neq R_\mathfrak{p}$ if and only if $\mathfrak{a} \subset \mathfrak{p}$.*
(3) *$R_\mathfrak{p}$ is a local ring with unique maximal ideal $\mathfrak{p}R_\mathfrak{p}$.*
(4) *The field $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ is the field of fractions of the integral domain $R/\mathfrak{p}$.*

Proof (1) and (2) are immediate by Lemma 1.133, and (3) follows immediately from (2).

(4) is left as an exercise to the reader. □

Exercise 1.135 Let R be a local principal ideal domain with unique maximal ideal mR. Prove that

$$\mathrm{Frac}(R) = R\left[\frac{1}{m}\right].$$

Exercise 1.136 If k is a field, prove that the ring of Laurent series $k((X))$ is the field of fractions of $k[\![X]\!]$, which contains $k(X)$ (a special case of the previous exercise).

More Exercises on Sect. 1.2

Exercise 1.137 Is the inverse image of a prime (resp. maximal) ideal under a ring morphism still prime (resp. maximal)?

Exercise 1.138

(1) Let R be a commutative ring, and let $\mathfrak{p}$ be a prime ideal of R. Assume that $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of R such that $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$. Prove that if $\mathfrak{a}$ is not contained in $\mathfrak{p}$, then $\mathfrak{b}$ is contained in $\mathfrak{p}$.
(2) Let $\mathfrak{q}$ be an ideal which is *not* prime. Prove that there exist two ideals $\mathfrak{a}$ and $\mathfrak{b}$ such that $\mathfrak{q} \subsetneq \mathfrak{a}$, $\mathfrak{q} \subsetneq \mathfrak{b}$, and nevertheless $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{q}$.

Exercise 1.139 Let R be a commutative ring, and Let p be a prime element of R (i.e., the ideal Rp is prime).

Let $n \in \mathbb{N}$, and let us denote by x the image of X under the canonical morphism from $R[X]$ onto the ring $R[X]/(X^n - p)$.

(1) Prove that R embeds into $R[X]/(X^n - p)$. For x the image of X in $R[X]/(X^n - p)$, we set $R[x] = R[X]/(X^n - p)$ (why is the notation $R[x]$ justified?).
(2) Prove that the ideal $xR[x]$ is prime in $R[x]$

HINT: One may show that the natural morphism $R \to R[x]$ induces an isomorphism $R/pR \xrightarrow{\sim} R[x]/xR[x]$.

Exercise 1.140 Let m and n be two relatively prime integers.

(1) Define a morphism $\mathbb{Z}[X, Y] \to \mathbb{Z}[T]$ with kernel the ideal generated by $X^m - Y^n$.
(2) Deduce that the ideal $(X^m - Y^n)\mathbb{Z}[X, Y]$ is a prime ideal in $\mathbb{Z}[X, Y]$.

Exercise 1.141 Let k be an algebraically closed field of characteristic p. Let $\boldsymbol{\mu}(k)$ be the group of all roots of unity of k.

Prove that there is an isomorphism

$$\boldsymbol{\mu}(k)_{(\times)} \xrightarrow{\sim} (\mathbb{Z}_{(p)}/\mathbb{Z})_{(+)}.$$

Exercise 1.142 Let R be a principal ideal domain with field of fractions F.

(1) Let S be a nonempty multiplicatively closed subset of $R \setminus \{0\}$. Prove that $S^{-1}R$ is a principal ideal domain.
(2) Prove that any subring of F containing R is $R[S^{-1}]$ for some multiplicatively closed subset of $R \setminus \{0\}$.

Exercise 1.143 Let R be a local principal ideal domain which is not a field. Prove that R is a maximal proper subring of its field of fractions.

Exercise 1.144 Let R be an integral domain, with field of fractions F. Let $a \in R$, $a \neq 0$.

(1) Describe the subring $R[a^{-1}]$ of F generated by R and a^{-1}.
(2) For $P(X) \in R[X]$, we define

$$P^*(X) := X^{\deg(P)+\mathrm{val}(P)} P(1/X).$$

Check that

(a) $P^*(X) \in R[X]$,
(b) $P^{**}(X) = P(X)$,
(c) If $P_1(X), P_2(X) \in R[X]$, then

$$\big(P_1(X)P_2(X)\big)^* = P_1(X)^* P_2(X)^*.$$

(3) Let $P(X) \in R[X]$ such that $P(a^{-1}) = 0$. Prove that $P^*(X)$ is divisible (in $R[X]$) by $X - a$, and deduce that $P(X)$ is divisible in $R[X]$ by $aX - 1$.
(4) Define an isomorphism $R[X]/(aX-1) \xrightarrow{\sim} R[a^{-1}]$.

Exercise 1.145 Let R be an integral domain, with field of fractions F. For all $\mathfrak{p} \in \mathrm{Spec}(R)$, we have $R \subset R_{\mathfrak{p}} \subset F$. Prove that

$$R = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} R_{\mathfrak{p}}.$$

1.3 Divisibility and Irreducible Elements

1.3.1 Divisors and Irreducible Elements

From now on, we assume R is an *integral domain*.

- Two elements a and b of R are said to be *associated* if they generate the same ideal, i.e., if there exists $u \in R^\times$ such that $b = ua$.
- One says that *b divides a* if there exists $q \in R$ such that $a = bq$, i.e., if $Ra \subseteq Rb$.

- One says that n elements $a_1, a_2, \ldots, a_n$ are *relatively prime* if the units of R are their only common divisors.
- One says that a is *irreducible* if it is nonzero, non invertible, and if the only divisors of a are the elements of $R^\times$ and the elements ua for $u \in R^\times$.

Remark 1.146 Notice that if the element a is nonzero and generates a prime ideal, then a is irreducible.

The converse is false in general, as shown by the following example.

Example 1.147 Let us first notice that the elements 2 and $1 + \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$.

Indeed, for $m + n\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, let us set

$$N(m + n\sqrt{-5}) = (m + n\sqrt{-5})(m - n\sqrt{-5}) = m^2 + 5n^2 .$$

We see that, for $u \in R$, if $N(u) = 1$ then $u \in R^\times$.

Since $N(2) = 4$, we see that if 2 were reducible, then there would exist $a \in \mathbb{Z}[\sqrt{-5}]$ such that $N(a) = 2$, which is impossible. Since $N(1 + \sqrt{-5}) = 6$, the same argument shows that $1 + \sqrt{-5}$ is irreducible.

The formula $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ shows that $(1 + \sqrt{-5})(1 - \sqrt{-5})$ belongs to the ideal generated by 2. Since neither $1 + \sqrt{-5}$ nor $1 - \sqrt{-5}$ belongs to that ideal, this shows that the ideal generated by 2 is not prime.

In the next definition, we call *"factorial ring"* what is often called *"unique factorization domain"* (abbreviated *UFD*).

Definition 1.148 One says that an integral domain R is *factorial* if

- every element of R is the product of a finite number of irreducible elements,
- if $a = p_1p_2 \cdots p_r = q_1q_2 \cdots q_s$ where all p_i and q_j are irreducible, then $r = s$ and, up to permuting the indices, for all i, p_i and q_i are associated.

The fundamental property of factorial rings known as *Gauß' Lemma* shows that, in such rings, any irreducible element generates a prime ideal. It is an immediate consequence of the above Definition 1.148.

Lemma 1.149 (Gauß' Lemma) *If R is factorial, and if an irreducible element $p \in R$ divides a product ab, then it divides a or b. In other words, any irreducible element generates a prime ideal.*

Example 1.150 The ring $\mathbb{Z}[\sqrt{-5}]$ is not factorial, for example since the element 2, which is irreducible, does not generate a prime ideal. One may also notice that the element $a = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ has two distinct decompositions into products of irreducible elements.

Proposition 1.151 *Any principal ideal domain is factorial.*

Proof Let R be a principal ideal domain.

(1) We first prove that each element of R is a product of irreducible elements.

Let us call “decomposable” an element which is a product of irreducible elements. If there exists a non decomposable element a which is nonzero and not invertible, such an element is not irreducible, hence is the product of a non decomposable element a_1 by a non invertible element b_1. Replacing a by a_1 we get $a_1 = a_2 b_2$ where a_2 is non decomposable and b_2 is non invertible. Going on this way we build an infinite sequence (a_n) of non decomposable elements, such that the sequence of ideals Ra_n is strictly increasing.

But there is no strictly increasing sequence $(\mathfrak{a}_n)$ of ideals in a principal ideal domain.

Indeed, the ideal $\mathfrak{a} := \bigcup_n \mathfrak{a}_n$ is principal, hence is generated by an element a. There exists N such that $a \in \mathfrak{a}_N$, hence $\mathfrak{a} = \mathfrak{a}_N$ and $\mathfrak{a}_{N+1} = \mathfrak{a}_N$, which is a contradiction.

(2) To prove the unicity of decomposition, we let the reader check that it suffices to prove that R satisfies the conclusion of Gauß’ Lemma, i.e., that if an irreducible element $p \in R$ divides a product ab, then p divides a or b.

If p does not divide a, the ideal generated by a and p is R (for it is Rd, where d divides a and divides p, hence is invertible), and so there exist α and $\lambda \in R$ such that $\alpha a + \lambda p = 1$. Now if p does not divide b, there exist β and $\mu \in R$ such that $\beta b + \mu p = 1$. It follows that $1 = \alpha\beta ab + (\lambda\beta b + \alpha a\mu + \lambda\pi p)p$, which proves that p cannot possibly divide ab. □

1.3.2 Euclidean Rings

1.3.2.1 Definition and First Properties

An integral domain R is said to be *Euclidean* if there exists a map $N : R \to \mathbb{N}$ with the following properties:

- For $a \in R$, we have $N(a) = 0 \Leftrightarrow a = 0$,
- for all $a, b \in R \setminus R^\times$ and $b \neq 0$, there exist q and r such that $a = bq + r$ and $N(r) < N(b)$.

Examples 1.152

- $\mathbb{Z}$ is Euclidean, with $N(n) = |n|$.
- If k is a (commutative) field, $k[X]$ is Euclidean, with $N(P(X)) = \deg(P(X)) + 1$ if $P(X) \neq 0$, and $N(0) = 0$.

  Indeed, this results from Proposition 1.16.

- The Gauß ring $\mathbb{Z}[i]$ is Euclidean, with $N(m+ni) := m^2 + n^2$.

  [Notice first (make a picture) that for all $z \in \mathbb{C}$ there exists an element $q \in \mathbb{Z}[i]$ such that $N(z-q) \leq 1/2$. Then for a and b in $\mathbb{Z}[i]$ with $b \neq 0$, let q be such that $N(a/b - q) \leq 1/2$, and set $r := a - bq$. It is clear that $N(r) \leq N(b)/2 < N(b)$.]

Remarks 1.153 The quotient and the remainder are unique in the case where $R = k[X]$ (k a field), but they are unique neither for $\mathbb{Z}$ nor $\mathbb{Z}[i]$ (give examples!).

Exercise 1.154 Prove that for k a field $k[\![X]\!]$ is Euclidean.

The following proposition is well known and its proof is left to the reader.

Proposition 1.155 *Any Euclidean ring is a principal ideal domain*

The following property of Euclidean rings is sometimes useful to prove that a given ring is *not* Euclidean.

Lemma 1.156 *If R is a Euclidean ring there exists an irreducible element m such that every nonzero element of R/mR is the image of a unit.*

Proof If R is a field, we may choose $m = 0$. Assume that R is not a field, and choose $m \notin R^\times$, $m \neq 0$, such that $N(m)$ is minimal. Then whenever $a \in R$, we have $a = mq + r$ with $N(r) < N(m)$, hence $r = 0$ or $r \in R^\times$ by minimality of m. This implies that R/mR is a field, hence that m is irreducible. □

Remark 1.157 Here are some possible choices for m in the usual cases:

- For $R = \mathbb{Z}$, one may take $m = 2$,
- for $R = k[X]$ (k a field), one may choose $m = X$,
- for $R = \mathbb{Z}[i]$, on may choose $m = 1 - i$.

1.3.2.2 Various Examples with Quadratic Extensions of $\mathbb{Z}$

- We have already seen that $\mathbb{Z}[\sqrt{-5}]$ is not factorial.

Let m be an integer not divisible by a square. We call *ring of integers* (see Corollary 2.75) of the field $\mathbb{Q}[\sqrt{m}]$ the ring $\mathbb{Z}[\omega_m]$ where

$$\omega_m := \begin{cases} \sqrt{m} & \text{if } m \equiv 2 \text{ or } -1 \mod 4, \\ \frac{1+\sqrt{m}}{2} & \text{if } m \equiv 1 \mod 4. \end{cases}$$

As we shall see, a complex number z is said to be an (algebraic) integer if it is the root of a monic polynomial with coefficients in $\mathbb{Z}$. One may notice that

- for $m \equiv 2$ or $-1 \bmod 4$, ω_m is a root of $X^2 - m$,
- for $m \equiv 1 \bmod 4$, ω_m is a root of $X^2 - X + \frac{1-m}{4}$.

Thus

- the ring of integers of $\mathbb{Q}[\sqrt{-5}]$ is $\mathbb{Z}[\sqrt{-5}]$,
- the ring of integers of $\mathbb{Q}[\sqrt{-3}]$ is $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$,
- the ring of integers of $\mathbb{Q}[\sqrt{-19}]$ is $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$.

One can prove (check the literature!) the following theorem:

Theorem 1.158

(1) *For $d \geq 1$, the ring of integers of $\mathbb{Q}[\sqrt{-d}]$ $(d > 0)$ is a principal ideal domain if and only if*

$$d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

(2) *For $m \in \mathbb{Z} \setminus \{0\}$, the ring of integers of $\mathbb{Q}[\sqrt{m}]$ is Euclidean if and only if*

$$m \in \{-1, \pm 2, \pm 3, 5, 6, \pm 7, \pm 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

(3) *The ring $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a principal ideal domain but is not Euclidean.*

1.3.3 GCD and LCM

1.3.3.1 About Factorial Rings

For all pairs of elements a and b in a factorial ring R, there exist

- an element denoted $a \wedge b$, called the *gcd* (*"greatest common divisor"*) of a and b, characterized (up to association) by the following condition: an element of R divides both a and b if and only if it divides $a \wedge b$,
- an element denoted $a \vee b$, called the *lcm* (*"least common multiple"*) of a and b, characterized (up to association) by the following condition: an element of R is a multiple both of a and b if and only if it is a multiple of $a \vee b$.

Indeed, if

$$a = \prod_p p^{v_p(a)} \quad \text{and} \quad b = \prod_p p^{v_p(b)}$$

are the prime factorizations, we have

$$a \wedge b = \prod_p p^{\min(v_p(a), v_p(b))} \quad \text{and} \quad a \vee b = \prod_p p^{\max(v_p(a), v_p(b))}.$$

Notice that two elements a and b are relatively prime if and only if $a \wedge b = 1$.

(!) **Attention** (!) If the ideals Ra and Rb satisfy the "Bézout relation" $Ra + Rb = R$, then a and b are relatively prime. The converse is false in general (if the ring R is not a principal ideal domain). Thus the elements 2 and X are relatively prime in $\mathbb{Z}[X]$, but the ideals they generate respectively do not satisfy the "Bézout relation" (prove it!).

Lemma 1.159 *In the following statements, equalities are "up to associates".*

(1) *We have* $(a \wedge b)(a \vee b) = ab$.
(2) *Set* $a = (a \wedge b)a_1$ *and* $b = (a \wedge b)b_1$. *Then* a_1 *and* b_1 *are relatively prime, and we have* $a \vee b = ab_1 = a_1 b$.

1.3.3.2 About Principal Ideal Domains

Let R be a principal ideal domain. The gcd and the lcm of two elements a and b are characterized by the following conditions:

- $R(a \wedge b) = Ra + Rb$,
- $R(a \vee b) = Ra \cap Rb$.

Two elements a and b of R are relatively prime if and only if ("property of Bézout") there exist $\lambda, \mu \in R$ such that $1 = \lambda a + \mu b$.

1.3.3.3 About Euclidean Rings: Euclid's Algorithm

Let us describe how to compute the gcd of two nonzero elements a and b in a Euclidean ring through a finite number of divisions.

Let us set $x_0 := a$, $x_1 := b$. We denote by x_2 the remainder of the Euclidean division of x_0 by x_1. Then we denote

- by x_3 the remainder of the Euclidean division of x_1 by x_2,
- by x_4 the remainder of the Euclidean division of x_2 by x_3,

and so on.

Since for all $n \geq 2$, either $x_n = 0$ or $N(x_n) < N(x_{n-1})$, there exists an integer $m \geq 0$ such that $x_m \neq 0$ and $x_{m+1} = 0$.

Then x_m is a gcd of a and b.

Indeed, it is immediate that the ideal generated by (a, b) is equal to the ideal generated by (x_1, x_2), which in turn is equal to the ideal generated by (x_2, x_3), etc., hence equal to the ideal generated by x_m.

1.3.4 Case of $\mathbb{Z}[i]$ and Application

We recall that the ring of Gauß integers is the ring generated by i, i.e., the ring

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

For $z = a + bi \in \mathbb{Z}[i]$, let us set $N(z) := zz^* = (a + bi)(a - bi) = a^2 + b^2$; we see that N is a multiplicative map from $\mathbb{Z}[i]$ to $\mathbb{N}$, i.e., $N(zz') = N(z)N(z')$. It follows that if an element u of $\mathbb{Z}[i]$ is invertible (in $\mathbb{Z}[i]$), then $N(u)$ is invertible (in $\mathbb{Z}$), hence $N(u) = 1$, and so $u \in \{1, -1, i, -i\}$. Since conversely the elements ± 1 and $\pm i$ are clearly invertible, we have the equality

$$\mathbb{Z}[i]^\times = \{1, -1, i, -i\}.$$

Remark 1.160 The finite Abelian (multiplicative) group $\mathbb{Z}[i]^\times$ is isomorphic to the additive group $\mathbb{Z}/4\mathbb{Z}$.

Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[i]$. The natural injection $\varphi : \mathbb{Z} \hookrightarrow \mathbb{Z}[i]$, composed with the canonical surjection $\mathbb{Z}[i] \twoheadrightarrow \mathbb{Z}[i]/\mathfrak{p}$, provides a ring morphism $\mathbb{Z} \longrightarrow \mathbb{Z}[i]/\mathfrak{p}$ with kernel $\mathfrak{p} \cap \mathbb{Z}$. The prime subring of $\mathbb{Z}[i]/\mathfrak{p}$ is then isomorphic to $\mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z})$.

If $\mathfrak{p} \neq \{0\}$, we have $\mathfrak{p} \cap \mathbb{Z} \neq \{0\}$, for if z is a nonzero element of $\mathfrak{p}$, $N(z)$ is a nonzero element of $\mathfrak{p} \cap \mathbb{Z}$. It follows that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime number p.

Theorem 1.161 *Let p be a prime number. The following assertions are equivalent.*

(i) *p is a reducible element of $\mathbb{Z}[i]$.*
(ii) *There exist two integers a and b such that $p = a^2 + b^2$.*
(iii) *-1 is a square in $\mathbb{Z}/p\mathbb{Z}$.*
(iv) *$p = 2$ or $p \equiv 1 \bmod 4$.*

If the above assertions are true, then there exists an irreducible element $\pi \in \mathbb{Z}[i]$ such that $p = \pi\pi^*$.

Proof (i)⇒(ii): Assume p reducible in $\mathbb{Z}[i]$, i.e., assume that there exist two non invertible elements z and z' of $\mathbb{Z}[i]$ such that $p = zz'$. We have then $p^2 = N(z)N(z')$ and since neither $N(z)$ nor $N(z')$ is invertible, we deduce $N(z) = N(z') = p$. If we set $z = a + bi$, we then see that $p = a^2 + b^2$.

(ii)⇒(iii): If $p = a^2 + b^2$, since neither a nor b is divisible by p, a and b are invertible modulo p and we have the following equality in $\mathbb{Z}/p\mathbb{Z}$: $-1 = (ab^{-1})^2$.

(iii)⇔(i): The following two isomorphisms

$$\mathbb{Z}[X]/\big(X^2 + 1, p\big) \xrightarrow{\sim} \mathbb{Z}[i]/(p)$$

$$\mathbb{Z}[X]/\big(X^2 + 1, p\big) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})[X]/\big(X^2 + 1\big)$$

show that $\mathbb{Z}[i]/(p)$ is an integral domain if and only if $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2 + 1)$ is an integral domain, in other words that p is irreducible in $\mathbb{Z}[i]$ if and only if $X^2 + 1$ is irreducible in $(\mathbb{Z}/p\mathbb{Z})[X]$.

(iii)⇔(iv): This is Corollary 1.63.

If p is reducible, it follows from what precedes that there exists $z \in \mathbb{Z}[i]$ such that $N(z) = p$. Thus we have $p = zz^*$, and z is irreducible since its norm is irreducible in $\mathbb{Z}$. □

Example 1.162 We have $13 = 3^2 + 2^2$, $61 = 6^2 + 5^2$. What about the prime number $p = 49993$?

Exercise 1.163 Prove that the irreducible elements of $\mathbb{Z}[i]$ are (up to units)

(1) the prime integers p such that $p \equiv 3 \bmod 4$,
(2) the elements $m + in$ such that $m^2 + n^2$ is prime in $\mathbb{Z}$.

1.3.5 Irreducibility Criteria in $R[X]$

In what follows, we denote by R an integral domain, with field of fractions F.

Definition 1.164 Let $P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ be a nonzero element of $R[X]$. One says that $P(X)$ is *primitive* if it has degree at least 1 and if its coefficients are relatively prime.

We denote by $\operatorname{Prim} R[X]$ the set of primitive polynomials of $R[X]$.

1.3.5.1 Primitive and Irreducible Polynomials

Notice that the irreducible elements of R are also irreducible in $R[X]$.

Indeed, a nonzero element a of R (a degree 0 element of $R[X]$) can only decompose in $R[X]$ into degree 0 elements.

Proposition 1.165

(1) *Every irreducible element of degree at least* 1 *of* $R[X]$ *is primitive.*
(2) *If* $P(X) \in \operatorname{Prim} R[X]$ *and if* $P(X)$ *is irreducible in* $F[X]$, *then it is irreducible in* $R[X]$.

ⓘ **Attention** ⓘ Notice that the element $2X$ is irreducible in $F[X]$, but not irreducible in $R[X]$.

Proof of Proposition 1.165

(1) If $P(X)$ is not primitive, there exists a non invertible element $a \in R$ (hence non invertible in $R[X]$) and a polynomial $P_1(X) \in R[X]$ of degree at least 1 (hence non invertible in $R[X]$) such that $P(X) = aP_1(X)$. Thus, $P(X)$ is not irreducible in $R[X]$.
(2) If $P(X)$ is primitive, and if it is equal to a product of two non invertible elements of $R[X]$, these two elements have both nonzero degrees—so $P(X)$ is reducible in $F[X]$. □

From now on, we denote by $\operatorname{Irr} R$ the set of irreducible elements of a ring R.

Let us in particular emphasize the following general inclusion:

$$\operatorname{Irr} R \sqcup \big(\operatorname{Prim} R[X] \cap \operatorname{Irr} F[X]\big) \subseteq \operatorname{Irr} R[X].$$

We shall see later (see Theorem 1.175) that if R is factorial that inclusion is an equality.

1.3.5.2 Reduction Modulo a Prime Ideal

Proposition 1.166 *Let $P(X) \in \operatorname{Prim} R[X]$, and let $\mathfrak{p}$ be a prime ideal of R which does not contain the coefficient of the highest degree term of $P(X)$, i.e., if $\overline{P}(X)$ denotes the image of $P(X)$ in $(R/\mathfrak{p})[X]$, $\deg \overline{P}(X) = \deg P(X)$.*

Then if $\overline{P}(X)$ is irreducible in $(R/\mathfrak{p})[X]$, $P(X)$ is irreducible in $R[X]$.

Remark 1.167 The example of $R = \mathbb{Z}$, $P(X) = 2X$ and $\mathfrak{p} = 3\mathbb{Z}$ shows that the hypothesis of primitivity is necessary.

Proof of Proposition 1.166 Assume $P(X)$ reducible in $R[X]$: we have $P(X) = P_1(X)P_2(X)$, where $P_1(X)$ and $P_2(X)$ are two non invertible elements of $R[X]$. It follows that $\overline{P}(X) = \overline{P}_1(X)\overline{P}_2(X)$; since $\overline{P}(X)$ is irreducible, it follows that one of the two factors, for example $\overline{P}_1(X)$, is invertible, hence is of degree zero. We see then that $\overline{P}_2(X)$ has same degree as $\overline{P}(X)$, hence as $P(X)$; consequently $P_2(X)$ has same degree as $P(X)$. Hence $P_1(X)$ has degree zero, which is a contradiction since $P(X)$ is primitive. □

Example 1.168 The polynomial $X^2 + Y^2 + 1$ is irreducible in $\mathbb{R}[X, Y]$.

Indeed, viewed as an element of $\mathbb{R}[X][Y]$, it is monic (hence in particular primitive), and by reducing modulo the prime ideal of $\mathbb{R}[X]$ generated by X, it becomes the irreducible polynomial $Y^2 + 1 \in \mathbb{R}[Y]$.

(!) **Attention** (!) One can prove that the polynomial $X^4 + 1$ is irreducible in $\mathbb{Z}[X]$ but is reducible in $\mathbb{F}_p[X]$ for all prime numbers p (see Exercise 1.102).

1.3.5.3 Case of $R[X]$ for R Factorial

In what follows, we denote by R a factorial ring, with field of fractions F. We shall describe the irreducible elements of $R[X]$, and prove that $R[X]$ is also factorial.

Proposition 1.169 (Gauß' Lemma again) *Let $P(X) \in R[X]$, of degree at least 2. Assume that $P(X)$ is reducible in $F[X]$ and that $P(X) = P_1(X)P_2(X)$ with $P_1(X), P_2(X) \in F[X]$, both of degree at least 1. Then there exist $\lambda_1, \lambda_2 \in F$ such that*

- *both $\lambda_1 P_1(X)$ and $\lambda_2 P_2(X)$ belong to $R[X]$,*
- *$P(X) = (\lambda_1 P_1(X))(\lambda_2 P_2(X))$.*

In particular, $P(X)$ is reducible in $R[X]$.

Proof Multiplying both sides of the equality $P(X) = P_1(X)P_2(X)$ by the product of denominators of nonzero coefficients of $P_1(X)$ and $P_2(X)$, we get

$$aP(X) = \big(bP_1(X)\big)\big(cP_2(X)\big) \tag{f}$$

where $a, b, c \in R$ and $aP(X), bP_1(X), cP_2(X) \in R[X]$.

If a is not invertible, let us choose a prime number p which divides a, and let us set $a = pa_1$. Through the canonical morphism $R[X] \twoheadrightarrow (R/pR)[X]$, the preceding equality becomes

$$0 = \overline{bP}_1(X)\overline{cP}_2(X).$$

Since $(R/pR)[X]$ is an integral domain, we see that one of the two factors—for example $\overline{bP}_1(X)$—is zero. In that case p divides $bP_1(X)$, hence $bP_1(X) = pb_1P_1(X)$ with $b_1P_1(X) \in R[X]$.

Thus, we have replaced the equality (f) by the equality

$$a_1P(X) = \big(b_1P_1(X)\big)\big(cP_2(X)\big) \tag{f_1}$$

where there are strictly less irreducible factors in a decomposition of a_1 than in a decomposition of a.

Repeating that process, we get to the case where a is invertible, which proves Gauß' lemma. □

Corollary 1.170 *Let $P(X) \in R[X]$ be monic of degree at least 2. Assume that $P(X) = P_1(X)P_2(X)$ with $P_1(X), P_2(X) \in F[X]$ and assume that $P_1(X)$ and $P_2(X)$ are monic.*

Then $P_1(X), P_2(X) \in R[X]$.

Proof By Proposition 1.169, we know that there exist $\lambda_1, \lambda_2 \in F$ such that $P(X) = \lambda_1 P_1(X)\lambda_2 P_2(X)$ and $\lambda_1 P_1(X), \lambda_2 P_2(X) \in R[X]$.

By monicity of $P_i(X)$ (for $i = 1, 2$), the coefficient of the highest degree term of $\lambda_i P_i(X)$ is λ_i, which implies $\lambda_i \in R$. By monicity of $P(X)$, we see that $\lambda_1\lambda_2 = 1$, so $\lambda_1, \lambda_2 \in R^\times$. Thus $P_i(X) = \lambda_i^{-1}(\lambda_i P_i(X)) \in R[X]$. □

As an application of the preceding corollary (applied to the case where $R = \mathbb{Z}$), we can now prove the irreducibility of the cyclotomic polynomials.

Theorem 1.171 *For each natural integer $n \geq 1$, the cyclotomic polynomial $\Phi_n(X)$ is irreducible in $\mathbb{Q}[X]$.*

Proof Let ζ be a root of unity of order n, and let $P(X)$ be the monic minimal polynomial of ζ over $\mathbb{Q}$. Then, since $P(X)$ divides $X^n - 1$ in $\mathbb{Q}[X]$, it follows from Corollary 1.170 that $P(X)$ is a monic element of $\mathbb{Z}[X]$.

We shall prove that $P(X) = \Phi_n(X)$, and for that purpose, we shall prove that, whenever ζ' has order n, then $P(\zeta') = 0$.

Since $\zeta' = \zeta^m$ where m is prime to n, it is enough to prove that, for all primes p $(1 \leq p \leq n-1)$ which do not divide n, we have $P(\zeta^p) = 0$.

Assume that this is not the case, i.e., $P(\zeta^p) \neq 0$. We shall then find a contradiction.

Let $Q(X)$ be the monic minimal polynomial of ζ^p over $\mathbb{Q}$ (again a monic element of $\mathbb{Z}[X]$). Thus $Q(\zeta^p) = 0$ and $Q(X) \neq P(X)$.

Thus there exists $R(X) \in \mathbb{Z}[X]$ such that $X^n - 1 = P(X)Q(X)R(X)$.

Since the polynomial $Q(X^p)$ vanishes at $X = \zeta$, we see that $P(X)$ divides $Q(X^p)$ (in $\mathbb{Q}[X]$, hence in $\mathbb{Z}[X]$). Denoting by $\overline{P}(X)$ and $\overline{Q}(X)$ the images of $P(X)$ and $Q(X)$ through the natural reduction morphism $\mathbb{Z}[X] \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})[X]$, we see that $\overline{P}(X)$ divides $\overline{Q}(X^p)$. Since $\overline{Q}(X^p) = \overline{Q}(X)^p$ (see Exercise 1.28), it follows that $\overline{P}(X)$ divides $\overline{Q}(X)^p$, and so $\overline{P}(X)$ and $\overline{Q}(X)$ are not relatively prime.

The derivative of the relation $X^n - 1 = P(X)Q(X)R(X)$ shows the existence of $P_1(X), Q_1(X) \in \mathbb{Z}[X]$ such that

$$nX^{n-1} = P(X)P_1(X) + Q(X)Q_1(X), \quad \text{hence}$$
$$\overline{n}X^{n-1} = \overline{P}(X)\overline{P}_1(X) + \overline{Q}(X)\overline{Q}_1(X),$$

which implies that the only possible common divisors of $\overline{P}(X)$ and $\overline{Q}(X)$ in $(\mathbb{Z}/p\mathbb{Z})[X]$ are powers of X. But X does not divide $X^n - 1$, hence does not divide $\overline{P}(X)$. Thus we have found a contradiction and $P(\zeta^p) = 0$, which establishes Theorem 1.171. □

We are now going to formalize Gauß' Lemma 1.169, and reprove it by using the convenient notions of content and of primitive part.

1.3.5.4 Content and Primitive Part

The following lemma will be used.

Lemma 1.172 *If R is factorial, the product of two primitive elements of $R[X]$ is still primitive.*

Proof Let $P_1(X), P_2(X) \in \operatorname{Prim} R[X]$. If there exists an irreducible element $p \in R$ which divides $P_1(X)P_2(X)$, we see (applying the morphism $R[X] \twoheadrightarrow (R/pR)[X]$, and since $(R/pR)[X]$ is an integral domain) that p must divide one of the factors $P_1(X)$ or $P_2(X)$, which is impossible. □

Proposition 1.173 *Let $P(X) \in F[X]$, $P(X) \neq 0$.*

(1) *There exists a pair*

$$\big(c(P), \mathrm{pr}(P)(X)\big) \quad \textit{where } c(P) \in F \textit{ and } \mathrm{pr}(P)(X) \in R[X],$$

unique up to multiplication by (u, u^{-1}) *where* $u \in R^{\times}$, *such that*

$$P(X) = c(P)\,\mathrm{pr}(P)(X) \quad \textit{and} \quad \mathrm{pr}(P)(X) \quad \textit{is primitive.}$$

(2) *We have the following equivalences*:

$$\begin{aligned} P(X) \in R[X] \quad &\Longleftrightarrow \quad c(P) \in R \\ P(X) \in \mathrm{Prim}\, R[X] \quad &\Longleftrightarrow \quad c(P) \in R^{\times}. \end{aligned}$$

(3) *Let* $P(X), Q(X) \in F[X]$. *Then*

$$c(PQ) = c(P)c(Q) \quad \textit{and} \quad \mathrm{pr}(PQ)(X) = \mathrm{pr}(P)(X)\,\mathrm{pr}(Q)(X).$$

The scalar $c(P)$ (defined up to multiplication by an invertible element of R) is called the *content* of $P(X)$. The polynomial $\mathrm{pr}(P)(X)$ (defined up to multiplication by an invertible element of R) is called the *primitive part* of $P(X)$.

Proof Proof of (1)

Existence. There exists $\lambda \in R \setminus \{0\}$ such that $\lambda P(X) \in R[X]$. We denote by d a gcd of the coefficients of $\lambda P(X)$, and we define $c(P) := d/\lambda$, then define $\mathrm{pr}(P)(X)$ by the equality $\lambda P(X) = d\,\mathrm{pr}(P)(X)$.

Unicity. Assume $P(X) = \lambda_1 P_1(X) = \lambda_2 P_2(X)$, where $\lambda_1, \lambda_2 \in F^{\times}$ and where $P_1(X)$ and $P_2(X)$ are primitive in $R[X]$. We may replace $P(X)$ by a multiple by an element of R, and so we may assume that λ_1 and λ_2 belong to R, hence that $P(X) \in R[X]$. Then we see that λ_1 and λ_2 are gcd's of the coefficients of $P(X)$, hence are associated.

(2) is clear.

(3) We have $P(X) = c(P)\,\mathrm{pr}(P)(X)$ and $Q(X) = c(Q)\,\mathrm{pr}(Q)(X)$ hence $P(X)Q(X) = c(P)c(Q)\,\mathrm{pr}(P)(X)\,\mathrm{pr}(Q)(X)$, and it suffices to prove that $\mathrm{pr}(P)(X)\,\mathrm{pr}(Q)(X)$ is primitive, which is Lemma 1.172. □

The following corollary is nothing but a reformulation of Gauß' Lemma 1.169 using the notions of content and primitive part. We leave the proof to the reader.

Corollary 1.174

(1) *Let* $P(X) \in R[X]$ *be a primitive polynomial, and assume* $P(X) = P_1(X)P_2(X)$ *where* $P_1(X), P_2(X) \in F[X]$. *Then*

$$P(X) = \mathrm{pr}(P_1)(X)\,\mathrm{pr}(P_2)(X).$$

(2) *Assume* $P(X) \in R[X]$, $\deg P(X) \geq 1$, *and* $P(X) = P_1(X)P_2(X)$ *where* $P_1(X), P_2(X) \in F[X]$. *Then*

$$P(X) = \big(c(P)\,\mathrm{pr}(P_1)(X)\big)\big(\mathrm{pr}(P_2)(X)\big),$$

and $c(P)\,\mathrm{pr}(P_1)(X)$, $\mathrm{pr}(P_2)(X) \in R[X]$, *with*

$$c(P)\,\mathrm{pr}(P_1)(X) = \lambda_1 P_1(X) \quad \textit{where } \lambda_1 = \frac{c(P)}{c(P_1)},$$

$$\mathrm{pr}(P_2)(X) = \lambda_2 P_2(X) \quad \textit{where } \lambda_2 = \frac{1}{c(P_2)}.$$

Theorem 1.175 *Let R be a factorial domain, with field of fractions F.*

(1) $\mathrm{Irr}\, R[X] = \mathrm{Irr}\, R \cup (\mathrm{Prim}\, R[X] \cap \mathrm{Irr}\, F[X])$.
(2) $R[X]$ *is factorial.*

Proof of 1.175 (1) We know that $\mathrm{Irr}\, R \cup (\mathrm{Prim}\, R[X] \cap \mathrm{Irr}\, F[X]) \subseteq \mathrm{Irr}\, R[X]$. It is clear that a degree 0 irreducible element of $R[X]$ belongs to $\mathrm{Irr}\, R$. We also know that if $P(X) \in \mathrm{Irr}\, R[X]$ has degree at least 1, then $P(X) \in \mathrm{Prim}\, R[X]$.

It remains to prove that such an element $P(X)$ belongs also to $\mathrm{Irr}\, F[X]$. If not, then $P(X) = P_1(X)P_2(X)$ where $P_1(X), P_2(X) \in F[X]$ have degrees at least 1. By Corollary 1.174, (1), we have $P(X) = \mathrm{pr}(P_1)(X)\,\mathrm{pr}(P_2)(X)$, hence $P(X) \notin \mathrm{Irr}\, R[X]$, a contradiction.

(2) Let $P(X) \in R[X]$. We have $P(X) = c(P)\,\mathrm{pr}(P)(X)$; we decompose $c(P)$ into a product of irreducibles in R, and $\mathrm{pr}(P)$ into a product of irreducibles of $F[X]$, then (by Corollary 1.174, (1)) into a product of irreducibles of $R[X]$, and so we have gotten a decomposition of $P(X)$ into a product of irreducibles of $R[X]$.

We are left with proving the unicity of the decomposition into products of irreducible elements: this results from the unicity of the decomposition $P(X) = c(P)\,\mathrm{pr}(P)(X)$, and from the unicity of the decomposition both in R and in $F[X]$. □

1.3.5.5 Example–Exercise: The Decimal Numbers

Notice that $\mathbb{D} := \mathbb{Z}[1/10]$ is the ring of decimal numbers.

Lemma 1.176 *The morphism $\mathbb{Z}[X] \twoheadrightarrow \mathbb{D}$ which sends X to $1/10$ induces an isomorphism*

$$\mathbb{Z}[X]/(10X - 1) \xrightarrow{\sim} \mathbb{D}.$$

Proof of 1.176 Notice that Exercise 1.144 provides a proof in a general context. Here we provide a proof using our formulation of Gauß' Lemma.

It is clear that the kernel of the morphism $\mathbb{Z}[X] \twoheadrightarrow \mathbb{D}$ which sends X to $1/10$ contains the ideal generated by $10X - 1$.

Let us prove that conversely if $P(X) \in \mathbb{Z}[X]$ is such that $P(1/10) = 0$, then $P(X)$ is divisible (in $\mathbb{Z}[X]$) by $10X - 1$.

Since $1/10$ is a root of $P(X)$ in $\mathbb{Q}$, we know that $P(X)$ is divisible (in $\mathbb{Q}[X]$) by $X - 1/10$. By Lemma 1.174, (2), we see that $P(X)$ is divisible in $\mathbb{Z}[X]$ by $\mathrm{pr}(X - 1/10)$, which is equal to $10X - 1$. □

Exercise 1.177 Prove that the ring $\mathbb{D}$ is Euclidean.

1.3.5.6 An Application: Automorphisms of $k(X)$

Here we denote by k a (commutative) field.

Lemma 1.178 *Let $P(X, Y) \in k[X, Y]$ be an element of the following type*:

$$P(X, Y) = a(X)Y + b(X)$$

where $a(X), b(X) \in k[X]$.

Then the element $P(X, Y)$ is irreducible in $k[X, Y]$ if and only if

- *either $a(X) = 0$ and $b(X)$ is irreducible in $k[X]$,*
- *or $a(X) \neq 0$ and then $a(X) \wedge b(X) = 1$.*

Proof Indeed, it suffices to note by Theorem 1.175 that $P(X, Y)$ is irreducible in $k[X, Y]$ if and only if

$$a(X)Y + b(X) \in \mathrm{Irr}\, k[X] \sqcup \big(\mathrm{Prim}\, k[X][Y] \cap \mathrm{Irr}\, k(X)[Y]\big)$$

and to notice that, if $a(X) \neq 0$, the polynomial $a(X)Y + b(X)$ is irreducible (since it has degree 1) in $k(X)[Y]$. □

Proposition 1.179 *Let $u \in k(X)$, $u \notin k$. We write $u = \frac{a(X)}{b(X)}$, where $a(X)$ and $b(X)$ are relatively prime.*

(1) *The element X is algebraic over the field $k(u)$.*
(2) *Its minimal polynomial is $P(Y) := a(Y) - ub(Y) \in k(u)[Y]$.*
(3) *Viewed as a $k(u)$-vector space, the field $k(X)$ has dimension*

$$\big[k(X) : k(u)\big] = \max\big\{\deg a(X), \deg b(X)\big\}.$$

Proof (1), (2): X is a root of the polynomial $P(Y) := a(Y) - ub(Y) \in k(u)[Y]$, hence is algebraic, and its minimal polynomial is $P(Y)$ by Lemma 1.178.

(3) follows from the fact that $\max\{\deg a(X), \deg b(X)\}$ is the degree of $P(Y)$. □

Let us denote by $\mathrm{Aut}(k(X)/k)$ the *automorphism group of the extension $k(X)/k$*, that is, the set of all automorphisms of the field $k(X)$ viewed as a k-algebra.

Let us denote by $\mathrm{GL}_2(k)$ the group of units of $\mathrm{Mat}_2(k)$, i.e.,

$$\mathrm{GL}_2(k)=\left\{\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\,\middle|\,(\alpha,\beta,\gamma,\delta\in k)(\alpha\delta-\beta\gamma\neq 0)\right\}$$

and by $\mathrm{PGL}_2(k)$ the quotient of $\mathrm{GL}_2(k)$ by its center

$$Z\big(\mathrm{GL}_2(k)\big)=\left\{\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}\,\middle|\,\lambda\in k^\times\right\}.$$

Proposition 1.180 *The map*

$$\begin{aligned}\sigma:\mathrm{GL}_2(k)&\longrightarrow \mathrm{Aut}\big(k(X)/k\big)\\ g=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}&\mapsto\quad \sigma(g)=\left(f(X)\mapsto f\left(\frac{\alpha X+\beta}{\gamma X+\delta}\right)\right),\end{aligned}$$

induces a group isomorphism

$$\mathrm{PGL}_2(k)\xrightarrow{\sim}\mathrm{Aut}\big(k(X)/k\big).$$

Proof It is easy to check that for $g\in\mathrm{GL}_2(k)$, the maps $\sigma(g)$ and $\sigma(g^{-1})$ are inverse maps, so that σ is indeed a morphism from $\mathrm{GL}_2(k)$ into $\mathrm{Aut}(k(X)/k)$. Moreover, the kernel of σ is clearly $Z(\mathrm{GL}_2(k))$. Let us prove that any element of $\mathrm{Aut}(k(X)/k)$ is $\sigma(g)$ for some $g\in\mathrm{GL}_2(k)$. The image of X under an automorphism of $k(X)$ is $u=\frac{a(X)}{b(X)}$, where $a(X)$ and $b(X)$ are relatively prime. Since we have $k(u)=k(X)$ it follows from Proposition 1.180 that

$$\max\big\{\deg a(X),\deg b(X)\big\}=1,$$

and since $a(X)=\alpha X+\beta$ and $b(X)=\gamma X+\delta$ are relatively prime, we have $\alpha\delta-\beta\gamma\neq 0$. □

1.3.5.7 Eisenstein Criterion

Proposition 1.181 (Eisenstein criterion) *Let R be a factorial ring with field of fractions F, let $P(X)=a_dX^d+a_{d-1}X^{d-1}+\cdots+a_0$ be an element of degree d of $R[X]$, and let p be an irreducible element of R such that*

- *p does not divide a_d,*
- *p divides a_k for all $k<d$,*
- *p^2 does not divide a_0.*

Then $P(X)$ is irreducible in $F[X]$. Moreover, if $P(X)$ is primitive, it is irreducible in $R[X]$.

Proof of 1.181 If $P(X)$ is reducible in $F[X]$, it is equal to a product of two polynomials with degrees respectively d_1 and d_2 at least 1, and we know by Gauß' Lemma 1.169 that $P(X) = P_1(X)P_2(X)$ where $P_1(X)$ and $P_2(X)$ are two elements of $R[X]$ with degrees respectively d_1 and d_2 at least 1. Reducing modulo p, we get

$$\overline{a}_d X^d = \overline{P}_1(X)\overline{P}_2(X).$$

Viewing the preceding equality as written in the ring $L[X]$ where L denotes the field of fractions of the integral domain R/pR, we see (since that ring is factorial) that $\overline{P}_1(X) = X^e$ and $\overline{P}_2(X) = X^f$. It follows that the constant terms $P_1(0)$ and $P_2(0)$ are divisible by p, hence that $a_0 = P(0) = P_1(0)P_2(0)$ is divisible by p^2, which is contrary to the hypothesis. □

Application 1.182 For each integer d there are infinitely many irreducible polynomials of degree d in $\mathbb{Q}[X]$.

Indeed, for all integers $d \geq 1$ and all prime numbers p, the polynomial $X^d - p$ satisfies the hypothesis of Eisenstein criterion.

(!) **Attention** (!) In $\mathbb{R}[X]$, all polynomials of degree at least 3 are reducible. Thus the polynomial $X^4 + 1$ is *reducible* in $\mathbb{R}[X]$—note that nevertheless it has no roots in $\mathbb{R}$.

1.3.5.8 More on Irreducible Elements in $k[X]$

Again we denote by k a commutative field.

We first give a criterion of irreducibility which is sometimes useful.

Proposition 1.183 *Let $P(X) \in k[X]$ be an element of degree $d \geq 1$. The following assertions are equivalent.*

(i) *$P(X)$ is irreducible in $k[X]$.*
(ii) *Whenever K is an extension of k such that $[K : k] \leq d/2$, $P(X)$ has no root in K.*

Proof (i)⇒(ii): Assume that $P(X)$ is irreducible in $k[X]$, and that it has a root x in K. Then $k[x] \subseteq K$ and $[k[x] : k] = d$, so $[K : k] \geq d$.

(ii)⇒(i): Assume that $P(X)$ is reducible, i.e., $P(X) = P_1(X)P_2(X)$ where $\deg P_1(X) \leq d/2$ or $\deg P_2(X) \leq d/2$. If for example $\deg P_1(X) \leq d/2$, and if $Q(X)$ is an irreducible divisor of $P_1(X)$ in $k[X]$, then the extension $k_Q = k[X]/(Q(X))$ of k contains a root of $P(X)$ and has degree $\leq d/2$. □

The next result concerns the roots of an irreducible polynomial in an extension. We shall come back later (see Sect. 1.3) to that type of question ("separability").

Proposition 1.184 *Let $P(X) \in k[X]$ be irreducible. Whenever K is an extension of k, $P(X)$ has no multiple root in K, unless*

(1) *k is an infinite field of characteristic $p > 0$, and*
(2) *there exists $Q(X) \in k[X]$ such that $P(X) = Q(X^p)$.*

Proof Let $P'(X)$ be the derivative of $P(X)$. If $P'(X) \neq 0$, we have $\deg P'(X) < \deg P(X)$, hence $P'(X)$ cannot be divisible by $P(X)$, which implies that $P'(X)$ and $P(X)$ are relatively prime. Thus there exist $U(X), V(X) \in k[X]$ such that $U(X)P(X) + V(X)P'(X) = 1$, and we see that $P(X)$ and $P'(X)$ cannot have a common root, i.e., $P(X)$ has no multiple root.

An immediate computation shows that we can have $P'(X) = 0$ only if k has nonzero characteristic p and if there exists $Q(X) \in k[X]$ such that $P(X) = Q(X^p)$.

It remains to prove that k must be infinite. This follows from the next lemma, which shows in particular that a polynomial of the type $Q(X^p)$ cannot be irreducible over a finite field.

Lemma 1.185 *Let R be a finite commutative ring of characteristic $p > 0$ (in other words, a finite commutative $\mathbb{F}_p$-algebra).*

(1) *The Frobenius endomorphism*

$$R \to R, \qquad x \mapsto x^p,$$

is an $\mathbb{F}_p$-algebra endomorphism of R.
(2) *For $Q(X) \in R[X]$, there exists $Q_1(X) \in R[X]$ such that $Q(X^p) = Q_1(X)^p$.*

Proof of Lemma 1.185 (1) The Frobenius map is clearly $\mathbb{F}_p$-linear. It is a ring morphism (see Exercise 1.28).

(2) If $Q(X) = b_e X^e + \cdots + b_1 X + b_0$, by (1) there exist $c_0, c_1, \ldots, c_e \in R$ such that, for all j, $b_j = c_j^p$. Then if $Q_1(X) := c_e X^e + \cdots + c_1 X + c_0$, applying the Frobenius map gives $Q_1(X)^p = Q(X^p)$. □

□

ⓘ The Frobenius endomorphism is not necessarily injective. For example, if $R := \mathbb{F}_p[X]/(X^2)$ and if x denotes the image of X in R, then x is a nonzero element of the kernel of the Frobenius endomorphism.

The next result gives an example of an irreducible polynomial with multiple roots.

Lemma 1.186 *Let $k := \mathbb{F}_p(T)$ where T is an indeterminate. Let $P(X) := X^p - T \in k[X]$. Then*

(1) *$P(X)$ is irreducible in $k[X]$,*
(2) *In the field $k_P = k[X]/(P(X)) = k[x]$ where x is a root of $P(X)$, we have $P(X) = (X - x)^p$.*

Proof (1) $P(X)$ is irreducible in $\mathbb{F}_p(X)[T]$, since it has degree 1 as a polynomial in T. Hence it is irreducible in $\mathbb{F}_p[X][T]$ since it is primitive. Since $\mathbb{F}_p[X][T] =$

$\mathbb{F}_p[X, T] = \mathbb{F}_p[T][X]$, it is irreducible in $\mathbb{F}_p[T][X]$, hence irreducible in $\mathbb{F}_p(T)[X]$ by Gauß' Lemma.

(2) If x is a root of $P(X)$, we have $x^p = T$, hence $P(X) = X^p - x^p = (X - x)^p$ since the Frobenius map is an algebra endomorphism. □

More Exercises on Sect. 1.3

Exercise 1.187 Let $P(X), Q(X) \in \mathbb{Q}[X]$. Assume $P(X)$ irreducible. Prove that if $P(X)$ and $Q(X)$ have a common zero in $\mathbb{C}$, then $P(X)$ divides $Q(X)$.

Exercise 1.188 Let $R := \mathbb{Z}[\sqrt{-6}]$.

(1) Describe the group $R^\times$ of units of R.
(2) Prove that $1 + \sqrt{-6}$ is irreducible in R.
(3) Describe an isomorphism $R/(1 + \sqrt{-6})R \xrightarrow{\sim} \mathbb{Z}/7\mathbb{Z}$.

Exercise 1.189

(1) Check that the polynomial $X^3 + X + 1$ is irreducible in $\mathbb{F}_2[X]$.
(2) Prove that the polynomial $3X^2 + 15X - 9$ is irreducible in $\mathbb{Q}[X]$. Is it irreducible in $\mathbb{Z}[X]$?

Exercise 1.190 Let k be a (commutative) field.

(1) Prove that $k[X, Y]/(X^3 - Y^2 - X)$ is not factorial.

> HINT: Show that the image of Y in $k[X, Y]/(X^3 - Y^2 - X)$ is irreducible but not prime.

(2) Prove that $k[X, Y]/(XY - 1)$ is a principal ideal domain, and deduce that $\mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$ is a principal ideal domain.
(3) Prove that $\mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$ is not factorial.

Exercise 1.191 Let R be a factorial ring. Assume that, for all $a, b \in R$, their gcd satisfies the Bézout identity (i.e., the ideal $Ra + Rb$ is principal). Prove that R is a principal ideal domain.

Exercise 1.192 If r is the remainder of the Euclidean division of a by b ($a, b, r \in \mathbb{N}$), show that $X^r - 1$ is the remainder of the Euclidean division of $X^a - 1$ by $X^b - 1$ in $\mathbb{Q}[X]$.

Exercise 1.193 Let $a_1, a_2, \ldots, a_n$ be n pairwise distinct elements of $\mathbb{Z}$. Prove that the polynomial

$$P(X) = (X - a_1)(X - a_2) \cdots (X - a_n) - 1$$

is irreducible in $\mathbb{Z}[X]$.

Exercise 1.194 Let k be a commutative field. Let $P(X,Y)$, $Q(X,Y)$ be two relatively prime elements of $k[X,Y]$.

(1) Prove that there exist

$$\begin{cases} E(X) \in k[X], \qquad F(Y) \in k[Y], \\ A(X,Y),\ B(X,Y),\ C(X,Y),\ D(X,Y) \in k[X,Y] \end{cases}$$

such that

$$\begin{cases} E(X) = A(X,Y)P(X,Y) + B(X,Y)Q(X,Y) \\ F(Y) = C(X,Y)P(X,Y) + D(X,Y)Q(X,Y). \end{cases}$$

HINT. One may consider the rings $k(X)[Y]$ and $k(Y)[X]$.

(2) For $S(X,Y) \in k[X,Y]$ we set

$$\mathcal{V}(S) = \big\{(x,y) \in k^2 \mid S(x,y) = 0\big\}.$$

Prove that $\mathcal{V}(P) \cap \mathcal{V}(Q)$ is finite.

(3) Prove that $k[X,Y]/(P,Q)$ is a finite dimensional k-vector space. Deduce that if $S(X,Y)$ is irreducible, then every nonzero prime ideal of the integral domain $k[X,Y]/(S)$ is maximal (we then say that $k[X,Y]/(S)$ "has dimension 1").

Exercise 1.195 The following ring is a localization of the polynomial ring $\mathbb{Z}[X]$:

$$\mathcal{R}(X) := \mathbb{Z}\big[X, X^{-1}, \{(X^n - 1)^{-1}\}_{n \geq 1}\big],$$

and it is called the *Rouquier ring*.

(1) Prove that the group of units of $\mathcal{R}(X)$ is

$$\mathcal{R}(X)^\times = \left\{\pm X^m \prod_{n \geq 1} \Phi_n(X)^{m_n}\right\}_{m, m_n \in \mathbb{Z}}$$

(where the m_n are almost all zero).

(2) Prove that the nonzero prime ideals of $\mathcal{R}(X)$ are

- $p\mathcal{R}(X)$ for all prime numbers p,
- $P(X)\mathcal{R}(X)$ where $P(X)$ is an irreducible element of $\mathbb{Z}[X]$ of degree ≥ 1, not equal to X nor to a cyclotomic polynomial.

1.4 Polynomial Rings in Several Indeterminates

1.4.1 Universal Property, Substitutions

For R a commutative ring, we assume the reader knows the definition of the ring $R[X_1, X_2, \ldots, X_n]$ of polynomials in n indeterminates $X_1, X_2, \ldots, X_n$ over R: it is the R-algebra generated by the commuting indeterminates $X_1, X_2, \ldots, X_n$.

The following property (*"universal property of the ring of polynomials in n indeterminates over R"*) is both immediate and fundamental.

Theorem 1.196 *Let R and R' be two (commutative) rings, let $f : R \longrightarrow R'$ be a morphism, and let $x_1, x_2, \ldots, x_n$ be n elements of R'. Then there exists one and only one morphism*

$$R[X_1, X_2, \ldots, X_n] \longrightarrow R'$$

which induces f on R and (for all j, $1 \le j \le n$) sends X_j onto x_j.

Example 1.197 A well known application of the universal property in Theorem 1.196 is the notion of *remarkable identity*.

For example, the equality

$$(a-b)(a+b) = a^2 - b^2, \tag{♣}$$

known to be true "for any numbers a and b", is actually a consequence of a *single* identity in the polynomial ring $\mathbb{Z}[X, Y]$, namely

$$(X-Y)(X+Y) = X^2 - Y^2. \tag{♠}$$

Indeed, given any ring R and two commuting elements $a, b \in R$, there is a unique morphism $\mathbb{Z}[X, Y] \to R$ such that $X \mapsto a$ and $Y \mapsto b$, and under that morphism (♠) becomes (♣).

A more difficult remarkable identity is the equation

$$^t\mathrm{Com}(M).M = \det(M)1_n, \tag{◇}$$

for any commutative ring and any matrix $M = (x_{i,j}) \in \mathrm{Mat}_n(R)$.

As above, (◇) follows from a single equation concerning a matrix defined below.

Definition 1.198 The *generic matrix* is

$$M_0 := (X_{i,j}) \in \mathrm{Mat}_n\big(\mathbb{Z}\big[\{X_{i,j}\}_{1 \le i,j \le n}\big]\big),$$

which is a matrix with entries in the polynomial ring in n^2 indeterminates over $\mathbb{Z}$.

We may view that matrix M_0 as a matrix with entries in the field of fractions $\mathbb{Q}(\{X_{i,j}\}_{1\leq i,j\leq n})$. Now from any undergraduate course on linear algebra (which deals with matrices with entries in a field), the reader knows that

$$^t\mathrm{Com}(M_0).M_0 = \det(M_0)1_n. \qquad (\heartsuit)$$

But that last equality is nothing but a series of equalities written in the ring $\mathbb{Z}[\{X_{i,j}\}_{1\leq i,j\leq n}]$. Now the unique morphism

$$\mathbb{Z}\big[\{X_{i,j}\}_{1\leq i,j\leq n}\big] \to R, \quad X_{i,j} \mapsto x_{i,j},$$

transforms these equalities to equalities expressing equation ($\diamondsuit$).

1.4.1.1 First Particular Case

Assume given a ring morphism $f : R \longrightarrow R'$, and let $R'[Y_1, \ldots, Y_n]$ be the ring of polynomials in the n indeterminates $Y_1, \ldots, Y_n$ with coefficients in R'.

The morphism f defines also (by composition with the inclusion of R' in $R'[Y_1, Y_2, \ldots, Y_n]$) a morphism still denoted

$$f : R \longrightarrow R'[Y_1, Y_2, \ldots, Y_n].$$

We apply Theorem 1.196, replacing R' by $R'[Y_1, Y_2, \ldots, Y_n]$ and setting $x_j := Y_j$. We get:

Corollary 1.199 *Given a ring morphism $f : R \longrightarrow R'$, there exists one and only one morphism*

$$R[X_1, X_2, \ldots, X_n] \longrightarrow R'[Y_1, Y_2, \ldots, Y_n]$$

which extends f and sends X_j onto Y_j, for $1 \leq j \leq n$.

1.4.1.2 Second Particular Case: Evaluation Function

Choose R' to be the R-algebra $\mathrm{Func}(R^n, R)$ of functions from R^n to R, where the additive and multiplicative laws are defined as the pointwise addition and multiplication of functions.

We denote by $c : R \longrightarrow \mathrm{Func}(R^n, R)$ the morphism which sends $a \in R$ to the constant function with value a.

One defines the elements $\pi_1, \pi_2, \ldots, \pi_n$ of $\mathrm{Func}(R^n, R)$ by

$$\pi_j : R^n \longrightarrow R, \qquad (a_1, a_2, \ldots, a_n) \mapsto a_j.$$

The morphism

$$R[X_1, X_2, \ldots, X_n] \longrightarrow \mathrm{Func}\big(R^n, R\big), \qquad X_j \mapsto \pi_j,$$

which extends c and sends X_j onto π_j (see Theorem 1.196) is called the *evaluation morphism*. It takes a polynomial in n variables over R to the corresponding polynomial function on R^n.

Thus, to a polynomial $P(X_1, X_2, \dots, X_n)$ we associate the *polynomial function* on R^n defined by

$$(a_1, a_2, \dots, a_n) \mapsto P(a_1, a_2, \dots, a_n).$$

! **Attention** ! That morphism is not necessarily injective: it may happen that a nonzero polynomial defines the zero polynomial function. For example, if q is a power of a prime number and if $\mathbb{F}_q$ is a field with q elements, the polynomial $X^q - X \in \mathbb{F}_q[X]$ is nonzero (and of degree q) while it defines the zero function on $\mathbb{F}_q$.

Remark 1.200 More generally, given a ring morphism $f : R \longrightarrow R'$, we have an evaluation morphism

$$R[X_1, X_2, \dots, X_n] \longrightarrow \mathrm{Func}\big(R'^n, R'\big)$$

defined by the composition of the evaluation morphism defined above with the morphism

$$R[X_1, X_2, \dots, X_n] \longrightarrow R'[Y_1, Y_2, \dots, Y_n]$$

which extends f.

1.4.1.3 Third Particular Case: Substitution

Suppose we have chosen polynomials $\xi_1, \dots, \xi_n \in R[X_1, \dots, X_n]$.

We apply Theorem 1.196 replacing R' by the ring $R[X_1, X_2, \dots, X_n]$, and choosing for f the natural injection from R into R', and $x_j := \xi_j$. We get:

Proposition 1.201 *Given $\xi_1, \xi_2, \dots, \xi_n \in R[X_1, X_2, \dots, X_n]$, there exists one and only one endomorphism of $R[X_1, X_2, \dots, X_n]$ which induces the identity on R and sends X_j to ξ_j.*

That morphism consists in substituting the polynomial ξ_j to the indeterminate X_j in any polynomial $P(X_1, X_2, \dots, X_n)$, that is:

$$P(X_1, X_2, \dots, X_n) \mapsto P(\xi_1, \xi_2, \dots, \xi_n).$$

1.4.1.4 Fourth Particular Case: Specialization

It is easy to check (for example thanks to Theorem 1.196—how?) that there is one and only one isomorphism

$$R[X_1, X_2, \dots, X_j, \dots, X_n] \xrightarrow{\sim} R[X_1, X_2, \dots, \widehat{X}_j, \dots, X_n][X_j]$$

which induces the identity on R and sends X_k to X_k for all k.

We shall systematically identify

$$R[X_1, X_2, \dots, X_j, \dots, X_n] \quad \text{with } R[X_1, X_2, \dots, \widehat{X}_j, \dots, X_n][X_j]$$

through that isomorphism.

The following result is a special case of Proposition 1.201 (why?).

Proposition 1.202

1. *Let $a \in R$. There exists one and only one morphism*

$$R[X_1, X_2, \dots, X_j, \dots, X_n] \longrightarrow R[X_1, X_2, \dots, \widehat{X}_j, \dots, X_n]$$

which induces the identity on $R[X_1, \dots, \widehat{X}_j, \dots, X_n]$, and which sends X_j to a.

2. *More generally, let*

$$\alpha(X_1, X_2, \dots, X_{j-1}, X_{j+1}, \dots, X_n) \in R[X_1, X_2, \dots, \widehat{X}_j, \dots, X_n].$$

There exists one and only one morphism

$$R[X_1, X_2, \dots, X_j, \dots, X_n] \longrightarrow R[X_1, X_2, \dots, \widehat{X}_j, \dots, X_n]$$

which induces the identity on $R[X_1, \dots, \widehat{X}_j, \dots, X_n]$, and which sends

$$X_j \quad \textit{to} \quad \alpha(X_1, X_2, \dots, X_{j-1}, X_{j+1}, \dots, X_n).$$

These morphisms are denoted respectively

$$P(X_1, X_2, \dots, X_j, \dots, X_n) \mapsto P(X_1, X_2, \dots, a, \dots, X_n),$$

and

$$P(X_1, \dots, X_j, \dots, X_n)$$
$$\mapsto P\big(X_1, \dots, X_{j-1}, \alpha(X_1, \dots, X_{j-1}, X_{j+1}, \dots, X_n), X_{j+1} \dots, X_n\big).$$

Proposition 1.203 *Let $\alpha(X_1, X_2, \dots, X_{j-1}, X_{j+1}, \dots, X_n) \in R[X_1, X_2, \dots, \widehat{X}_j, \dots, X_n]$. For $P(X_1, X_2, \dots, X_n) \in R[X_1, X_2, \dots, , X_n]$, the following assertions are equivalent:*

(i) $P(X_1, X_2, \dots, \alpha, \dots, X_n) = 0$,

(ii) $P(X_1, X_2, \dots, X_j, \dots, X_n)$ *is divisible by* $X_j - \alpha$ (*in the polynomial ring* $R[X_1, X_2, \dots, X_j, \dots, X_n]$).

Proof of 1.203 This follows from the general property of Euclidean division in rings of polynomials (Proposition 1.16).

We apply Proposition 1.16 where we replace R by the ring of polynomials in $n-1$ indeterminates $R[X_1, X_2, \dots, \widehat{X}_j, \dots, X_n]$, the polynomial $P(X)$ by $P(X_1, X_2, \dots, X_{j-1}, X, X_{j+1}, \dots, X_n)$ and we choose $M(X) := X - \alpha$. □

Corollary 1.204 *Let $P(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$. For $i < j$, the following assertions are equivalent.*

(1) *$P(X_1, \ldots, X_i, \ldots, X_j, \ldots, X_n)$ is divisible by $X_i - X_j$.*
(2) *$P(X_1, \ldots, X_i, \ldots, X_i, \ldots, X_n) = 0$.*

1.4.2 Transfer Properties

1.4.2.1 Transfer of Some Properties to Polynomial Rings

We have seen that a certain number of properties are transferable from R to $R[X]$ (such as being an integral domain, or being factorial). It follows that the same properties are transferable from R to $R[X_1, X_2, \ldots, X_n]$.

Theorem 1.205

(1) *If R is an integral domain, then $R[X_1, X_2, \ldots, X_n]$ is an integral domain, and $R[X_1, X_2, \ldots, X_n]^\times = R^\times$.*
(2) *If R is factorial, then $R[X_1, X_2, \ldots, X_n]$ is factorial. Moreover, denoting by F the field of fractions of R, for all j $(1 \le j \le n)$, we have*

$$\operatorname{Irr} R[X_1, X_2, \ldots, X_n] = \begin{cases} \operatorname{Irr} R[X_1, \ldots, \widehat{X_j}, \ldots, X_n] \\ \sqcup \\ \operatorname{Prim} R[X_1, \ldots, \widehat{X_j}, \ldots, X_n][X_j] \cap \operatorname{Irr} F(X_1, \ldots, \widehat{X_j}, \ldots, X_n)[X_j] \end{cases}$$

Example 1.206 More on the generic matrix Let $n \geq 1$ be an integer, and let $M_0 := (X_{i,j})$ be the $n \times n$ generic matrix (see Definition 1.198).

Let us denote by $\Gamma_{M_0}(X) \in \mathbb{Z}[\{X_{i,j}\}, X]$ its characteristic polynomial.

Lemma 1.207 *The polynomial $\Gamma_{M_0}(X)$ is irreducible in $\mathbb{Q}(\{X_{i,j}\})[X]$.*

Proof of 1.207 Since $\Gamma_{M_0}(X)$ has degree (as a polynomial in X) at least equal to 1, it suffices (by the above Theorem 1.205) to check that $\Gamma_{M_0}(X)$ is irreducible in $\mathbb{Z}[\{X_{i,j}\}][X]$.

Since the highest degree term of $\Gamma_{M_0}(X)$ is X^n, $\Gamma_{M_0}(X)$ is primitive in $\mathbb{Z}[\{X_{i,j}\}][X]$ and it suffices (cf. Proposition 1.166) to find a prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\{X_{i,j}\}]$ such that the reduction of $\Gamma_{M_0}(X)$ modulo $\mathfrak{p}$ is irreducible.

Consider for example the surjective morphism

$$\mathbb{Z}\big[\{X_{i,j}\}\big] \twoheadrightarrow \mathbb{Z}$$

which sends the matrix M_0 onto the matrix

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & p \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

An easy computation of the characteristic polynomial of that last matrix (not necessary if you solved Exercise 1.1) shows that the image of $\varGamma_{M_0}(X)$ is $X^n - p$, which is irreducible by Eisenstein's criterion. □

1.4.2.2 Yet Another Proof of Cayley–Hamilton Theorem

We shall use the irreducibility of the characteristic polynomial of the generic matrix to give another proof of Cayley–Hamilton theorem (see Theorem 1.22), which we recall here.

Theorem 1.208 (Cayley–Hamilton) *Let R be a commutative ring, $n \geq 1$ an integer, and $M \in \mathrm{Mat}_n(R)$. Let $\varGamma_M(X) = \det(X1_n - M)$ be the characteristic polynomial of M. Then*

$$\varGamma_M(M) = 0.$$

Proof It suffices to prove the result in the case where the ring is $\mathbb{Z}[\{X_{i,j}\}]$ and M is the generic matrix M_0.

Indeed, by Theorem 1.196, there is a unique ring morphism $\mathbb{Z}[\{X_{i,j}\}] \to R$ which sends the generic matrix M_0 onto M, hence the characteristic polynomial $\varGamma_{M_0}(X)$ onto $\varGamma_M(X)$, hence $\varGamma_{M_0}(M_0)$ onto $\varGamma_M(M)$.

From now on we assume $R = \mathbb{Z}[\{X_{i,j}\}]$ and $M = M_0$. Since $\varGamma_{M_0}(X)$ is irreducible in $\mathbb{Q}(\{X_{i,j}\})[X]$ (by Lemma 1.207), it results from Proposition 1.184 that, if K is an extension of $\mathbb{Q}(\{X_{i,j}\})$ in which $\varGamma_{M_0}(X)$ is a product of degree one elements, then $\varGamma_{M_0}(X)$ has no multiple root in K.

Thus the matrix M_0 is diagonalizable over K. In order to prove that $\varGamma_{M_0}(M_0) = 0$ we may then assume that M_0 is diagonal, and in that case it is trivial. □

1.4.3 Symmetric Polynomials

Here, for Ω a set, we denote by $\mathfrak{S}_\Omega$ the group of all permutations of Ω, and we denote by $\mathfrak{S}_n$ the group of all permutations of the set $\{1, 2, \ldots, n\}$.

Here R is any commutative ring.

1.4.3.1 Definition and Fundamental Theorem

For all $\sigma \in \mathfrak{S}_n$, there is a unique algebra endomorphism of the polynomial algebra $R[X_1, X_2, \dots, X_n]$ which induces the identity on R and, for all j $(1 \leq j \leq n)$, sends X_j to $X_{\sigma(j)}$. We still denote that endomorphism by σ. Thus, we have

$$\begin{cases} \sigma : R[X_1, X_2, \dots, X_n] \longrightarrow R[X_1, X_2, \dots, X_n], \\ \sigma\big(P(X_1, X_2, \dots, X_n)\big) = P(X_{\sigma(1)}, X_{\sigma(2)}, \dots, X_{\sigma(n)}), \end{cases}$$

so that

$$\begin{cases} \sigma(P + Q) = \sigma(P) + \sigma(Q), \\ \sigma(PQ) = \sigma(P)\sigma(Q), \end{cases}$$

for all $P, Q \in R[X_1, X_2, \dots, X_n]$.

Example 1.209 The transposition τ of $\mathfrak{S}_{\{X,Y\}}$ defines the endomorphism $P(X, Y) \mapsto P(Y, X)$ of $\mathbb{Z}[X, Y]$. Notice that the polynomial $X - Y$ is not fixed under τ, while the polynomial $X^2Y + XY^2$ is fixed.

The map which sends $\sigma \in \mathfrak{S}_n$ to the endomorphism σ of the R-algebra $R[X_1, X_2, \dots, X_n]$ defines an *action* of $\mathfrak{S}_n$ on $R[X_1, X_2, \dots, X_n]$, i.e., for all $\sigma, \sigma' \in \mathfrak{S}_n$ and $P \in R[X_1, X_2, \dots, X_n]$, we have

$$\sigma\big(\sigma'(P)\big) = \big(\sigma\sigma'\big)(P).$$

It follows that the endomorphisms σ are actually automorphisms.

Definition 1.210 We denote by $R[X_1, X_2, \dots, X_n]^{\mathfrak{S}_n}$ the R-subalgebra of fixed points of $\mathfrak{S}_n$ on the R-algebra $R[X_1, X_2, \dots, X_n]$, that is

$$R[X_1, X_2, \dots, X_n]^{\mathfrak{S}_n} = \big\{P \in R[X_1, \dots, X_n] \;\big|\; (\forall \sigma \in \mathfrak{S}_n)\big(\sigma(P) = P\big)\big\}$$

and we call *symmetric polynomials* the elements of $R[X_1, X_2, \dots, X_n]^{\mathfrak{S}_n}$.

Notice that $R[X_1, X_2, \dots, X_n]^{\mathfrak{S}_n}$ is a subring of $R[X_1, X_2, \dots, X_n]$.

Example 1.211 For all $P \in R[X_1, X_2, \dots, X_n]$, the elements

$$\sum_{\sigma \in \mathfrak{S}_n} \sigma(P) \quad \text{and} \quad \prod_{\sigma \in \mathfrak{S}_n} \sigma(P)$$

are symmetric.

Thus $\sum_{1 \leq j \leq n} X_j^2(X_j + 1)$ and $\prod_{1 \leq j \leq n}(X_j^3 + 2X_j + 1)$ are symmetric polynomials.

Since the group $\mathfrak{S}_n$ acts on the ring $R[X_1, X_2, \ldots, X_n]$, it acts also on the ring of polynomials $R[X_1, X_2, \ldots, X_n][T]$ (by fixing T).

Consider the *generic polynomial*

$$P(T) := (T - X_1)(T - X_2)\cdots(T - X_n).$$

It is clear that $P(T)$ is fixed by $\mathfrak{S}_n$, i.e.,

$$P(T) \in R[X_1, X_2, \ldots, X_n]^{\mathfrak{S}_n}[T].$$

An immediate computation gives:

$$P(T) = T^n - \Sigma_1 T^{n-1} + \cdots + (-1)^j \Sigma_j T^{n-j} + \cdots + (-1)^n \Sigma_n,$$

where

$$\begin{cases} \Sigma_1 = X_1 + X_2 + \cdots + X_n, \\ \Sigma_2 = X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n, \\ \vdots \\ \Sigma_j = \displaystyle\sum_{i_1<i_2<\cdots<i_j} X_{i_1}X_{i_2}\cdots X_{i_j}, \\ \vdots \\ \Sigma_n = X_1X_2\cdots X_n, \end{cases}$$

are the *elementary symmetric polynomials* in $X_1, \ldots, X_n$.

One can prove the following fundamental theorem (see the literature).

Theorem 1.212 *Let $Y_1, Y_2, \ldots, Y_n$ be n indeterminates. Then the map*

$$\begin{cases} R[Y_1, , Y_2, \ldots, Y_n] \longrightarrow R[X_1, X_2, \ldots, X_n], \\ \textit{for each } j = 1, \ldots, n,\ Y_j \mapsto \Sigma_j, \end{cases}$$

defines an R-algebra isomorphism

$$R[Y_1, , Y_2, \ldots, Y_n] \xrightarrow{\sim} R[X_1, X_2, \ldots, X_n]^{\mathfrak{S}_n},$$

that is, each invariant polynomial is a polynomial in the elementary symmetric polynomials $(\Sigma_j)_{j=1,\ldots,n}$.

1.4.3.2 Newton Formulae

Set

$$\Lambda(T) := T^n P(1/T) = (1 - X_1T)(1 - X_2T)\cdots(1 - X_nT).$$

Thus, we have

$$\Lambda(T) = 1 - \Sigma_1 T + \cdots + (-1)^j \Sigma_j T^j + \cdots + (-1)^n \Sigma_n T^n.$$

Now we turn to computations in the ring $R[X_1, \ldots, X_n][\![T]\!]$.

Computing the logarithmic derivative of $\Lambda(T)$ gives

$$-\frac{\Lambda'(T)}{\Lambda(T)} = \sum_{j=1}^{j=n} \frac{X_j}{1 - X_j T} = \sum_{k=0}^{\infty} P_{k+1}(X_1, X_2, \ldots, X_n) T^k$$

where we set

$$P_k(X_1, X_2, \ldots, X_n) := X_1^k + X_2^k + \cdots + X_n^k.$$

From the formula

$$-\Lambda'(T) = \Lambda(T)\left(-\frac{\Lambda'(T)}{\Lambda(T)}\right),$$

we get

$$\Sigma_1 + \cdots + (-1)^{j+1} j \Sigma_j T^{j-1} + \cdots + (-1)^{n+1} n \Sigma_n T^{n-1}$$
$$= \left\{ \begin{array}{l} \big(1 - \Sigma_1 T + \cdots + (-1)^k \Sigma_k T^k + \cdots + (-1)^n \Sigma_n T^n\big) \\ \quad \times \left(\displaystyle\sum_{l=0}^{\infty} P_{l+1}(X_1, X_2, \ldots, X_n) T^l\right). \end{array} \right.$$

The preceding formula provides the equalities ("Newton formulae"):

$$\begin{cases} \text{For } m \geq n: \\ \quad \displaystyle\sum_{k+l=m} (-1)^k \, \Sigma_k(X_1, \ldots, X_n) P_{l+1}(X_1, \ldots, X_n) = 0, \\ \text{For } m < n: \\ \quad \displaystyle\sum_{k+l=m} (-1)^k \, \Sigma_k(X_1, \ldots, X_n) P_{l+1}(X_1, \ldots, X_n) = (-1)^m (m+1) \Sigma_{m+1}. \end{cases}$$

1.4.3.3 Symmetric Rational Fractions

Let F be the field of fractions of the integral domain R.

The group $\mathfrak{S}_n$ acts on the field of fractions $F(X_1, X_2, \ldots, X_n)$ by the formula

$$\sigma(P/Q) := \sigma(P)/\sigma(Q)$$

for all $\sigma \in \mathfrak{S}_n$, $P, Q \in R[X_1, X_2, \ldots, X_n]$, $Q \neq 0$ (check that this is well defined).

The rational fractions fixed by $\mathfrak{S}_n$ are called the *symmetric rational fractions*. The set of symmetric rational fractions is a subfield of the field $F(X_1, X_2, \dots, X_n)$, denoted $F(X_1, X_2, \dots, X_n)^{\mathfrak{S}_n}$.

The isomorphism

$$\begin{cases} R[Y_1, Y_2, \dots, Y_n] \xrightarrow{\sim} R[X_1, X_2, \dots, X_n]^{\mathfrak{S}_n} \\ P(Y_1, Y_2, \dots, Y_n) \mapsto P(\Sigma_1, \Sigma_2, \dots, \Sigma_n) \end{cases}$$

from Theorem 1.212 induces an isomorphism

$$F(Y_1, Y_2, \dots, Y_n) \xrightarrow{\sim} F(\Sigma_1, \Sigma_2, \dots, \Sigma_n).$$

Proposition 1.213 *We have*

$$F(X_1, X_2, \dots, X_n)^{\mathfrak{S}_n} = F(\Sigma_1, \Sigma_2, \dots, \Sigma_n).$$

Proof of Proposition 1.213 It is clear that $F(\Sigma_1, \Sigma_2, \dots, \Sigma_n)$ is contained in the field of symmetric rational fractions. Conversely, let us prove that any symmetric rational fraction belongs to $F(\Sigma_1, \Sigma_2, \dots, \Sigma_n)$.

Notice first that any element of $F(X_1, X_2, \dots, X_n)$ can be written P/Q where Q is a symmetric polynomial. Indeed, if P/Q is any fraction, we have

$$\frac{P}{Q} = \frac{P \prod_{\sigma \neq 1} \sigma(Q)}{\prod_{\sigma} \sigma(Q)},$$

where σ runs over $\mathfrak{S}_n$.

Now such a fraction P/Q is symmetric if and only if P is symmetric. □

1.4.3.4 Antisymmetric Polynomials

One defines the element $\delta(X_1, X_2, \dots, X_n) \in R[X_1, X_2, \dots, X_n]$ by the formula

$$\delta(X_1, X_2, \dots, X_n) := \prod_{1 \leq i < j \leq n} (X_j - X_i).$$

Lemma 1.214 *For all $\sigma \in \mathfrak{S}_n$, we have*

$$\sigma(\delta) = \mathrm{sgn}(\sigma)\delta$$

where

$$\mathrm{sgn} : \mathfrak{S}_n \to \{\pm 1\}$$

is the “signature” *morphism.*

Proof of Lemma 1.214 It is clear that there exists a function $\varepsilon : \mathfrak{S}_n \longrightarrow \{\pm 1\}$ such that $\sigma(\delta) = \varepsilon(\sigma)\delta$. Since that function ε is clearly a group morphism and since it takes the value -1 on every transposition (exercise!), it coincides with the signature. □

A polynomial $P(X_1, X_2, \dots, X_n)$ is said to be *antisymmetric* if it satisfies the condition

$$\sigma\big(P(X_1, X_2, \dots, X_n)\big) = \operatorname{sgn}(\sigma) P(X_1, X_2, \dots, X_n)$$

for all $\sigma \in \mathfrak{S}_n$.

Proposition 1.215 *Assume R factorial and of characteristic different from* 2.

A polynomial $P(X_1, X_2, \dots, X_n)$ is antisymmetric if and only if it is of the type

$$P(X_1, X_2, \dots, X_n) = \delta(X_1, X_2, \dots, X_n) P_0(X_1, X_2, \dots, X_n)$$

where $P_0(X_1, X_2, \dots, X_n)$ is a symmetric polynomial.

Proof of Proposition 1.215 If P is antisymmetric, for all i and j such that $i < j$ we have

$$P(X_1, X_2, \dots, X_n)_{|X_i = X_j} = 0,$$

hence (by Proposition 1.203 with $\alpha = X_i$) $P(X_1, X_2, \dots, X_n)$ is divisible by $X_j - X_i$. Since the polynomials $X_j - X_i$ are irreducible (why?) and the ring $R[X_1, X_2, \dots, X_n]$ is factorial, $P(X_1, X_2, \dots, X_n)$ is divisible by their product, i.e., is divisible by δ. It is then clear that the quotient is symmetric. □

1.4.4 Resultant and Discriminant

1.4.4.1 Resultant of Two Polynomials

Convention. For a system of vectors $(v_1, v_2, \dots, v_n)$ in a vector space, which are linear combinations of elements $(e_1, e_2, \dots, e_n)$ of another system of vectors:

$$\begin{cases} v_1 = a_{1,1}e_1 + a_{1,2}e_2 + \cdots + a_{1,n}e_n \\ v_2 = a_{2,1}e_1 + a_{2,2}e_2 + \cdots + a_{2,n}e_n \\ \vdots \qquad \vdots \qquad \vdots \qquad \vdots \\ v_n = a_{n,1}e_1 + a_{n,2}e_2 + \cdots + a_{n,n}e_n, \end{cases}$$

we call

- *matrix of the system* $(v_1, v_2, \dots, v_n)$ *on* $(e_1, e_2, \dots, e_n)$ the matrix $(a_{i,j})_{1\le i,j\le n}$,
- and *determinant of the system* $(v_1, v_2, \dots, v_n)$ *on* $(e_1, e_2, \dots, e_n)$ the determinant of that matrix $(a_{i,j})_{1\le i,j\le n}$.

If ϕ is an endomorphism of a vector space with basis $(e_1, e_2, \dots, e_n)$, the matrix Φ of ϕ with respect to that basis is by definition *the transposed* of the matrix of the system $(\phi(e_1), \phi(e_2), \dots, \phi(e_n))$ on $(e_1, e_2, \dots, e_n)$ (in other words, the *columns* of the matrix Φ are the coordinates of the vectors $\phi(e_1), \phi(e_2), \dots, \phi(e_n)$).

Let R be an integral domain, let m and n be two nonnegative integers, and let $P(X)$ and $Q(X)$ be two elements of $R[X]$, of degrees respectively at most m and n.

Definition 1.216 The resultant $\mathrm{Res}_{m,n}(P, Q)$ is by definition the determinant, on the basis

$$\{X^{m+n-1}, X^{m+n-2}, \dots, X, 1\}$$

of the system

$$\{X^{n-1}P(X), X^{n-2}P(X), \dots, P(X), X^{m-1}Q(X), X^{m-2}Q(X), \dots, Q(X)\}.$$

In other words, if

$$P(X) = p_m X^m + p_{m-1}X^{m-1} + \cdots + p_1 X + p_0,$$

$$Q(X) = q_n X^n + q_{n-1}X^{n-1} + \cdots + q_1 X + q_0,$$

we have $\mathrm{Res}_{m,n}(P, Q) = \det M_{m,n}(P, Q)$ where

$$M_{m,n}(P, Q) = \begin{pmatrix} p_m & p_{m-1} & \cdots & \cdots & \cdots & p_0 & 0 & \cdots & 0 \\ 0 & p_m & \cdots & \cdots & \cdots & p_1 & p_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & p_m & \cdots & \cdots & \cdots & \cdots & p_0 \\ q_n & q_{n-1} & \cdots & \cdots & q_0 & \cdots & 0 & \cdots & 0 \\ 0 & q_n & \cdots & \cdots & q_1 & q_0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & q_n & \cdots & q_0 \end{pmatrix}$$

is a square matrix with $m+n$ lines and $m+n$ columns, whose first n lines contain the coefficients of $P(X)$ (and some zeros), and the last m lines contain the coefficients of $Q(X)$ (and some zeros).

Examples 1.217

(1) Choose $P(X) = X - a$ and $Q(X) = X - b$. We have:

$$\mathrm{Res}_{1,1}(P, Q) = \begin{vmatrix} 1 & -a \\ 1 & -b \end{vmatrix} = a - b = -P(b) = Q(a).$$

(2) Choose $P(X) = aX^2 + bX + c$ and $Q(X) = X - d$. Then

$$\mathrm{Res}_{2,1}(P, Q) = \begin{vmatrix} a & b & c \\ 1 & -d & 0 \\ 0 & 1 & -d \end{vmatrix} = ad^2 + bd + c = P(d) = aQ(\alpha_1)Q(\alpha_2),$$

where α_1 and α_2 denote the roots of $P(X)$.

We shall see how to generalize the properties that we have just noticed.

1.4.4.2 First Properties

(1) If $p_m = q_n = 0$, we have $\mathrm{Res}_{m,n}(P, Q) = 0$.
(2) We have the *reciprocity formula*:

$$\mathrm{Res}_{m,n}(P, Q) = (-1)^{mn}\mathrm{Res}_{n,m}(Q, P).$$

(3) For a natural integer n, let us denote by $R[X]_n$ the subgroup (actually, the R-submodule) consisting of elements of $R[X]$ with degree less or equal to n.

Lemma 1.218 *The following two assertions are equivalent*:

(i) $\mathrm{Res}_{m,n}(P, Q) = 0$.
(ii) *There exists $U(X) \in R[X]_{m-1}$ and $V(X) \in R[X]_{n-1}$ such that*

$$U(X)Q(X) + V(X)P(X) = 0.$$

Proof It suffice to write that the determinant of the system

$$\left\{X^{n-1}P(X), X^{n-2}P(X), \ldots, P(X), X^{m-1}Q(X), X^{m-2}Q(X), \ldots, Q(X)\right\}$$

on the basis $\{X^{m+n-1}, X^{m+n-2}, \ldots, X, 1\}$ is zero if and only if there exists a linear combination of these vectors which is zero. □

Corollary 1.219 *Assume R factorial, with field of fractions F, and assume $p_m q_n \neq 0$. The following two assertions are equivalent*:

(i) $\mathrm{Res}_{m,n}(P, Q) = 0$.
(ii) *$P(X)$ and $Q(X)$ are not relatively prime in $F[X]$.*

Proof (i) ⇒ (ii): By Lemma 1.218, we know that there exist $U(X) \in R[X]_{m-1}$ and $V(X) \in R[X]_{n-1}$ such that $U(X)Q(X) = -V(X)P(X)$. If $P(X)$ and $Q(X)$ are relatively prime, by Gauß' Lemma one gets that $P(X)$ divides $U(X)$ which is impossible for degree reasons.

(ii) ⇒ (i): Assume that there exists $D(X)$, of degree at least 1, such that $P(X) = D(X)P_1(X)$ and $Q(X) = D(X)Q_1(X)$. We see then that $P_1(X)Q(X) - Q_1(X)P(X) = 0$, so $\mathrm{Res}_{m,n}(P, Q) = 0$ by Lemma 1.218. □

(4) Let us generalize the preceding property. Consider the linear map

$$\mathrm{R}_{m,n} : \begin{cases} R[X]_{n-1} \times R[X]_{m-1} \longrightarrow R[X]_{m+n-1} \\ \big(V(X), U(X)\big) \mapsto V(X)P(X) + U(X)Q(X). \end{cases}$$

Then the matrix of that map with respect to the pair of bases

$$\big\{\big(X^{n-1},0\big),\big(X^{n-2},0\big),\dots,(1,0),\big(0,X^{m-1}\big),\big(0,X^{m-2}\big),\dots,(0,1)\big\}$$

and

$$\big\{X^{m+n-1},X^{m+n-2},\dots,X,1\big\}$$

is the matrix ${}^tM_{m,n}(P,Q)$.

Let $\mathrm{Com}\,M_{m,n}(P,Q)$ be the comatrix of $M_{m,n}(P,Q)$ (i.e., its matrix of cofactors). Since we have

$$\begin{aligned}{}^tM_{m,n}(P,Q)\,\mathrm{Com}M_{m,n}(P,Q) &= \det M_{m,n}(P,Q)\,1_{m+n}\\ &= \mathrm{Res}_{m,n}(P,Q)\,1_{m+n},\end{aligned}$$

we see that the image of the map $\mathrm{R}_{m,n}$ contains $\mathrm{Res}_{m,n}(P,Q)\,R[X]_{m+n-1}$. Hence we have proved:

Proposition 1.220 *There exist $U(X)\in R[X]_{m-1}$ and $V(X)\in R[X]_{n-1}$ such that*

$$U(X)Q(X)+V(X)P(X)=\mathrm{Res}_{m,n}(P,Q).$$

1.4.4.3 Resultant and Roots

Recall that we denote by F the field of fractions of the integral domain R.

Assume $P(X)=p_mX^m+p_{m-1}X^{m-1}+\cdots+p_1X+p_0$ has degree m, i.e., $p_m\neq 0$. Then the quotient $F[X]/(P(X))$ is an F-vector space of dimension m.

The map

$$\mu_X : F[X]\longrightarrow F[X],\qquad P(X)\mapsto XP(X),$$

induces by quotient an endomorphism of the vector space $F[X]/(P(X))$, which is still denoted by μ_X. More generally, if $Q(X)\in F[X]$, the endomorphism $Q(\mu_X)$ is induced by the multiplication by $Q(X)$. We then denote by $(\frac{Q(X)}{P(X)})$ the determinant of that multiplication by $Q(X)$ in the vector space $F[X]/(P(X))$.

Example 1.221 Consider the second case in the Example 1.217, i.e., the case where $P(X)=aX^2+bX+c$ and $Q(X)=X-d$. Then the matrix of the multiplication by $X-d$ in $F[X]/(aX^2+bX+c)$ is $\left(\begin{smallmatrix}-d & -c/a\\ 1 & -d-b/a\end{smallmatrix}\right)$ hence its determinant is $P(d)/a$.

Lemma 1.222 *Assume $P(X)=p_mX^m+p_{m-1}X^{m-1}+\cdots+p_1X+p_0$ with $p_m\neq 0$, and $Q(X)$ of degree at most n. We have*

$$\mathrm{Res}_{m,n}(P,Q)=p_m^n\left(\frac{Q(X)}{P(X)}\right).$$

Proof For a polynomial $T(X) \in F[X]$, let us denote by $R_P(T)$ the remainder of the Euclidean division of $T(X)$ by $P(X)$.

For all integers $j < m$, we have $X^j Q(X) = S_j(X)P(X) + R_P(X^j Q(X))$ where $S_j(X)$ is a polynomial of degree at most $n-1$.

It follows that $\mathrm{Res}_{m,n}(P, Q)$ is the determinant,

- on the basis $\{X^{m+n-1}, X^{m+n-2}, \ldots, X, 1\}$,
- of the system

$$\begin{aligned}\bigl\{&X^{n-1}P(X), X^{n-2}P(X), \ldots, XP(X), P(X),\\ &R_P\bigl(X^{m-1}Q(X)\bigr), R_P\bigl(X^{m-2}Q(X)\bigr), \ldots, R_P\bigl(Q(X)\bigr)\bigr\}.\end{aligned}$$

Thus, $\mathrm{Res}_{m,n}(P, Q)$ is the determinant of an $(m+n) \times (m+n)$ matrix of type $\left(\begin{smallmatrix} T & T' \\ 0 & M \end{smallmatrix}\right)$ where T is an upper triangular $n \times n$ matrix of type

$$T = \begin{pmatrix} p_m & \cdots & \cdots & \cdots \\ 0 & p_m & \cdots & \cdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p_m \end{pmatrix}$$

and where M is the matrix of $\mu_{Q(X)}$. □

Remark 1.223 Assume $P(X)$ and $Q(X)$ are monic and of degrees respectively m and n. We have then the following formula

$$\left(\frac{Q(X)}{P(X)}\right) = (-1)^{mn}\left(\frac{P(X)}{Q(X)}\right).$$

Notice the analogy with the celebrated Gauß quadratic reciprocity formula in arithmetic (see for example [7], §5.5, Theorem 1) which concerns the Legendre symbol (see Exercise 1.101): if p and q are two odd prime numbers,

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

Proposition 1.224

(1) *Assume* $p_m \neq 0$ *and*

$$P(X) = p_m(X-a_1)(X-a_2)\cdots(X-a_m).$$

Then

$$\mathrm{Res}_{m,n}(P, Q) = p_m^n Q(a_1)Q(a_2)\cdots Q(a_m).$$

(2) *Assume moreover* $q_n \neq 0$ *and*

$$Q(X) = q_n(X - b_1)(X - b_2) \cdots (X - b_n).$$

Then

$$\mathrm{Res}_{m,n}(P, Q) = p_m^n q_n^m \prod_{i,j}(a_i - b_j).$$

Proof It suffices to note that the minimal polynomial (hence also the characteristic polynomial) of the endomorphism μ_X of the vector space $F[X]/(P(X))$ is $P(X)$, hence μ_X is triangularizable with eigenvalues $a_1, a_2, \ldots, a_m$. Assertion (1) follows then from Lemma 1.222. Assertion (2) is immediate from (1). □

Corollary 1.225 *Let* ϕ *be an endomorphism of a vector space of finite dimension* m *over a field* F, *and let* $\Gamma_\phi(X)$ *be its characteristic polynomial. Let* $Q(X)$ *be an element of degree at most* n *of* $F[X]$. *We have*

$$\det Q(\phi) = \mathrm{Res}_{m,n}(\Gamma_\phi, Q).$$

Proof Since we may increase the underlying base field, we may assume that $\Gamma_\phi(X)$ is split (i.e., product of factors of degree 1). The endomorphism ϕ is then triangularizable. If $a_1, a_2, \ldots, a_m$ are its eigenvalues, we have $\det Q(\phi) = Q(a_1)Q(a_2)\cdots Q(a_m)$, hence we get the wanted formula. □

1.4.4.4 A Geometric Application

Let $P(X, Y, Z)$ and $Q(X, Y, Z)$ be two elements of $\mathbb{C}[X, Y, Z]$, which define two algebraic surfaces S_P and S_Q in $\mathbb{C}^3$ by

$$S_P = \{(x, y, z) \in \mathbb{C}^3 \mid P(x, y, z) = 0\},$$
$$S_Q = \{(x, y, z) \in \mathbb{C}^3 \mid Q(x, y, z) = 0\}.$$

Let us view the polynomials $P(X, Y, Z)$ and $Q(X, Y, Z)$ as elements of $\mathbb{C}[X, Y][Z]$:

$$P(X, Y, Z) =: p_m(X, Y)Z^m + \cdots + p_1(X, Y)Z + p_0(X, Y),$$
$$Q(X, Y, Z) =: q_n(X, Y)Z^n + \cdots + q_1(X, Y)Z + q_0(X, Y),$$

and let us denote by $\mathrm{Res}^{(Z)}_{m,n}(P, Q)(X, Y)$ their resultant, which belongs to $\mathbb{C}[X, Y]$.

We denote by C_{p_m} and C_{q_n} the curves in $\mathbb{C}^2$ defined respectively by the equations

$$C_{p_m} := \{(x, y) \in \mathbb{C}^2 \mid p_m(x, y) = 0\},$$
$$C_{q_n} := \{(x, y) \in \mathbb{C}^2 \mid q_n(x, y) = 0\}.$$

Let us denote by $\mathrm{pr}_{x,y} : \mathbb{C}^3 \twoheadrightarrow \mathbb{C}^2$ the projection defined by $(x, y, z) \mapsto (x, y)$.

Proposition 1.226 *The set $S^{(Z)}_{P,Q}$ of points of $\mathbb{C}^2$ defined by*

$$S^{(Z)}_{P,Q} := \left\{(x, y) \in \mathbb{C}^2 \;\middle|\; \mathrm{Res}^{(Z)}_{m,n}(P, Q)(x, y) = 0\right\}$$

is equal to

$$(C_{p_m} \cap C_{q_n}) \cup \mathrm{pr}_{x,y}\,(S_P \cap S_Q).$$

1.4.4.5 Discriminant

Definition 1.227 Let $P(X) = p_m(X - a_1)(X - a_2) \cdots (X - a_m) \in R[X]$. We call *discriminant of* $P(X)$ and we denote by Discr $P(X)$ the element defined by

$$\mathrm{Discr}\ P(X) := p_m^{2m-2}\Bigg(\prod_{1\le i<j\le m}(a_i - a_j)\Bigg)^2.$$

Notice that by definition Discr $P(X)$ is the square of

$$\pm\, p_m^{m-1} \prod_{1\le i<j\le m} (a_i - a_j).$$

We see also that

$$\mathrm{Discr}\ P(X) = p_m^{2m-2}(-1)^{m(m-1)/2} \prod_{1\le i\neq j\le m} (a_i - a_j).$$

Example 1.228 If $P(X) = aX^2 + bX + c$, one checks that Discr $P(X) = b^2 - 4ac$.

From now on, we assume $P(X)$ monic, i.e., $p_m = 1$.
Since

$$P'(X) = \sum_{i=1}^{i=m}(X - a_1)(X - a_2) \cdots (\widehat{X - a_i}) \cdots (X - a_m),$$

we see that

$$\mathrm{Discr}\ P(X) = (-1)^{m(m-1)/2} \prod_{1\le i\le m} P'(a_i) = (-1)^{m(m-1)/2}\, \mathrm{Res}_{m,m-1}\big(P, P'\big)$$

hence

$$\mathrm{Discr}\ P(X) = (-1)^{m(m-1)/2}\left(\frac{P'(X)}{P(X)}\right).$$

Example 1.229 Let $P(X) = X^3 + pX + q$.

We have $m = 3$, hence $m(m-1)/2 = 3$, and $P'(X) = 3X^2 + p$. Hence

$$\operatorname{Discr} P(X) = -\operatorname{Res}_{3,2}\bigl(P, P'\bigr) = -\operatorname{Res}_{2,3}\bigl(P', P\bigr) = -3^3\left(\frac{X^3 + pX + q}{3X^2 + p}\right)$$
$$= -27\begin{vmatrix} q & -2p^2/9 \\ 2p/3 & q \end{vmatrix} = -4p^3 - 27q^2.$$

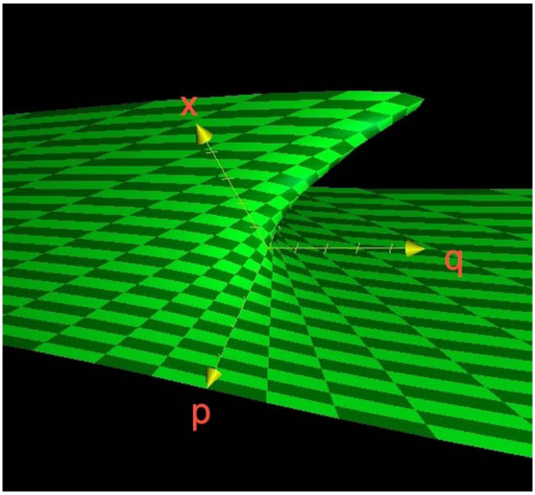
Remark 1.230 For the above computation to be correct, we must assume that the field F has characteristic different from 3.

We leave to the reader the computation in the case when F has characteristic 3.

Let us give a geometrical application of that formula.

Consider the surface defined by

$$S := \bigl\{(p, q, x) \in \mathbb{C}^3 \bigm| x^3 + px + q = 0\bigr\}.$$



Then the curve C defined by

$$C := \bigl\{(p, q) \in \mathbb{C}^2 \mid 4p^3 + 27q^2 = 0\bigr\}$$

is the apparent contour of S "seen from the plane (p, q)".

More Exercises on Sect. 1.4

Exercise 1.231 Let k be a commutative field. Let $X_1, X_2, \ldots, X_m, Y_1, Y_2, \ldots, Y_n$ be $m + n$ indeterminates. Let $a_1, a_2, \ldots, a_m \in k[Y_1, Y_2, \ldots, Y_n]$ be relatively prime.

Prove that

$$\sum_{i=1}^{i=m} a_i(Y_1, \dots, Y_n)X_i$$

is irreducible in $k[X_1, \dots, X_m, Y_1, \dots, Y_n]$.

Exercise 1.232 Let $P(X) = X^3 - X - 1 \in \mathbb{Z}[X]$.

(1) Prove that $P(X)$ is irreducible in $\mathbb{Q}[X]$.

(2) Let x, y, z be the three (distinct, why?) roots of $P(X)$ in $\mathbb{C}$. Prove the following equalities:

$$\begin{cases} x + y + z = 0, \qquad xy + yz + zx = -1, \qquad xyz = 1, \\ \big((y - x)(z - y)(x - z)\big)^2 = -23. \end{cases}$$

(3) Show that the field generated by the roots of $P(X)$ is $\mathbb{Q}[x, y, z]$.

(4) Let $\delta := \sqrt{-23}$. Prove that, for $\xi = x, y$ or z,

$$\mathbb{Q}[x, y, z] = \mathbb{Q}[\xi, \delta].$$

From now on, you may need a computer.

(5) For all prime numbers p, let us denote by N_p the number of distinct roots of $P(X)$ in $\mathbb{F}_p$. Compute N_p for $p \leq 61$. What can be said a priori about N_{23}?

(6) Let us define the sequence of integers a_n $(n \in \mathbb{N})$ by

$$X \prod_{n=1}^{\infty} \big(1 - X^n\big)\big(1 - X^{23n}\big) = \sum_{n=1}^{\infty} a_n X^n \quad .$$

Compare N_p and a_p.

Look in the literature [10], on the Web, or ask well chosen mathematicians, to explain what is going on here.

Exercise 1.233 For p a prime number, we set $P_p(X) := X^p - X + 1$ (such a polynomial is called an *Artin–Schreier polynomial*).

(1) Prove that

$$\mathrm{Disc}(P) = (-1)^{(p-1)/2}\big(p^p - (p - 1)^{p-1}\big).$$

(2) View $P_5(X)$ as an element of a polynomial ring over a field of characteristic 19, and assume that $P_5(X)$ is split over that field. Show that $P(X)$ has a multiple root.

We shall now prove that $P(X)$ is irreducible in $\mathbb{Q}[X]$. For that, we shall prove that $P(X)$ is irreducible in $\mathbb{F}_p[X]$ (why is it sufficient?). So from now on we view $P(X)$ as an element of $\mathbb{F}_p[X]$.

(3) Let k be a characteristic p field containing a root α of $P(X)$. Show that

$$P(X) = \prod_{i=0}^{p-1} (X - \alpha - i).$$

(4) Let n be an integer such that $1 \leq n < p$. Prove that if $\alpha_1, \alpha_2, \ldots, \alpha_n$ are n distinct roots of $P(X)$ in a characteristic p field, then

$$\alpha_1 + \alpha_2 + \cdots + \alpha_n \notin \mathbb{F}_p.$$

(5) Prove that $P(X)$ is irreducible in $\mathbb{F}_p[X]$.

Exercise 1.234 Let $P(X)$ and $Q(X)$ be two irreducible monic elements of $\mathbb{Q}[X]$. We denote by $\mathrm{Ro}(P)$ (resp. $\mathrm{Ro}(Q)$) the set of all roots of $P(X)$ (resp. of $Q(X)$) in $\mathbb{C}$ (we recall that they are all simple roots).

Viewing $P(Y)$ and $Q(X - Y)$ as elements of $\mathbb{Q}[X][Y]$, we denote by $Z(X) \in \mathbb{Q}[X]$ their resultant.

(1) Prove that

$$Z(X) = \prod_{\substack{x \in \mathrm{Ro}(P) \\ y \in \mathrm{Ro}(Q)}} \big(X - (x + y)\big).$$

(2) Is $Z(X)$ irreducible?

(3) Find an element of $\mathbb{Q}[X]$ which vanishes on xy for all $x \in \mathrm{Ro}(P)$ and $y \in \mathrm{Ro}(Q)$.

(4) Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.

Chapter 2
Modules

2.1 Definitions and Conventions

2.1.1 Definitions

2.1.1.1 Two Definitions for "Module"

In what follows, R denotes a (unitary) *commutative* ring. Moreover, if R is an integral domain, we denote by F its field of fractions. Note that, unless otherwise specified, we may have $R = F$.

We recall (see Definition 1.7) that an R-*module* M is an additive group endowed with a multiplication

$$R \times M \longrightarrow M, \qquad (\lambda, m) \mapsto \lambda m,$$

with the following properties (for all $m, n \in M$, $\lambda, \mu \in R$):

(BIL) it is bilinear, i.e.,

$$(\lambda + \mu)m = \lambda m + \mu m \quad \text{and} \quad \lambda(m + n) = \lambda m + \lambda n,$$

(UNI) $1_R m = m$,

(ASS) it is associative, i.e.,

$$(\lambda\mu)m = \lambda(\mu m).$$

It follows that

$$\begin{cases} 0_R m = 0_M, \\ (-\lambda)m = -(\lambda m). \end{cases}$$

The following lemma provides another equivalent definition of the notion of R-module, namely:

An R-module is an Abelian (additive) group M together with a ring morphism

$$\rho : R \to \mathrm{End}(M).$$

M. Broué, *Some Topics in Algebra*, Mathematical Lectures from Peking University, DOI 10.1007/978-3-642-41269-1_2, © Springer-Verlag Berlin Heidelberg 2014

Lemma 2.1

(1) *An Abelian group M endowed with a map*

$$R \times M \longrightarrow M, \qquad (\lambda, m) \mapsto \lambda m,$$

is an R-module if and only if the map

$$R \longrightarrow \mathrm{End}(M), \qquad \lambda \mapsto (m \mapsto \lambda m),$$

is a ring morphism.

(2) *Assume M is an Abelian group endowed with a ring morphism $\rho : R \longrightarrow$ $\mathrm{End}(M)$, then the multiplication defined by*

$$R \times M \longrightarrow M, \qquad (\lambda, m) \mapsto \rho(\lambda)(m),$$

induces on M a structure of R-module.

2.1.1.2 Morphisms

For M and N two R-modules, we recall (see Definition 1.7) that a *morphism of R-modules* (or *R-module morphism*, or simply *morphism*) $\phi : M \longrightarrow N$ is a morphism of Abelian groups such that $\phi(\lambda m) = \lambda\phi(m)$ for all $\lambda \in R$ and $m \in M$.

We denote by $\mathrm{Hom}_R(M, N)$ the set of all R-module morphisms from M to N endowed with the structure of R-module defined by

$$\begin{aligned} &\big(\phi + \phi'\big)(m) := \phi(m) + \phi'(m) \quad \text{for all } \phi, \phi' \in \mathrm{Hom}_R(M, N), m \in M, \\ &(\lambda\phi)(m) := \lambda\phi(m) \quad \text{for all } \lambda \in R, \phi \in \mathrm{Hom}_R(M, N), m \in M. \end{aligned}$$

In particular, we call *dual* of M the R-module

$$M^* := \mathrm{Hom}_R(M, R).$$

Given a morphism $\phi : M \to N$, the *dual morphism* (also called transpose) $\phi^* :$ $N^* \to M^*$ is defined by

$$\phi^* = (\xi : N \to R) \mapsto (\xi.\phi : M \to N \to R).$$

Given $M \xrightarrow{\phi} M' \xrightarrow{\phi'} M''$, we have $(\phi'\phi)^* = \phi^*\phi'^* : M''^* \xrightarrow{\phi'^*} M'^* \xrightarrow{\phi^*} M^*$.

(!) The dual of a nonzero module may be zero. Consider for example (exercise) the case of the $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$.

Examples 2.2

(1) An Abelian group G (written additively) is naturally endowed with a unique structure of $\mathbb{Z}$-module, called the *natural structure* of $\mathbb{Z}$-module, defined by

$$ng := \underbrace{g + g + \cdots + g}_{n \text{ times}} \quad \text{for } g \in G \text{ and } n \geq 0,$$

$$ng := -\underbrace{(g + g + \cdots + g)}_{|n| \text{ times}} \quad \text{for } g \in G \text{ and } n < 0.$$

The morphisms of Abelian groups are the morphisms of $\mathbb{Z}$-modules.

(2) If k is a field, the k-modules are the vector spaces over k and the morphisms of k-modules are the linear maps.

(3) A ring R is naturally endowed with a structure of R-module by its multiplicative law.

More generally, if $\mathfrak{a}$ is an ideal of R, $\mathfrak{a}$ and $R/\mathfrak{a}$ are naturally endowed with structures of R-modules. The natural injection $\mathfrak{a} \hookrightarrow R$ and the natural surjection $R \twoheadrightarrow R/\mathfrak{a}$ are morphisms of R-modules.

ⓘ **Attention** ⓘ A ring may have different module structures over itself. Consider for example the ring of polynomials $R[X, Y]$. Let us denote by $\mathrm{End}(R[X, Y])$ the ring of (additive) group endomorphisms of $R[X, Y]$. Define the ring morphism $\rho : R[X, Y] \to \mathrm{End}(R[X, Y])$ by

$$\rho : \begin{cases} X \mapsto \dfrac{\partial}{\partial X}, \\ Y \mapsto \dfrac{\partial}{\partial Y}, \end{cases}$$

where $\frac{\partial}{\partial X}$ and $\frac{\partial}{\partial Y}$ are the endomorphisms of $R[X, Y]$ which send respectively $X^m Y^n$ to $mX^{m-1}Y^n$ and to $nX^m Y^{n-1}$. Then ρ gives $R[X, Y]$ a structure of $R[X, Y]$-module which is different from the usual one (exercise!).

(4) Let V be a k-vector space. Let $\phi \in \mathrm{End}(V)$. Then the natural morphism

$$k[X] \longrightarrow \mathrm{End}(V), \qquad P(X) \mapsto P(\phi),$$

induces on V a structure of $k[X]$-module, which we shall denote V_ϕ.

The endomorphisms of the $k[X]$-module V_ϕ are those endomorphisms of the k-vector space V which commute with ϕ.

(5) Let I be a (not necessarily finite) set. Then the set R^I (set of all families $(\lambda_i)_{i \in I}$ with $\lambda_i \in R$) is naturally endowed with a structure of R-module, by the laws (with obvious notation):

- $(\lambda_i)_{i\in I} + (\mu_i)_{i\in I} := (\lambda_i + \mu_i)_{i\in I}$,
- $\lambda(\lambda_i)_{i\in I} := (\lambda\lambda_i)_{i\in I}$.

We denote by $\mathbf{e}_i$ the element of R^I all coordinates of which are zero but the ith, which is 1.

(!) If I is infinite, it is *not* true (why?) that every element $\boldsymbol{\lambda} = (\lambda_i)_{i\in I}$ can be written

$$\boldsymbol{\lambda} = \sum_{i\in I} \lambda_i \mathbf{e}_i.$$

2.1.2 Submodules

2.1.2.1 Definition, Generation

As expected, a submodule of an R-module M is

- a subset N of M,
- endowed with a structure of R-module,
- such that the inclusion $N \hookrightarrow M$ is a module morphism.

It is straightforward to check that a nonempty subset N of M is a submodule if and only if, whenever $n, n' \in N$ and $\lambda \in R$,

- $n + n' \in N$,
- $\lambda n \in N$.

Examples 2.3

(1) The $\mathbb{Z}$-submodules of an Abelian group are nothing but its subgroups.
(2) The R-submodules of a ring R (for the trivial structure) are the ideals of R.
(3) For V a k-vector space and $\phi \in \mathrm{End}(V)$, the $k[X]$-submodules of the $k[X]$-module V_ϕ are the subspaces of V which are stable under ϕ.
(4) Let I be a (not necessarily finite) set. We define the submodule $R^{(I)}$ of R^I as follows: $R^{(I)}$ is the set of all families $(\lambda_i)_{i\in I}$ such that $\lambda_i = 0$ for almost all $i \in I$ (i.e., for all indices i but a finite number). We may notice that

   - every element $\boldsymbol{\lambda} = (\lambda_i)_{i\in I} \in R^{(I)}$ can be written $\boldsymbol{\lambda} = \sum_{i\in I} \lambda_i \mathbf{e}_i$,
   - if I is finite, then $R^{(I)} = R^I$.

The following property follows easily from the definition.

Lemma 2.4 *Let M be an R-module.*

(1) *Any intersection of submodules of M is a submodule.*
(2) *If Ω is any subset of an R-module M, there is a smallest submodule of M containing Ω, namely the intersection of all submodules of M which contain Ω.*

With the notation of the above lemma, the smallest submodule containing Ω is called *the submodule generated by* Ω and is denoted by $\langle \Omega \rangle$.

Definitions 2.5

(1) Let M_1 and M_2 be two submodules of M. We denote by $M_1 + M_2$ the submodule of M generated by $M_1 \cup M_2$. One can easily check (exercise!) that

$$M_1 + M_2 = \big\{m_1 + m_2 \bigm| (m_1 \in M_1)(m_2 \in M_2)\big\}.$$

More generally, if $(M_i)_{i\in I}$ is a family of submodules of M, we denote by $\sum_{i\in I} M_i$ the submodule of M generated by $\bigcup_{i\in I} M_i$.

(2) When $X = \{m\}$ is a singleton, the submodule it generates is denoted by $\langle m\rangle$ and is sometimes called *cyclic*. We have $\langle m\rangle = Rm = \{\lambda m \mid \lambda \in R\}$.

2.1.2.2 Direct Sums

Assume that M_1 and M_2 are submodules of an R-module M, we say that the sum $M_1 + M_2$ is direct and we then write $M_1 + M_2 = M_1 \oplus M_2$ if $M_1 \cap M_2 = \{0\}$. We have $M_1 + M_2 = M_1 \oplus M_2$ if and only if, for all $m_1, m_1' \in M_1$, $m_2, m_2' \in M_2$, then

$$\big(m_1 + m_2 = m_1' + m_2'\big) \quad \Leftrightarrow \quad \big(m_1 = m_1'\big) \quad \text{and} \quad \big(m_2 = m_2'\big).$$

More generally, for a family $(M_i)_{i\in I}$ of submodules of M, we say that its sum is direct and we write

$$\sum_{i\in I} M_i = \bigoplus_{i\in I} M_i$$

if any element of $\sum_{i\in I} M_i$ can be written in a unique way as $\sum_{i\in I} m_i$ where, for $i \in I$, $m_i \in M_i$ (and $m_i = 0$ for almost all $i \in I$).

Exercises 2.6 (Another version of the Chinese Lemma)

(1) Prove that

$$\mathbb{Z}/6\mathbb{Z} = 2\mathbb{Z}/6\mathbb{Z} \oplus 3\mathbb{Z}/6\mathbb{Z}.$$

(2) Prove that if $a, b \in \mathbb{Z}$ are relatively prime, then

$$\mathbb{Z}/ab\mathbb{Z} = a\mathbb{Z}/ab\mathbb{Z} \oplus b\mathbb{Z}/ab\mathbb{Z}.$$

(3) Let k be a (commutative) field, let V be a finite dimensional k-vector space, let ϕ be an endomorphism of V, let $M(X) \in k[X]$ be the minimal polynomial of ϕ. Assume that $M(X) = P(X)Q(X)$ where $P(X)$ and $Q(X)$ are two relatively prime elements of $k[X]$. We define two submodules of V_ϕ by

$$V_\phi(P) := \ker\big(P(\phi)\big) \quad \text{and} \quad V_\phi(Q) := \ker\big(Q(\phi)\big).$$

Prove that

$$V_\phi = V_\phi(P) \oplus V_\phi(Q).$$

Example 2.7 One has

$$R^{(I)} = \bigoplus_{i \in I} R\mathbf{e}_i .$$

Definition 2.8 An R-module M is said to be *indecomposable* if any decomposition $M = M_1 \oplus M_2$ implies $M_1 = 0$ or $M_2 = 0$.

Exercise 2.9

(1) Let $n \geq 2$ be an integer. Prove that the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ is indecomposable if and only if n is a power of a prime number.

(2) Let $P(X) \in k[X]$ be a polynomial with coefficients in a field k, of degree at least 1. Prove that the $k[X]$-module $k[X]/(P(X))$ is indecomposable if and only if $P(X)$ is a power of an irreducible polynomial.

2.1.2.3 Quotients

The reader is certainly familiar with the following result.

Lemma 2.10 *If N is a submodule of an R-module M, there is one and only one structure of R-module on the factor group M/N such that the natural surjection*

$$\pi_N : M \twoheadrightarrow M/N$$

is an R-module morphism.

Note that the kernel of π_N (as an R-module morphism) is the submodule N.

The pair $(M/N, \pi_N)$ satisfies the following universal property, whose proof is left to the reader.

Proposition 2.11 *Let (M', ϕ) be a pair (M' a module, $\phi : M \to M'$ a morphism) such that $N \subseteq \ker(\phi)$. Then there exists a unique morphism $\phi_N : M/N \to M'$ such that the following diagram commutes*:

$$\begin{tikzcd}
M \arrow[rr, "\phi"] \arrow[dr, "\pi_N"'] & & M' \\
& M/N \arrow[ur, "\phi_N"'] &
\end{tikzcd}$$

Moreover, the kernel of ϕ_N is $\ker(\phi)/N$.

Remark 2.12 As usual, the reader may check that the above universal property in Proposition 2.11 implies the uniqueness of the pair $(M/N, \pi_N)$ up to *unique isomorphism*, in the following sense:

If (M', π') is a pair such that

- M' is a module,
- $\pi' : M \twoheadrightarrow M'$ is a surjective morphism,

satisfying the property of $(M/N, \pi_N)$ described in Proposition 2.11, then there exists a unique isomorphism $\sigma : M/N \xrightarrow{\sim} M'$ such that the following diagram commutes:

$$\begin{tikzcd}
 & M \arrow[dl, "\pi_N"'] \arrow[dr, "\pi'"] & \\
M/N \arrow[rr, dash, "\sigma"'] & & M'
\end{tikzcd}$$

2.1.2.4 Kernels, Images, Cokernels, Coimages

Let $\phi : M \to N$ be a morphism of R-modules.

The kernel $\ker(\phi)$ and the image $\mathrm{im}(\phi)$ are the submodules of respectively M and N defined by

$$\ker(\phi) := \{m \in M \mid \phi(m) = 0\} \quad \text{and} \quad \mathrm{im}(\phi) := \{\phi(m) \mid m \in M\}.$$

The cokernel $\mathrm{coker}(\phi)$ and the coimage $\mathrm{coim}(\phi)$ are the quotients of respectively N and M defined by

$$\mathrm{coker}(\phi) := N/\,\mathrm{im}(\phi) \quad \text{and} \quad \mathrm{coim}(\phi) := M/\ker(\phi).$$

The proof of the following lemma is left to the reader.

Lemma 2.13 *There exists a unique isomorphism* $\overline{\phi} : \mathrm{coim}(\phi) \xrightarrow{\sim} \mathrm{im}(\phi)$ *such that the following diagram* (*where the diagonal arrows are the natural morphisms*)

$$\begin{tikzcd}
M \arrow[rrr, "\phi"] \arrow[dr] & & & N \\
 & \mathrm{coim}(\phi) \arrow[r, "\overline{\phi}"] & \mathrm{im}(\phi) \arrow[ur] &
\end{tikzcd}$$

commutes.

Exercises 2.14

(1) Let M_1 and M_2 be two submodules of an R-module M. Then the natural injection of M_1 into $M_1 + M_2$ induces an isomorphism

$$M_1/(M_1 \cap M_2) \xrightarrow{\sim} (M_1 + M_2)/M_2.$$

(2) Let M' and N be two submodules of an R-module M such that $N \subseteq M'$. Then the natural surjection $M/N \twoheadrightarrow M/M'$ induces an isomorphism

$$(M/N)/\big(M'/N\big) \xrightarrow{\sim} M/M'.$$

(3) Let $\phi : M \to M'$ be a morphism of R-modules, and let N and N' respectively be submodules of M and M' such that $\phi(N) \subset N'$. Prove that there exists a unique morphism $\widetilde{\phi} : M/N \to M'/N'$ such that the following diagram commutes:

$$\begin{tikzcd}
M \arrow[r, "\phi"] \arrow[d, "\pi_N"'] & M' \arrow[d, "\pi_{N'}"] \\
M/N \arrow[r, "\widetilde{\phi}"] & M'/N'
\end{tikzcd}$$

2.1.2.5 Exact Sequences

Given a composition

$$M' \xrightarrow{\iota} M \xrightarrow{\pi} M''$$

of morphisms, one says that it is exact if $\mathrm{im}(\iota) = \ker(\pi)$.

A sequence of compositions

$$\cdots \to M_{n-1} \xrightarrow{\phi_{n-1}} M_n \xrightarrow{\phi_n} M_{n+1} \xrightarrow{\phi_{n+1}} M_{n+2} \to \cdots$$

is said to be *exact* if all subcompositions are exact, namely

$$\ldots, \quad \mathrm{im}(\phi_{n-1}) = \ker(\phi_n), \quad \mathrm{im}(\phi_n) = \ker(\phi_{n+1}), \quad \ldots$$

A *short sequence* is a composition of morphisms

$$0 \longrightarrow M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \longrightarrow 0.$$

It is *exact* if and only if it is exact in the sense of the previous definition, i.e.,

$$\begin{cases} \ker(\iota) = 0 \quad \text{that is, } \iota \text{ injective,} \\ \mathrm{im}(\iota) = \ker(\pi), \\ \mathrm{im}(\pi) = M'' \quad \text{that is, } \pi \text{ surjective.} \end{cases}$$

Exercise 2.15 Let $0 \longrightarrow M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \longrightarrow 0$ be a short exact sequence.

(1) Prove that the sequence $0 \longrightarrow M''^* \xrightarrow{\pi^*} M^* \xrightarrow{\iota^*} M'^*$ is exact,
(2) but give an example where the sequence

$$0 \longrightarrow M''^* \xrightarrow{\pi^*} M^* \xrightarrow{\iota^*} M'^* \longrightarrow 0$$

is not exact.

Definition 2.16 We say that a submodule N of a module M is a *summand* of M if there exists a submodule N' of M such that $N \oplus N' = M$.

Such a module N' is then called a *complement* of N in M.

⚠ A submodule needs not have a complement. This is the case, for example (exercise) of $2\mathbb{Z}$ as a submodule of $\mathbb{Z}$.

The next proposition describes, in terms of exact sequences, necessary and sufficient conditions for a submodule to have a complement. Its proof is left as an exercise for the reader.

Proposition 2.17 (Exercise) *Let N be a submodule of M. Let $\iota_N : N \to M$ be the natural inclusion and $\pi_N : M \to M/N$ be the natural surjection, so that we have the short exact sequence*

$$0 \longrightarrow N \xrightarrow{\iota_N} M \xrightarrow{\pi_N} M/N \longrightarrow 0.$$

The following assertions are equivalent.

(i) *There exists a morphism $\iota'_N : M \to N$ such that $\iota'_N \iota_N = \mathrm{Id}_N$.*
(ii) *There exists a morphism $\pi'_N : M/N \to M$ such that $\pi_N \pi'_N = \mathrm{Id}_{M/N}$.*
(iii) *There exist morphisms $\iota'_N : M \to N$ and $\pi'_N : M/N \to M$ such that $\iota_N \iota'_N + \pi'_N \pi_N = \mathrm{Id}_M$.*

Moreover, if the above properties hold,

- $M = \iota_N(N) \oplus \pi'_N(M/N)$,
- *the sequence*

$$0 \longrightarrow M/N \xrightarrow{\pi'_N} M \xrightarrow{\iota'_N} N \longrightarrow 0$$

is also exact,
- *the endomorphisms $e' := \iota_N \iota'_N$ and $e'' := \pi'_N \pi_N$ of M are idempotents, that is $e'^2 = e'$, $e''^2 = e''$.*

2.1.2.6 Ideals and Modules

Let M be an R-module and $\mathfrak{a}$ be an ideal of R. We denote by $\mathfrak{a}M$ the submodule of M generated by all the elements am for $a \in \mathfrak{a}$ and $m \in M$. Thus, $\mathfrak{a}M$ is the set of all (finite!) sums $\sum am$ for $a \in \mathfrak{a}$ and $m \in M$.

The following properties are straightforward and will be often implicitly used.

Lemma 2.18

(1) *Let M be an R-module. The structural morphism $R \to \mathrm{End}(M)$ factorizes through the natural surjection $\pi_{\mathfrak{a}} : R \twoheadrightarrow R/\mathfrak{a}$ if and only if $\mathfrak{a}M = 0$.*

In other words, M inherits a natural structure of $R/\mathfrak{a}$-module if and only if $\mathfrak{a}M = 0$.

Reciprocally any $R/\mathfrak{a}$-module inherits (by composition of its structural morphism $\rho_{\mathfrak{a}}$ with the natural surjection $\pi_{\mathfrak{a}} : R \twoheadrightarrow R/\mathfrak{a}$) a structure of R-module.

$$\begin{tikzcd} R \arrow[rr, "\rho"] \arrow[dr, "\pi_{\mathfrak{a}}"'] & & \mathrm{End}(M) \\ & R/\mathfrak{a} \arrow[ur, "\rho_{\mathfrak{a}}"'] & \end{tikzcd}$$

(2) *The module $M/\mathfrak{a}M$ is naturally endowed with a structure of $R/\mathfrak{a}$-module.*

(3) *For $\phi : M \to N$ a morphism, we have $\phi(\mathfrak{a}M) \subset \mathfrak{a}N$ and so ϕ induces a morphism of $R/\mathfrak{a}$-modules $\phi_{\mathfrak{a}} : M/\mathfrak{a}M \to N/\mathfrak{a}N$.*

(4) *If $M = M_1 \oplus M_2$, then $M/\mathfrak{a}M = (M_1/\mathfrak{a}M_1) \oplus (M_2/\mathfrak{a}M_2)$.*

(5) *If I is a set, we have*

$$R^I/\mathfrak{a}R^I = (R/\mathfrak{a})^I \quad \textit{and} \quad R^{(I)}/\mathfrak{a}R^{(I)} = (R/\mathfrak{a})^{(I)}.$$

Examples 2.19

(1) Let G be an additive Abelian group and let p be a prime number. If $pG = 0$, then G is naturally endowed with a structure of $\mathbb{F}_p$-vector space.

(2) (Exercise) Let V be a Euclidean (real) vector space of dimension 2, and let ρ be a nontrivial rotation on V. Then the $\mathbb{R}[X]$-module V_ρ has a natural structure of $\mathbb{C}$-vector space.

2.1.3 Torsion Elements, Torsion Submodule

2.1.3.1 Cyclic Modules

We recall that a module is *cyclic* if it may be generated by one element.

Let M be an R-module and let $m \in M$. Then the cyclic submodule $\langle m \rangle$ generated by m is $\langle m \rangle = Rm = \{\lambda m \mid \lambda \in R\}$. Hence one has a surjective R-module morphism $\pi_m : R \twoheadrightarrow Rm, \lambda \mapsto \lambda m$, which induces an isomorphism $R/\mathrm{Ann}_R(m) \xrightarrow{\sim} Rm$ where the ideal $\mathrm{Ann}_R(m)$ is defined by

$$\mathrm{Ann}_R(m) := \{\lambda \in R \mid \lambda m = 0\}.$$

Remark 2.20 What precedes shows that the cyclic R-modules are, up to isomorphism, the R-modules $R/\mathfrak{a}$ for $\mathfrak{a}$ an ideal of R.

Indeed, we have seen above that a cyclic module is of that type. Reciprocally, given the R-module $R/\mathfrak{a}$, let us denote by m the image of 1 under the natural surjection $\pi_{\mathfrak{a}} : R \twoheadrightarrow R/\mathfrak{a}$. It is then clear that $R/\mathfrak{a}$ is generated by m, hence is cyclic.

More generally, if E is a subset of M, we call *annihilator of E* and we denote by $\mathrm{Ann}_R(E)$ the ideal of R

$$\mathrm{Ann}_R(E) := \bigcap_{m\in E} \mathrm{Ann}_R(m).$$

2.1.3.2 Torsion and Torsion Free Elements

An element $m \in M$ is said to be

- a torsion element if $\mathrm{Ann}_R(m) \neq 0$,
- torsion free if $m \neq 0$ and $\mathrm{Ann}_R(m) = 0$.

Examples 2.21

- The Abelian group ($\mathbb{Z}$-module) $\mathbb{Q}$ has no torsion element but 0.
- R is an integral domain if and only if (considered as an R-module in the natural way) it has no torsion element but 0. In that case, the R-modules R^I and $R^{(I)}$ have no torsion element but 0.
- If $\mathfrak{a}$ is a nonzero proper ideal of R, all the elements of the R-module $R/\mathfrak{a}$ are torsion elements. Viewed as an $R/\mathfrak{a}$-module, $R/\mathfrak{a}$ has no torsion element but 0 if and only if $\mathfrak{a}$ is prime.
- More generally, if $\mathfrak{a}$ is a nonzero ideal of R, and if M is an R-module, all the elements of the R-module $M/\mathfrak{a}M$ are torsion elements.

Lemma 2.22 *If R is an integral domain, the subset of M*

$$\mathrm{tor}(M) := \big\{m \in M \bigm| \mathrm{Ann}_R(m) \neq \{0\}\big\},$$

(*consisting of all torsion elements of M*) *is a submodule of M.*

Proof It is clear that if m is a torsion element and $\lambda \in R$, then λm is still a torsion element. Let us check that if m and n are torsion elements, so is $m + n$. Indeed, there are nonzero elements $\lambda, \mu \in R$ such that $\lambda m = \mu n = 0$. Then $\lambda\mu(m + n) = 0$. Since R is an integral domain, $\lambda\mu \neq 0$, which shows that $m + n$ is a torsion element. □

Exercise 2.23 Give an example of an R-module M (R not an integral domain) such that the subset $\mathrm{tor}(M) := \{m \in M \mid \mathrm{Ann}_R(m) \neq \{0\}\}$ is not a submodule.

If R is an integral domain, the submodule $\operatorname{tor}(M)$ is called *the torsion submodule* of M. We say that M is

- a *torsion module* if $M = \operatorname{tor}(M)$,
- *torsion free* if $\operatorname{tor}(M) = \{0\}$.

Examples 2.24

(1) Let k be a field. View its multiplicative group $k^\times$ as endowed with its (unique) structure of $\mathbb{Z}$-module. Then

$$\operatorname{tor}\bigl(k^\times\bigr) = \boldsymbol{\mu}(k),$$

the group of roots of unity of k.

Thus

$$\operatorname{tor}\bigl(\mathbb{R}^\times\bigr) = \operatorname{tor}\bigl(\mathbb{Q}^\times\bigr) = \{\pm 1\}, \qquad \operatorname{tor}\bigl(\mathbb{Q}(i)\bigr) = \{\pm 1, \pm i\}, \qquad \operatorname{tor}(\mathbb{F}_p) = \mathbb{F}_p^\times,$$

and

$$\operatorname{tor}\bigl(\mathbb{C}^\times\bigr) = \bigl\{e^{2\pi i k/n} \bigm| (k, n \in \mathbb{Z})(n \neq 0)\bigr\} \cong \mathbb{Q}/\mathbb{Z}.$$

(2) Here $R = \mathbb{Z}$. We have

$$\operatorname{tor}(\mathbb{Q}) = \{0\}, \qquad \mathbb{Q}/\mathbb{Z} = \operatorname{tor}(\mathbb{Q}/\mathbb{Z}), \qquad \operatorname{tor}\bigl((\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}\bigr) = (\mathbb{Z}/2\mathbb{Z}) \times \{0\}.$$

Note that

$$\bigl((\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}\bigr) \bigm/ \operatorname{tor}\bigl((\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}\bigr) \cong \mathbb{Z}.$$

(3) For R an integral domain and M an R-module, $\operatorname{tor}(M^*) = 0$.

(!) This shows in particular that not any module can be a dual. It follows that in general we do not have $M \cong M^{**}$.

Proposition 2.25 *Assume R is an integral domain. For any R-module M we have*:

(1) $\operatorname{tor}(\operatorname{tor}(M)) = \operatorname{tor}(M)$.
(2) $\operatorname{tor}(M/\operatorname{tor}(M)) = \{0\}$.

Proof of Proposition 2.25 (1) is obvious. Let us prove (2). Let $m \in M$ such that its image in $M/\operatorname{tor}(M)$ is annihilated by a nonzero element $\lambda \in R$. Thus, $\lambda m \in \operatorname{tor}(M)$. Hence there is a nonzero element $\lambda' \in R$ such that $\lambda'\lambda m = 0$. Since R is an integral domain, we have $\lambda'\lambda \neq 0$ and $m \in \operatorname{tor}(M)$. □

2.1.4 Free and Generating Systems, Free Modules

2.1.4.1 Free Systems, Generating Systems, Bases

Let I be a (not necessarily finite) set and let $(x_i)_{i \in I}$ be a family of elements of the R-module M. The submodule generated by $(x_i)_{i \in I}$ is denoted by $\sum_{i \in I} Rx_i$.

One defines a morphism of R-modules with image $\sum_{i\in I} Rx_i$ by

$$\phi : R^{(I)} \longrightarrow M, \qquad (\lambda_i)_{i\in I} \mapsto \sum_{i\in I} \lambda_i x_i .$$

Definition 2.26

(1) We say that the system $(x_i)_{i\in I}$ is respectively *free*, *generator*, *a basis*, if and only if the morphism ϕ is respectively injective, surjective, an isomorphism.
(2) If M has a basis, one says that M is *free*.

(!) A singleton (x) (a single element family) is free if and only if $\mathrm{Ann}_R(x) = \{0\}$. The proof of the next lemma is left as an exercise.

Lemma 2.27 *If $(x_i)_{i\in I}$ is free, then*

(1) *each subfamily $(x_i)_{i\in J}$ $(J \subset I)$ is free,*
(2) $\sum_{i\in I} Rx_i = \bigoplus_{i\in I} Rx_i$.

(!) **Attention** (!) One may have

$$M = \bigoplus_{i\in I} Rx_i$$

without $(x_i)_{i\in I}$ being a basis of M (example?).

2.1.4.2 A Property of Free Modules

The proof of the following lemma is obvious.

Lemma 2.28 *Let L be a free R-module with basis $(x_i)_{i\in I}$. For any R-module M, the map*

$$\begin{cases} \mathrm{Hom}_R(L, M) \to M^I \\ \phi \mapsto \big(\phi(x_i)\big)_{i\in I}, \end{cases}$$

is a bijection.

Proposition 2.29 *Let L be a free R-module.*

(1) *Let $X \xrightarrow{\pi} Y \to 0$ be an exact sequence of R-modules (that is, the morphism $\pi : X \to Y$ is surjective), and let $\phi : L \to Y$ be a morphism. Then there exists a*

morphism $\widetilde{\phi} : L \to X$ *such that the following diagram commutes*

$$\begin{tikzcd}
X \arrow[r, "\pi"] & Y \arrow[r] & 0 \\
& L \arrow[ul, dashed, "\widetilde{\phi}"] \arrow[u, "\phi"'] &
\end{tikzcd}$$

(2) *In particular, for any* R*-module* M, *any surjective morphism* $\pi : M \twoheadrightarrow L$ *has a section, that is, there is a morphism* $\sigma : L \to M$ *such that* $\pi.\sigma = \mathrm{Id}_L$. *In that case,* σ *is injective,* $\mathrm{im}(\sigma) \cong L$ *and we have*

$$M = \ker(\pi) \oplus \mathrm{im}(\sigma).$$

Proof (1) Let $(e_i)_{i \in I}$ be a basis of L. For all $i \in I$, let x_i be an element of X such that $\pi(x_i) = \phi(e_i)$. We then define $\widetilde{\phi}$ (see Lemma 2.28) by $\widetilde{\phi}(e_i) := x_i$.

(2) This is a particular case of (1) :

$$\begin{tikzcd}
M \arrow[r, "\pi"] & L \arrow[r] & 0 \\
& L \arrow[ul, dashed, "\sigma"] \arrow[u, "\mathrm{Id}_L"'] &
\end{tikzcd}$$

Since $\pi.\sigma = \mathrm{Id}_L$, σ is injective. For $m \in M$, we have $m = \sigma(\pi(m)) + (m - \sigma(\pi(m)))$. Since $m - \sigma(\pi(m)) \in \ker(\pi)$, it follows that

$$M = \ker(\pi) + \mathrm{im}(\sigma).$$

Again since $\pi.\sigma = \mathrm{Id}_L$, we have $\ker(\pi) \cap \mathrm{im}(\sigma) = \{0\}$, and the sum is direct. □

Exercise 2.30 Let P be a summand (see Definition 2.16) of a free module L. Show that whenever $X \xrightarrow{\pi} Y \to 0$ is an exact sequence and $\phi : P \to Y$ is a morphism, there exists a morphism $\widetilde{\phi} : P \to X$ such that the diagram

$$\begin{tikzcd}
X \arrow[r, "\pi"] & Y \arrow[r] & 0 \\
& P \arrow[ul, dashed, "\widetilde{\phi}"] \arrow[u, "\phi"'] &
\end{tikzcd}$$

commutes.

2.1.4.3 Projective Modules

Proposition 2.31 *Let* P *be an* R*-module. The following assertions are equivalent.*

(i) *Whenever* $X \xrightarrow{\pi} Y \to 0$ *is an exact sequence of* R*-modules and* $\phi : P \to Y$ *is a morphism, there exists a morphism* $\widetilde{\phi} : P \to X$ *such that the diagram*

$$\begin{tikzcd}
X \arrow[r, "\pi"] & Y \arrow[r] & 0 \\
& P \arrow[u, "\phi"'] \arrow[ul, dashed, "\widetilde{\phi}"] &
\end{tikzcd}$$

commutes.

(ii) P *is a summand* (*see Definition* 2.16) *of a free* R*-module.*

Proof For the implication (ii)⇒(i), see Exercise 2.30. Let us prove (i)⇒(ii).

There exists a free module F and a surjective morphism $\pi : F \twoheadrightarrow P$. Indeed, one may choose $F := R^{(P)}$, and denote by π the obvious surjective morphism $R^{(P)} \twoheadrightarrow P$.

Considering the diagram

$$\begin{tikzcd}
F \arrow[r, "\pi"] & P \arrow[r] & 0 \\
& P \arrow[u, "\mathrm{Id}_P"'] &
\end{tikzcd}$$

we see that there exists a morphism $\sigma : P \to F$ such that $\pi.\sigma = \mathrm{Id}_P$. This shows that P is isomorphic to a summand of F (see the proof of Proposition 2.29, (2)). □

Definition 2.32 A module P which satisfies the properties of the above proposition is called a *projective module*.

The proof of (i)⇒(ii) given above provides also a proof of the following lemma.

Lemma 2.33 *If* P *is a projective module, and if* $\pi : M \twoheadrightarrow P$ *is a surjective morphism, there exists a section of* π, *i.e., a morphism* $\sigma : P \to M$ *such that* $\pi.\sigma = \mathrm{Id}_P$.

In particular, P *is isomorphic to a summand of* M.

Examples 2.34 There are modules which are projective but not free:

- If $R = R_1 \times R_2$ is a product of two nonzero rings, then R_1, viewed as an R-module, is projective (since it is isomorphic to a summand of R), but not free (why?).
- We shall see that all ideals of a Dedekind domain R are projective (see below Definition 2.159); moreover if R is not a principal ideal domain (for example, $R = \mathbb{Z}[\sqrt{-5}]$), there are non free ideals.
- If R is a principal ideal domain, or if R is a local ring (see Proposition 2.136), or if $R = k[X_1, \ldots, X_n]$ for k a field (see Remark 2.139), we shall see that all finitely generated projective R-modules are free.

2.1.5 Constructions: Direct Sums, Products, Tensor Products

2.1.5.1 Direct Sums (Coproducts) and Products

Let I be a (not necessarily finite) set, and let $(M_i)_{i\in I}$ be a family of R-modules indexed by that set.

Definition 2.35

(1) The *coproduct* (or *direct sum*) of the family $(M_i)_{i\in I}$ is a pair $(\mathrm{Coprod}((M_i)_{i\in I}), (\iota_i)_{i\in I})$ where

- $\mathrm{Coprod}((M_i)_{i\in I})$ is an R-module,
- $(\iota_i)_{i\in I}$ is a family of morphisms

$$\iota_i : M_i \to \mathrm{Coprod}\big((M_i)_{i\in I}\big),$$

satisfying the following universal property:

Given an R-module M and a family $(\phi_i : M_i \to M)_{i\in I}$ of morphisms, there exists a unique morphism $\phi : \mathrm{Coprod}((M_i)_{i\in I}) \to M$ such that the following diagrams commute for all $i \in I$:

$$\begin{tikzcd}
M_i \arrow[rr, "\phi_i"] \arrow[dr, "\iota_i"'] & & M \\
& \mathrm{Coprod}((M_i)_{i\in I}) \arrow[ur, dashed, "\phi"'] &
\end{tikzcd}$$

(2) The *product* of $(M_i)_{i\in I}$ is a pair $(\mathrm{Prod}((M_i)_{i\in I}), (\pi_i)_{i\in I})$ where

- $\mathrm{Prod}((M_i)_{i\in I})$ is an R-module,
- $(\pi_i)_{i\in I}$ is a family of morphisms

$$\pi_i : \mathrm{Prod}\big((M_i)_{i\in I}\big) \to M_i,$$

satisfying the following universal property:

Given an R-module M and a family $(\psi_i : M \to M_i)_{i\in I}$ of morphisms, there exists a unique morphism $\psi : M \to \mathrm{Prod}((M_i)_{i\in I})$ such that the following diagrams commute for all $i \in I$:

$$\begin{tikzcd}
M \arrow[rr, "\psi_i"] \arrow[dr, dashed, "\psi"'] & & M_i \\
& \mathrm{Prod}((M_i)_{i\in I}) \arrow[ur, "\pi_i"'] &
\end{tikzcd}$$

As usual, if they exist, the coproduct and the product are unique up to unique isomorphisms.

Their existence is immediate:

- We set $\prod_{i\in I} M_i := \{(m_i)_{i\in I} \mid \text{for all } i \in I, m_i \in M_i\}$, endowed with the obvious "component by component" module structure, and we denote by $\pi_j : \prod_{i\in I} M_i \to M_j$ the obvious projection. Then (exercise) the pair $(\prod_{i\in I} M_i, (\pi_i)_{i\in I})$ is the product of $(M_i)_{i\in I}$.
- We denote by $\coprod_{i\in I} M_i$ the submodule of $\prod_{i\in I} M_i$ consisting of the families $(m_i)_{i\in I}$ where $m_i = 0$ for almost every $i \in I$, and we denote by $\iota_i : M_i \to \coprod_{i\in I} M_i$ the obvious injection. Then (exercise) the pair $(\coprod_{i\in I} M_i, (\iota_i)_{i\in I})$ is the coproduct of $(M_i)_{i\in I}$.

Remarks 2.36

- Let us set $\widetilde{M}_i := \iota_i(M_i)$. Then we have
$$\coprod_{i\in I} M_i = \bigoplus_{i\in I} \widetilde{M}_i .$$
We shall identify M_i with its image $\widetilde{M}_i$ in $\coprod_{i\in I} M_i$, and so we shall write (abuse of notation)
$$\coprod_{i\in I} M_i = \bigoplus_{i\in I} M_i .$$
- We have $R^I = \prod_{i\in I} R$ and $R^{(I)} = \coprod_{i\in I} R$.
- If I is finite, $\coprod_{i\in I} M_i = \prod_{i\in I} M_i$.

Exercise 2.37 Let $(M_i)_{i\in I}$ be a family of R-modules and let M be an R-module. Describe isomorphisms of R-modules

$$\mathrm{Hom}_R\Big(\coprod_{i\in I} M_i, M\Big) \xrightarrow{\sim} \prod_{i\in I} \mathrm{Hom}_R(M_i, M)$$
$$\mathrm{Hom}_R\Big(M, \prod_{i\in I} M_i\Big) \xrightarrow{\sim} \prod_{i\in I} \mathrm{Hom}_R(M, M_i).$$

The proof of the next proposition is left to the reader. It is a slight generalization of Proposition 2.17.

Proposition 2.38 *Let*

$$0 \to M' \xrightarrow{\alpha'} M \xrightarrow{\alpha''} M'' \to 0 \tag{2.1}$$

be a short exact sequence of R-modules.

The following assertions are equivalent.

(i) *There exists a morphism* $\beta' : M \to M'$ *such that* $\beta'\alpha' = \mathrm{Id}_{M'}$.
(ii) *There exists a morphism* $\beta'' : M'' \to M$ *such that* $\alpha''\beta'' = \mathrm{Id}_{M''}$.
(iii) *There exist morphisms* $\beta' : M \to M'$ *and* $\beta'' : M'' \to M$ *such that* $\alpha'\beta' + \beta''\alpha'' = \mathrm{Id}_M$.
(iv) *There exists an isomorphism* $\sigma : M \xrightarrow{\sim} M' \oplus M''$ *such that the following diagram is commutative*:

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "\alpha'"] \arrow[d, equal] & M \arrow[r, "\alpha''"] \arrow[d, "\sigma"] & M'' \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & M' \arrow[r, hook] & M' \oplus M'' \arrow[r, two heads] & M'' \arrow[r] & 0
\end{tikzcd}$$

Moreover, if the above properties hold,

- *the sequence*
$$0 \longrightarrow M'' \xrightarrow{\beta''} M \xrightarrow{\beta'} M' \longrightarrow 0 \tag{2.2}$$
is also exact,
- *the endomorphisms* $e' := \alpha'\beta'$ *and* $e'' := \beta''\alpha''$ *of* M *are idempotents, that is* $e'^2 = e'$, $e''^2 = e''$.

If the above properties hold, we say that the sequence (2.1) (and the sequence (2.2)) is *split*.

The next result is then an application of Lemma 2.33.

Proposition 2.39 *Let*

$$0 \to M' \xrightarrow{\alpha'} M \xrightarrow{\alpha''} M'' \to 0 \tag{2.3}$$

be a short exact sequence of R*-modules. Assume* M'' *is projective. Then the sequence is split, and in particular it induces an isomorphism* $M \xrightarrow{\sim} M' \oplus M''$.

If such a short exact sequence as above is split, we see that both M' and M'' are isomorphic to summands of M.

In that case, by some abuse of language, we sometimes say that *M' and M'' are summands of M*.

2.1.5.2 Tensor Products

The tensor product $M \otimes_R N$ of two R-modules M and N *"linearizes the bilinear maps"* in the following sense.

Definition 2.40 The tensor product of M and N is a pair $(M \otimes_R N, t_{M,N})$ where

- $M \otimes_R N$ is an R-module
- $t_{M,N} : M \times N \to M \otimes_R N$ is a bilinear map, usually denoted

$$(m, n) \mapsto m \otimes_R n,$$

which satisfies the following universal property:

Whenever X is an R-module and $f : M \times N \to X$ is a bilinear map, there exists a unique R-module morphism $\overline{f} : M \otimes_R N \to X$ such that the diagram

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[d, "t_{M,N}"'] & X \\ M \otimes_R N \arrow[ur, dashed, "\overline{f}"'] & \end{tikzcd}$$

is commutative.

We shall prove now that the tensor product exists.

Indeed, let us consider the module $R^{(M \times N)}$, and its submodule B generated by the following set:

$$\{\mathbf{e}_{(m_1+m_2,n)} - \mathbf{e}_{(m_1,n)} - \mathbf{e}_{(m_2,n)}, \mathbf{e}_{(m,n_1+n_2)}, - \mathbf{e}_{(m,n_1)} - \mathbf{e}_{(m,n_2)},$$
$$\lambda\mathbf{e}_{(m,n)} - \mathbf{e}_{(\lambda m,n)}, \lambda\mathbf{e}_{(m,n)} - \mathbf{e}_{(m,\lambda n)}\}_{m,m_1,m_2 \in M, n,n_1,n_2 \in N, \lambda \in R}$$

We define

$$\begin{cases} M \otimes_R N := R^{(M \times N)}/B, \\ t_{M,N} : M \times N \to M \otimes_R N, (m, n) \mapsto \pi_B(\mathbf{e}_{(m,n)}). \end{cases}$$

Exercise 2.41

(1) Check that the map $t_{M,N}$ is well defined and is bilinear.
(2) Check that the pair $(M \otimes_R N, t_{M,N})$ just defined is a tensor product.

Exercise 2.42 Assume that $a, b \in \mathbb{Z}$ are relatively prime. Prove that

$$(\mathbb{Z}/a\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/b\mathbb{Z}) = 0.$$

First properties.

(1) Since it solves a universal problem, the tensor product (as a pair $(M \otimes_R N, t_{M,N})$) is unique up to unique isomorphism.
(2) The set of elements $\{m \otimes_R n\}_{m \in M, n \in N}$, called *elementary tensors*, generates $M \otimes_R N$.

Indeed, this follows from the very definition. But, since $(M \otimes_R N, t_{M,N})$ is unique up to unique isomorphism, the reader is invited to find a proof which does not depend on the construction which has been given.

ⓘ But by no way is the family $(m \otimes_R n)_{m\in M, n\in N}$ the set of all elements of $M \otimes_R N$ nor a basis of $M \otimes_R N$, even if M and N are finite dimensional vector spaces—see below Exercise 2.45.

(3) Whenever $m \in M$, the map

$$N \to M \otimes_R N, \qquad n \mapsto m \otimes_R n$$

is a morphism of R-modules. Hence its image $m \otimes_R N := \{m \otimes_R n \mid n \in N\}$ is a submodule of $M \otimes_R N$, isomorphic to a quotient of N.

In the next proposition, the isomorphisms are defined by their action on elementary tensors. The proofs are left as exercises to the reader.

Proposition 2.43

(1) *We have unique isomorphisms*

$$\begin{cases} (M_1 \otimes_R M_2) \otimes_R M_3 \xrightarrow{\sim} M_1 \otimes_R (M_2 \otimes_R M_3) \\ (m_1 \otimes_R m_2) \otimes_R m_3 \mapsto m_1 \otimes_R (m_2 \otimes_R m_3), \end{cases}$$

$$\begin{cases} M_1 \otimes_R M_2 \xrightarrow{\sim} M_2 \otimes_R M_1 \\ m_1 \otimes_R m_2 \mapsto m_2 \otimes_R m_1, \end{cases}$$

(2) *as well as*

$$\begin{cases} M_1 \otimes_R (M_2 \oplus M_3) \xrightarrow{\sim} (M_1 \otimes_R M_2) \oplus (M_1 \otimes_R M_3) \\ m_1 \otimes_R (m_2 + m_3) \mapsto (m_1 \otimes_R m_2) + (m_1 \otimes_R m_3), \end{cases}$$

and more generally

$$\begin{cases} M \otimes_R \left(\bigoplus_{i\in I} M_i\right) \xrightarrow{\sim} \bigoplus_{i\in I} (M \otimes_R M_i) \\ m \otimes_R \left(\sum_{i\in I} m_i\right) \mapsto \sum_{i\in I} (m \otimes_R m_i), \end{cases}$$

(3) *as well as*

$$\begin{cases} R \otimes_R M \xrightarrow{\sim} M \\ \lambda \otimes_R m \mapsto \lambda m, \end{cases}$$

and more generally

$$\begin{cases} R^{(I)} \otimes_R M \xrightarrow{\sim} M^{(I)} \\ (\lambda_i)_{i\in I} \otimes_R m \mapsto (\lambda_i m)_{i\in I}. \end{cases}$$

Corollary 2.44

(1) *Assume that M is a free module with basis $(e_i)_{i\in I}$. Then we have*

$$M \otimes_R N = \bigoplus_{i\in I} e_i \otimes_R N.$$

(2) *Assume moreover that N is a free module with basis $(f_j)_{j\in J}$. Then $M \otimes_R N$ is a free module with basis $(e_i \otimes_R f_j)_{i\in I, j\in J}$.*

Exercises 2.45

(1) Let k be a field, and let V_1 and V_2 be finite dimensional k-vector spaces. Prove that the bilinear map

$$\begin{cases} V_1^* \times V_2 \longrightarrow \mathrm{Hom}_k(V_1, V_2) \\ (\xi_1, v_2) \mapsto \big(v_1 \mapsto \xi_1(v_1)v_2\big) \end{cases}$$

induces an isomorphism

$$V_1^* \otimes_k V_2 \xrightarrow{\sim} \mathrm{Hom}_k(V_1, V_2).$$

Remark 2.46 Through the preceding isomorphism, the elementary tensors correspond to the rank (at most) one linear maps from V_1 to V_2.

(2) Describe natural inverse isomorphisms

$$\mathrm{Hom}_R(L \otimes_R M, N) \overset{\sim}{\longleftrightarrow} \mathrm{Hom}_R\big(L, \mathrm{Hom}_R(M, N)\big)$$

for R-modules L, M, N.

(3) Here is a statement and a "proof" of that statement. Show that the statement is false, and find a mistake in the proof.

Statement. Let M be an R-module, and let $X = Rx$ be a cyclic module. Then $M \otimes_R X \simeq M$.

"Proof". We have $M \otimes_R X = M \otimes_R x$. The morphisms

$$M \otimes_R x \to M, \qquad m \otimes_R x \mapsto m, \quad \text{and} \quad M \to M \otimes_R x, \qquad m \mapsto m \otimes_R x,$$

are inverse one of the other.

The next proposition allows to "extend the scalars" for modules.

Proposition 2.47

(1) *Assume that R is a subring of a ring R', and let M be an R-module. Then the bilinear map*

$$\begin{cases} R' \times \big(R' \otimes_R M\big) \to R' \otimes_R M \\ \big(\lambda_1', \lambda_2' \otimes_R m\big) \mapsto \lambda_1'\lambda_2' \otimes_R m \end{cases}$$

defines a structure of R'-module on the R-module $R' \otimes_R M$.

(2) *More generally, let $f : R \to T$ be a ring morphism. View T as an R-module defined by*

$$R \times T \to T, (\lambda, \mu) \mapsto f(\lambda)\mu.$$

Then the bilinear map

$$\begin{cases} T \times (T \otimes_R M) \to T \otimes_R M \\ (\mu_1, \mu_2 \otimes_R m) \mapsto \mu_1\mu_2 \otimes_R m \end{cases}$$

defines a structure of T-module on the R-module $T \otimes_R M$.

Exercise 2.48 Let $\mathfrak{a}$ be an ideal of R and let M be an R-module. Show that the morphism of R-modules

$$M \to (R/\mathfrak{a}) \otimes_R M, \qquad m \mapsto 1_{R/\mathfrak{a}} \otimes_R m,$$

induces an isomorphism

$$M/\mathfrak{a}M \xrightarrow{\sim} (R/\mathfrak{a}) \otimes_R M.$$

2.1.5.3 Complement: Exact Sequences, Hom_R and $\otimes_R$

For $\phi : M \to N$ an R-module morphism, whenever X is an R-module, we define the following R-module morphisms:

- $\mathrm{Hom}_R(\phi, X) : \mathrm{Hom}_R(N, X) \to \mathrm{Hom}_R(M, X), \nu \mapsto \nu.\phi$,
- $\mathrm{Hom}_R(X, \phi) : \mathrm{Hom}_R(X, M) \to \mathrm{Hom}_R(X, N), \mu \mapsto \phi.\mu$.

Proposition 2.49

(1) *Let* $M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \to 0$ *be a sequence of morphisms of R-modules. The following assertions are equivalent.*

(i) $M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \to 0$ *is exact.*

(ii) *For all R-modules X, the induced sequence*

$$0 \to \operatorname{Hom}_R(M'', X) \xrightarrow{\operatorname{Hom}_R(\pi, X)} \operatorname{Hom}_R(M, X) \xrightarrow{\operatorname{Hom}_R(\iota, X)} \operatorname{Hom}_R(M', X)$$

is exact.

(2) *Let* $0 \to M' \xrightarrow{\iota} M \xrightarrow{\pi} M''$ *be a sequence of morphisms of R-modules. The following assertions are equivalent*:

(i) $0 \to M' \xrightarrow{\iota} M \xrightarrow{\pi} M''$ *is exact,*
(ii) *for all R-modules X, the sequence*

$$0 \to \operatorname{Hom}_R(X, M') \xrightarrow{\operatorname{Hom}_R(X, \iota)} \operatorname{Hom}_R(X, M) \xrightarrow{\operatorname{Hom}_R(X, \pi)} \operatorname{Hom}_R(X, M'')$$

is exact.

The proof is left to the reader.

Remark 2.50 Referring to the property expressed in the above proposition, one says that $\operatorname{Hom}_R(\cdot, \cdot)$ *is left exact.*

Let us consider an R-module morphism $\phi : M \to N$. The *transpose* of ϕ is the morphism

$$\phi^* := \operatorname{Hom}_R(\phi, R) : N^* \to M^*, \qquad \psi \mapsto \psi \cdot \phi.$$

The following statement is an immediate consequence of Proposition 2.49, (1).

Corollary 2.51 *If $\phi : M \to N$ is a surjective R-module morphism, then its transpose $\phi^* : N^* \to M^*$ is injective.*

Proposition 2.52 *Let* $M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \to 0$ *be a sequence of morphisms of R-modules. The following assertions are equivalent*:

(i) $M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \to 0$ *is exact,*
(ii) *for all R-modules X, the induced sequence*

$$M' \otimes_R X \xrightarrow{\iota \otimes 1} M \otimes_R X \xrightarrow{\pi \otimes 1} M'' \otimes_R X \to 0$$

is exact.

Proof It relies on Proposition 2.49 and on the canonical isomorphism given in Exercise 2.45, (2). □

Remark 2.53 Referring to the property expressed in the above proposition, one says that $(\cdot \otimes_R \cdot)$ *is right exact*.

(!) As an exercise, give an example of an injective morphism $\iota : M' \to M$ and a module X such that the morphism $\iota \otimes 1 : M' \otimes_R X \to M \otimes_R X$ is *not* injective.

2.1.6 Localization

2.1.6.1 Definition and First Properties

In all what follows, R denotes an integral domain with field of fractions F, and S is a nonempty multiplicatively closed subset of $R \setminus \{0\}$. We recall (see Notation 1.131) that

$$S^{-1}R := R\bigl[S^{-1}\bigr] = \left\{ \frac{\lambda}{s} \;\middle|\; (\lambda \in R)(s \in S) \right\}$$

is a subring of F containing R.

We denote by $\iota_S : R \hookrightarrow S^{-1}R$ the natural injection. The pair $(S^{-1}R, \iota_S)$ satisfies the following universal property (check it!).

Whenever $f : R \to T$ is a ring morphism such that, for all $s \in S$, $f(s)$ is invertible in T, then there exists a unique ring morphism $S^{-1}f : S^{-1}R \to T$ such that the following diagram commutes:

$$\begin{tikzcd}
R \arrow[rr, "\iota_S"] \arrow[dr, "f"'] & & S^{-1}R \arrow[dl, "S^{-1}f"] \\
& T &
\end{tikzcd}$$

Now let M be an R-module. One extends to M the construction of the localized ring $S^{-1}R$ as follows.

Definition 2.54 $S^{-1}M$ is the quotient of the set $M \times S$ by the equivalence relation (check that this is indeed an equivalence relation)

$$\bigl((m_1, s_1) \sim (m_2, s_2)\bigr) \iff \exists s \in S \quad \text{such that} \quad s(s_2 m_1 - s_1 m_2) = 0,$$

endowed with obvious laws (which ones?) defining a structure of $S^{-1}R$-module.

For $s \in S$ and $m \in M$ we denote by m/s the equivalence class of (m, s).

Remark 2.55 The above definition applies as well to define $S^{-1}R$ for a ring R which is not necessarily an integral domain.

The reader is invited to play with this definition.

The following lemma shows that the module $S^{-1}M$ is nothing but the extension of scalar from R to $S^{-1}R$.

Lemma 2.56 *The map $f : (\lambda/s) \otimes_R m \mapsto (\lambda/s)m$ defines an isomorphism of $S^{-1}R$-modules*:

$$S^{-1}R \otimes_R M \xrightarrow{\sim} S^{-1}M.$$

Proof We let the reader check that the map f does define a morphism of $S^{-1}R$-modules. It is clearly surjective. We shall prove that it is injective.

Let us first prove that any element of $S^{-1}R \otimes_R M$ can be written $1/s \otimes_R m$ for some $s \in S$ and $m \in M$.

Indeed, let $\sum_i \frac{\lambda_i}{s_i} \otimes_R m_i$ be an arbitrary element of $S^{-1}R \otimes_R M$. Let us set $s := \prod_i s_i$, and for all i, $s'_i := \prod_{j \neq i} s_j$. Then

$$\sum_i \frac{\lambda_i}{s_i} \otimes_R m_i = \sum_i \frac{\lambda_i s'_i}{s} \otimes_R m_i = \sum_i \frac{1}{s} \otimes_R \lambda_i s'_i m_i = \frac{1}{s} \otimes_R \left(\sum_i \lambda_i s'_i m_i \right).$$

We can now prove the injectivity of f. Assume that $f(1/s \otimes_R m) = 0$. Then $(1/s)m = 0$, that is, there is $t \in S$ such that $tm = 0$, and so $(1/s)m = (t/ts)m = (1/ts)tm = (1/ts)0 = 0$. □

Lemma 2.56 has the following important consequence.

Proposition 2.57 *Let F be the field of fractions of R. We set $FM := F \otimes_R M$. The kernel of the following natural R-module morphism*

$$M \to FM, \qquad m \mapsto 1 \otimes_R m,$$

is $\mathrm{tor}(M)$.

Proof We first remark that $F = S^{-1}R$ where $S = R \setminus \{0\}$.

By Lemma 2.56, $1 \otimes_R m = 0$ if and only if $m = 0$ in $S^{-1}M$, that is, there exists $s \in S = R \setminus \{0\}$ such that $sm = 0$, which means $m \in \mathrm{tor}(M)$. □

The following statement is an immediate consequence of Proposition 2.57.

Corollary 2.58

(1) $F \otimes_R \mathrm{tor}(M) = 0$.

(2) *The following assertions are equivalent.*

(i) *The natural R-module morphism*

$$M \to FM, \qquad m \mapsto 1 \otimes_R m,$$

is injective.

(ii) *M is torsion free.*

2.1.6.2 Local Properties of Modules

For $\mathfrak{p}$ a prime ideal of R and $S_\mathfrak{p} = R \setminus \mathfrak{p}$, we set $M_\mathfrak{p} := S_\mathfrak{p}^{-1}M$.

By Lemma 2.56 above, the map $m \mapsto 1 \otimes_R m$ identifies $M_\mathfrak{p}$ and $R_\mathfrak{p} \otimes M$.

If $\phi : M \to N$ is an R-module morphism, we define a morphism of $R_\mathfrak{p}$-modules by

$$\phi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}, \qquad \phi_\mathfrak{p}(m/s) := \phi(m)/s.$$

Notice that *if M is torsion free*, it follows from Corollary 2.58 that M is identified with an R-submodule of the F-vector space FM, and (this is an exercise) for all prime ideals $\mathfrak{p}$ of R we have $M \subset M_\mathfrak{p} \subset FM$.

Notice also that $M_{\{0\}} = FM$.

The following proposition provides examples of *local properties* , i.e., properties determined by the localizations at all prime ideals.

Proposition 2.59 *Let R be an integral domain with field of fractions F. Let M be an R-module.*

(1) *The following assertions are equivalent*:

 (i) $M = 0$,

 (ii) *for all* $\mathfrak{p} \in \mathrm{Spec}(R)$, $M_\mathfrak{p} = 0$.

(2) *Let $\phi : M \to N$ be an R-module morphism. For all* $\mathfrak{p} \in \mathrm{Spec}(R)$

$$\ker(\phi_\mathfrak{p}) \cong (\ker\phi)_\mathfrak{p} \quad \textit{and} \quad \mathrm{im}(\phi_\mathfrak{p}) \cong (\mathrm{im}\,\phi)_\mathfrak{p}.$$

(3) *The following assertions are equivalent*:

 (i) *ϕ is injective* (*resp. surjective*),

 (ii) *for all* $\mathfrak{p} \in \mathrm{Spec}(R)$, *$\phi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ is injective* (*resp. surjective*).

(4) *Assume M is torsion free. Then M and all the $M_\mathfrak{p}$ are embedded into FM, and*

$$M = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} M_\mathfrak{p}.$$

Proof (1) (i)⇒(ii) is trivial. Let us prove (ii)⇒(i). Assume $M \neq 0$, let $x \in M, x \neq 0$. Then $\mathrm{Ann}_R(x)$ is a proper ideal of R, hence is contained in a maximal (hence prime) ideal $\mathfrak{p}$. Then $M_\mathfrak{p} \neq 0$, since $x/1$ is a nonzero element of $M_\mathfrak{p}$. Indeed, for $y \in M$, if $y/1 = 0$ in $M_\mathfrak{p}$ there exists $s \in S_\mathfrak{p}$ (hence $s \notin \mathrm{Ann}_R(x)$) such that $sy = 0$.

(2) We shall use the following more general lemma.

For S a nonempty multiplicatively closed subset of $R \setminus \{0\}$, any R-module morphism $\phi : M \to N$ gives rise naturally to the morphism of $S^{-1}R$-modules

$$S^{-1}\phi : S^{-1}M \to S^{-1}N, m/s \mapsto \phi(m)/s.$$

Lemma 2.60 *Whenever* $M' \xrightarrow{\phi'} M \xrightarrow{\phi''} M''$ *is an exact sequence of R-module morphisms,*

$$S^{-1}M' \xrightarrow{S^{-1}\phi'} S^{-1}M \xrightarrow{S^{-1}\phi''} S^{-1}M''$$

is exact.

Proof of Lemma 2.60 Since $(S^{-1}\phi'').(S^{-1}\phi') = S^{-1}(\phi''.\phi')$, $\operatorname{im}(S^{-1}\phi') \subset \ker(S^{-1}\phi'')$. Let us prove the reverse inclusion. Let $x/s \in \ker(S^{-1}\phi'')$ ($x \in M$, $s \in S$). Since $\phi''(x)/s = 0$, there exists $t \in S$ such that $t\phi''(x) = 0$. Since $t\phi''(x) = \phi''(tx)$, we see that $tx \in \ker\phi''$ hence $tx \in \operatorname{im}\phi'$ and there exists $x' \in M'$ such that $tx = \phi'(x')$. It follows that $x/s = tx/ts = \phi'(x')/ts = (S^{-1}\phi')(x'/ts)$ and $x/s \in \operatorname{im}(S^{-1}\phi')$. □

Now we prove (2).

Consider the exact sequence $0 \to \ker\phi \to M \xrightarrow{\phi} N$. It follows from Lemma 2.60 that for all $\mathfrak{p} \in \operatorname{Spec}(R)$ the sequence $0 \to (\ker\phi)_{\mathfrak{p}} \to M_{\mathfrak{p}} \xrightarrow{\phi_{\mathfrak{p}}} N_{\mathfrak{p}}$ is exact, which implies $\ker(\phi_{\mathfrak{p}}) \cong (\ker\phi)_{\mathfrak{p}}$. We let the reader write the proof for the images.

(3) (i)⇒(ii) is an immediate consequence of (2). Indeed, if $0 \to M \to N$ (resp. $M \to N \to 0$) is exact, then $0 \to M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ (resp. $M_{\mathfrak{p}} \to N_{\mathfrak{p}} \to 0$) is exact.

(ii)⇒(i) follows from (1) and (2).

(4) Let $m/s \in \bigcap_{\mathfrak{p} \in \operatorname{Spec}(R)} M_{\mathfrak{p}}$. For all $\mathfrak{p} \in \operatorname{Spec}(R)$, $s \notin \mathfrak{p}$, which implies that s is invertible in R and $m/s \in M$. □

2.1.6.3 On Localization and Projectivity

The easy proof of the next proposition is left to the reader.

Proposition 2.61 *Let R be an integral domain. Let M be a projective R-module.*

(1) *Let S be a nonempty multiplicatively closed subset of $R \setminus \{0\}$. Then $S^{-1}M$ is a projective $S^{-1}R$-module.*
(2) *For all $\mathfrak{p} \in \operatorname{Spec}(R)$, $M_{\mathfrak{p}}$ is a projective $R_{\mathfrak{p}}$-module.*

(!) In general, projectivity is not a local property, that is, statement (2) above does not imply that M is projective (check the literature). Nevertheless, we shall prove that it is the case if R is a Noetherian ring and M is finitely generated (see Proposition 2.138).

More Exercises on Sect. 2.1

Throughout, R is a commutative ring.

Exercise 2.62 Let M be a nonzero R-module, and let N be an indecomposable R-module. Assume given morphisms

$$\alpha : M \to N \quad \text{and} \quad \beta : N \to M$$

such that $\beta\alpha$ is an automorphism of M.

Prove that both α and β are isomorphisms.

Exercise 2.63 Let M and N be R-modules, let M^* and N^* be their dual modules, $\phi : M \to N$ a morphism, $\phi^* : N^* \to M^*$ its transpose.

(1) Prove that if ϕ is surjective, ϕ^* is injective.
(2) Does the injectivity of ϕ imply the surjectivity of ϕ^*?

Exercise 2.64 Let $n \geq 1$ be an integer and let k be a field. Let $V := k[X]_{2n-1}$ be the $2n$-dimensional k-vector space comprised of 0 and all polynomials of degree at most $2n-1$. Let $x_1, \ldots, x_n$ be n distinct elements of k. We define the following system of $2n$ elements of V^*:

$$\text{for } j = 1, \ldots, n, \begin{cases} \alpha_j : V \to k,\ P(X) \mapsto P(x_j) \\ \beta_j : V \to k,\ P(X) \mapsto \frac{dP}{dX}(x_j) \end{cases}$$

Prove that $(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n)$ is a basis of V^*.

Exercise 2.65 Let V be an $\mathbb{R}$-vector space of odd dimension, and let $\phi : V \to V$ be an endomorphism of V. Prove that there is a hyperplane of V stable under ϕ.

Exercises 2.66 Localizations In what follows, R is an integral domain with field of fractions F, S is a nonempty multiplicatively closed subset of $R \setminus \{0\}$, and L is an R-module.

1. Assume that M and N are submodules of L. Prove that

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

2. Prove that there is a unique isomorphism of $S^{-1}R$-modules

$$\begin{cases} S^{-1}M \otimes_{S^{-1}R} S^{-1}N \xrightarrow{\sim} S^{-1}(M \otimes_R N), \\ (x/s) \otimes_{S^{-1}R} (y/t) \mapsto (x \otimes_R y)/st. \end{cases}$$

(!) **Attention** (!) There is no such general result when the tensor product $\cdot \otimes_R \cdot$ is replaced by $\mathrm{Hom}_R(\cdot, \cdot)$ (see Proposition 2.113 for an analogous result).

Exercise 2.67 (Snake lemma) Let

$$\begin{tikzcd}
 & M' \arrow[r, "\alpha"] \arrow[d, "f'"] & M \arrow[r, "\alpha'"] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "\beta"] & N \arrow[r, "\beta'"] & N'' &
\end{tikzcd}$$

be a commutative diagram where the rows are exact sequences. Prove that there exists a morphism $d : \ker f'' \to \operatorname{coker} f'$

$$\begin{tikzcd}
 & \ker f' \arrow[r] \arrow[d] & \ker f \arrow[r] \arrow[d] & \ker f'' \arrow[d] \arrow[dddll, rounded corners, "d"] & \\
 & M' \arrow[r, "\alpha"] \arrow[d, "f'"] & M \arrow[r, "\alpha'"] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "\beta"] \arrow[d] & N \arrow[r, "\beta'"] \arrow[d] & N'' \arrow[d] & \\
 & \operatorname{coker} f' \arrow[r] & \operatorname{coker} f \arrow[r] & \operatorname{coker} f'' &
\end{tikzcd}$$

such that the sequence

$$\ker f' \to \ker f \to \ker f'' \xrightarrow{d} \operatorname{coker} f' \to \operatorname{coker} f \to \operatorname{coker} f''$$

is exact.

Hint: http://www.math.harvard.edu/~knill/mathmovies/swf/myturn_snake.html.

2.2 Finitely Generated Modules

Throughout this section, R denotes a commutative ring.

Definition 2.68 We say that an R-module M is finitely generated if it has a finite generating system. In other words, M is finitely generated if there exists an integer

n and a surjective morphism

$$R^n \twoheadrightarrow M.$$

Examples 2.69

(1) $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-module.
Indeed, let $N := \sum_{1 \le i \le n} \mathbb{Z}(a_i/b_i)$ be a finitely generated submodule of $\mathbb{Q}$. Let $b := b_1 b_2 \cdots b_n$. Then $bN \subset \mathbb{Z}$. Let p be a prime number which does not divide b. Then $1/p \notin N$, which shows that $N \neq \mathbb{Q}$.

(2) If V is a finite dimensional k-vector space and if ϕ is an endomorphism of V, the $k[X]$-module V_ϕ is finitely generated.

The following lemma is obvious.

Lemma 2.70 *Let S be a nonempty multiplicatively closed subset of $R \setminus \{0\}$ and let M be a finitely generated R-module.*
Then $S^{-1}M$ is a finitely generated $S^{-1}R$-module.

2.2.1 Application: Integrality over a Ring

All throughout this section, R is assumed to be a subring of a commutative ring T.

2.2.1.1 Definition and Characterization

Definition 2.71 Let $x \in T$. We say that x is *integral over R* if there exists a *monic* polynomial $P(X) \in R[X]$ such that $P(x) = 0$.

Examples 2.72

(1) All roots of unity of $\mathbb{C}$ are integral over $\mathbb{Z}$.
(2) For k a field and X an indeterminate, set $R := k[X^2]$ and $T := k[X]$. Then X is integral over R.

Exercise 2.73

(1) Prove that $x \in \mathbb{Q}$ is integral over $\mathbb{Z}$ if and only if $x \in \mathbb{Z}$.
(2) More generally, let R be a factorial ring, with field of fractions F. For $x \in F$, prove that x is integral over R if and only if $x \in R$.

Proposition 2.74 *Let $x \in T$. The following assertions are equivalent*:

(i) *the element x is integral over R*,
(ii) *the subring $R[x]$ of T generated by R and x is a finitely generated R-module*,

(iii) *there exists a subring R' of T, containing x, which is a finitely generated R-module.*

Proof (i)⇒(ii): Assume that $x^r - \lambda_{r-1}x^{r-1} - \cdots - \lambda_1 x - \lambda_0 = 0$. We shall prove that $R[x]$ is generated by $\{1, x, \ldots, x^{r-1}\}$.

Since $R[x]$ is generated by $\{x^n\}_{n\in\mathbb{N}}$, it suffices to prove that, for all $n \geq 0$, x^{r+n} is a linear combination of $\{1, x, \ldots, x^{r-1}\}$. It is clear for $n = 0$. The proof by induction on n is easy.

(ii)⇒(iii): trivial.

(iii)⇒(i): Assume that $\{x_1, \ldots, x_m\}$ is a generating system for R'. Since $x \in R'$, there are $\lambda_{i,j} \in R$ $(1 \leq i, j \leq m)$ such that for all i, $xx_i = \sum_{j=1}^{m} \lambda_{i,j} x_j$. Let Λ be the $m \times m$ square matrix with entries $\lambda_{i,j} \in R$ $(1 \leq i, j \leq m)$. The above equations give

$$(x1_m - \Lambda)\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Multiplying to the left by ${}^t\mathrm{Com}(x1_m - \Lambda)$ gives then

$$\det(x1_m - \Lambda)\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

so

$$\det(x1_m - \Lambda)R' = 0 \quad \text{hence} \quad \det(x1_m - \Lambda) = 0.$$

Now $\det(X1_m - \Lambda)$ is a monic element of $R[X]$, which proves (i). □

Corollary 2.75 *The set of all elements of T which are integral over R is a subring of T which contains R.*

Proof We must prove that whenever x and y are two elements of T which are integral over R, then $x + y$ and xy are integral over R. This follows from the fact that all the elements of the ring $R[x, y]$ are integral over R, which we prove now.

By Proposition 2.74, it suffices to prove that $R[x, y]$ is a finitely generated R-module. This follows from the following lemma (which generalizes part of Lemma 1.67).

Lemma 2.76 *Assume that $R = R_0 \subset R_1 \subset \cdots \subset R_m$ is a tower of commutative rings, where (for all $i = 0, \ldots, m-1$) R_i is a subring of R_{i+1}. If, for all $i = 0, \ldots, m-1$, R_{i+1} is a finitely generated R_i-module, then R_m is a finitely generated R-module.*

Proof of Lemma 2.76 We sketch a proof in the case where $m = 2$ (which is sufficient). Let us set $S := R_1$ and $T := R_2$. Let $\{s_1, \ldots, s_m\}$ be a generating system of

S as an R-module, and let $\{t_1, \dots, t_n\}$ be a generating system of T as an S-module. Then it can be checked (do it!) that $\{s_i t_j\}_{1 \le i \le m, 1 \le j \le n}$ is a generating system of T as an R-module. □

□

2.2.1.2 Integral Extensions

Definition 2.77

(1) The ring of elements of T which are integral over R is called *the integral closure* of R in T.

(2) One says that T is *integral over* R (or that the extension T/R is integral) if T is the integral closure of R in T.

(3) An integral domain R is said to be *integrally closed* if it is equal to its integral closure in its field of fractions.

Exercise 2.78 Assume R and T are integral domains. For S a nonempty multiplicatively stable subset of $R \setminus \{0\}$, if $\overline{R}$ denotes the integral closure of R in T, prove that $S^{-1}\overline{R}$ is the integral closure of $S^{-1}R$ in $S^{-1}T$.

Examples 2.79

- A factorial (i.e., unique factorisation) domain is integrally closed (see above Exercise 2.73).
- The polynomial ring $R[X_1, X_2, \dots, X_r]$ is integrally closed if and only if R is integrally closed (see for example [2], Chap. 5, §1, no. 3, or below Exercise 2.146).

Definition 2.80 One says that T is *finite over* R (or that T/R is finite) if T is a finitely generated R-module.

We say that T is a *finitely generated* R*-algebra* if there is a finite set $\{t_1, \dots, t_m\} \subset T$ such that T is generated (as a ring) by $R \cup \{t_1, \dots, t_m\}$, i.e., $T = R[t_1, \dots, t_m]$.

Proposition 2.81 *The following assertions are equivalent*:

(i) *The extension T/R is finite.*

(ii) *T is a finitely generated R-algebra and is integral over R.*

(iii) *T is generated as an R-algebra by a finite number of elements which are integral over R.*

Proof (i)⇒(ii): If $\{t_1, \dots, t_m\}$ generates T as an R-module, it generates a fortiori T as an R-algebra. Moreover, T is integral by Proposition 2.74.

(ii)⇒(iii): trivial.

(iii)⇒(i): Assume that $T = R[t_1, \dots, t_m]$, where each t_i is integral over R. Then each t_i is a fortiori integral over $R[t_1, \dots, t_{i-1}]$, hence we have a tower

$$R \subset R[t_1] \subset \cdots \subset R[t_1, \dots, t_i] \subset \cdots \subset R[t_1, \dots, t_m] = T,$$

where for each i, the ring $R[t_1, \dots, t_i]$ is finitely generated as a module over the subring $R[t_1, \dots, t_{i-1}]$. It follows then from Lemma 2.76 that T is finitely generated as an R-module. □

Corollary 2.82

(1) *Let $R \subset S \subset T$ be a tower of rings. The following assertions are equivalent.*

  (i) *S/R and T/S are integral extensions.*
  (ii) *T/R is an integral extension.*

(2) *Let S and T be subrings of a ring R'*

$$\begin{tikzcd}
 & R' & \\
S \arrow[ur, dash] & & T \arrow[ul, dash] \\
 & R \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

which both contain a subring R. We denote by $S[T]$ or $T[S]$ the subring of R' generated by $S \cup T$. The following assertions are equivalent.

  (i) *S/R and T/R are integral extensions.*
  (ii) *$S[T]/R$ is an integral extension.*

Proof (1) (i)⇒(ii): Let $t \in T$. By assumption, there exist $s_0, s_1, \dots, s_{m-1} \in S$ such that $t^m + s_{m-1}t^{m-1} + \cdots + s_1 t + s_0 = 0$. Thus t is integral over the ring $R[s_0, s_1, \dots, s_{m-1}]$, which implies that the extension of rings

$$R[s_0, s_1, \dots, s_{m-1}][t]/R[s_0, s_1, \dots, s_{m-1}]$$

is finite. Moreover, since each s_i is integral over R, it follows from 2.76 that $R[s_0, s_1, \dots, s_{m-1}]/R$ is finite, hence finally $R[s_0, s_1, \dots, s_{m-1}][t]/R$ is finite, which proves that t is integral over R.

(ii)⇒(i): trivial.

(2) (i)⇒(ii): Exercise!

(ii)⇒(i): trivial. □

In what precedes, a special case is that all our rings R, R', S, T are fields. In that case, an integral element is called *algebraic* (see Definition 1.49) and an integral extension is called an *algebraic extension*.

Actually, when we consider integral extensions, it suffices to assume that one of the rings is a field for the other to be a field as well, as shown by the next proposition.

Proposition 2.83 *Assume that T is integral over R. The following assertions are equivalent.*

(i) *T is a field.*
(ii) *R is a field.*

Proof (i)⇒(ii): Let $r \in R$, $r \neq 0$. Then r has an inverse $r^{-1} \in T$. Since r^{-1} is integral over R, there exist $\lambda_0, \dots, \lambda_{m-1} \in R$ such that

$$r^{-m} - \lambda_{m-1} r^{-(m-1)} - \cdots - \lambda_1 r^{-1} - \lambda_0 = 0.$$

Multiplying the preceding equality by r^{m-1} we get

$$r^{-1} = \lambda_{m-1} + \cdots + \lambda_1 r^{m-2} + \lambda_0 r^{m-1}$$

which shows that $r^{-1} \in R$, and so that R is a field.

(ii)⇒(i): For each $t \in T$, $t \neq 0$, t is algebraic over the field R, hence (see Proposition 1.50) $R[t]$ is a field which shows that t has an inverse which belongs to $R[t]$, hence to T. □

2.2.1.3 Integrality and Localization

Proposition 2.84 *Let R be a subring of a commutative ring T. Let $S \subset R \setminus \{0\}$ be a nonempty multiplicatively closed subset.*

(1) *If T is integral over R, then $S^{-1}T$ is integral over $S^{-1}R$.*
(2) *If R' is the integral closure of R in T, then $S^{-1}R'$ is the integral closure of $S^{-1}R$ in $S^{-1}T$.*

Proof (1) If $x \in T$ satisfies $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, then for $s \in S$, x/s satisfies $(x/s)^n + (a_{n-1}/s)(x/s)^{n-1} + \cdots + (a_0/s^n) = 0$, so is integral over $S^{-1}R$.

(2) By (1), we see that $S^{-1}R'$ is integral over $S^{-1}R$. Now assume that $y/s \in S^{-1}T$ is integral over $S^{-1}R$, i.e., satisfies an equation

$$(y/s)^n + (a_{n-1}/s_{n-1})(y/s)^{n-1} + \cdots + a_0/s_0 = 0$$

where $a_j \in R$ and $s_j \in S$ for $j = 0, \dots, n-1$. Define $t := s_0 \cdots s_{n-1}$. Multiplying the above equation by $(st)^n$, gives

$$(yt)^n + \cdots + (a_0/s_0)(st)^n = 0,$$

which shows that yt is integral over R, hence that $yt \in R'$. It follows that $y/s = ty/ts \in S^{-1}R'$. □

The following result is an immediate consequence of the above proposition.

Corollary 2.85 *Let R be an integral domain. Let $S \subset R \setminus \{0\}$ be nonempty and multiplicatively closed.*

If R is integrally closed, so is $S^{-1}R$.

The next proposition shows that integral closure is a local property.

Proposition 2.86 *Let R be an integral domain. The following assertions are equivalent*:

(i) *R is integrally closed.*
(ii) *For all $\mathfrak{p} \in \operatorname{Spec}(R)$, $R_{\mathfrak{p}}$ is integrally closed.*

Proof Let R' be the integral closure of R in its field of fractions F. Then, for all $\mathfrak{p} \in \operatorname{Spec}(R)$, it follows from Proposition 2.84, (2) that $R'_{\mathfrak{p}}$ is the integral closure of $R_{\mathfrak{p}}$ in F.

Assumption (i) means that the natural inclusion $\iota : R \to R'$ is an isomorphism.

Assumption (ii) means that, for all $\mathfrak{p} \in \operatorname{Spec}(R)$, $\iota_{\mathfrak{p}} : R_{\mathfrak{p}} \to R'_{\mathfrak{p}}$ is an isomorphism.

Thus the result is a consequence of Proposition 2.59. □

2.2.1.4 Integral Closure and Field Extensions

Proposition 2.87 *Let R be an integral domain with field of fractions F, and let L be an algebraic field extension of F. Let R_L denote the integral closure of R in L.*

(1) *Any element of L can be written $\mu\lambda^{-1}$ where $\mu \in R_L$ and $\lambda \in R$.*
(2) *L is the field of fractions of R_L.*
(3) *R_L is an integrally closed domain.*

Proof Let $x \in L$. Its minimal polynomial $P(X)$ over F (1.49) may be written

$$P(X) = X^m + \frac{\lambda_{m-1}}{\lambda} X^{m-1} + \cdots + \frac{\lambda_1}{\lambda} X + \frac{\lambda_0}{\lambda} \quad \text{where } \lambda_i, \lambda \in R.$$

Let us set $Q(X) := \lambda^m P(\lambda^{-1} X)$. Then

$$Q(X) = X^m + \lambda_{m-1} X^{m-1} + \cdots + \lambda_1 \lambda^{m-2} X + \lambda_0 \lambda^{m-1},$$

and λx is a root of $Q(X)$. Thus $\lambda x \in R_L$.

The last two assertions are now obvious. □

Proposition 2.88 *Let R be an integral domain with field of fractions F, and let R_F be its integral closure in F. Let L be an algebraic extension of F, let x be an element of L which is integral over R and let $P(X) \in F[X]$ be the minimal polynomial of x over F. Then $P(X) \in R_F[X]$.*

Proof Over a large enough extension field of L, $P(X)$ factorizes as

$$P(X) = (X - x_1)(X - x_2) \cdots (X - x_m)$$

(where for example $x = x_1$). Since the coefficients of $P(X)$ are the elementary symmetric polynomials evaluated at $(x_1, x_2, \dots, x_m)$, it suffices to check that each x_i is integral over R.

For all i, there is an F-algebra isomorphism $F[X]/(P(X)) \xrightarrow{\sim} F[x_i]$, hence an F-algebra isomorphism $F[x] \xrightarrow{\sim} F[x_i]$. This implies that since x is a root of a monic element of $R[X]$, x_i is also a root of the same polynomial, hence is integral over R. □

2.2.2 Complement: Jacobson Rings, Hilbert's Nullstellensatz

This section, although an application of the notions previously introduced, is more difficult and may be omitted during the first reading. The reader may refer to [4],[1] *§4.5, for a similar approach.*

2.2.2.1 On Maximal Ideals of Polynomial Algebras

Throughout, R is a commutative ring.

Whenever $\mathfrak{A}$ is an ideal of $R[X]$, let us denote by $\overline{R}$ and x respectively the images of R and X under the natural epimorphism $R[X] \twoheadrightarrow R[X]/\mathfrak{A}$. Thus we have

$$\overline{R} = R/(R \cap \mathfrak{A}) \quad \text{and} \quad R[X]/\mathfrak{A} = \overline{R}[x].$$

Note (see Lemma 1.110) that if $\mathfrak{P}$ is a prime ideal of $R[X]$, then $\mathfrak{P} \cap R$ is a prime ideal of R. We shall be concerned with the case of *maximal* ideals.

Let us point out two very different behaviours of maximal ideals of $R[X]$ with respect to R.

- If $\mathfrak{M}$ is a maximal ideal of $\mathbb{Z}[X]$, then $\mathfrak{M} \cap \mathbb{Z} \neq \{0\}$ (this will be proved below: see Proposition 2.90, (3)).

  As a consequence, a maximal ideal $\mathfrak{M}$ of $\mathbb{Z}[X]$ can be described as in Proposition 1.112, which we recall here: there is a prime number p and a polynomial $P(X) \in \mathbb{Z}[X]$ which stays irreducible in $(\mathbb{Z}/p\mathbb{Z})[X]$ such that $\mathfrak{M} = p\mathbb{Z}[X] + P(X)\mathbb{Z}[X]$.

  Thus the quotients of $\mathbb{Z}[X]$ by maximal ideals are finite fields.
- Let p be a prime number, and let $\mathbb{Z}_{(p)} := \{a/b \mid (a, b \in \mathbb{Z})(p \nmid b)\}$. Then $\mathbb{Z}_{(p)}[1/p] = \mathbb{Q}$, which shows that $\mathfrak{M} := (1 - pX)\mathbb{Z}_{(p)}[X]$ is a maximal ideal of $\mathbb{Z}_{(p)}[X]$. Notice that here $\mathfrak{M} \cap \mathbb{Z}_{(p)} = \{0\}$.

Let us examine these questions through the following proposition.

Notation 2.89 We denote by $\operatorname{Spec}^*(R)$ *the set of all nonzero prime ideals of* R.

[1] Since I don't have the TeX file, I don't know how you refer to it now.

Proposition 2.90 *Let R be a commutative ring.*

(1) *If there is $\mathfrak{M} \in \operatorname{Spec}^{\max}(R[X])$ such that $\mathfrak{M} \cap R = \{0\}$, then there exists $a \in R \setminus \{0\}$ such that $(1 - aX)R[X] \in \operatorname{Spec}^{\max}(R[X])$.*

In other words: if there exists x in an extension of R such that $R[x]$ is a field, then there is $a \in R \setminus \{0\}$ such that $R[1/a]$ is a field.

(2) *We have*

$$\bigcap_{\mathfrak{p} \in \operatorname{Spec}^*(R)} \mathfrak{p} = \{0\} \cup \bigl\{a \in R \setminus \{0\} \bigm| R[1/a] \text{ is a field}\bigr\}.$$

(3) *Assume $\bigcap_{\mathfrak{p} \in \operatorname{Spec}^*(R)} \mathfrak{p} = \{0\}$. Then for all $\mathfrak{M} \in \operatorname{Spec}^{\max}(R[X])$ we have $\mathfrak{M} \cap R \neq \{0\}$.*

In other words: in any extension T of R, there is no $x \in T$ such that $R[x]$ is a field.

Proof (1) Assume that $R[x]$ is a field. Then R is an integral domain, and if F denotes its field of fractions, we have $R[x] = F[x]$. Since $F[x]$ is a field, x is algebraic over F, hence a root of a polynomial with coefficients in R. If a is the coefficient of the highest degree term of that polynomial, x is integral over $R[1/a]$. Whence $R[x]$ is integral over $R[1/a]$, and since $R[x]$ is a field, it follows that $R[1/a]$ is a field by Proposition 2.83.

(2) Assume first that $a \in \bigcap_{\mathfrak{p} \in \operatorname{Spec}^*(R)} \mathfrak{p}$ and $a \neq 0$. We must show that $R[1/a]$ is a field.

There is a maximal ideal $\mathfrak{M}$ of $R[X]$ containing $(1 - aX)R[X]$.

- We then have $\mathfrak{M} \cap R = \{0\}$. Indeed, if it were not the case, we would have $\mathfrak{M} \cap R \in \operatorname{Spec}^*(R)$, hence $a \in \mathfrak{M} \cap R$, then $a \in \mathfrak{M}$, $aX \in \mathfrak{M}$, so $1 \in \mathfrak{M}$.
- Let x be the image of X in $R[X]/\mathfrak{M}$. Thus $R[x]$ is a field. But $1 - ax = 0$, proving that $x = 1/a$ and $R[1/a]$ is a field.

Assume now that $R[1/a]$ is a field.

Hence $(1 - aX)R[X] \in \operatorname{Spec}^{\max}(R[X])$. Let $\mathfrak{p} \in \operatorname{Spec}^*(R)$. Then $\mathfrak{p} \not\subseteq (1 - aX)R[X]$, since $(1 - aX)R[X] \cap R = \{0\}$. It follows that

$$\mathfrak{p}R[X] + (1 - aX)R[X] = R.$$

Interpreted in the polynomial ring $(R/\mathfrak{p})[X]$, that equality shows that the polynomial $1 - \overline{a}X$ is invertible, which implies that $\overline{a} = 0$, i.e., $a \in \mathfrak{p}$.

(3) Assume that $R[x]$ is a field. By (1), there is $a \in R \setminus \{0\}$ such that $R[1/a]$ is a field. By (2), we know that $a \in \bigcap_{\mathfrak{p} \in \operatorname{Spec}^*(R)} \mathfrak{p}$, a contradiction. □

Remark 2.91 If R is a principal ideal domain with infinitely many prime ideals, then $\bigcap_{\mathfrak{p} \in \operatorname{Spec}^*(R)} \mathfrak{p} = \{0\}$ (why?). Thus the third assertion of the preceding proposition shows in particular that, in that case, whenever $\mathfrak{M} \in \operatorname{Spec}^{\max}(R[X])$, we have $\mathfrak{M} \cap R \neq \{0\}$, hence $\mathfrak{M} \cap R \in \operatorname{Spec}^{\max}(R)$.

Notice that $\mathbb{Z}$ and $F[X]$ have infinitely many prime ideals, while $\mathbb{Z}_{(p)}$ has only one nonzero prime ideal.

Theorem–Definition 2.92 *For a commutative ring R, the following assertions are equivalent*:

(J1) *Whenever* $\mathfrak{p} \in \operatorname{Spec}(R)$, *we have*

$$\mathfrak{p} = \bigcap_{\substack{\mathfrak{m} \in \operatorname{Spec}^{\max}(R) \\ \mathfrak{p} \subseteq \mathfrak{m}}} \mathfrak{m}.$$

(J2) *Whenever* $\mathfrak{M} \in \operatorname{Spec}^{\max}(R[X])$, *we have* $\mathfrak{M} \cap R \in \operatorname{Spec}^{\max}(R)$.

A ring which fulfills the preceding conditions is called a Jacobson ring.

Proof Let us first notice that both properties (J1) and (J2) transfer to quotients: if R satisfies (J1) (respectively (J2)), and if $\mathfrak{a}$ is an ideal of R, then $R/\mathfrak{a}$ satisfies (J1) (respectively (J2)) as well.

Let us show (J1) $\Rightarrow$ (J2). Let $\mathfrak{M} \in \operatorname{Spec}^{\max}(R[X])$. We set $R[X]/\mathfrak{M} = (R/\mathfrak{M} \cap R)[x]$.

We have $\mathfrak{M} \cap R \in \operatorname{Spec}(R)$, hence $\mathfrak{M} \cap R$ is an intersection of maximal ideals of R. If $\mathfrak{M} \cap R$ is not maximal, it is an intersection of maximal ideals in which it is properly contained, thus in the ring $R/(\mathfrak{M} \cap R)$, we have

$$\bigcap_{\mathfrak{p} \in \operatorname{Spec}^*(R/(\mathfrak{M} \cap R))} \mathfrak{p} = \{0\},$$

which shows (by Proposition 2.90, (3)) that $(R/\mathfrak{M} \cap R)[x]$ cannot be a field, a contradiction.

Let us show (J2) $\Rightarrow$ (J1). Let $\mathfrak{p} \in \operatorname{Spec}(R)$. Working in $R/\mathfrak{p}$, we see that it suffices to prove that if R is an integral domain which satisfies (J2), then the intersection of its maximal ideals is $\{0\}$.

Let $a \in \bigcap_{\mathfrak{m} \in \operatorname{Spec}^{\max}(R)} \mathfrak{m}$. Thus whenever $\mathfrak{M} \in \operatorname{Spec}^{\max}(R[X])$, we have $a \in \mathfrak{M}$, hence $aX \in \mathfrak{M}$, which shows that $aX \in \operatorname{Rad}(R[X])$, hence by Definition 1.117 $1 - aX$ is invertible, and $a = 0$. □

Let us emphasize the defining property of Jacobson rings, by stating the following proposition (which is nothing but a reformulation of property (J2)).

Proposition 2.93 *The following assertions are equivalent*:

(i) *R is a Jacobson ring.*
(ii) *If $\overline{R}[x]$ is a quotient of $R[X]$ which is a field, then $\overline{R}$ is a field and x is algebraic over $\overline{R}$.*

Remark 2.94 Let us immediately quote some examples and nonexamples of Jacobson rings:

- Examples of Jacobson rings: fields, principal ideal domains with infinitely many prime ideals, quotients of Jacobson rings.

- Non Jacobson rings: local principal ideal domains which are not fields.

The next theorem enlarges the set of examples of Jacobson ring to all finitely generated algebras over a Jacobson ring.

Theorem 2.95 *Let R be a Jacobson ring.*

(1) *The polynomial ring $R[X]$ is a Jacobson ring.*
(2) *If B is a finitely generated R-algebra, then B is a Jacobson ring.*

Corollary 2.96

(1) *Let R be a Jacobson ring. Let $\overline{R}[v_1, v_2, \dots, v_r]$ be the quotient of the polynomial ring $R[X_1, \dots, X_r]$ by a maximal ideal. Then $\overline{R}$ is a field, and $\overline{R}[v_1, v_2, \dots, v_r]$ is an algebraic (hence finite) extension of $\overline{R}$.*
(2) *Let k be a field. If $k[v_1, v_2, \dots, v_r]$ is a finitely generated k-algebra which is a field, then it is an algebraic (hence finite) extension of k.*
(3) *Let K be an algebraically closed field. If $K[v_1, v_2, \dots, v_r]$ is a finitely generated K-algebra which is a field, then it coincides with K.*

Assertion (3) of the preceding corollary may be reformulated as Hilbert's Nullstellensatz.

Theorem 2.97 (Hilbert's Nullstellensatz) *Let K be an algebraically closed field, and let $K[v_1, v_2, \dots, v_r]$ be a finitely generated K-algebra. The map*

$$\begin{aligned} K^r &\longrightarrow \operatorname{Spec}^{\max}\bigl(K[v_1, v_2, \dots, v_r]\bigr) \\ (\lambda_1, \lambda_2, \dots, \lambda_r) &\mapsto \langle v_1 - \lambda_1, v_2 - \lambda_2, \dots, v_r - \lambda_r \rangle \end{aligned}$$

(the ideal of $K[v_1, v_2, \dots, v_r]$ generated by $\{v_1 - \lambda_1, \dots, v_r - \lambda_r\}$) is a bijection.

Proof of Theorem 2.95 Let us prove (1).

Let $\mathfrak{M}$ be a maximal ideal of $R[X, Y]$. We set

$$\begin{aligned} &\overline{R} := R/(\mathfrak{M} \cap R), \\ &\overline{R}[x] := R[X]/\bigl(\mathfrak{M} \cap R[X]\bigr) \quad \text{and} \quad \overline{R}[y] := R[Y]/\bigl(\mathfrak{M} \cap R[Y]\bigr), \\ &\overline{R}[x, y] := R[X, Y]/\mathfrak{M}. \end{aligned}$$

We have to prove that $\overline{R}[x]$ is a field.

Since $\overline{R}[x, y]$ is a field, $\overline{R}$ is an integral domain, and if F denotes its field of fractions, we have $\overline{R}[x, y] = F[x, y]$.

Since $F[x, y]$ is a field, x is not transcendental (by Proposition 2.90, (3)) over F, hence $F[x]$ is a field. As in the proof of Proposition 2.90, (1), we see that there exists $a \in R \setminus \{0\}$ such that x is integral over $\overline{R}[1/a]$.

Similarly, there exists $b \in R \setminus \{0\}$ such that y is integral over $\overline{R}[1/b]$. It follows that $\overline{R}[x, y]$ is integral over $\overline{R}[1/ab]$. Since $\overline{R}[x, y]$ is a field, this implies that $\overline{R}[1/ab]$ is a field.

Now since R is a Jacobson ring, it follows from Proposition 3 that $\overline{R}$ is a field, i.e., $\overline{R} = F$. We have already seen that $F[x]$ is a field, proving that $\overline{R}[x]$ is a field.

Let us prove (2).

By induction on r, it follows from (1) that, for all r, $R[X_1, X_2, \dots, X_r]$ is a Jacobson ring. So are the quotients of these algebras, which are the finitely generated R-algebras. □

Proof of Corollary 2.96 (1) Assume that $\overline{R}[v_1, v_2, \dots, v_r]$ is a field. Since $\overline{R}[v_1, v_2, \dots, v_{r-1}]$ is a finitely generated R-algebra, it is a Jacobson ring (by Theorem 2.95, (2)). Thus by Corollary 2.96, (2), $\overline{R}[v_1, v_2, \dots, v_{r-1}]$ is a field over which v_r is algebraic. Repeating the argument leads to the required statement.

(2) and (3) are immediate consequences of (1) □

2.2.2.2 Application to Algebraic Varieties

If R is a Jacobson ring, it follows from Theorem–Definition 2.92 that

$$\mathrm{Rad}(R) = \mathrm{Nilrad}(R).$$

Applying that remark to a quotient of a Jacobson ring by an ideal $\mathfrak{a}$, we get the following proposition.

Lemma 2.98 *Let R be a Jacobson ring, and let $\mathfrak{a}$ be an ideal of R. We have*

$$\bigcap_{\substack{\mathfrak{m} \in \mathrm{Spec}^{\max}(R) \\ \mathfrak{a} \subseteq \mathfrak{m}}} \mathfrak{m} = \left\{ a \in R \;\middle|\; (\exists n \geq 0)\big(a^n \in \mathfrak{a}\big) \right\}.$$

Remark 2.99 The ideal $\bigcap_{\mathfrak{m} \in \mathrm{Spec}^{\max}(R)}$ is called the *radical of the ideal* $\mathfrak{a}$.

Applying the preceding lemma to the case where $R = K[X_1, \dots, X_r]$ for k algebraically closed gives the “strong form” of Hilbert’s Nullstellensatz.

Corollary 2.100 (Strong Nullstellensatz) *Let K be an algebraically closed field. For $\mathfrak{A}$ an ideal of $K[X_1, X_2, \dots, X_r]$, let us set*

$$\mathcal{V}(\mathfrak{A}) := \left\{ (\lambda_1, \lambda_2, \dots, \lambda_r) \in K^r \;\middle|\; (\forall P \in \mathfrak{A})\big(P(\lambda_1, \lambda_2, \dots, \lambda_r) = 0\big) \right\}.$$

If $Q \in K[X_1, X_2, \dots, X_r]$ is such that

$$\big(\forall (\lambda_1, \lambda_2, \dots, \lambda_r) \in \mathcal{V}(\mathfrak{A})\big), \quad \big(Q(\lambda_1, \lambda_2, \dots, \lambda_r) = 0\big),$$

then there exists $n \geq 0$ such that $Q^n \in \mathfrak{A}$.

Proof of Corollary 2.100 Translating via the dictionary $K^r \longleftrightarrow \mathrm{Spec}^{\max}(K[X_1, X_2, \ldots, X_r])$ (from Theorem 2.97) we see that

$$\mathcal{V}(\mathfrak{A}) \longleftrightarrow \left\{\mathfrak{M} \in \mathrm{Spec}^{\max}\bigl(K[X_1, X_2, \ldots, X_r]\bigr) \;\middle|\; \mathfrak{A} \subseteq \mathfrak{M}\right\},$$

while the hypothesis on Q translates to

$$Q \in \bigcap_{\substack{\mathfrak{M} \in \mathrm{Spec}^{\max}(K[X_1, X_2, \ldots, X_r]) \\ \mathfrak{A} \subseteq \mathfrak{M}}} \mathfrak{M},$$

and we apply Lemma 2.98. □

2.2.3 Noetherian Rings and Modules

2.2.3.1 Noetherian Modules

Theorem 2.101 *Let R be a (commutative) ring and let M be an R-module. The following conditions are equivalent.*

(i) *Every nonempty family of submodules of M has a maximal element.*
(ii) *Every increasing (ascending) sequence of submodules $M_0 \subset M_1 \subset \cdots \subset M_n \subset \cdots$ of M is stationary.*
(iii) *Every submodule of M is finitely generated.*

The following definition is in honor of Emmy Noether.

Definition 2.102 A module satisfying the above equivalent conditions is said to be *Noetherian*.

Proof of Theorem 2.101 (i)⇒(iii) Let N be a submodule of M, and let $\mathcal{F}(N)$ be the family of all finitely generated submodules of N. Since $\mathcal{F}(N)$ contains the trivial module 0, it is nonempty hence it has a maximal element, say N'. Let us show that

$N' = N$. Let $x \in N$. The module $N' + Rx$ is finitely generated, hence $N' + Rx = N'$, showing that $x \in N'$.

(iii)⇒(ii) Let $(M_n)_{n\geq 0}$ be an increasing sequence of submodules of M. It is easy to check that $M_\infty := \bigcup_{n\geq 0} M_n$ is a submodule of M. Since it is finitely generated, there exists $m \in \mathbb{N}$ such that M_m contains a set of generators, which implies $M_\infty = M_m$, hence that the sequence $(M_n)_{n\geq 0}$ is stationary.

(ii)⇒(i) The proof relies on the following lemma. Note that this lemma uses the axiom of choice (where?).

Lemma 2.103 *Let Ω be a (partially) ordered set. The following assertions are equivalent.*

(i) *Every nonempty subset of Ω has a maximal element.*
(ii) *Every increasing sequence $(\omega_n)_{n\geq 0}$ of elements of Ω is stationary.*

Proof of Lemma 2.103 (i)⇒(ii): Let $(\omega_n)_{n\geq 0}$ be an increasing sequence. If ω_m is a maximal element, we have $\omega_n = \omega_m$ for all $n \geq m$, which shows that the sequence is stationary.

(ii)⇒(i): Assume (i) is false, and let Ω' be a nonempty subset of Ω which has no maximal element. Let $\omega_0 \in \Omega'$. We can then build by induction a strictly increasing sequence $(\omega_n)_{n\geq 0}$ in Ω' as follows: Assume ω_n known. Since ω_n is not maximal in Ω', we may pick $\omega_{n+1} \in \Omega'$ such that $\omega_{n+1} > \omega_n$. □

□

Proposition 2.104 *Let $0 \to M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \to 0$ be a short exact sequence of R-modules. Then the following assertions are equivalent:*

(i) *M is Noetherian.*
(ii) *M' and M'' are Noetherian.*

Proof (i)⇒(ii): Any increasing sequence of submodules of M' (or M'') gives rise to an increasing sequence of submodules of M, hence is stationary.

(ii)⇒(i): Let us prove that any submodule N of M is finitely generated. By assumption, the submodule $\iota^{-1}(N)$ of M' and the submodule $\pi(N)$ of M'' are finitely generated. Let $(x_1, \ldots, x_m)$ be the image under ι of a set of generators of $\iota^{-1}(N)$, and let $(y_1, \ldots, y_n)$ be a set of preimages under π of generators of $\pi(N)$. The reader will check as an exercise that $(x_1, \ldots, x_m, y_1, \ldots, y_n)$ is a set of generators of N. □

Corollary 2.105 *If $M_1, M_2, \ldots, M_r$ are Noetherian R-modules, so is $\bigoplus_{n=1}^r M_n$.*

Proof Applying Proposition 2.104 to the short exact sequence $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$ gives that $M_1 \oplus M_2$ is Noetherian, and now an easy induction on r proves the claim. □

2.2.3.2 Noetherian Rings

Definition 2.106 A ring is a *Noetherian ring* if it is Noetherian as a module over itself.

❗ Let k be a field. Then the polynomial ring $k[(X_n)_{n\geq 0}]$ in a countable set of indeterminates is *not* Noetherian. That ring is a subring of its field of fractions $k((X_n)_{n\geq 0})$, hence a subring of a Noetherian ring needs not be Noetherian.

Proposition 2.107 *Let R be a commutative Noetherian ring.*

(1) *If $\mathfrak{a}$ is an ideal of R, the ring $R/\mathfrak{a}$ is Noetherian.*
(2) *Any finitely generated R-module is Noetherian.*
(3) *If R is a subring of a ring T which is a finitely generated R-module, then T is a Noetherian ring.*

Proof (1) $R/\mathfrak{a}$ is Noetherian as an R-module by Proposition 2.104, hence is Noetherian as an $R/\mathfrak{a}$-module, that is, is a Noetherian ring.

(2) Assume M is an image of R^m for some integer m. Since R^m is a Noetherian R-module by Corollary 2.105, M is Noetherian by Proposition 2.104.

(3) T is a Noetherian R-module by (2) above, hence a fortiori a Noetherian T-module, hence a Noetherian ring. □

The following property of ideals of Noetherian domains will be used to characterize Dedekind domains (see Theorem 2.241).

Lemma 2.108 *Let R be a Noetherian domain. Then, for each proper ideal $\mathfrak{a}$ of R, there is a finite number of prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ such that*

$$\mathfrak{p}_1 \cdots \mathfrak{p}_m \subset \mathfrak{a}.$$

Proof Assume this is not the case. Then by Noetherianity, there is a proper ideal $\mathfrak{a}$ which is maximal among ideals which do not contain the product of a finite number of prime ideals. In particular, $\mathfrak{a}$ itself is not prime, hence there exist two ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$ such that $\mathfrak{a} \subsetneq \mathfrak{a}_j$ for $j = 1, 2$ and $\mathfrak{a}_1\mathfrak{a}_2 \subset \mathfrak{a}$ (see Exercise 1.138). Now by maximality of $\mathfrak{a}$, both $\mathfrak{a}_1$ and $\mathfrak{a}_2$ contain a product of a finite number of prime ideals, hence so does $\mathfrak{a}_1\mathfrak{a}_2$, hence $\mathfrak{a}$ contains the product of a finite number of prime ideals, a contradiction. □

2.2.3.3 Hilbert's Basis Theorem

Theorem 2.109 (Hilbert's Basis Theorem) *Let R be a Noetherian ring. Then the polynomial ring $R[X_1, \ldots, X_r]$ in a finite number of indeterminates is Noetherian.*

Proof It suffices to prove that $R[X]$ is Noetherian.

Let $\mathfrak{A}$ be an ideal of $R[X]$. We shall prove that $\mathfrak{A}$ is finitely generated.

The leading coefficients of the elements of $\mathfrak{A}$ form an ideal $\mathfrak{a}$ in R. That ideal is finitely generated since R is Noetherian. Let $a_1, \dots, a_m$ be a set of generators of $\mathfrak{a}$. Let $P_1(X), \dots, P_m(X) \in \mathfrak{A}$ whose leading coefficients are respectively $a_1, \dots, a_m$ and let us denote by $\mathfrak{B}$ the ideal of $R[X]$ generated by $P_1(X), \dots, P_m(X)$.

For $1 \le i \le m$, we set $d_i := \deg P_i(X)$, and $r := \max\{d_1, \dots, d_m\}$. Let $R[X]_r$ be the R-submodule of $R[X]$ generated by $\{1, X, \dots, X^{r-1}\}$. In order to prove that $\mathfrak{A}$ is finitely generated, we shall prove that

$$\mathfrak{A} = \big(\mathfrak{A} \cap R[X]_r\big) + \mathfrak{B}. \tag{2.4}$$

Since $\mathfrak{B}$ is finitely generated by definition, and $\mathfrak{A} \cap R[X]_r$ is finitely generated as an R-module (since it is an R-submodule of the finitely generated R-module $R[X]_r$ and R is Noetherian), that will prove the result.

Let $P(X) \in \mathfrak{A}$. Let $d := \deg P(X)$. We may assume that $d > r$. Let a be its leading coefficient. We have $a = \lambda_1 a_1 + \cdots + \lambda_m a_m$ for some $\lambda_i \in R$. Then the polynomial

$$P(X) - \sum_{i=1}^{m} \lambda_i X^{d-d_i} P_i(X)$$

has degree strictly smaller than d. Repeating that operation, we get $P(X)$ as the sum of an element of $R[X]_r$ and an element of $\mathfrak{B}$, thus proving the announced equality (2.4). □

Corollary 2.110 *If R is a Noetherian ring, any finitely generated R-algebra is a Noetherian ring.*

Proof Indeed, it is an immediate consequence of Theorem 2.109 and of Proposition 2.107, (1). □

2.2.3.4 Localization over Noetherian Rings

First, let us notice that Noetherianity is preserved under localization.

Proposition 2.111 *Let R be a Noetherian integral domain.*

(1) *Let S be a nonempty multiplicatively closed subset of $R \setminus \{0\}$. Then $S^{-1}R$ is a Noetherian integral domain.*
(2) *For all $\mathfrak{p} \in \operatorname{Spec}(R)$, $R_\mathfrak{p}$ is a Noetherian integral domain.*

Proof Indeed, if the ideals of R are finitely generated, so are the ideals of $S^{-1}R$ by Lemma 1.133. □

ⓘ **Attention** ⓘ Noetherianity is *not* a local property.

For examples of *integral domains* R which are not Noetherian although $R_{\mathfrak{p}}$ is Noetherian for all $\mathfrak{p} \in \operatorname{Spec}(R)$, one may look at Sect. 2 of W. Heinzer and J. Ohm, *Locally Noetherian Commutative Rings,* Trans. Am. Math. Soc. **158**, 273–284 (1971).

The following exercise provides an example of a non Noetherian ring R such that $R_{\mathfrak{p}}$ is Noetherian for all $\mathfrak{p} \in \operatorname{Spec}(R)$, but here R is *not* an integral domain (see Remark 2.55 for the meaning of $R_{\mathfrak{p}}$ in that case).

Exercise 2.112 Let $R := \mathbb{F}_2^{\mathbb{N}} = \mathbb{F}_2 \times \mathbb{F}_2 \times \cdots \times \mathbb{F}_2 \times \cdots$.

(1) Find an increasing sequence of ideals in R which is not stationary.
(2) Prove that for any prime ideal $\mathfrak{p}$ of R, then $R_{\mathfrak{p}} = \mathbb{F}_2$.

> Hint. *Use the fact that $x^2 = x$ for all $x \in R$, to prove first that every prime ideal is maximal, hence that for all* $\mathfrak{p} \in \operatorname{Spec}(R)$, $R_{\mathfrak{p}}\mathfrak{p} = 0$ *since then* $R_{\mathfrak{p}}\mathfrak{p} = \operatorname{Nil}\operatorname{Rad}(R_{\mathfrak{p}})$.

For finitely generated modules over a Noetherian integral domain, localization behaves well the construction of morphisms, as shown by the next proposition.

Proposition 2.113 *Let R be a Noetherian integral domain, let S a non empty multiplicatively closed subset of $R \setminus \{0\}$. Let M be a finitely generated R-module.*

Then, whenever N is an R-module, the natural morphism of $S^{-1}R$-modules

$$\begin{cases} S^{-1}\operatorname{Hom}_R(M, N) \to \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N), \\ \phi/s \mapsto [x/t \mapsto \phi(x)/ts] \quad (\text{for } x \in M \text{ and } s, t \in S) \end{cases}$$

is an isomorphism.

Proof The conclusion is obviously true if $M = R$. Then it is easy to deduce that it is also true if $M = R^n$, a free R-module of rank n for some integer n.

In general, M is finitely generated, there is an integer $m \geq 1$ and a surjective R-module morphism $R^m \twoheadrightarrow M$. Since R is Noetherian, the kernel of that morphism is also finitely generated, and so there exists an integer $n \geq 1$ and an exact sequence

$$\begin{tikzcd} R^n \arrow[r, "\nu"] & R^m \arrow[r, "\mu"] & M \arrow[r] & 0. \end{tikzcd}$$

- By Proposition 2.49, we get the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Hom}_R(M, N) \arrow[r, "\operatorname{Hom}_R(\mu, N)"] & \operatorname{Hom}_R\big(R^m, N\big) \arrow[r, "\operatorname{Hom}_R\left(\nu, N\right)"] & \operatorname{Hom}_R(R^n, N) \end{tikzcd}$$

hence, since localization preserves exactness (see Lemma 2.60), we get the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & S^{-1}\operatorname{Hom}_R(M, N) \arrow[r] & S^{-1}\operatorname{Hom}_R\big(R^m, N\big) \arrow[r] & S^{-1}\operatorname{Hom}_R\big(R^n, N\big) \end{tikzcd}$$

• On the other hand, again since localization preserves exactness (see Lemma 2.60), we get the exact sequence

$$(S^{-1}R)^n \xrightarrow{S^{-1}\nu} (S^{-1}R)^m \xrightarrow{S^{-1}\mu} S^{-1}M \longrightarrow 0,$$

and by Proposition 2.49, we get the exact sequence

$$0 \to \mathrm{Hom}_{S^{-1}R}\big(S^{-1}M, S^{-1}N\big) \to \mathrm{Hom}_{S^{-1}R}\big((S^{-1}R)^m, S^{-1}N\big) \to \mathrm{Hom}_{S^{-1}R}\big((S^{-1}R)^n, S^{-1}N\big)$$

• Now, introducing as vertical arrows the natural morphisms described in the statement, we get the following commutative diagram, where the last two right-hand vertical arrows represent isomorphisms, and the left-hand horizontal arrows are injective:

$$\begin{tikzcd}
\mathrm{Hom}_{S^{-1}R}\big(S^{-1}M, S^{-1}N\big) \arrow[r, hook] & \mathrm{Hom}_{S^{-1}R}\big((S^{-1}R)^m, S^{-1}N\big) \arrow[r] & \mathrm{Hom}_{S^{-1}R}\big((S^{-1}R)^n, S^{-1}N\big) \\
S^{-1}\,\mathrm{Hom}_R(M, N) \arrow[u] \arrow[r, hook] & S^{-1}\,\mathrm{Hom}_R\big(R^m, N\big) \arrow[u, "\|"'] \arrow[r] & S^{-1}\,\mathrm{Hom}_R\big(R^n, N\big) \arrow[u, "\|"']
\end{tikzcd}$$

It is now an easy exercise (an example of what is called *"diagram chasing"*) to prove that the left-hand vertical arrow is an isomorphism as well. □

Remark 2.114 The reader may have noticed that, instead of assuming R Noetherian, we might as well have assumed that there is an exact sequence

$$R^n \xrightarrow{\nu} R^m \xrightarrow{\mu} M \longrightarrow 0$$

in order to get the same conclusion.

Such a module M is said to be *finitely presented.*

2.2.4 Finitely Generated Free Modules

2.2.4.1 Rank and Basis of a Finitely Generated Free Module

Theorem 2.115 *Let M be a free R-module. Assume that M has a basis with r elements.*

(1) *Every generating system of M has at least r elements.*
(2) *Every generating system of M with cardinality r is a basis.*
(3) *Every basis of M has cardinality r.*

Proof (1) Assume that $(e_i)_{1\le i\le r}$ is a basis of M, and let $(x_j)_{1\le j\le n}$ be a generating system.

Let P and Q be the matrices (with entries in R) defined by

$$\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_r \end{pmatrix} = P \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = Q \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_r \end{pmatrix}.$$

It follows that

$$\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_r \end{pmatrix} = PQ \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_r \end{pmatrix} \quad \text{hence} \quad PQ = 1_r.$$

Assume $r \ge n$. We shall prove then that $r = n$.

The matrix P has r lines and n columns. Let us complete it to a square $r \times r$ matrix $\widetilde{P}$ by adding to the left $(r-n)$ columns made of 0's. Similarly, let us complete the matrix Q to a square $r \times r$ matrix, denoted $\widetilde{Q}$, by adding at the top $(r-n)$ lines made of 0's.

Then

$$\widetilde{P}\widetilde{Q} = 1_r.$$

By Lemma 2.116 below, this implies

$$\widetilde{Q}\widetilde{P} = 1_r,$$

which proves $r = n$.

The proofs of (2) and (3) are left as exercises to the reader. □

Lemma 2.116 *Let A and B be $(r \times r)$-matrices with entries in R. If $AB = 1_r$, then $BA = 1_r$.*

Proof For A a square matrix, let us denote by $\mathrm{Com}(A)$ the matrix of its cofactors. It is known that

$$A.{}^t\mathrm{Com}(A) = {}^t\mathrm{Com}(A).A = \det(A)1_r.$$

Now $AB = 1_r$ implies that $\det(A)$ is invertible. Thus, multiplying both sides of the equality $AB = 1_r$ by $\det(A)^{-1}{}^t\mathrm{Com}(A)$ gives $B = \det(A)^{-1}{}^t\mathrm{Com}(A)$, from which we deduce $BA = 1_r$. □

Definition 2.117 The common cardinality of all bases of a finitely generated free R-module M is called the *rank* of M.

Notice that by definition an R-module M is of rank r if and only if M is isomorphic to R^r.

! Attention !

- A minimal generating system of a free module needs not be a basis (for example, the system $\{2, 3\}$ is a minimal generating system of $\mathbb{Z}$ but is not a basis).
- A maximal free system of a free module needs not be a basis (for example, the system $\{2\}$ is a maximal free system of $\mathbb{Z}$ but is not a basis).
- A free system of cardinality r of a free module of rank r needs not be a basis (for example, the system $\{2\}$ is a free system of $\mathbb{Z}$ but is not a basis).

Corollary 2.118 *Let $\phi : M \twoheadrightarrow N$ be a surjective morphism between free modules of the same (finite) rank. Then ϕ is an isomorphism*

! An injective morphism between free modules of the same (finite) rank needs not be an isomorphism (example?).

Proof of Corollary 2.118 Indeed, if r denotes the common rank of M and N, the image under ϕ of a basis of M is a generating system of N with r elements, hence is a basis by Theorem 2.115. □

2.2.4.2 Rank: Another Proof

To prove that two finite bases of a module M have the same cardinality, it suffices to prove that if R^m is isomorphic to R^n, then $m = n$.

Assume $R^m \cong R^n$. Let $\mathfrak{m}$ be a maximal ideal of R. Then

$$R^m/\mathfrak{m}R^m \cong R^n/\mathfrak{m}R^n \quad \text{hence} \quad (R/\mathfrak{m})^m \cong (R/\mathfrak{m})^n .$$

Since $R/\mathfrak{m}$ is a field, this implies $m = n$.

Remark 2.119 If R is an integral domain, a free R-module M has no nonzero torsion element: if M is free and if $x \in M$, $x \neq 0$, then $\mathrm{Ann}_R(x) = \{0\}$.

2.2.4.3 The Dual of a Free Module of Finite Rank

Preliminary remarks.

Proposition 2.120 *Let M be a free R-module of rank r.*

(1) *The dual module M^* is a free R-module of rank r.*
(2) *The map $M \to M^{**}, m \mapsto m^{**} := (\varphi \mapsto \varphi(m))$, is an isomorphism.*

Proof (1) If M is free with basis $(e_i)_{1\leq i\leq r}$, then the system $(e_i^*)_{1\leq i\leq r}$ defined by

$$e_i^*(e_j) := \delta_{i,j}$$

is a basis of M^* (called the *dual basis* of $(e_i)_{1\leq i\leq r}$).

(2) It is clear that, with the above notation, the system $(e_i^{**})_{1\leq i\leq r}$ is the dual basis of $(e_i^*)_{1\leq i\leq r}$. □

Thus the dual of R^m is isomorphic to R^m, a remark which is the key for the next corollary.

Corollary 2.121 *If M is finitely generated with m generators, M^* is isomorphic to a submodule of R^m.*

Proof The module M can be generated by m elements if and only if there exists a surjective morphism $\pi : R^m \twoheadrightarrow M$. The dual morphism $\pi^* : M^* \longrightarrow (R^m)^*$ is then injective by Corollary 2.51. □

Notice that for any R-module M and for all $x \in M$, the set

$$M^*(x) := \{\varphi(x) \mid \varphi \in M^*\}$$

is an ideal of R.

Lemma 2.122 *Let M be a free R-module with basis $(e_i)_{1\leq i\leq r}$. Let $x = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_r e_r$ be an element of M. Then*

$$M^*(x) = R\lambda_1 + R\lambda_2 + \cdots + R\lambda_r.$$

Proof Let $(e_i^*)_{1\leq i\leq r}$ be the dual basis of $(e_i)_{1\leq i\leq r}$. Since $M^*(x)$ is generated by $(e_i^*(x))_{1\leq i\leq r}$, and since $e_i^*(x) = \lambda_i$, the lemma follows. □

Proposition 2.123 *Assume R is an integral domain. Let M be a free R-module with basis $(e_i)_{1\leq i\leq r}$ and let $x = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_r e_r$ be a nonzero element of M. The following properties are equivalent.*

(i) $M^*(x) = R$.
(ii) $\sum_{i=1}^r R\lambda_i = R$.
(iii) *There exists $\varphi \in M^*$ such that $\varphi(x) = 1$.*
(iv) *There exists a submodule M_1 of M such that $M = Rx \oplus M_1$.*

Proof (i)⇔(ii): follows from Lemma 2.122.

(ii)⇒(iii): by definition of $M^*(x)$.

(iii)⇒(iv): Let $M_1 := \ker(\varphi)$. For all $y \in M$ we have:

$$y = \varphi(y)x + \big(y - \varphi(y)x\big),$$

where $\varphi(y)x \in Rx$ and $(y - \varphi(y)x) \in M_1$ since $\varphi(x) = 1$. Moreover, it is clear that $Rx \cap M_1 = \{0\}$, so $M = Rx \oplus M_1$.

(iv)⇒(i): Since M is free and R is an integral domain, no nonzero element of M is torsion (see 2.119), hence the map

$$R \longrightarrow Rx, \qquad \lambda \mapsto \lambda x,$$

is an isomorphism. Its inverse is a linear form on Rx which sends x onto 1. By composition with the composed morphism

$$M \twoheadrightarrow M/M_1 \xrightarrow{\sim} Rx,$$

we get a linear form on M which sends x onto 1. Thus, the ideal $M^*(x)$ contains 1, hence is equal to R. □

The next proposition follows immediately from Lemma 2.122.

Proposition 2.124 *Let M be a free R-module of finite rank and let $x \in M$. Let $d \in R$. The following properties are equivalent.*

(i) $M^*(x) \subseteq Rd$.
(ii) *There exists $y \in M$ such that $x = dy$ (i.e., x is "divisible by d").*

Proof (ii)⇒(i) is obvious. Let us prove that (i)⇒(ii). Assume $(e_i)_{1\leq i\leq r}$ is a basis of M and $x = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_r e_r$. For all i, $\lambda_i = e_i^*(x)$ is divisible by d, so there exists $\mu_i \in R$ such that $\lambda_i = d\mu_i$. We then set $y := \mu_1 e_1 + \mu_2 e_2 + \cdots + \mu_r e_r$. □

2.2.4.4 About Finitely Generated Torsion-Free Modules

A free module is torsion-free. The next proposition shows more connections between "torsion-freeness" and "freeness".

Proposition 2.125 *Assume that R is an integral domain. Then any finitely generated torsion-free R-module is isomorphic to a submodule of a free R-module of finite rank.*

Proof Assume that M is a torsion-free R-module, which is generated by a finite system of nonzero elements $\{x_1, \ldots, x_n\}$. Up to reordering that system, we may assume that there exists $r \leq n$ such that $(x_1, \ldots, x_r)$ is a maximal free subsystem. The submodule $M_0 := Rx_1 + \cdots + Rx_r = Rx_1 \oplus \cdots \oplus Rx_r$ is free. We shall see that M is isomorphic to a submodule of M_0.

If $r = n$, $M = M_0$. So we assume $r < n$. Then for each j, $0 < j \leq n - r$, there is $\lambda_j \in R$, $\lambda_j \neq 0$, such that $\lambda_j x_{r+j} \in M_0$. Set $\lambda := \lambda_1 \cdots \lambda_{n-r}$. Then $\lambda M \subset M_0$.

Since M is torsion free, the map $M \to M_0, m \mapsto \lambda m$, is injective, which proves that M is indeed isomorphic to a submodule of M_0. □

2.2.5 Finitely Generated Projective Modules

2.2.5.1 Characterization, Dual

Proposition 2.126 *Let P be an R-module. The following assertions are equivalent*:

(i) *P is a finitely generated projective R-module*,

(ii) *P is isomorphic to a summand of a free R-module of finite rank.*

Proof (i)⇒(ii): Since P is finitely generated, there is a natural integer n and a surjective morphism $R^n \twoheadrightarrow P$. By Lemma 2.33 above, we see that P is isomorphic to a summand of R^n.

(ii)⇒(i): If P is isomorphic to a summand of R^n, we see in particular that there is a surjective morphism $R^n \twoheadrightarrow P$, which shows that P is finitely generated. Besides, we know by Proposition 2.31 that P is projective. □

Corollary 2.127 *Let P be a finitely generated projective R-module. The morphism*

$$P \to P^{**}, \qquad v \mapsto v^{**} : \big(\varphi \mapsto \varphi(v)\big),$$

is an isomorphism.

Proof The following two diagrams summarize the proof.

$$\begin{tikzcd}
P \arrow[rr, "\mathrm{Id}_P"] \arrow[dr, "\iota"'] & & P \\
& F \arrow[ur, "\pi"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
P^* \arrow[rr, "\mathrm{Id}_{P^*}"] \arrow[dr, "\pi^*"'] & & P^* \\
& F^* \arrow[ur, "\iota^*"'] &
\end{tikzcd}$$

If P is a finitely generated projective R-module, then so is its dual P^*. Indeed, since P is isomorphic to a summand of a free R-module of finite rank F, P^* is isomorphic to a summand of F^*, which is also free of (same) finite rank, hence is projective.

The morphism

$$F \to F^{**}, \qquad x \mapsto x^{**} : \big(\varphi \mapsto \varphi(x)\big),$$

is an isomorphism by Proposition 2.120.

Let us prove that the morphism

$$P \to P^{**}, \qquad v \mapsto v^{**} : \big(\varphi \mapsto \varphi(v)\big),$$

is surjective. Given $\psi \in P^{**}$, we shall find $v \in P$ such that, for all $\varphi \in P^*$, we have $\psi(\varphi) = \varphi(v)$. Given ψ, we have $\psi.\iota^* \in F^{**}$, hence there exists a unique $x \in F$ such that for all $\alpha \in F^*$, $\psi(\iota^*(\alpha)) = \alpha(x)$, i.e., $\psi(\alpha.\iota) = \alpha(x)$. Now, given $\varphi \in P^*$, we have $\varphi.\pi \in F^*$, hence $\psi(\varphi.\pi.\iota) = \varphi(\pi(x))$, and, setting $v := \pi(x)$, we get $\psi(\varphi) = \varphi(v)$.

We leave the proof of injectivity to the reader. □

2.2.5.2 Projective Morphisms

For R-modules X, Y and M, the composition of morphisms defines a morphism

$$\begin{cases} \mathrm{Hom}_R(X, M) \otimes_R \mathrm{Hom}_R(M, Y) \to \mathrm{Hom}_R(X, Y) \\ \varphi \otimes_R \psi \mapsto \psi.\varphi. \end{cases}$$

Proposition 2.128 *The image* $\mathrm{Hom}_R^{(M)}(X, Y)$ *of the above morphism is comprised of those morphisms from X to Y which factor through some finite power of M:*

$$\begin{tikzcd} X \arrow[rr] \arrow[dr] & & Y \\ & M^n \arrow[ur] & \end{tikzcd}$$

Proof An element of the image is $\sum_{i \in I} \psi_i.\varphi_i$, where $(\varphi_i)_{i \in I}$ and $(\psi_i)_{i \in I}$ are finite families in respectively $\mathrm{Hom}_R(X, M)$ and $\mathrm{Hom}_R(M, Y)$, hence correspond respectively (see Definition 2.35) to

- a morphism $\varphi : X \to M^I$, and
- a morphism $\psi : M^I \to Y$. □

Consider the particular case where $M = R$. Then

- $\mathrm{Hom}_R(R, Y)$ is canonically isomorphic to Y (exercise!),
- and $\mathrm{Hom}_R(X, R)$ is the dual X^*,

so we get a morphism

$$\tau_{X,Y} : X^* \otimes_R Y \to \mathrm{Hom}_R(X, Y)$$

whose image is comprised of those morphisms from X to Y which factor through some finite power of R:

$$\begin{tikzcd} X \arrow[rr] \arrow[dr] & & Y \\ & R^n \arrow[ur] & \end{tikzcd}$$

It results immediately from Lemma 2.126 that a morphism from X to Y factors through some finite power of R if and only if it factors through a finitely generated projective module P:

$$\begin{tikzcd}
X \arrow[rr] \arrow[dr] & & Y \\
& P \arrow[ur] &
\end{tikzcd}$$

Definition 2.129 The image of $\tau_{X,Y}$ is denoted by $\mathrm{Hom}_R^{\mathrm{pr}}(X, Y)$, and its elements are called the *projective morphisms* from X to Y.

The following lemma is an immediate consequence of the definition.

Lemma 2.130 *For any R-module M, $\mathrm{Hom}_R^{\mathrm{pr}}(M, M)$ is a twosided ideal in the R-algebra $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$.*

Remark 2.131 More generally, for any R-modules X', X, Y, Y', for any $\alpha \in \mathrm{Hom}_R(X', X)$, $\beta \in \mathrm{Hom}_R(Y, Y')$, and $\varphi \in \mathrm{Hom}_R^{\mathrm{pr}}(X, Y)$, we have $\beta.\varphi.\alpha \in \mathrm{Hom}_R^{\mathrm{pr}}(X', Y')$:

$$\begin{tikzcd}
X' \arrow[r, "\alpha"] & X \arrow[rr, "\varphi"] \arrow[dr] & & Y \arrow[r, "\beta"] & Y' \\
& & R^n \arrow[ur] & &
\end{tikzcd}$$

That property may be stated as follows: $\mathrm{Hom}_R^{\mathrm{pr}}(\cdot, \cdot)$ is a twosided ideal in the category of R-modules.

2.2.5.3 A Series of Characterizations

Theorem 2.132 *Let P be an R-module. The following assertions are equivalent.*

(i) *P is a finitely generated projective module.*

(ii) $\mathrm{Hom}_R(P, P) = \mathrm{Hom}_R^{\mathrm{pr}}(P, P)$.

(iii) *For any R-module X, the morphism*

$$\tau_{X,P} : X^* \otimes_R P \to \mathrm{Hom}_R(X, P)$$

is an isomorphism.

(iv) *For any R-module X, the morphism*

$$\tau_{P,X} : P^* \otimes_R X \to \mathrm{Hom}_R(P, X)$$

is an isomorphism.

(v) *The morphism* $\tau_{P,P} : P^* \otimes_R P \to \mathrm{End}_R(P)$ *is an isomorphism.*

Proof (i)⇒(ii): Since P is isomorphic to a summand of R^n for some integer n, there exist morphisms $\iota : P \to R^n$ and $\pi : R^n \to P$ such that $\pi.\iota = \mathrm{Id}_P$:

$$\begin{tikzcd}
P \arrow[rr, "\mathrm{Id}_P"] \arrow[dr, "\iota"'] & & P \\
& R^n \arrow[ur, "\pi"'] &
\end{tikzcd}$$

Thus Id_P belongs to the ideal $\mathrm{Hom}_R^{\mathrm{pr}}(P, P)$ of the R-algebra $\mathrm{Hom}_R(P, P)$, which proves (ii) (see Lemma 2.130).

(ii)⇒(iii): Assume that

$$\mathrm{Id}_P = \tau_{P,P}\Big(\sum_{i\in I} \varphi_i \otimes_R m_i\Big),$$

i.e., for all $v \in P$, we have $\sum_{i\in I} \varphi_i(v)m_i = v$.

Consider the morphism

$$\sigma : \begin{cases} \mathrm{Hom}_R(X, P) \to X^* \otimes_R P \\ \alpha \mapsto \sum_{i\in I} \varphi_i.\alpha \otimes_R m_i . \end{cases}$$

We shall check that σ is the inverse of $\tau_{X,P}$.

- The composed morphism

$$\mathrm{Hom}_R(X, P) \xrightarrow{\sigma} X^* \otimes_R P \xrightarrow{\tau_{X,P}} \mathrm{Hom}_R(X, P)$$

is

$$\alpha \mapsto \Big(x \mapsto \sum_{i\in I} \varphi_i\big(\alpha(x)\big)m_i = \alpha(x)\Big)$$

hence is the identity.
- In order to check that the composed morphism

$$X^* \otimes_R P \xrightarrow{\tau_{X,P}} \mathrm{Hom}_R(X, P) \xrightarrow{\sigma} X^* \otimes_R P$$

is the identity, me must check

$$\psi \otimes_R v = \sum_{i\in I} \varphi_i.\tau_{X,P}(\psi \otimes_R v) \otimes_R m_i .$$

Indeed, we have

$$\varphi_i(v)\psi = \varphi_i.\tau_{X,P}(\psi \otimes_R v)$$

(as one sees easily by applying both sides to an element of X), hence

$$\begin{aligned}\psi \otimes_R v = \psi \otimes_R \sum_{i\in I} \varphi_i(v)m_i &= \sum_{i\in I} \psi \otimes_R \varphi_i(v)m_i \\ = \sum_{i\in I} \varphi_i(v)\psi \otimes_R m_i &= \sum_{i\in I} \varphi_i.\tau_{X,P}(\psi \otimes_R v) \otimes_R m_i.\end{aligned}$$

(ii)⇒(iv): The proof is analogous to what precedes and is left to the reader.

(iii)⇒(v) and (iv)⇒(v): trivial.

(v)⇒(i): Since Id_P is a projective morphism, there exist morphisms ι and π such that Id_P factorizes through a free module of finite rank:

$$\begin{tikzcd} P \arrow[rr, "\mathrm{Id}_P"] \arrow[dr, "\iota"'] & & P \\ & R^n \arrow[ur, "\pi"'] & \end{tikzcd}$$

and we see that P is isomorphic to a summand of R^n, hence is finitely generated and projective by Proposition 2.126. □

Corollary 2.133 *Let M be a finitely generated projective R-module. Then whenever*

$$\begin{tikzcd} 0 \arrow[r] & X' \arrow[r, "\iota"] & X \arrow[r, "\pi"] & X'' \arrow[r] & 0 \end{tikzcd}$$

is a short exact sequence of R-modules, then

$$\begin{tikzcd} 0 \arrow[r] & M \otimes_R X' \arrow[r, "1_M \otimes_R \iota"] & M \otimes_R X \arrow[r, "1_M \otimes_R \pi"] & M \otimes_R X'' \arrow[r] & 0 \end{tikzcd}$$

is exact.

Proof By Proposition 2.52, it suffices to check that the map $1_M \otimes_R \iota$ is injective. By Theorem 2.132 and by Corollary 2.127, we have

$$M \otimes_R X \simeq \mathrm{Hom}_R\big(M^*, X\big)$$

and under that isomorphism, the map $1_M \otimes_R \iota$ becomes equal to the map $\mathrm{Hom}_R(1_{M^*}, \iota)$ (see Sect. 2.1.5.3 for the notation). Thus the proposition results from Proposition 2.49, (2). □

Corollary 2.134 *Let M be a finitely generated projective R-module and let S be a nonempty multiplicatively closed subset of $R \setminus \{0\}$. Then $S^{-1}M$ is a finitely generated projective $S^{-1}R$-module.*

Proof One can notice that if M is a summand of R^n for some integer $n \geq 1$, it is clear that $S^{-1}M$ is a summand of $(S^{-1}R)^n$, which proves Corollary 2.134.

…Why then did we call it "Corollary"? Because one can also give the following proof.

By Theorem 2.132, (ii), an R-module M is a finitely generated projective R-module if and only if the map $\tau_{M,M}$ is onto, that is if there exist two finite families $(\varphi_i)_{i\in I}$ and $(m_i)_{i\in I}$ (with $\varphi_i \in M^*$ and $m_i \in M$) such that

$$\text{for all } m \in M, \quad \sum_{i\in I} \varphi_i(m)m_i = m.$$

It is clear that if $((\varphi_i)_{i\in I}, (m_i)_{i\in I})$ is such a pair of families for M, then $((S^{-1}\varphi_i)_{i\in I}, (m_i/1)_{i\in I})$ is such a pair for the $S^{-1}R$-module $S^{-1}M$ (for the notation $S^{-1}\varphi$, see Exercises 2.66). □

2.2.5.4 The Case of Local Rings

We shall prove in this section that a finitely generated projective module over a local ring is free. The next proposition is fundamental.

Proposition 2.135 (Nakayama's lemma) *Assume that R is local, with unique maximal ideal $\mathfrak{m}$.*

Let M be a finitely generated R-module.

(1) *If $M = \mathfrak{m}M$, then $M = 0$.*
(2) *If $\varphi : M \to N$ is a morphism which induces a surjective morphism $\overline{\varphi} : M/\mathfrak{m}M \twoheadrightarrow N/\mathfrak{m}N$, then φ is surjective.*
(3) *If N is a submodule of M such that the inclusion $N \hookrightarrow M$ induces an isomorphism $N/\mathfrak{m}N \xrightarrow{\sim} M/\mathfrak{m}M$, then $N = M$.*

Proof (1) Assume M is generated by $\{x_1, \ldots, x_m\}$. If $M = \mathfrak{m}M$, there exist $r_{i,j} \in \mathfrak{m}$ $(1 \leq i, j \leq m)$ such that for all i, we have $x_i = \sum_{j=1}^{m} r_{i,j}x_j$. Let A be the $m \times m$ matrix with entries $r_{i,j}$ $(1 \leq i, j \leq m)$. The above equations give

$$(1_m - A)\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Multiplying to the left by ${}^t\mathrm{Com}(1_m - A)$ gives then

$$\det(1_m - A)\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

so

$$\det(1_m - A)M = 0.$$

Now $\det(1_m - A) = 1 - r$ for some $r \in \mathfrak{m}$. Since $1 - r$ is invertible (see Corollary 1.121), this implies $M = 0$.

(2) The morphism $\overline{\varphi} : M/\mathfrak{m}M \twoheadrightarrow N/\mathfrak{m}N$ is surjective if and only if (see Exercises 2.14) $\varphi(M) + \mathfrak{m}N = N$, i.e., $\mathfrak{m}(N/\varphi(M)) = N/\varphi(M)$, and it follows from (1) that $N = \varphi(M)$.

(3) This is a particular case of (2). □

Proposition 2.136 *Assume that R is local, with unique maximal ideal $\mathfrak{m}$. Then any finitely generated projective R-module is free.*

Proof Let X be a finitely generated projective R-module. Then the module $X/\mathfrak{m}X$ is a finite dimensional vector space over the field $R/\mathfrak{m}$. Let r denote its dimension. The isomorphism $(R/\mathfrak{m})^r \xrightarrow{\sim} X/\mathfrak{m}X$ can be lifted (by projectivity of R^r) to a morphism $R^r \to X$, which is onto by Nakayama's lemma 2.135. Since X is projective, we get a split short exact sequence

$$0 \to X' \to R^r \to X \to 0.$$

Note that X' is then a direct summand of R^r, hence is also finitely generated. By tensoring with $R/\mathfrak{m}$, this exact sequence gives (since it is split) the short exact sequence

$$0 \to X'/\mathfrak{m}X' \to (R/\mathfrak{m})^r \to X/\mathfrak{m}X \to 0,$$

which shows that $X'/\mathfrak{m}X' = 0$, hence again by Nakayama's lemma 2.135 $X' = 0$. Thus we get that X is isomorphic to R^r. □

Corollary 2.137 *Let R be an integral domain and $\mathfrak{p}$ be a prime ideal of R. Whenever M is a finitely generated projective R-module, $M_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module of finite rank.*

Proof Indeed, if M is a finitely generated projective R-module it follows from Corollary 2.134 that $M_\mathfrak{p}$ is a finitely generated projective $R_\mathfrak{p}$-module. By Proposition 2.136, we then see that $M_\mathfrak{p}$ is free of finite rank. □

⚠ There are examples of non-finitely generated non-projective modules M such that $M_\mathfrak{p}$ is free for all $\mathfrak{p} \in \mathrm{Spec}(R)$.

Nevertheless, the converse is true if R is Noetherian, as shown by the following proposition (so being *finitely generated projective* is a local notion over a Noetherian ring).

Proposition 2.138 *Let R be a Noetherian integral domain. Let M be a finitely generated R-module. The following assertions are equivalent*:

(i) *M is projective*,
(ii) *for all $\mathfrak{p} \in \operatorname{Spec}(R)$, $M_\mathfrak{p}$ is free*.

Proof (i)⇒(ii) is just Proposition 2.137.

(ii)⇒(i) To prove that M is projective we must prove that for every surjective R-module morphism $\phi : P \twoheadrightarrow Q$, the induced morphism $\operatorname{Hom}_R(M, \phi) : \operatorname{Hom}_R(M, P) \to \operatorname{Hom}_R(M, Q)$ is surjective. So it suffices to prove (see Proposition 2.59, (4)) that, for all prime ideals $\mathfrak{p}$, the localized morphism $\operatorname{Hom}_R(M, \phi)_\mathfrak{p} : \operatorname{Hom}_R(M, P)_\mathfrak{p} \to \operatorname{Hom}_R(M, Q)_\mathfrak{p}$ is surjective.

Since R is Noetherian and M is finitely generated, it follows from Proposition 2.113 that there exist natural isomorphisms (vertical arrows in the diagram below) which make the following diagram commutative

$$\begin{tikzcd}
\operatorname{Hom}_R(M, P)_\mathfrak{p} \arrow[r, "\operatorname{Hom}_R(M,\phi)_\mathfrak{p}"] \arrow[d, "\simeq"'] & \operatorname{Hom}_R(M, Q)_\mathfrak{p} \arrow[d, "\simeq"] \\
\operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, P_\mathfrak{p}) \arrow[r, "\operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p},\phi_\mathfrak{p})"] & \operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, Q_\mathfrak{p}).
\end{tikzcd}$$

Now, since $M_\mathfrak{p}$ is free, the bottom horizontal morphism is surjective, which proves that the top horizontal morphism is also surjective. □

Remark 2.139 Local rings are not the only example for which finitely generated projective modules are free.

We shall see later that finitely generated projective modules over a principal ideal domain are free.

Let us give a much less easy example.

Let k be a field and $n \geq 2$. In his article known as *"FAC"* [8] J.-P. Serre wrote (in 1955)

> *"(…) On ignore s'il existe des $k[X_1, \dots, X_n]$-modules projectifs de type fini qui ne soient pas libres (…)" ("it is not known if there exist projective $k[X_1, \dots, X_n]$-modules of finite type which are not free").*

The fact that finitely generated projective $k[X_1, \dots, X_n]$-modules are indeed free has been proved by Quillen and Suslin in 1976. A proof can be found in [6] (XXI, §4, Theorem 3.7).

More Exercises on Sect. 2.2

Exercise 2.140 Prove that the ring $\mathbb{Z}[\sqrt{-3}]$ is not integrally closed.

Exercise 2.141 Let R be a Noetherian ring and let A be a finitely generated commutative R-algebra. Let G be a finite group of algebra automorphisms of A, and let A^G be the subalgebra of all elements of A fixed by G. Prove that A^G is a finitely generated R-algebra (a result due to Hilbert).

Exercise 2.142 Let M be a Noetherian R-module. Prove that any surjective endomorphism of M is an automorphism.

Exercise 2.143 Let Hol be the ring of all holomorphic functions $\mathbb{C} \to \mathbb{C}$.

(1) Prove that Hol is an integral domain. What is its field of fractions?
(2) Prove that Hol is not Noetherian.

HINT. Consider the ideals of Hol defined by

$$I_n := \{ f \in \mathrm{Hol} \mid f(z) = 0 \forall z \in \mathbb{N} \setminus \{0, 1, \dots, n\} \},$$

and the function $\sin \pi z$.

(3) Prove that an element $u \in \mathrm{Hol}$ is invertible if and only if there exists $g \in \mathrm{Hol}$ such that $u = \exp(g)$.
Prove that an element $f \in \mathrm{Hol}$ is irreducible if and only if f has a unique zero, which is simple.
(4) Prove that Hol is not factorial.

From now on, k denotes a (commutative) field.

Exercise 2.144 Let R be the subring of $k[X, Y]$ defined by

$$R := \left\{ \sum_{i>j} a_{i,j} X^i Y^j \right\}.$$

Check that $R = k[\{X^{i+1} Y^i\}_{i \geq 0}]$ and prove that R is not Noetherian.

Exercise 2.145 Let $E(X) \in k(X)$, $E(X) \notin k$. We write $E(X) = P(X)/Q(X)$ where $P(X), Q(X) \in k[X]$ are relatively prime, $n := \max\{\deg(P), \deg(Q)\}$. Let L be the subfield of $k(X)$ generated by $E(X)$ over k.

(1) Check that X is algebraic over L and that $E(X)$ is transcendental over k.
(2) Prove that $[k(X):L]=n$.

Exercise 2.146

Theorem 2.147 *Whenever R is a (commutative) integral domain which is integrally closed, then so is $R[X]$.*

One may prove the above theorem under the supplementary assumption that R is Noetherian, as follows.

Let F be the field of fractions of R, and let $E(X)\in F(X)$ be integral over $R[X]$.

(1) Prove that $E(X)\in F[X]$.
(2) Prove that there exists $P(X)\in F[X]$ such that $P(X)E(X)^j\in R[X]$ for all nonnegative integers j.
(3) Assume $E(X)=u_nX^n+u_{n-1}X^{n-1}+\cdots+u_1X+u_0$. Prove that u_n is integral over R.

Exercise 2.148 Let $R=\mathbb{Z}[\sqrt{-5}]$. Let $\mathfrak{a}$ be the ideal of R generated by 2 and $1+\sqrt{-5}$. Prove that $\mathfrak{a}$ is a projective R-module.

2.3 Finitely Generated Modules over Dedekind Domains

2.3.1 Fractional Modules, Dedekind Domains

2.3.1.1 Projective Modules and Fractional Modules

All throughout this section we denote by R an *integral domain*, with field of fractions F. Whenever M is an R-module, it defines the F-vector space

$$FM := F\otimes_R M.$$

If M is finitely generated, the F-vector space FM is finite dimensional.

Proposition 2.149 *If M is a finitely generated projective R-module, the natural morphism $M\to FM$ is injective.*

Proof It is an immediate consequence of Corollary 2.58 since a projective module is always torsion free since it is isomorphic to a submodule of a free module (Proposition 2.31, (ii)). □

Definition 2.150 The *rank of a finitely generated torsion free R-module* (and in particular the *rank of a finitely generated projective R-module*) M is by definition the dimension of the F-vector space FM.

Notice that for a free module, this agrees with the previous definition of rank.

Remark 2.151 A finitely generated torsion free R-module M of rank one is isomorphic to a finitely generated R-submodule of F.

Indeed, if $FM = Fe$, then $\mathfrak{a} := \{\lambda \in F \mid \lambda e \in M\}$ is an R-submodule of F. We have $M = \mathfrak{a}e$.

Exercise 2.152 Let $\mathfrak{p} \in \operatorname{Spec}(R)$, and let M be a finitely generated projective R-module. Set $M_\mathfrak{p} := R_\mathfrak{p} \otimes_R M$. Prove that

(1) $M_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module of finite rank.
(2) The rank of $M_\mathfrak{p}$ equals the rank of M as defined above.

Proposition 2.149 shows that any finitely generated projective R-module may be viewed as an R-submodule of the finite dimensional F-vector space FM. That submodule generates FM, and given any basis $(e_i)_{1\le i\le r}$ of FM, since M is finitely generated, there exists $\lambda \in R$, $\lambda \neq 0$, such that $\lambda M \subset \bigoplus_{i=1}^r Re_i$.

Definition 2.153 Let V be an F-vector space of finite dimension r. A *fractional R-module* in V is an R-submodule M of V such that

(1) M generates V as a vector space,
(2) given any basis $(e_i)_{1\le i\le r}$ of V, there exists $\lambda \in R$, $\lambda \neq 0$, such that $\lambda M \subset \bigoplus_{i=1}^r Re_i$.

In the case where $V = F$, such a fractional module is called a *fractional ideal*. It is a nonzero R-submodule $\mathfrak{a}$ of F for which there exists $\lambda \in R$, $\lambda \neq 0$, such that $\lambda\mathfrak{a} \subset R$ (note that then $\lambda\mathfrak{a}$ is an ideal of R).

Examples 2.154

- Every finitely generated R-submodule of F is a fractional ideal, and if R is Noetherian these are all the fractional ideals of R.
- For $R = \mathbb{Z}$ and $V = M = \mathbb{Q}$, the property (1) of Definition 2.153 is satisfied, but the property (2) is not.

The proof of the following lemma is left to the reader.

Lemma 2.155 *Let M be a finitely generated torsion free R-module, let $V = FM$ (so M is identified with an R-submodule of FM).*

(1) *If $\lambda M \subset \bigoplus_{i=1}^r Re_i$ for some basis $(e_i)_{1\le i\le r}$ of V and some $\lambda \in R$, $\lambda \neq 0$, then whenever $(f_i)_{1\le i\le r}$ is a basis of V there exists $\mu \in R$, $\mu \neq 0$, such that $\mu M \subset \bigoplus_{i=1}^r Rf_i$.*
(2) *Condition* (1) *in the Definition* 2.153 *may be replaced by*

    (1′) *given a basis $(e_i)_{1\le i\le r}$ of V, there exists $\mu \in R$, $\mu \neq 0$, such that $\mu \bigoplus_{i=1}^r Re_i \subset M$.*

(3) *If M_1 and M_2 are fractional modules in V, then $M_1 + M_2$ and $M_1 \cap M_2$ are also fractional modules.*

Part 3 of the above lemma shows in particular that, whenever $(e_i)_{1 \le i \le r}$ is a basis of V and $(\mathfrak{a}_i)_{1 \le i \le r}$ is a family of fractional ideals, then

$$M := \bigoplus_{i=1}^{r} \mathfrak{a}_i e_i$$

is a fractional module.

For the particular case of fractional ideals, we have the obvious following examples of construction of fractional ideals.

Lemma 2.156 *Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional ideals.*

(1) $\mathfrak{a} + \mathfrak{b}$ (*the R-submodule of F generated by* $\mathfrak{a} \cup \mathfrak{b}$) *is a fractional ideal.*
(2) $\mathfrak{a} \cap \mathfrak{b}$ *is a fractional ideal.*
(3) $\mathfrak{a}\mathfrak{b}$ (*the R-submodule of F generated by all ab for $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$*) *is a fractional ideal.*

We recall that for any R-module M, its dual is $M^* = \mathrm{Hom}_R(M, R)$.

Proposition 2.157

(1) *For any fractional ideal* $\mathfrak{a}$, *there is a natural identification*

$$\mathfrak{a}^* = \{x \in F \mid x\mathfrak{a} \subset R\},$$

which is again a fractional ideal.

(2) *Let V be an r-dimensional F-vector space, let $(e_i)_{1 \le i \le r}$ be a basis of V, and let $(\mathfrak{a}_i)_{1 \le i \le r}$ be a family of fractional ideals. Set*

$$M := \bigoplus_{i=1}^{r} \mathfrak{a}_i e_i .$$

(a) *The duality between V and V^* induces an identification*

$$M^* = \bigoplus_{i=1}^{r} \mathfrak{a}_i^* e_i^* .$$

(b) *The fractional module M is a finitely generated projective R-module if and only if for all i $(1 \le i \le r)$, we have $\mathfrak{a}_i^* \mathfrak{a}_i = R$.*

In particular a fractional ideal $\mathfrak{a}$ is a finitely generated projective R-module if and only if $\mathfrak{a}^* \mathfrak{a} = R$.

Proof (1) Let $\lambda \in R \setminus \{0\}$ such that $\lambda\mathfrak{a} \subseteq R$. Let $\varphi \in \mathrm{Hom}_R(\mathfrak{a}, R)$.

Whenever $x, y \in \mathfrak{a}$, we have

$$\varphi(\lambda xy) = \lambda\varphi(xy) = \lambda x\varphi(y) = \lambda y\varphi(x),$$

and since R is an integral domain, we get

$$\varphi(xy) = x\varphi(y) = y\varphi(x).$$

Thus we may define $h_\varphi \in F$ by the equality

$$h_\varphi := \varphi(x)x^{-1} \quad \text{for all } x \in \mathfrak{a} \setminus \{0\}.$$

It is immediate to check that the map $\varphi \mapsto h_\varphi$ is an isomorphism from $\mathrm{Hom}_R(\mathfrak{a}, R)$ onto $\mathfrak{a}^*$. Moreover, $\mathfrak{a}^*$ is indeed a fractional ideal, since for each $a \in \mathfrak{a}$ we have $a\mathfrak{a}^* \subset R$.

(2)(a) By assumption, M is isomorphic to $\bigoplus_{i=1}^r \mathfrak{a}_i$. Thus its dual is isomorphic to $\bigoplus_{i=1}^r \mathfrak{a}_i^*$ by (1), and the statement follows.

(2)(b) The module M is finitely generated projective if and only if, for all i, $\mathfrak{a}_i e_i$ is finitely generated projective. So it is enough to prove that a fractional ideal $\mathfrak{a}$ is finitely generated projective if and only if $\mathfrak{a}\mathfrak{a}^* = R$.

We know by Theorem 2.132 that $\mathfrak{a}$ is finitely generated projective if and only if there exists $\sum_i b_i \otimes_R a_i \in \mathfrak{a}^* \otimes_R \mathfrak{a}$ such that, for all $x \in \mathfrak{a}$, we have $\sum_i xb_ia_i = x$, i.e., $\sum_i b_ia_i = 1$, i.e., if and only if $\mathfrak{a}^*\mathfrak{a} = R$. □

Exercise 2.158 If $\mathfrak{a}$ is a finitely generated projective fractional ideal, prove that $\mathrm{Hom}_R(\mathfrak{a}, \mathfrak{a}) = R$.

2.3.1.2 Dedekind Domains: Definition

Definition 2.159

- We recall that a *principal ideal domain* is an integral domain R all ideals of which are free (hence of rank one).
- A *Dedekind domain* is an integral domain R all ideals of which are finitely generated projective.

Example 2.160 There are Dedekind domains which are not principal ideal domains. We shall see that the ring $R := \mathbb{Z}[\sqrt{-5}]$, as the ring of integers of a finite extension of $\mathbb{Q}$, is a Dedekind domain, i.e., all of its ideals are finitely generated projective. In particular, its ideal $2R + (1 + \sqrt{-5})R$ is projective. Nevertheless the reader may check that this ideal is not free (i.e., not principal).

Remark 2.161 Of course, a principal ideal domain is a Dedekind domain. In a sense, the notion of Dedekind domain is to the notion of principal ideal domain what the notion of projective module is to the notion of free module.

The notion of Dedekind domain is a central notion in mathematics. In particular the integral closure of a Dedekind domain of characteristic zero in a finite extension of its field of fractions is still a Dedekind domain (while the integral closure of a principal ideal domain in a finite extension of its field of fractions needs not be a principal ideal domain).

Thus in particular, if K is a finite extension of $\mathbb{Q}$, the integral closure $\mathbb{Z}_K$ of $\mathbb{Z}$ in K is a Dedekind domain.

(!) **Attention** (!) The ring $\mathbb{Z}_K$ needs not be a principal ideal domain (e.g., consider the case $K = \mathbb{Q}[\sqrt{-5}]$). Moreover, if L is a finite extension of K, we shall see that the ring $\mathbb{Z}_L$ is a finitely generated projective $\mathbb{Z}_K$-module, but it needs not be free. For example (see [3], Exercise 22, Chap. 2, p. 130), if $K = \mathbb{Q}[\sqrt{10}]$ and $L = K[i]$, then $\mathbb{Z}_L$ is not free over $\mathbb{Z}_K$.

(!) **Attention** (!) Let R be a Dedekind domain.

- Then $R[X]$ needs not be a Dedekind domain: prove, for example, that $\mathbb{Z}[X]$ is not a Dedekind domain.

  Nevertheless, the ring $R((X))$ of Laurent formal series is indeed a Dedekind domain: see [5], Exercise 2, p. 634.
- A finite extension of R needs not be a Dedekind domain. For example, $\mathbb{Z}[\sqrt{-3}]$ is not a Dedekind domain. Indeed, it is not integrally closed (see Exercise 2.140) and we shall prove below (see Corollary 2.172) that a Dedekind domain is integrally closed.

The proof of the following proposition is easy and left to the reader.

Proposition 2.162 *Let R be an integral domain. Let S be a nonempty multiplicatively closed subset of $S \setminus \{0\}$.*

- *If R is a principal ideal domain, so is $S^{-1}R$.*
- *If R is a Dedekind domain, so is $S^{-1}R$.*

By Proposition 2.136, we see that if R is a *local* Dedekind domain, its ideals are all free (and of course of rank one), hence are principal ideals. This implies the following proposition.

Proposition 2.163 *A local Dedekind domain is a* (*local*) *principal ideal domain.*

Remark 2.164 A local principal ideal domain which is not a field is also called *discrete valuation ring* (see [9], Chap. 1 or [1], Chap. 9).

The above proposition, together with Proposition 2.162, allows to prove the next property.

Corollary 2.165 *Let R be a Dedekind domain. For each nonzero prime ideal $\mathfrak{p}$ of R, $R_\mathfrak{p}$ is a* (*local*) *principal ideal domain.*

We shall see below (Theorem 2.241) a local characterization of Dedekind domains.

We recall (see Proposition 2.157, (2)) that a fractional ideal $\mathfrak{a} \subset F$ is a finitely generated projective R-module if and only if $\mathfrak{a}\mathfrak{a}^* = R$.

A finitely generated projective fractional ideal is called *invertible*.

Lemma 2.166 *An integral domain R is a Dedekind domain if and only if all its fractional ideals are invertible.*

Proof If all fractional ideals are finitely generated projective, so are in particular the ideals of R, which is the very definition of a Dedekind domain.

Reciprocally, assume R is a Dedekind domain. Given a fractional ideal $\mathfrak{a}$, if $\lambda\mathfrak{a} \subset R$, the map $\mathfrak{a} \to \lambda\mathfrak{a}$, $a \mapsto \lambda a$, is an isomorphism between $\mathfrak{a}$ and an ideal of R and so $\mathfrak{a}$ is invertible. □

Notation 2.167 From now on, *the dual of a fractional ideal $\mathfrak{a}$ of a Dedekind domain will be denoted $\mathfrak{a}^{-1}$.*

With that notation in mind, the following statement is even clearer.

Proposition 2.168 *Let R be a Dedekind domain. The set of fractional ideals of R is an Abelian group under multiplication. The identity element is R, and the inverse of a fractional ideal $\mathfrak{a}$ is $\mathfrak{a}^{-1}$.*

That group is called the *ideal group* of R.

We shall see now how to do arithmetic in Dedekind domains when replacing elements by ideals.

Definition 2.169

- A fractional ideal $\mathfrak{a}$ is said to be *integral* if $\mathfrak{a} \subset R$.
- Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional ideals in R. We say that $\mathfrak{b}$ divides $\mathfrak{a}$ if there exists an integral ideal $\mathfrak{q}$ such that $\mathfrak{a} = \mathfrak{b}\mathfrak{q}$.

Lemma 2.170 *Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional ideals in R. The following assertions are equivalent.*

(i) $\mathfrak{a} \subset \mathfrak{b}$.
(ii) $\mathfrak{b}$ *divides* $\mathfrak{a}$.

Proof (ii)⇒(i) is clear. Let us prove that (i)⇒(ii). We have $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ where $\mathfrak{c} := \mathfrak{b}^{-1}\mathfrak{a}$. As $\mathfrak{a} \subset \mathfrak{b}$, we have $\mathfrak{b}^{-1}\mathfrak{a} \subset \mathfrak{b}^{-1}\mathfrak{b} = R$, hence $\mathfrak{c}$ is integral. □

The following consequence of Lemma 2.170 is an obvious generalization of a well known property of principal ideal domains.

Corollary 2.171 *Every nonzero prime ideal of a Dedekind domain is maximal.*

Proof Assume that $\mathfrak{p}$ is a nonzero prime ideal and that $\mathfrak{p} \subset \mathfrak{a}$ for an ideal $\mathfrak{a}$. We shall prove that either $\mathfrak{p} = \mathfrak{a}$ or $\mathfrak{a} = R$. By the preceding lemma, there exists an ideal $\mathfrak{a}'$ such that $\mathfrak{p} = \mathfrak{a}\mathfrak{a}'$, and since $\mathfrak{p}$ is prime (see Exercise 1.138), either $\mathfrak{a} \subset \mathfrak{p}$ hence $\mathfrak{p} = \mathfrak{a}$, or $\mathfrak{a}' \subset \mathfrak{p}$. In the latter case, we have $\mathfrak{p} = \mathfrak{a}\mathfrak{p}$, which implies $\mathfrak{a} = R$ (since the set of fractional ideals is a group). □

Corollary 2.172 *A Dedekind domain is integrally closed.*

Proof Let R be a Dedekind domain, and let F be its field of fractions. Let $x \in F$ be integral over R, satisfying $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ with $a_j \in R$ for $j = 0, \ldots, n-1$.

Then x belongs to the fractional ideal $\mathfrak{a}$ generated by $\{1, x, \ldots, x^{n-1}\}$. It is immediate to check that $\mathfrak{a}^2 = \mathfrak{a}$, and since the set of fractional ideals is a group, this implies $\mathfrak{a} = R$ (just multiply by $\mathfrak{a}^{-1}$!), which shows that $x \in R$. □

That property will be revisited and included in the various characterizations of Dedekind domains given in the final section below.

2.3.1.3 Arithmetic with Ideals in Dedekind Domains

Theorem 2.173 *Let R be a Dedekind domain. Then every nonzero proper ideal of R can be written in a unique way as a product of prime ideals.*

Proof Let us prove that any proper ideal is a product of prime ideals. Assume not, so (by Noetherianity of R), there exists an ideal $\mathfrak{a}$ which is maximal among proper ideals which are not products of prime ideals. In particular $\mathfrak{a}$ is not prime, hence not maximal, hence there exists an ideal $\mathfrak{b}$ such that $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq R$. Thus $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ for some ideal $\mathfrak{c}$ by Lemma 2.170. It follows that $\mathfrak{a} \subset \mathfrak{c}$, and if $\mathfrak{a} = \mathfrak{c}$ then $\mathfrak{b} = R$ which is impossible, hence we have also $\mathfrak{a} \subsetneq \mathfrak{c} \subsetneq R$. By maximality of $\mathfrak{a}$, both $\mathfrak{b}$ and $\mathfrak{c}$ are products of prime ideals, hence so is $\mathfrak{a}$, which is a contradiction.

Let us prove the uniqueness. Assume that $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_m = \mathfrak{q}_1 \cdots \mathfrak{q}_n$ where $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are all prime ideals. We argue by induction on m.

We have $\mathfrak{q}_1 \cdots \mathfrak{q}_n \subset \mathfrak{p}_1$, hence since $\mathfrak{p}_1$ is prime there exists j such that $\mathfrak{q}_j \subset \mathfrak{p}_1$ (see Exercise 1.138). We assume $j = 1$. Then by Corollary 2.171, $\mathfrak{p}_1 = \mathfrak{q}_1$. It follows that $\mathfrak{p}_2 \cdots \mathfrak{p}_m = \mathfrak{q}_2 \cdots \mathfrak{q}_n$, and we can apply the inductive hypothesis to conclude. □

Now let $\mathfrak{a}$ be a fractional ideal. There exist integral ideals $\mathfrak{b}$ and $\mathfrak{c}$ such that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$.

Indeed, there exists $\lambda \in (R \cap \mathfrak{a}^*) \setminus \{0\}$, so that $\lambda\mathfrak{a} \subset R$ and $R\lambda \subset R$. We set $\mathfrak{b} := \lambda\mathfrak{a}$ and $\mathfrak{c} := R\lambda$.

It follows then from Theorem 2.173 that any fractional ideal $\mathfrak{a}$ can be written

$$\mathfrak{a} = \prod_{\mathfrak{p} \in \operatorname{Spec}^*(R)} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})} \quad \big(v_\mathfrak{p}(\mathfrak{a}) \in \mathbb{Z}\big).$$

We call $v_\mathfrak{p}(\mathfrak{a})$ the *valuation of* $\mathfrak{a}$ *at* $\mathfrak{p}$.

Notice that almost all integers $v_\mathfrak{p}(\mathfrak{a})$ (i.e., all but a finite number of them) are zero.

With that notation, we can in particular define the gcd and the lcm of a finite family of (fractional) ideals.

Lemma 2.174 *For all fractional ideals* $\mathfrak{a}$, $\mathfrak{b}$,

(1) $\mathfrak{a} + \mathfrak{b} = \gcd(\mathfrak{a}, \mathfrak{b}) = \prod_{\mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p}^{\min(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b}))}$
(2) $\mathfrak{a}\mathfrak{b} = \prod_{\mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a}) + v_\mathfrak{p}(\mathfrak{b})}$
(3) $\mathfrak{a} \cap \mathfrak{b} = \operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \prod_{\mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p}^{\max(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b}))}$.

Definitions 2.175 We say that two fractional ideals $\mathfrak{a}$, $\mathfrak{b}$ are *coprime* or *relatively prime* if $\gcd(\mathfrak{a}, \mathfrak{b}) = R$.

Note that if $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, they are both integral.

More generally, given a family $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ of fractional ideals, we say that $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ are relatively prime if $\mathfrak{a}_1 + \cdots + \mathfrak{a}_r = R$.

The proof of the next lemma is an easy exercise left to the reader.

Lemma 2.176 *Let* $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ *be a family of integral ideals. The following assertions are equivalent*:

(i) $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ *are relatively prime*,
(ii) *for each* $\mathfrak{p} \in \operatorname{Spec}(R)$, $\min\{v_\mathfrak{p}(\mathfrak{a}_i)_{1 \le i \le r}\} = 0$
(iii) *no prime ideal of R divides* (*i.e.*, *contains*) *all the* $\mathfrak{a}_i$*'s*.

The following set of familiar properties is easy to check.

Lemma 2.177 *Let* $\mathfrak{d} := \gcd(\mathfrak{a}, \mathfrak{b})$ *and* $\mathfrak{m} := \operatorname{lcm}(\mathfrak{a}, \mathfrak{b})$. *We define* $\mathfrak{a}', \mathfrak{b}', \mathfrak{a}'', \mathfrak{b}''$ *by the equalities*

$$\mathfrak{a} = \mathfrak{d}\mathfrak{a}', \qquad \mathfrak{b} = \mathfrak{d}\mathfrak{b}' \quad \textit{and} \quad \mathfrak{m} = \mathfrak{a}\mathfrak{a}'', \qquad \mathfrak{m} = \mathfrak{b}\mathfrak{b}''.$$

(1) $\mathfrak{a}\mathfrak{b} = \mathfrak{m}\mathfrak{d}$.
(2) $\mathfrak{a}'$ *and* $\mathfrak{b}'$ *are coprime*, *and similarly* $\mathfrak{a}''$ *and* $\mathfrak{b}''$ *are coprime*.
(3) $\mathfrak{a}'\mathfrak{a}'' = \mathfrak{b}'\mathfrak{b}''$, *and* $\mathfrak{m} = \mathfrak{a}\mathfrak{b}' = \mathfrak{b}\mathfrak{a}'$.

Moreover, we set the following notation.

Notation 2.178

$$\mathfrak{a}^{(\mathfrak{p})} := \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})} \quad \text{and} \quad \mathfrak{a}^{(\mathfrak{p}')} := \mathfrak{p}^{-v_\mathfrak{p}(\mathfrak{a})}\mathfrak{a} = \prod_{\mathfrak{q}\neq\mathfrak{p}} \mathfrak{q}^{v_\mathfrak{q}(\mathfrak{a})}.$$

2.3.2 Finitely Generated Projective Modules over Dedekind Domains

Proposition 2.179 *Let R be a principal ideal domain (resp. a Dedekind domain).*

(1) *Any finitely generated torsion-free R-module is free (resp. projective).*
(2) *Any finitely generated projective R-module is isomorphic to a direct sum of fractional ideals.*

Proof Let M be a finitely generated torsion-free R-module. We know by Proposition 2.125 that M is isomorphic to a submodule of a free R-module of finite rank R^n. From now on we assume $M \subset R^n$.

If $n = 1$, the conclusion of the proposition is an immediate application of the definitions (both of principal ideal and of Dedekind domains). Hence assume $n > 1$ and let us argue by induction on n. We identify R^{n-1} with the submodule of R^n of elements $(x_1, \dots, x_{n-1}, 0)$, so we have an obvious short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & R^{n-1} \arrow[r, "\iota"] & R^n \arrow[r, "\pi"] & R \arrow[r] & 0 \end{tikzcd},$$

which induces the following exact sequence

$$\begin{tikzcd} 0 \arrow[r] & M \cap R^{n-1} \arrow[r, "\iota"] & M \arrow[r, "\pi"] & \pi(M) \arrow[r] & 0 \end{tikzcd}.$$

By assumption, the ideal $\pi(M)$ of R is free (resp. projective), hence in any case projective, which shows that the above short exact sequence is split.

This implies that $M \cap R^{n-1}$ is an image of M, hence is finitely generated, so by the inductive hypothesis $M \cap R^{n-1}$ is free (resp. projective) and isomorphic to a direct sum of fractional ideals. Moreover, M is isomorphic to the direct sum $(M \cap R^{n-1}) \oplus \pi(M)$, hence is free (resp. projective) and isomorphic to a direct sum of fractional ideals. □

(!) **Attention** (!) The $\mathbb{Z}$-module $\mathbb{Q}$ is torsion-free, but it is not free. Indeed, every system comprising of two elements in $\mathbb{Q}$ is not free (why?), hence if $\mathbb{Q}$ were free it would have rank one.

Assertion (1) of the above Proposition 2.179 has the following consequence.

Corollary 2.180 *Let R be a Dedekind domain, and let M be a finitely generated R-module.*

(1) *The module $M/\operatorname{tor}(M)$ is finitely generated projective.*
(2) *The canonical exact sequence*

$$0 \longrightarrow \operatorname{tor}(M) \longrightarrow M \longrightarrow M/\operatorname{tor}(M) \longrightarrow 0$$

is split, hence

$$M \cong \operatorname{tor}(M) \oplus M/\operatorname{tor}(M),$$

thus any finitely generated R-module is the direct sum of a finitely generated torsion R-module and a finitely generated projective R-module.

Proof (1) By Proposition 2.25, (2), it is a direct application of Proposition 2.179, (1).

(2) By Lemma 2.33 and Proposition 2.39, (2) is also a consequence of the projectivity of $M/\operatorname{tor}(M)$. □

(!) **Attention** (!) The decomposition of a finitely generated module

$$M = \operatorname{tor}(M) \oplus P \tag{2.5}$$

(where P is projective) is not unique. Indeed, let us set $R = \mathbb{Z}$ and

$$M := \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}. \tag{2.6}$$

Then (2.6) is a decomposition like (2.5), since

$$\operatorname{tor}(M) = \mathbb{Z}/2\mathbb{Z}$$

(identified to the submodule $\{(0,a) \mid a \in \mathbb{Z}/2\mathbb{Z}\}$), and the submodule $\mathbb{Z}$ (identified to the submodule $\{(n,0) \mid n \in \mathbb{Z}\}$) is free. Let us set

$$P := \left\{(n,\overline{n}) \,\middle|\, n \in \mathbb{Z}\right\},$$

where $\overline{n}$ denotes the image of n modulo 2. Then we get another decomposition of M like (2.5), namely:

$$M = \operatorname{tor}(M) \oplus P.$$

Assertion (2) of the above Proposition 2.179 may be reformulated as follows.

Corollary 2.181 *Let R be a Dedekind domain, and let M be a finitely generated projective R-module of rank r.*

There exists a free system $(e_i)_{1\le i\le r}$ in M, and a family $(\mathfrak{a}_i)_{1\le i\le r}$ of fractional ideals, such that

$$M = \bigoplus_{i=1}^{r} \mathfrak{a}_i e_i.$$

The above corollary may be reformulated as follows:

Let M be a finitely generated projective R-module. Then there exists a system $(E_i)_{1\leq i\leq r}$ of rank one projective submodules of M (thus $E_i = \mathfrak{a}_i e_i$ for some $e_i \in M$ and some ideal $\mathfrak{a}_i$ of R) such that

$$M = E_1 \oplus E_2 \oplus \cdots \oplus E_r .$$

Such a system $(E_i)_{1\leq i\leq r}$ of rank one submodules will be called here a *pseudo-basis* of M.

The preceding Corollary 2.181 may also be rephrased as follows:

Whenever M is a finitely generated projective R-module, there exists a family $(\mathfrak{a}_i)_{1\leq i\leq r}$ of fractional ideals such that

$$M \cong \mathfrak{a}_1 \oplus \mathfrak{a}_2 \oplus \cdots \oplus \mathfrak{a}_r .$$

Assume that N is yet another finitely generated projective R-module, such that

$$N \cong \mathfrak{b}_1 \oplus \mathfrak{b}_2 \oplus \cdots \oplus \mathfrak{b}_s$$

for some family $(\mathfrak{b}_i)_{1\leq i\leq s}$ of fractional ideals.

Let us set $V := FM$ and $W := FN$. Then there exists an isomorphism of M onto N if and only if there exists an isomorphism of V onto W which sends M to N. Choosing appropriate bases for V and W, we get the following criterion.

Lemma 2.182 *There exists an isomorphism of M onto N if and only if $r = s$ and there exists an invertible matrix $\Lambda \in \mathrm{GL}_r(F)$ such that*

$$\Lambda \begin{pmatrix} \mathfrak{a}_1 \\ \vdots \\ \mathfrak{a}_r \end{pmatrix} \subset \begin{pmatrix} \mathfrak{b}_1 \\ \vdots \\ \mathfrak{b}_r \end{pmatrix} \quad \textit{and} \quad \Lambda^{-1} \begin{pmatrix} \mathfrak{b}_1 \\ \vdots \\ \mathfrak{b}_r \end{pmatrix} \subset \begin{pmatrix} \mathfrak{a}_1 \\ \vdots \\ \mathfrak{a}_r \end{pmatrix} .$$

It follows from the above lemma that two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ are isomorphic as R-modules if and only if there exists $\lambda \in F^\times$ such that $\mathfrak{b} = \lambda\mathfrak{a}$.

In that case we write $\mathfrak{a} \cong \mathfrak{b}$.

Definition 2.183 The quotient of the group of all fractional ideals by the subgroup comprised of *principal* fractional ideals is called the *class group* of R.

Thus $\mathfrak{a} \cong \mathfrak{b}$ if and only if $\mathfrak{a}$ and $\mathfrak{b}$ have the same image in the class group.

Theorem 2.184 *Let $(\mathfrak{a}_i)_{1\leq i\leq r}$ be a family of fractional ideals of the Dedekind domain R.*

(1) *We have the following isomorphism of R-modules*

$$\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_{r-1} \oplus \mathfrak{a}_r \cong \underbrace{R \oplus \cdots \oplus R}_{r-1 \textit{ summands}} \oplus \mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_r .$$

(2) *Let* $(\mathfrak{b}_j)_{1\leq j\leq t}$ *be a family of fractional ideals. The following assertions are equivalent.*

(i) $\mathfrak{a}_1 \oplus \mathfrak{a}_2 \oplus \cdots \oplus \mathfrak{a}_r \cong \mathfrak{b}_1 \oplus \mathfrak{b}_2 \oplus \cdots \oplus \mathfrak{b}_t$.
(ii) $r = t$ *and* $\mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_r \cong \mathfrak{b}_1\mathfrak{b}_2 \cdots \mathfrak{b}_t$.

As a consequence of the above theorem, we may give the following definition.

Definition 2.185 Let R be a Dedekind domain and let M be a finitely generated torsion free R-module. Whenever $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ are fractional ideals such that $M \cong \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_{r-1} \oplus \mathfrak{a}_r$, the isomorphism type (i.e., its image in the class group) of the ideal

$$\mathrm{St}(M) := \mathfrak{a}_1 \cdots \mathfrak{a}_{r-1}\mathfrak{a}_r$$

depends only on the isomorphism class of M. It is called the *Steinitz class* of M.

The following corollary is an immediate consequence of Theorem 2.184 and of the preceding Definition 2.185.

Corollary 2.186 *Let R be a Dedekind domain.*

(1) *Two finitely generated torsion free R-modules are isomorphic if and only if their Steinitz classes are equal.*
(2) *In particular a finitely generated torsion free R-module M is free if and only if* $\mathrm{St}(M) = R$.

Proof of Theorem 2.184 (1) It suffices to prove that

$$\mathfrak{a}_1 \oplus \mathfrak{a}_2 \cong R \oplus \mathfrak{a}_1\mathfrak{a}_2 \tag{2.7}$$

(and then to use an easy induction).

To prove (2.7), let us first assume that $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are coprime, that is $\mathfrak{a}_1 \oplus \mathfrak{a}_2 = R$. It is a consequence of the following lemma.

Lemma 2.187 *Let $\mathfrak{a}_1$ and $\mathfrak{a}_2$ be integral ideals of a Dedekind domain. Then*

$$\mathfrak{a}_1 \oplus \mathfrak{a}_2 \cong \mathrm{lcm}(\mathfrak{a}_1, \mathfrak{a}_2) \oplus \mathrm{gcd}(\mathfrak{a}_1, \mathfrak{a}_2).$$

Proof of Lemma 2.187 Let us first notice that, given any ring R and any R-module M, if M_1 and M_2 are submodules of M, we have an obvious short exact sequence

$$0 \to M_1 \cap M_2 \to M_1 \oplus M_2 \to M_1 + M_2 \to 0,$$

where $M_1 \cap M_2$ and $M_1 + M_2$ are submodules of M, and $M_1 \oplus M_2$ denotes the coproduct $M_1 \sqcup M_2$ (see Definition 2.35).

In particular, if R is a Dedekind domain and $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are ideals of R, we have a short exact sequence

$$0 \to \mathrm{lcm}(\mathfrak{a}_1, \mathfrak{a}_2) \to \mathfrak{a}_1 \oplus \mathfrak{a}_2 \to \gcd(\mathfrak{a}_1, \mathfrak{a}_2) \to 0.$$

Since R is a Dedekind domain, the ideal $\gcd(\mathfrak{a}_1, \mathfrak{a}_2)$ is projective, hence the above short exact sequence is split, which implies Lemma 2.187. □

In order to prove the first assertion of Theorem 2.184, it remains to show that we can assume $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are coprime. This follows from the next lemma.

Lemma 2.188 *Let $\mathfrak{a}_1$ and $\mathfrak{a}_2$ be fractional ideals. Then there exist nonzero $x_1 \in \mathfrak{a}_1^{-1}$ and $x_2 \in \mathfrak{a}_2^{-1}$ such that $\mathfrak{a}_1 x_1$ and $\mathfrak{a}_2 x_2$ are coprime.*

Proof of Lemma 2.188 We shall actually prove a more precise result which will also be useful later (see proof of Proposition 2.196), namely

Lemma 2.189 *Let $\mathfrak{a}_1$ and $\mathfrak{a}_2$ be fractional ideals. Given any nonzero $x_2 \in \mathfrak{a}_2^{-1}$, there exists a nonzero $x_1 \in \mathfrak{a}_1^{-1}$ such that $\mathfrak{a}_1 x_1$ and $\mathfrak{a}_2 x_2$ are coprime.*

Proof of Lemma 2.189 Let us pick $x_2 \in \mathfrak{a}_2^{-1}$, hence $\mathfrak{a}_2 x_2$ is integral, and let $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ be all the distinct prime ideals which divide $\mathfrak{a}_2 x_2$. For each i $(1 \le i \le s)$, we have

$$\mathfrak{a}_1^{-1}\mathfrak{p}_1 \cdots \mathfrak{p}_i \cdots \mathfrak{p}_s \subsetneq \mathfrak{a}_1^{-1}\mathfrak{p}_1 \cdots \widehat{\mathfrak{p}_i} \cdots \mathfrak{p}_s,$$

so we can choose $y_i \in \mathfrak{a}_1^{-1}\mathfrak{p}_1 \cdots \widehat{\mathfrak{p}_i} \cdots \mathfrak{p}_s \setminus \mathfrak{a}_1^{-1}\mathfrak{p}_1 \cdots \mathfrak{p}_i \cdots \mathfrak{p}_s$. We set $x_1 := y_1 + \cdots + y_s$. Then

$$x_1 \in \mathfrak{a}_1^{-1}\left(\sum_{i=1}^{s} \mathfrak{p}_1 \cdots \widehat{\mathfrak{p}_i} \cdots \mathfrak{p}_s\right), \quad \text{hence} \quad x_1 \in \mathfrak{a}_1^{-1}.$$

Let us prove now that, for each i $(1 \le i \le s)$, $\mathfrak{p}_i$ does not divide $\mathfrak{a}_1 x_1$ (i.e., $\mathfrak{a}_1 x_1$ is not contained in $\mathfrak{p}_i$). Indeed,

$$\mathfrak{a}_1 x_1 = \mathfrak{a}_1(y_1 + \cdots + y_s) = \{a y_1 + \cdots + a y_s \mid a \in \mathfrak{a}_1\}.$$

For all $a \in \mathfrak{a}_1$, and for all $j \neq i$, we have $a y_j \in \mathfrak{p}_i$. Since $\mathfrak{a}_1 y_i$ is not contained in $\mathfrak{p}_i$, we see that $\mathfrak{a}_1 x_1$ is not contained in $\mathfrak{p}_i$.

This shows that $\mathfrak{a}_1 x_1$ is prime to $\mathfrak{a}_2 x_2$. □

□

We can now end the proof of the first assertion of Theorem 2.184. Using notations of the previous lemma,

$$\mathfrak{a}_1 \oplus \mathfrak{a}_2 \cong \mathfrak{a}_1 x_1 \oplus \mathfrak{a}_2 x_2 \cong R \oplus x_1 x_2 \mathfrak{a}_1 \mathfrak{a}_2 \cong R \oplus \mathfrak{a}_1 \mathfrak{a}_2.$$

(2) By (1) just proved, (ii)⇒(i). Let us prove that (i)⇒(ii)

First of all, the rank of $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$ is r, which proves that $r = t$.

Now assume (see Lemma 2.182) that there exists a matrix $\Lambda \in \mathrm{GL}_r(F)$such that

$$\Lambda \begin{pmatrix} \mathfrak{a}_1 \\ \vdots \\ \mathfrak{a}_r \end{pmatrix} \subset \begin{pmatrix} \mathfrak{b}_1 \\ \vdots \\ \mathfrak{b}_r \end{pmatrix} \quad \text{and} \quad \Lambda^{-1} \begin{pmatrix} \mathfrak{b}_1 \\ \vdots \\ \mathfrak{b}_r \end{pmatrix} \subset \begin{pmatrix} \mathfrak{a}_1 \\ \vdots \\ \mathfrak{a}_r \end{pmatrix}.$$

Assume $\Lambda = (\lambda_{i,j})$ and $\Lambda^{-1} = (\mu_{j,i})$. The above inclusions may be written

$$\text{for all } i \text{ and } j, \quad \sum_{i=1}^{r} \lambda_{i,j}\mathfrak{a}_i \subset \mathfrak{b}_j \quad \text{and} \quad \sum_{j=1}^{r} \mu_{j,i}\mathfrak{b}_j \subset \mathfrak{a}_i,$$

which is equivalent to

$$\text{for all } i \text{ and } j, \quad \lambda_{i,j}\mathfrak{a}_i \subset \mathfrak{b}_j \quad \text{and} \quad \mu_{j,i}\mathfrak{b}_j \subset \mathfrak{a}_i.$$

It follows that for any permutation $\sigma \in \mathfrak{S}_r$, we have

$$\lambda_{1,\sigma(1)} \cdots \lambda_{r,\sigma(r)}\mathfrak{a}_1 \cdots \mathfrak{a}_r \subset \mathfrak{b}_1 \cdots \mathfrak{b}_r,$$

which implies

$$\det \Lambda . \mathfrak{a}_1 \cdots \mathfrak{a}_r \subset \mathfrak{b}_1 \cdots \mathfrak{b}_r.$$

Similarly we get

$$\det \Lambda^{-1} . \mathfrak{b}_1 \cdots \mathfrak{b}_r \subset \mathfrak{a}_1 \cdots \mathfrak{a}_r,$$

which proves (ii). □

For the rest of this chapter, R denotes a Dedekind domain.

2.3.3 *Remarkable Decompositions of Finitely Generated Torsion Modules*

2.3.3.1 The $\mathfrak{p}$-Primary Decomposition and Applications

The next set of results may be seen as variations on the theme of the Chinese lemma 1.38.

Definition 2.190 For any finitely generated torsion R-module M, and for any prime ideal $\mathfrak{p}$ of R, the $\mathfrak{p}$-*primary component* of M is

$$M(\mathfrak{p}) := \{x \in M \mid (\exists m \in \mathbb{N})(\mathrm{Ann}_R(x) = \mathfrak{p}^m)\}.$$

For $\mathfrak{p}$ a prime ideal, a finitely generated torsion R-module M is said to be $\mathfrak{p}$-*primary* if $M = M(\mathfrak{p})$.

Theorem 2.191 ($\mathfrak{p}$-primary decomposition) *For any finitely generated torsion R-module M,*

$$M = \bigoplus_{\mathfrak{p}\in\mathrm{Spec}(R)} M(\mathfrak{p}).$$

Proof of Theorem 2.191 Let M be a finitely generated torsion R-module. Let $\mathfrak{p} \in \mathrm{Spec}(R)$.

Since $\mathrm{Ann}_R(M)^{(\mathfrak{p})}$ and $\mathrm{Ann}_R(M)^{(\mathfrak{p}')}$ (see Notation 2.178) are relatively prime, i.e.,

$$\mathrm{Ann}_R(M)^{(\mathfrak{p})} + \mathrm{Ann}_R(M)^{(\mathfrak{p}')} = R, \tag{2.8}$$

there exist $a^{(\mathfrak{p})} \in \mathrm{Ann}_R(M)^{(\mathfrak{p})}$ and $a^{(\mathfrak{p}')} \in \mathrm{Ann}_R(M)^{(\mathfrak{p}')}$ such that $1 = a^{(\mathfrak{p})} + a^{(\mathfrak{p}')}$, hence for each $x \in M$ we have $x = a^{(\mathfrak{p})}x + a^{(\mathfrak{p}')}x$, which proves that

$$M = \mathrm{Ann}_R(M)^{(\mathfrak{p})}M + \mathrm{Ann}_R(M)^{(\mathfrak{p}')}M.$$

Moreover, it is clear that

- $\mathrm{Ann}_R(M)^{(\mathfrak{p}')}$ is contained in the annihilator of $\mathrm{Ann}_R(M)^{(\mathfrak{p})}M$,
- $\mathrm{Ann}_R(M)^{(\mathfrak{p})}$ is contained in the annihilator of $\mathrm{Ann}_R(M)^{(\mathfrak{p}')}M$,

from which, again using (2.8) we deduce that

$$\mathrm{Ann}_R(M)^{(\mathfrak{p})}M \cap \mathrm{Ann}_R(M)^{(\mathfrak{p}')}M = 0,$$

hence that

$$M = \mathrm{Ann}_R(M)^{(\mathfrak{p})}M \oplus \mathrm{Ann}_R(M)^{(\mathfrak{p}')}M. \tag{2.9}$$

Let us now prove that $\mathrm{Ann}_R(M)^{(\mathfrak{p}')}M = M(\mathfrak{p})$.

From the definition of $M(\mathfrak{p})$ it follows that

$$\mathrm{Ann}_R(M)^{(\mathfrak{p}')}M \subset M(\mathfrak{p}).$$

Now if $x \in M(\mathfrak{p})$ and if $\mathrm{Ann}_R(x) = \mathfrak{p}^k$, then we also have

$$\mathfrak{p}^k + \mathrm{Ann}_R(M)^{(\mathfrak{p}')} = R,$$

which implies that $x \in \mathrm{Ann}_R(M)^{(\mathfrak{p}')}M$.

Thus we have proved that

$$M = M(\mathfrak{p}) \oplus \mathrm{Ann}_R(M)^{(\mathfrak{p})}M.$$

We shall now end the proof by induction on the number of prime divisors of $\mathrm{Ann}_R(M)$.

On one hand, if $\mathfrak{p}$ does divide $\mathrm{Ann}_R(M)$, the number of prime divisors of the annihilator of $\mathrm{Ann}_R(M)^{(\mathfrak{p})}M$ is strictly smaller than the number of prime divisors of $\mathrm{Ann}_R(M)$.

On the other hand, for $\mathfrak{q} \neq \mathfrak{p}$, we have $\mathrm{Ann}_R(M)^{(\mathfrak{p})}M(\mathfrak{q}) = M(\mathfrak{q})$. Indeed, it suffices to prove that $M(\mathfrak{q}) \subset \mathrm{Ann}_R(M)^{(\mathfrak{p})}M$. If $x \in M(\mathfrak{q})$, let $\mathfrak{q}^n$ be its annihilator. Then $\mathfrak{q}^n + \mathrm{Ann}_R(M)^{(\mathfrak{p})} = R$ and we see that $x \in \mathrm{Ann}_R(M)^{(\mathfrak{p})}M$. □

Notice that the preceding proof establishes as well the following property.

Lemma 2.192 *Let M be a finitely generated torsion R-module. Let $\mathfrak{p} \in \mathrm{Spec}(R)$.*

(1) $M(\mathfrak{p}) = \mathrm{Ann}_R(M)^{(\mathfrak{p}')}M$.
(2) $\mathrm{Ann}_R(M)^{(\mathfrak{p})}M = \bigoplus_{\mathfrak{q}\neq\mathfrak{p}} M(\mathfrak{q})$.
(3) $\mathrm{Ann}_R(M(\mathfrak{p})) = \mathrm{Ann}_R(M)^{(\mathfrak{p})}$.

We shall now apply what precedes to derive some results about cyclic modules.

2.3.3.2 On Quotients of Fractional Ideals

Proposition 2.193 *Let R be a Dedekind domain. Let $\mathfrak{p}$ be a nonzero prime ideal of R and let $m \geq 1$ be a natural integer. Then the inclusion $R \hookrightarrow R_{\mathfrak{p}}$ induces an isomorphism*

$$R/\mathfrak{p}^m \xrightarrow{\sim} R_{\mathfrak{p}}/\mathfrak{p}^m R_{\mathfrak{p}}.$$

Proof The kernel of the natural morphism $R \to R_{\mathfrak{p}}/\mathfrak{p}^m R_{\mathfrak{p}}$ is the set of elements $a \in R$ which may be written $a = x/\mu$ where $x \in \mathfrak{p}^m$ and $\mu \notin \mathfrak{p}$. Then $a\mu = x$, so $a\mu \in \mathfrak{p}^m$, i.e., $\mathfrak{p}^m$ divides $Ra \cdot R\mu$. Since $R\mu$ and $\mathfrak{p}$ are relatively prime, it follows that $a \in \mathfrak{p}^m$. Thus the morphism described in Lemma 2.193 is injective.

Let us prove the surjectivity. Let $\lambda/\mu \in R_{\mathfrak{p}}$, where $\mu \notin \mathfrak{p}$. Then $R\mu$ and $\mathfrak{p}^m$ are relatively prime, so there exists $\mu' \in R$ and $x \in \mathfrak{p}^m$ such that $1 = \mu'\mu + x$, hence $\lambda/\mu = \lambda\mu' + x\lambda/\mu$. This implies that $\lambda\mu^{-1} \equiv \lambda\mu' \mod R_{\mathfrak{p}}\mathfrak{p}^m$, hence that the natural composed morphism $R \hookrightarrow R_{\mathfrak{p}} \twoheadrightarrow R_{\mathfrak{p}}/R_{\mathfrak{p}}\mathfrak{p}^m$ is onto. □

Remark 2.194 For R an integral domain and $\mathfrak{p}$ a prime ideal, we recall that $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ is the field of fractions of $R/\mathfrak{p}$. Hence in case $m = 1$, the above proposition just expresses the fact that $\mathfrak{p}$ is maximal.

Corollary 2.195 *Let R be a Dedekind domain and let $\mathfrak{p}$ be a nonzero prime ideal. Let M be a finitely generated $\mathfrak{p}$-primary R-module.*

(1) *The structure of R-module of M induces a natural structure of $R_{\mathfrak{p}}$-module.*
(2) *In particular the $R_{\mathfrak{p}}$-submodules of M are nothing but the R-submodules of M.*

Proof Let M be a finitely generated R-module whose annihilator is $\mathfrak{p}^m$ for some natural integer m. Thus M has a natural structure of $R/\mathfrak{p}^m$-module, and since, by Lemma 2.193, the inclusion $R \hookrightarrow R_\mathfrak{p}$ induces an isomorphism $R/\mathfrak{p} \xrightarrow{\sim} R_\mathfrak{p}/R_\mathfrak{p}\mathfrak{p}^m$, we see that M inherits a natural structure of $R_\mathfrak{p}/R_\mathfrak{p}\mathfrak{p}^m$-module which extends naturally to a structure of $R_\mathfrak{p}$-module. □

The next result generalizes Proposition 2.193.

Proposition 2.196 *Let R be a Dedekind domain, with field of fractions F. Let $\mathfrak{a}$ be a fractional ideal, and let $\mathfrak{b}$ be a nonzero integral ideal. Then there is an isomorphism (of R-modules)*

$$\mathfrak{a}/\mathfrak{a}\mathfrak{b} \cong R/\mathfrak{b}.$$

Notice that the above proposition is trivial if $\mathfrak{a}$ is principal, so in particular if R is a principal ideal domain. Indeed, in that case $\mathfrak{a}$ is isomorphic (as an R-module) to R.

Proof We apply Lemma 2.189, with $\mathfrak{a}_1 := \mathfrak{a}$, $\mathfrak{a}_2 := \mathfrak{b}$, and $x_2 := 1$. So there exists $x \in \mathfrak{a}^{-1}$, $x \neq 0$, such that the ideals $x\mathfrak{a}$ and $\mathfrak{b}$ are coprime. Thus $x\mathfrak{a} + \mathfrak{b} = R$ and $x\mathfrak{a} \cap \mathfrak{b} = x\mathfrak{a}\mathfrak{b}$, which implies

$$R/\mathfrak{b} = (x\mathfrak{a} + \mathfrak{b})/\mathfrak{b} \cong x\mathfrak{a}/(x\mathfrak{a} \cap \mathfrak{b}) = x\mathfrak{a}/x\mathfrak{a}\mathfrak{b} \cong \mathfrak{a}/\mathfrak{a}\mathfrak{b}.$$ □

Corollary 2.197 *Let $\mathfrak{a}$ be an integral ideal, and assume that $\mathfrak{a} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_s^{m_s}$ is its decomposition into a product of prime ideals. Set $\mathfrak{a}_i := \mathfrak{p}_i^{-m_i}\mathfrak{a} = \mathfrak{p}_1^{m_1} \cdots \widehat{\mathfrak{p}_i^{m_i}} \cdots \mathfrak{p}_s^{m_s}$. Then*

(1) *for every i $(1 \leq i \leq s)$, the $\mathfrak{p}_i$-primary component of $R/\mathfrak{a}$ is $\mathfrak{a}_i/\mathfrak{a}$,*
(2) $\mathfrak{a}_i/\mathfrak{a} \cong R/\mathfrak{p}_i^{m_i}$,
(3) $R/\mathfrak{a} \cong \bigoplus_{i=1}^{s} R/\mathfrak{p}_i^{m_i}$.

Proof (1) follows from Lemma 2.192, (2).

(2) follows from Proposition 2.196.

(3) follows from Theorem 2.191. □

2.3.3.3 The Main Theorems About Torsion Modules

Let us recall (see Definition 2.8) that a nonzero R-module is said to be indecomposable if any decomposition $M = M_1 \oplus M_2$ implies $M_1 = 0$ or $M_2 = 0$.

Let us also recall that R denotes a Dedekind domain.

Theorem 2.198 (Jordan decomposition)

(1) *A finitely generated torsion R-module M is indecomposable if and only if it is cyclic and its annihilator is $\mathfrak{p}^m$ for some prime ideal $\mathfrak{p}$ and some natural integer $m \geq 1$ (thus $M \cong R/\mathfrak{p}^m$).*

(2) *Every finitely generated torsion R-module M is a direct sum of indecomposable modules: we have*

$$M = \bigoplus_{i=1}^{s} Rx_i$$

where, for each i $(1 \leq i \leq s)$ there is a prime ideal $\mathfrak{p}_i$ and a natural integer $m_i \geq 1$ such that the map $R \twoheadrightarrow Rx_i, a \mapsto ax_i$, induces an isomorphism $R/\mathfrak{p}_i^{m_i} \xrightarrow{\sim} Rx_i$.

In other words,

$$M \cong \bigoplus_{i=1}^{s} R/\mathfrak{p}_i^{m_i}.$$

(3) *Such a decomposition is unique in the following sense: let $(\mathfrak{p}_i)_{1\leq i\leq s}$ and $(\mathfrak{q}_j)_{1\leq j\leq t}$ be families of prime ideals, let $(m_i)_{1\leq i\leq s}$ and $(n_j)_{1\leq j\leq t}$ be families of nonzero natural integers such that*

$$\bigoplus_{i=1}^{s} R/\mathfrak{p}_i^{m_i} \cong \bigoplus_{j=1}^{t} R/\mathfrak{q}_j^{n_j},$$

then $s = t$ and up to a permutation of $\{1, \ldots, s\}$, for all i $(1 \leq i \leq s)$ we have $\mathfrak{p}_i = \mathfrak{q}_i$ and $m_i = n_i$.

Another decomposition into a direct sum of cyclic modules is given by the following theorem.

Theorem 2.199 (Invariants) *Let R be a Dedekind domain. Let M be a finitely generated torsion R-module.*

There exists a unique family of nontrivial integral ideals $(\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m)$ such that

(a) $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_m$,

(b) *there exists a family $x_1, x_2, \ldots, x_m$ of elements of M such that*

- *for all i*, $\mathrm{Ann}_R(x_i) = \mathfrak{a}_i$,
- $M = \bigoplus_{i=1}^{m} Rx_i$.

In other words,

$$M \cong \bigoplus_{i=1}^{m} R/\mathfrak{a}_i.$$

Definition 2.200 With the notation of the preceding theorem,

- the ideals $(\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_m)$ are called the *invariants* of M,
- the smallest invariant, namely $\mathfrak{a}_1$, which is also the annihilator of M, is called the *minimal ideal* of M.
- The product $\mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_m$ of the invariants is called the *characteristic ideal* of M.

Corollary 2.201 *Let M be a finitely generated torsion R-module with annihilator* $\operatorname{Ann}_R(M) = \mathfrak{a}$. *Then there exist an element $x \in M$ with annihilator* $\mathfrak{a}$, *and a submodule M_1 of M such that $M = Rx \oplus M_1$.*

2.3.3.4 Proofs of the Main Theorems

Proof of Theorem 2.198 (Jordan decomposition) By the $\mathfrak{p}$-primary decomposition theorem, we see that in order to prove the first two assertions of Theorem 2.198 we may assume that $M = M(\mathfrak{p})$ for some nonzero prime ideal $\mathfrak{p}$. So from now on we assume that $\operatorname{Ann}_R(M) = \mathfrak{p}^m$, and we view M as an $R/\mathfrak{p}^m$-module.

By Corollary 2.195, we know that the structure of R-module of M induces naturally a structure of $R_\mathfrak{p}$-module. We shall use that fact, together with the fact that $R_\mathfrak{p}$ is a principal ideal domain (see Corollary 2.165). So from now on, until the end of the proof of assertions (1) and (2), *we assume that R is a principal ideal domain.*

For each integer $n \geq 0$, we set $M_n := \{x \in M \mid \mathfrak{p}^n x = 0\}$, and so we get a sequence of submodules $0 = M_0 \subset M_1 \subset \cdots \subset M_m = M$.

For $x \in M$, we denote by $n(x)$ the integer such that $x \in M_{n(x)}$ and $x \notin M_{n(x)-1}$.

We set $V := M/\mathfrak{p}M$ and for all n we denote by V_n the image of M_n under the natural surjection $M \twoheadrightarrow V$. Hence we get a sequence of subspaces in the $R/\mathfrak{p}$-vector space V:

$$\begin{tikzcd}
0 = & M_0 \arrow[d] & \subset & M_1 \arrow[d] & \subset & \cdots & \subset & M_m = M \arrow[d] \\
0 = & V_0 & \subset & V_1 & \subset & \cdots & \subset & V_m = V.
\end{tikzcd}$$

Let us choose a basis B of the $R/\mathfrak{p}$-vector space V which is “adapted” to the above sequence, that is, B can be built up as follows: we start by choosing a basis B_1 of V_1, which we complete by B_2 to get a basis of V_2, etc. Thus for all n $(1 \leq n \leq m)$, $\bigcup_{1 \leq j \leq n} B_j$ is a basis of V_n.

For each element $b \in B$, choose a preimage $\widetilde{b}$ of b in M. Thus, if $b \in V_n \setminus V_{n-1}$, then $\widetilde{b} \in M_n \setminus M_{n-1}$.

We shall prove that the map

$$\delta : \bigoplus_{b \in B} R/\mathfrak{p}^{n(b)} \longrightarrow M, \qquad (\lambda_b)_{b \in B} \mapsto \sum_{b \in B} \lambda_b \widetilde{b},$$

is an isomorphism of R-modules.

• Let us prove that δ is surjective. Since B is a basis of $V = M/\mathfrak{p}M$, the composition of δ by the projection $M \twoheadrightarrow V$ is surjective, that is

$$M = \mathrm{im}(\delta) + \mathfrak{p}M.$$

It follows that for all $n \geq 1$ we have $M = \mathrm{im}(\delta) + \mathfrak{p}^n M$, and for $n = m$ we get $M = \mathrm{im}(\delta)$.

Remark 2.202 One could invoke Nakayama's lemma to prove that surjectivity (how?).

• Now we prove that δ is injective. Let us denote by p a generator of the ideal $\mathfrak{p}$, i.e., $\mathfrak{p} = Rp$.

Assume

$$\sum_{b\in B} \lambda_b \widetilde{b} = 0.$$

We shall prove by induction on n that, for all $b \in B$, p^n divides λ_b. The property is trivial for $n = 0$. Assume it holds for n. Then we have $\lambda_b = 0$ if $n(b) \leq n$, and $\lambda_b = p^n \mu_b$ for some $\mu_b \in R/\mathfrak{p}^{n(b)}$ for all b such that $n(b) > n$. So we only have to prove that p^{n+1} divides λ_b for all b such that $n(b) > n$.

Setting $B_{>n} := \bigcup_{j>n} B_j$, we have

$$p^n \sum_{b\in B_{>n}} \mu_b \widetilde{b} = 0.$$

Thus $\sum_{b\in B_{>n}} \mu_b \widetilde{b} \in M_n$, and consequently (denoting by $\overline{\mu}_b$ the image of μ_b in $R/\mathfrak{p}$),

$$\sum_{b\in B_{>n}} \overline{\mu}_b b \in V_n.$$

Now, by construction of the sets B_j, this implies that $\sum_{b\in B_{>n}} \overline{\mu}_b b = 0$. Thus for all b such that $n(b) > n$, p divides μ_b, hence p^{n+1} divides λ_b, which completes the proof.

Let us now prove (3).

Thus consider an R-module M such that

$$M \cong \bigoplus_{i=1}^{s} R/\mathfrak{p}_i^{m_i} \cong \bigoplus_{j=1}^{t} R/\mathfrak{q}_j^{n_j},$$

with $m_i, n_j \geq 1$ for all i and j.

Pick a nonzero prime ideal $\mathfrak{p}$. Then

$$M(\mathfrak{p}) \cong \bigoplus_{i|\mathfrak{p}_i=\mathfrak{p}} R/\mathfrak{p}_i^{m_i} \cong \bigoplus_{j|\mathfrak{q}_j=\mathfrak{p}} R/\mathfrak{q}_j^{n_j},$$

and so we may assume (which we do) that, for all i and j, $\mathfrak{p}_i = \mathfrak{q}_j = \mathfrak{p}$, i.e., $M = M(\mathfrak{p})$.

Since $(R/\mathfrak{p}^m)/\mathfrak{p}(R/\mathfrak{p}^m) \cong R/\mathfrak{p}$, we see that $M/\mathfrak{p}M$ has dimension s and t as well, hence $s = t$.

Moreover, if $\operatorname{Ann}(M) = \mathfrak{p}^m$, we see that

$$m = \max\{m_i \mid 1 \leq i \leq s\} = \max\{n_j \mid 1 \leq j \leq s\}.$$

Let us argue by induction on m. If $m = 0$, then $M = 0$ and the desired conclusion is obvious. So assume $m \geq 1$.

By Proposition 2.196, we have

$$\mathfrak{p}M \cong \bigoplus_{i=1}^{s} R/\mathfrak{p}^{m_i - 1} \cong \bigoplus_{j=1}^{s} R/\mathfrak{p}^{n_j - 1},$$

and so the induction hypothesis applied to $\mathfrak{p}M$ gives us the desired conclusion. □

Proof of Theorem 2.199 (Invariants) Existence. Suppose given an isomorphism

$$M \xrightarrow{\sim} \bigoplus_{\mathfrak{p}} \bigoplus_{i=1}^{m_{\mathfrak{p}}} R/\mathfrak{p}^{k_{\mathfrak{p},i}},$$

where, for each $\mathfrak{p}$,

$$0 < k_{\mathfrak{p},1} \leq k_{\mathfrak{p},2} \leq \cdots \leq k_{\mathfrak{p},m_{\mathfrak{p}}}.$$

Let $m := \max\{m_{\mathfrak{p}} \mid \mathfrak{p} \in \operatorname{Spec}(R)\}$. Adding a bunch of zeros at the beginning of the list of the integers $k_{\mathfrak{p},i}$, and up to changing their order numbering, we may assume (which we do) that for each $\mathfrak{p}$, we have $m_{\mathfrak{p}} = m$, with

$$0 \leq k_{\mathfrak{p},1} \leq k_{\mathfrak{p},2} \leq \cdots \leq k_{\mathfrak{p},m}.$$

For all i $(1 \leq i \leq m)$, we then define

$$\mathfrak{a}_i := \prod_{\mathfrak{p}} \mathfrak{p}^{k_{\mathfrak{p},m+1-i}}.$$

Then

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_m.$$

By Corollary 2.197, (3), it follows that

$$\bigoplus_{\mathfrak{p}} R/\mathfrak{p}^{k_{\mathfrak{p},m+1-i}} \cong R/\mathfrak{a}_i,$$

hence

$$M \cong \bigoplus_{i=1}^{m} R/\mathfrak{a}_i.$$

Unicity. Assume $M \cong \bigoplus_{i=1}^{m} R/\mathfrak{a}_i$ with $0 \neq \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_m \neq R$. Decompose $\mathfrak{a}_1$ into a product of prime ideals:

$$\mathfrak{a}_1 = \prod_{\mathfrak{p}} \mathfrak{p}^{k_{\mathfrak{p},m}} \qquad \text{with } 1 \leq k_{\mathfrak{p},m} \text{ for all } \mathfrak{p}.$$

Then, since $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_m$, for each $i < m$ we have

$$\mathfrak{a}_i = \prod_{\mathfrak{p}} \mathfrak{p}^{k_{\mathfrak{p},m+1-i}} \quad \text{where } 0 \leq k_{\mathfrak{p},1} \leq k_{\mathfrak{p},2} \leq \cdots \leq k_{\mathfrak{p},m}.$$

By Corollary 2.197, (3), we see that

$$M \cong \bigoplus_{\mathfrak{p}} \bigoplus_{i=1}^{m} R/\mathfrak{p}^{k_{\mathfrak{p},i}}$$

and it follows from the unicity part (part (3)) in Theorem 2.198 that the families $(k_{\mathfrak{p},i})_{\mathfrak{p},i}$ are uniquely determined, hence the ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ are also uniquely determined. □

Example 2.203 Here we choose $R = \mathbb{Z}$, and

$$M := (\mathbb{Z}/2\mathbb{Z})^3 \oplus (\mathbb{Z}/3\mathbb{Z})^4 \oplus (\mathbb{Z}/5\mathbb{Z}) \oplus \big(\mathbb{Z}/5^2\mathbb{Z}\big).$$

With the notation of the above proof, we see that $m = 4$, and that the list of integers $(k_{\mathfrak{p},i})_{\mathfrak{p},i}$ is:

$$\begin{array}{lllll}
p = 2: & k_{2,1} = 0, & k_{2,2} = 1, & k_{2,3} = 1, & k_{2,4} = 1, \\
p = 3: & k_{3,1} = 1, & k_{3,2} = 1, & k_{3,3} = 1, & k_{3,4} = 1, \\
p = 5: & k_{5,1} = 0, & k_{5,2} = 0, & k_{5,3} = 1, & k_{5,4} = 2,
\end{array}$$

hence $\mathfrak{a}_i = a_i\mathbb{Z}$ with

$$a_4 = 3, \qquad a_3 = 6, \qquad a_2 = 30, \qquad a_1 = 150,$$

and

$$M \cong (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/6\mathbb{Z}) \oplus (\mathbb{Z}/30\mathbb{Z}) \oplus (\mathbb{Z}/150\mathbb{Z}).$$

2.3.3.5 Completely Reducible Modules

Definition 2.204 Let A be a ring and M be a left A-module.

(1) We say that M is *irreducible* if M is nonzero and if it has no submodule but $\{0\}$ and M.

(2) We say that M is *completely reducible* if it is a direct sum of a finite number of irreducible submodules.

Proposition 2.205 *Let R be a Dedekind domain, and let M be a finitely generated torsion R-module.*

(1) *M is irreducible if and only if there exists a nonzero prime ideal $\mathfrak{p}$ of R such that M is isomorphic to $R/\mathfrak{p}$ (that is, M is cyclic with annihilator $\mathfrak{p}$).*
(2) *The following properties are equivalent:*

   (i) *M is completely reducible,*
   (ii) $\operatorname{Ann}_R(M)$ *is not divisible by a square in the ideal group,*
   (iii) *whenever N is a submodule of M, N has a complement in M (that is, there exists a submodule N' of M such that $M = N \oplus N'$).*

Proof (1) By Theorem 2.198, if M is irreducible then it is cyclic with annihilator $\mathfrak{p}^m$ for some nonzero prime ideal $\mathfrak{p}$ and some integer $m \geq 1$. If $m > 1$, the module $\mathfrak{p}^{m-1}/\mathfrak{p}^m$ is a nonzero proper submodule of $R/\mathfrak{p}^m$, hence we must have $m = 1$.

Conversely, $R/\mathfrak{p}$ is irreducible since its structure of R-module induces naturally a structure of one dimensional vector space over the field $R/\mathfrak{p}$.

(2) (i)⇒(iii). Using (1), we may write

$$M \cong \bigoplus_{\mathfrak{p}\in\operatorname{Spec}^*(R)} (R/\mathfrak{p})^{m_\mathfrak{p}},$$

hence for all $\mathfrak{p} \in \operatorname{Spec}^*(R)$,

$$M(\mathfrak{p}) \simeq (R/\mathfrak{p})^{m_\mathfrak{p}}.$$

Let N be a submodule of M. For all $\mathfrak{p} \in \operatorname{Spec}^*(R)$, we have

$$N(\mathfrak{p}) = N \cap M(\mathfrak{p}) \quad \text{and} \quad N = \bigoplus_{\mathfrak{p}\in\operatorname{Spec}^*(R)} N(\mathfrak{p}).$$

Since $M(\mathfrak{p})$ is an $(R/\mathfrak{p})$-vector space, $N(\mathfrak{p})$ has a complement $N'_\mathfrak{p}$ in $M(\mathfrak{p})$, and so

$$N' := \bigoplus_{\mathfrak{p}\in\operatorname{Spec}^*(R)} N'_\mathfrak{p}$$

is a complement of N in M. Notice that $N'(\mathfrak{p}) = N'_\mathfrak{p}$.

(iii)⇒(ii). By Theorem 2.198, it suffices to prove that if M' is a submodule of M isomorphic to $R/\mathfrak{p}^m$ for some nonzero prime ideal $\mathfrak{p}$ and some integer $m \geq 1$, then $m = 1$.

If $m > 1$, the submodule $\mathfrak{p}^{m-1}/\mathfrak{p}^m$ has no complement in $R/\mathfrak{p}^m$ (since that last module is indecomposable), hence the corresponding submodule of M has no complement in M. This shows that $m = 1$.

(ii)⇒(i). This follows immediately from Theorem 2.198. □

2.3.4 Adapted Pseudo-bases for Submodules of Finitely Generated Projective Modules

2.3.4.1 The Main Theorem

All the decompositions stated in the previous section follow from the following theorem (see Exercise 2.209 below).

Theorem 2.206 (Fundamental theorem) *Let R be a Dedekind domain. Let M be a finitely generated projective R-module of rank r, and let M' be a submodule of M.*

There exists a unique family $(\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_r)$ of integral ideals such that

(a) $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_r$,
(b) *there exists a pseudo-basis $(E_1, E_2, \dots, E_r)$ of M such that the family $(\mathfrak{a}_i E_i \mid \mathfrak{a}_i \neq 0)$ is a pseudo-basis of M'.*

Definition 2.207 With the notation of the previous theorem, the ideals $(\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_r)$ are called the *invariants of M' in M*, and a pseudo-basis as $(E_1, \dots, E_r)$ is said to be *adapted to M'*.

Remark 2.208 With the notation of the above theorem, the rank of M' is the number of invariants which are not equal to 0.

Proof of theorem 2.206 1. Unicity.

Assume that

$$M = E_1 \oplus \cdots \oplus E_r,$$
$$M' = \mathfrak{a}_1 E_1 \oplus \cdots \oplus \mathfrak{a}_r E_r,$$
$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_r.$$

Then it is easy to check that

$$M/M' = E_1/\mathfrak{a}_1 E_1 \oplus \cdots \oplus E_r/\mathfrak{a}_r E_r$$

which (by Proposition 2.196) implies

$$M/M' \cong R/\mathfrak{a}_1 \oplus \cdots \oplus R/\mathfrak{a}_r.$$

Thus the family of *nonzero proper ideals* among $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_r$ are the invariants of M/M', which are unique by Theorem 2.199.

2. Existence.

We know (see Corollary 2.180) that there exists a finitely generated projective submodule P of M/M' such that $M/M' = \mathrm{tor}(M/M') \oplus P$. By composition of the natural surjection $\pi_{M'} : M \to M/M'$ with the projection $p : M/M' \to P$, we get a surjective morphism $M \twoheadrightarrow P$. Since P is projective, that morphism is split, that is, there exists $\sigma : P \to M$ such that $p \cdot \pi_{M'} \cdot \sigma = \mathrm{Id}_P$. Consider the following diagram:

$$\begin{tikzcd}
M \arrow[rr, "\pi_{M'}"] & & M/M' \arrow[dl, "p"] \arrow[dr, "1-p"] & \\
& P \arrow[ul, "\sigma"] & \oplus & \mathrm{tor}(M/M')
\end{tikzcd}$$

We define submodules $P_1 := \sigma(P)$ and $M_1 := \ker(p \cdot \pi_{M'})$ of M, so that

- $M = M_1 \oplus P_1$,
- $M' \subset M_1$ and $M/M_1 = \mathrm{tor}(M/M')$.

Hence we may assume $M = M_1$, that is, that M and M' have the same rank, and M/M' is a finitely generated torsion R-module, which we do from now on.

We set $\mathfrak{a} := \mathrm{Ann}_R(M/M')$.

We shall argue by induction on r. If $V := F \otimes_R M$, we see that r is the dimension of the vector space V.

(a) Case where M has rank one.

In that case, $V = Fe$ for some $e \in V \setminus \{0\}$, which implies that $M = \mathfrak{b}e$ and $M' = \mathfrak{b}'e$ for some fractional ideals $\mathfrak{b}$ and $\mathfrak{b}'$ such that $\mathfrak{b}' \subset \mathfrak{b}$. We set $\mathfrak{a} := \mathfrak{b}^{-1}\mathfrak{b}'$. Then

(1) $\mathfrak{a}$ is integral,
(2) $M' = \mathfrak{a}M$.

(b) General case: construction of E and E', rank one projective submodules of M and M' respectively, such that $E' = \mathfrak{a}E$.

By Corollary 2.201, we know that there exists a *cyclic* submodule C of M/M' such that $\mathrm{Ann}_R(C) = \mathfrak{a}$.

Let $\widetilde{C}$ be a cyclic submodule of M which lifts C, and let $L := F\widetilde{C}$ be the line generated in V by $\widetilde{C}$.

• We set $E := L \cap M$. Thus E is a rank one (projective) submodule of M which contains $\widetilde{C}$.

Let us check that M/E is torsion free. Indeed, assume that $m \in M$ and $\lambda \in R$ ($\lambda \neq 0$) are such that $\lambda m \in E$. Then in particular $\lambda m \in L$, hence $m \in L$, which shows that $m \in E$.

• We set $E' := L \cap M'$, and a similar proof shows that M'/E' is torsion free. Note that $E' = M' \cap E$.

• Let us check that $E' = \mathfrak{a}E$. By the case a) above, we know that $E' = \mathfrak{a}'E$ for some integral ideal $\mathfrak{a}'$. It suffices then to prove that $\mathfrak{a}' = \mathfrak{a}$.

On one hand we have $\mathfrak{a}E = \mathfrak{a}(L \cap M) \subset L \cap M' = E'$, hence $\mathfrak{a} \subset \mathfrak{a}'$. On the other hand, $\mathfrak{a}'\widetilde{C} \subset M'$, hence $\mathfrak{a}'C = 0$ and so $\mathfrak{a}' \subset \mathfrak{a}$ since $\mathrm{Ann}_R(C) = \mathfrak{a}$.

(c) General case (continued): construction of M_1 and M_1' such that $M_1' \subset M_1, M = E \oplus M_1, M' = E' \oplus M_1'$.

Since M'/E' is torsion free (and finitely generated), it is projective, hence there exists a submodule M'_1 of M' such that $M' = E' \oplus M'_1$. Let us define $V_1 := FM'_1$. Thus $V = L \oplus V_1$, V_1 is an $(r-1)$-dimensional subspace of V and M'_1 is a projective R-module of rank $r-1$.

We set $M_1 := V_1 \cap M$. Note that $M'_1 = M' \cap M_1$. Let us prove that $M = E \oplus M_1$. Since $E \cap M_1 \subset L \cap V_1 = 0$, it suffices to check that $M = E + M_1$. We have $\mathfrak{a}M \subset M' = E' \oplus M'_1$, from which it follows that $M \subset \mathfrak{a}^{-1}E' \oplus \mathfrak{a}^{-1}M'_1 = E \oplus \mathfrak{a}^{-1}M'_1$. Thus, if $m \in M$, there exist $x \in E$ and $x' \in \mathfrak{a}^{-1}M'_1$ such that $m = x + x'$. But then $x' \in M$, so $x' \in V_1 \cap M$, which shows that $M = E + M_1$.

Thus

$$\begin{array}{ccccccc} M & = & E & \oplus & M_1 \\ \cup & & \cup & & \cup \\ M' & = & E' & \oplus & M'_1 \end{array}$$

(d) End of the proof.

By the induction hypothesis, since M_1 has rank $r-1$, there exist

(1) a family of integral ideals $\mathfrak{a}_2, \ldots, \mathfrak{a}_r$ such that $\mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_r$,
(2) and a family of rank one submodules $E_2, \ldots, E_r$ of M_1 such that

$$M_1 = E_2 \oplus \cdots \oplus E_r$$
$$M'_1 = \mathfrak{a}_2 E_2 \oplus \cdots \oplus \mathfrak{a}_r E_r .$$

Then we get

$$M = E \oplus E_2 \oplus \cdots \oplus E_r$$
$$M' = \mathfrak{a}E \oplus \mathfrak{a}_2 E_2 \oplus \cdots \oplus \mathfrak{a}_r E_r ,$$

and we do have $\mathfrak{a} \subset \mathfrak{a}_2$ since by hypothesis $\mathfrak{a} = \mathrm{Ann}_R(M/M')$, hence $\mathfrak{a} \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_r$. □

Exercise 2.209 Prove that the fundamental Theorem 2.206 above implies

(1) Theorem 2.199,
(2) Theorem 2.198,

(which are used here in its proof, though...).

2.3.4.2 On Characteristic Ideals of Finitely Generated Torsion Modules

We shall apply Theorem 2.206 to properties of characteristic ideals of finitely generated torsion R-modules (see Definition 2.200).

For M a finitely generated torsion R-module, let us denote by $\mathrm{char}(M)$ its characteristic ideal. Hence if $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ are the invariants of M,

$$\mathrm{char}(M) = \mathfrak{a}_1 \cdots \mathfrak{a}_m.$$

Remark 2.210

- In the case where $R = \mathbb{Z}$, M is nothing but an Abelian finite group, and $\mathrm{char}(M)$ is the ideal generated by the order $|M|$ of M.

  If N is a subgroup of M, we have $|M| = |N||M/N|$, hence $\mathrm{char}(M) = \mathrm{char}(N)\,\mathrm{char}(M/N)$.
- In the case where $R = k[X]$ (k a field) and $M = V_\phi$ (V a finite dimensional k-vector space and ϕ an endomorphism of V), $\mathrm{char}(M)$ is the ideal generated by the characteristic polynomial $\Gamma_{V,\phi}(X)$ of ϕ.

  If W is a ϕ-stable subspace of V, ϕ induces an endomorphism of W, hence a $k[X]$-module structure W_ϕ on W. Moreover, ϕ induces an endomorphism of V/W still denoted by ϕ, hence a $k[X]$-module structure $(V/W)_\phi$ on V/W. Then (with obvious notation), the reader may prove that $\Gamma_{V,\phi}(X) = \Gamma_{W,\phi}(X)\Gamma_{V/W,\phi}(X)$ hence

$$\mathrm{char}(V_\phi) = \mathrm{char}(W_\phi)\,\mathrm{char}\big((V/W)_\phi\big).$$

What follows is nothing but a generalization of that remark to any Dedekind domain.

Proposition 2.211 *Let R be a Dedekind domain. Let M be a finitely generated torsion R-module and let N be an R-submodule of M. Then*

$$\mathrm{char}(M) = \mathrm{char}(N)\,\mathrm{char}(M/N).$$

Corollary 2.212 *Let R be a Dedekind domain, let $M_1, \ldots, M_n$ be finitely generated torsion R-modules.*

(1) $\mathrm{char}(M_1 \oplus \cdots \oplus M_n) = \mathrm{char}(M_1) \cdots \mathrm{char}(M_n)$.
(2) *If* $0 \to M_1 \to \cdots \to M_n \to 0$ *is an exact sequence, then*

$$\prod_{j=1}^{n} \mathrm{char}(M_j)^{(-1)^j} = R.$$

Proof of Proposition 2.211 Assume that the invariants of M (resp. N, M/N) are $(\mathfrak{a}_i)_{1\le i\le s}$ (resp. $(\mathfrak{b}_j)_{1\le j\le t}$, $(\mathfrak{c}_k)_{1\le k\le u}$. Choose $r \ge s, t, u$, and add as many $\mathfrak{a}_i = R$ (resp. $\mathfrak{b}_j = R$, $\mathfrak{c}_k = R$) so that we get

$$\mathfrak{a}_1 \subset \cdots \subset \mathfrak{a}_s \subset \cdots \subset \mathfrak{a}_r$$
$$\mathfrak{b}_1 \subset \cdots \subset \mathfrak{b}_t \subset \cdots \subset \mathfrak{b}_r$$
$$\mathfrak{c}_1 \subset \cdots \subset \mathfrak{c}_u \subset \cdots \subset \mathfrak{c}_r$$

Let $P_M := R^r$. Since $M \cong R/\mathfrak{a}_1 \oplus \cdots \oplus R/\mathfrak{a}_s$, there is a surjective morphism $\pi : P_M \twoheadrightarrow M$. Let $P_0 := \ker(\pi)$.

Let us denote by P_N the inverse image of N under π, so that we have the commutative diagram

$$\begin{tikzcd}
P_0 \arrow[r, dash] \arrow[d] & P_N \arrow[r, dash] \arrow[d] & P_M \arrow[d] \\
0 \arrow[r, dash] & N \arrow[r, dash] & M,
\end{tikzcd}$$

and

$$P_M/P_0 \cong M,\ P_N/P_0 \cong N,\ P_M/P_N \cong M/N.$$

We set $V := F^r = FP$.

By Theorem 2.206 we know that there exist

- a basis $(e_1, \ldots, e_r)$ of V, and a family $(\mathfrak{e}_1, \ldots, \mathfrak{e}_r)$ of fractional ideals, such that
$$P_M = \bigoplus_{j=1}^{r} \mathfrak{e}_j e_j \quad \text{and} \quad P_0 = \bigoplus_{j=1}^{r} \mathfrak{a}_j \mathfrak{e}_j e_j,$$
- a basis $(f_1, \ldots, f_r)$ of V, and a family $(\mathfrak{f}_1, \ldots, \mathfrak{f}_r)$ of fractional ideals, such that
$$P_N = \bigoplus_{j=1}^{r} \mathfrak{f}_j f_j \quad \text{and} \quad P_0 = \bigoplus_{j=1}^{r} \mathfrak{b}_j \mathfrak{f}_j f_j,$$
- a basis $(g_1, \ldots, g_r)$ of V, and a family $(\mathfrak{g}_1, \ldots, \mathfrak{g}_r)$ of fractional ideals, such that
$$P_M = \bigoplus_{j=1}^{r} \mathfrak{g}_j g_j \quad \text{and} \quad P_N = \bigoplus_{j=1}^{r} \mathfrak{c}_j \mathfrak{g}_j f_j.$$

Let us denote by $\varLambda$ and $\varLambda'$ the matrices (with entries in F) such that

$$\varLambda \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_r \end{pmatrix} \quad \text{and} \quad \varLambda' \begin{pmatrix} f_1 \\ \vdots \\ f_r \end{pmatrix} = \begin{pmatrix} g_1 \\ \vdots \\ g_r \end{pmatrix}.$$

Let us call $\lambda_{i,j}$ and $\mu_{j,i}$ the entries of respectively $\varLambda$ and $\varLambda^{-1}$.

• In particular, for all $j = 1, \ldots, r$, we have $f_j = \sum_{i=1}^{r} \lambda_{i,j} e_i$.

Since both families $(\mathfrak{a}_i \mathfrak{e}_i e_i)_{1 \le i \le r}$ and $(\mathfrak{b}_j \mathfrak{f}_j f_j)_{1 \le j \le r}$ are pseudo-bases of P_0, it follows that

$$\mathfrak{b}_j \mathfrak{f}_j f_j \subset \sum_{i=1}^{r} \mathfrak{a}_i \mathfrak{e}_i e_i \quad (\text{for all } j = 1, \ldots, r),$$

hence

$$\lambda_{i,j}\mathfrak{b}_j\mathfrak{f}_j \subset \mathfrak{a}_i\mathfrak{e}_i \quad (\text{for all } i, j = 1, \dots, r).$$

Like in the proof of assertion (2) of Theorem 2.184, we deduce that

$$\det(\Lambda)\prod_{j=1}^{r}\mathfrak{b}_j\mathfrak{f}_j \subset \prod_{i=1}^{r}\mathfrak{a}_i\mathfrak{e}_i.$$

- Similarly, starting from the equality $e_i = \sum_{j=1}^{r}\mu_{j,i}f_j$ (for all $i = 1, \dots, r$), we get

$$\mu_{j,i}\mathfrak{a}_i\mathfrak{e}_i \subset \mathfrak{b}_j\mathfrak{f}_j \quad (\text{for all } i, j = 1, \dots, r),$$

hence

$$\det\bigl(\Lambda^{-1}\bigr)\prod_{i=1}^{r}\mathfrak{a}_i\mathfrak{e}_i \subset \prod_{j=1}^{r}\mathfrak{b}_j\mathfrak{f}_j,$$

so finally

$$\det(\Lambda)\prod_{j=1}^{r}\mathfrak{b}_j\mathfrak{f}_j = \prod_{i=1}^{r}\mathfrak{a}_i\mathfrak{e}_i. \qquad (\boldsymbol{\lambda})$$

- By a similar argument, using the matrix Λ', the bases (f_i) and (g_j) of V, and the pseudo-bases $(\mathfrak{f}_i f_i)_{1\le i\le r}$ and $(\mathfrak{c}_j\mathfrak{g}_j g_j)_{1\le j\le r}$ of P_N, we get

$$\det\bigl(\Lambda'\bigr)\prod_{j=1}^{r}\mathfrak{c}_j\mathfrak{g}_j = \prod_{i=1}^{r}\mathfrak{f}_i. \qquad (\boldsymbol{\lambda}')$$

- Moreover, using the matrix $\Lambda'\Lambda$, the bases (e_i) and (g_j) of V, and the pseudo-bases $(\mathfrak{e}_i e_i)_{1\le i\le r}$ and $(\mathfrak{g}_j g_j)_{1\le j\le r}$ of P_M, we get

$$\det\bigl(\Lambda'\bigr)\det(\Lambda)\prod_{j=1}^{r}\mathfrak{g}_j = \prod_{i=1}^{r}\mathfrak{e}_i. \qquad (\boldsymbol{\lambda\lambda}')$$

- Multiplying equalities ($\boldsymbol{\lambda}$) and ($\boldsymbol{\lambda}'$), and comparing to equality ($\boldsymbol{\lambda\lambda}'$) gives

$$\prod_{i=1}^{r}\mathfrak{a}_i\mathfrak{e}_i\left(\prod_{j=1}^{r}\mathfrak{b}_j\mathfrak{f}_j\right)^{-1}\prod_{i=1}^{r}\mathfrak{f}_i\Bigl(\prod\mathfrak{c}_j\mathfrak{g}_j\Bigr)^{-1} = \prod_{i=1}^{r}\mathfrak{e}_i\left(\prod_{j=1}^{r}\mathfrak{g}_j\right)^{-1},$$

hence

$$\prod_{i=1}^{r}\mathfrak{a}_i = \prod_{j=1}^{r}\mathfrak{b}_j\prod_{k=1}^{r}\mathfrak{c}_k,$$

that is,

$$\operatorname{char}(M) = \operatorname{char}(N)\operatorname{char}(M/N).$$

□

The proof of Corollary 2.212 is left to the reader.

2.3.5 Applications to Abelian Groups and Endomorphisms of Vector Spaces

WE RECALL THE FUNDAMENTAL FOLLOWING FACTS.

If $R = \mathbb{Z}$, a finitely generated torsion $\mathbb{Z}$-module is nothing but a finite Abelian group.

If $R = k[X]$ (k a field), a finitely generated torsion $k[X]$-module is nothing but a finite dimensional vector space endowed with an endomorphism ϕ (the endomorphism induced by the multiplication by X).

If V is a finite dimensional vector space endowed with an endomorphism ϕ, we denote by V_ϕ the $k[X]$-module defined by the rule $X.v := \phi(v)$ for all $v \in V$.

We shall reformulate the main results about finitely generated torsion modules over Dedekind domains for these particular cases, and we shall draw some consequences.

We shall use that

- ideals of $\mathbb{Z}$ are in natural bijection with natural integers,
- nonzero ideals of $k[X]$ are in natural bijection with monic elements of $k[X]$.

2.3.5.1 Decomposition into Indecomposables

Theorem 2.213 (Jordan decomposition)

(1) *Finite Abelian groups.*

(a) *A finite Abelian group is indecomposable if and only if it is isomorphic to* $\mathbb{Z}/p^m\mathbb{Z}$ *for some prime number* p *and some integer* $m \geq 1$.

(b) *Given a finite Abelian group* G, *there is*

- *a unique set* $\{p_1, \dots, p_s\}$ *of distinct prime numbers,*
- *for each* $j = 1, \dots, s$, *a unique family* $(m_{j,\alpha})_{\alpha=1,\dots,n_j}$ *of integers* $m_{j,\alpha} \geq 1$,

such that

$$G \cong \bigoplus_{\substack{1 \leq j \leq s \\ 1 \leq \alpha \leq n_j}} \mathbb{Z}/p_j^{m_{j,\alpha}}\mathbb{Z}.$$

(2) *Vector spaces with an endomorphism.*

Let V be a finite dimensional k-vector space, and let ϕ be an endomorphism of V.

(a) *A subspace W of V stable under ϕ is indecomposable (as a ϕ-stable subspace) if and only if there exist an irreducible polynomial $P(X) \in k[X]$ and an integer $m \geq 1$ such that*

$$W_\phi \cong k[X]/\big(P(X)^m\big),$$

g i.e., there is a an isomorphism of vector spaces

$$\sigma : W \xrightarrow{\sim} k[X]/\big(P(X)^m\big)$$

such that the following diagram is commutative:

$$\begin{tikzcd}
W \arrow[r, "\sigma"] \arrow[d, "\phi"'] & k[X]/(P(X)^m) \arrow[d, "\times X"] \\
W \arrow[r, "\sigma"] & k[X]/(P(X)^m)
\end{tikzcd}$$

(b) *There exist*

- *a unique set $\{P_1(X), \dots, P_s(X)\}$ of distinct monic prime polynomials, and*
- *for each $j = 1, \dots, s$, a unique family $(m_{j,\alpha})_{\alpha=1,\dots,n_j}$ of integers $m_{j,\alpha} \geq 1$,*

such that

$$W_\phi \cong \bigoplus_{\substack{1 \leq j \leq s \\ 1 \leq \alpha \leq n_j}} k[X]/\big(P_j(X)^{m_{j,\alpha}}\big).$$

Let us translate the last assertion of the preceding theorem in terms of matrices. Let

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in k[X]$$

be a monic polynomial of degree n. Let us choose n monic polynomials $E_0(X), \dots, E_{n-1}(X)$, all of degree $\leq n-1$, which define a basis of the vector space $k[X]/(P(X))$.

Let M_P denote the matrix of the endomorphism "multiplication by X" with respect to that basis.

Example 2.214

- We may of course choose $E_j(X) = X^j$, in which case

$$M_P = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & -a_{n-2} \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

- Let $P(X) = (X-a)^2 + b^2$ with $b \neq 0$ (notice that any degree 2 irreducible monic polynomial in $\mathbb{R}[X]$ has that form). Choose $E_0(X) := 1/b$ and $E_1(X) := (X-a)/b^2$. Then

$$M_P = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

- Assume $P(X) = (X-\lambda)^n$. Choose $E_j(X) := (X-\lambda)^{n-j}$. Then

$$M_P = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{pmatrix}$$

  (the reader may recognize a *Jordan block*).

We generalize the example of the Jordan block to any indecomposable component as follows.

Proposition 2.215 *Let $P(X) \in k[X]$, of degree n, and monic. Choose n polynomials*

$$E_0(X), \ldots, E_{n-1}(X), \quad \textit{all of degree } \leq n-1,$$

which define a basis of the vector space $k[X]/(P(X))$. Moreover, assume that

$$\begin{cases} \deg E_0(X) = n-1 & \textit{and} \quad E_0(X) \textit{ is monic}, \\ \deg E_j(X) < n-1 & \textit{for } j \neq 0. \end{cases}$$

Denote by M_P the matrix of the multiplication by X on $k[X]/(P(X))$ with respect to the basis defined by $E_0(X), \ldots, E_{n-1}(X)$.

Let us denote by $M_{P,m}$ the matrix of multiplication by X on the basis of the k-vector space $k[X]/(P(X)^m)$ defined by the system

$$P^{m-1}E_0, \ldots, P^{m-1}E_{n-1}, \ldots, PE_0, \ldots, PE_{n-1}, E_0, \ldots, E_{n-1}.$$

Then

$$M_{P,m} = \begin{pmatrix} \boxed{M_P} & \boxed{1_n} & \boxed{0} & \cdots & \boxed{0} & \boxed{0} \\ \boxed{0} & \boxed{M_P} & \boxed{1_n} & \cdots & \boxed{0} & \boxed{0} \\ \boxed{0} & \boxed{0} & \boxed{M_P} & \cdots & \boxed{0} & \boxed{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \boxed{0} & \boxed{0} & \boxed{0} & \cdots & \boxed{M_P} & \boxed{1_n} \\ \boxed{0} & \boxed{0} & \boxed{0} & \cdots & \boxed{0} & \boxed{M_P} \end{pmatrix}$$

Hint for a proof Assume that the entries of the matrix M_P are $(a_{i,j})$, that is, for all $j = 0, \dots, n-1$,

$$XE_j(X) \equiv \sum_{i=0}^{n-1} a_{i,j} E_i(X) \mod P(X).$$

The hypothesis about degrees of the polynomials $E_0(X), \dots, E_{n-1}(X)$, as well as the monicity of $P(X)$ and $E_0(X)$ imply in fact

$$\begin{cases} XE_j(X) = \sum_{i=0}^{n-1} a_{i,j} E_i(X) & \text{for } j \geq 1, \\ XE_0(X) = \sum_{i=0}^{n-1} a_{i,0} E_i(X) + P(X). \end{cases} \qquad \square$$

Example 2.216 The indecomposable blocks (which we might call *generalized Jordan blocks*) for matrices with entries in $\mathbb{R}$ may be described as

- either usual Jordan blocks (see above) with $\lambda \in \mathbb{R}$,
- or (by Ex. 2.214) matrices of the form

$$\begin{pmatrix} \boxed{\begin{matrix} a & -b \\ b & a \end{matrix}} & \boxed{\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}} & \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} & \cdots & \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} & \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} \\ \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} & \boxed{\begin{matrix} a & -b \\ b & a \end{matrix}} & \boxed{\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}} & \cdots & \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} & \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} \\ \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} & \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} & \boxed{\begin{matrix} a & -b \\ b & a \end{matrix}} & \cdots & \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} & \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} & \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} & \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} & \cdots & \boxed{\begin{matrix} a & -b \\ b & a \end{matrix}} & \boxed{\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}} \\ \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} & \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} & \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} & \cdots & \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} & \boxed{\begin{matrix} a & -b \\ b & a \end{matrix}} \end{pmatrix}$$

2.3.5.2 Invariants

Theorem 2.217 (Invariants)

(1) *Abelian finite groups.*

Let G be a finite Abelian group. There exists a unique sequence of natural integers $a_1, \dots, a_m$ all different from 1 *such that*

(a) $a_m \mid a_{m-1} \mid \cdots \mid a_1$,
(b) $G \cong (\mathbb{Z}/a_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/a_m\mathbb{Z})$.

The integers a_j are called the invariants of G. Moreover,

- a_1 *is the exponent of G (i.e., the smallest integer n such that $ng = 0$ for all $g \in G$),*
- *the product $a_1 \cdots a_m$ is the order $|G|$ of G.*

(2) *Vector spaces with an endomorphism.*

Let V be a finite dimensional k-vector space, and let ϕ be an endomorphism of V. There exists a unique sequence of monic polynomials $a_1(X), \dots, a_m(X) \in k[X]$ all non constant such that

(a) $a_m(X) \mid a_{m-1}(X) \mid \cdots \mid a_1(X)$,
(b) $V_\phi \cong (k[X]/(a_1(X))) \oplus \cdots \oplus (k[X]/(a_m(X)))$.

The polynomials $a_j(X)$ are called the invariants (or the invariant polynomials) of ϕ. Moreover,

- $a_1(X)$ *is the minimal polynomial of ϕ,*
- *the product $a_1(X) \cdots a_m(X)$is the characteristic polynomial of ϕ.*

The following properties are immediate consequences of the preceding theorem. Let us recall the following notation.

- The *exponent* $\exp(G)$ of a finite group G is by definition the least common multiple of the orders of the elements of G.
- If V is a finite dimensional k-vector space, v an element of V, and ϕ an endomorphism of V, the *minimal polynomial of ϕ at v* is the monic generator of the ideal comprising those elements $P(X) \in k[X]$ such that $P(\phi)(v) = 0$.

Corollary 2.218

(1) *Let G be a finite Abelian group.*

(a) *The exponent* $\exp(G)$ *divides the order $|G|$, and there is an integer $n \geq 1$ such that $|G|$ divides* $\exp(G)^n$.
(b) *There exists $g \in G$ of order the exponent of G.*
(c) *The exponent of G is equal to its order if and only if G is cyclic.*

(2) *Let V be a finite dimensional vector space, and let ϕ be an endomorphism of V.*

(a) *The minimal polynomial $M(X)$ of ϕ divides its characteristic polynomial $\Gamma(X)$, and there is an integer $n \geq 1$ such that $\Gamma(X)$ divides $M(X)^n$.*
(b) *There exists $v \in V$ such that the minimal polynomial of ϕ at v is equal to the minimal polynomial of ϕ.*
(c) *The minimal polynomial of ϕ is equal to its characteristic polynomial if and only if V_ϕ is cyclic, that is, if there exists $v \in V$ such that V is generated by $\{\phi^n(v) \mid n \geq 0\}$.*

Remark 2.219 This remark concerns the integer n mentioned in assertions (1)(a) and (2)(a) above.

Let us consider the general case of a finitely generated torsion module M over a Dedekind domain R, with invariants $\mathfrak{a}_1 \subset \cdots \subset \mathfrak{a}_m$. Write

$$\operatorname{char}(M) = \mathfrak{a}_1 \cdots \mathfrak{a}_m = \prod_{\mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p}^{v_\mathfrak{p}(\operatorname{char}(M))}.$$

Then for

$$n := \max\bigl\{v_\mathfrak{p}\bigl(\operatorname{char}(M)\bigr) \bigm| \mathfrak{p} \in \operatorname{Spec}(R)\bigr\}$$

we have

$$\operatorname{char}(M) \text{ divides } \mathfrak{a}_1^n.$$

In the particular case of a vector space endowed with an endomorphism, Theorem 2.217 has the following consequence (whose proof is immediate).

Corollary 2.220 *Let V be a finite dimensional k-vector space. Let ϕ and ϕ' be endomorphisms of V. The following assertions are equivalent.*

(i) *ϕ and ϕ' have the same invariants.*
(ii) *The $k[X]$-modules V_ϕ and $V_{\phi'}$ are isomorphic.*
(iii) *There exists an automorphism σ of V such that $\phi' = \sigma\phi\sigma^{-1}$.*

A consequence of the above property is the fact that conjugation of endomorphisms is an absolute property (that is, it is independent of the base field), in the following sense.

Corollary 2.221 *Let V be a finite dimensional k-vector space. Let ϕ and ϕ' be endomorphisms of V. Let K be a field, extension of k. The following assertions are equivalent.*

(i) *There exists an automorphism σ of V such that $\phi' = \sigma\phi\sigma^{-1}$.*
(ii) *There exists an automorphism τ of $K \otimes_k V$ such that $K \otimes_k \phi' = \tau(K \otimes_k \phi)\tau^{-1}$.*

Proof Indeed, this is an immediate consequence of the unicity of invariants, and of the fact that if

$$V_\phi \cong \bigl(k[X]/\bigl(a_1(X)\bigr)\bigr) \oplus \cdots \oplus \bigl(k[X]/\bigl(a_m(X)\bigr)\bigr),$$

then

$$(K \otimes_k V)_{K \otimes_k \phi} \cong \big(K[X]/\big(a_1(X)\big)\big) \oplus \cdots \oplus \big(K[X]/\big(a_m(X)\big)\big),$$

so that the invariants of ϕ are also the invariants of $K \otimes_k \phi$. □

We may as well speak of the *invariant polynomials of a square matrix*, and the above results may be reformulated as follows.

Corollary 2.222 *Let $M, M' \in \mathrm{Mat}_n(k)$. The following assertions are equivalent.*

(i) *M and M' have the same invariants.*
(ii) *M and M' are similar* (*i.e., there exists an invertible matrix $U \in \mathrm{GL}_n(k)$ such that $M' = UMU^{-1}$*).

A reformulation of Corollary 2.221 is that similarity between matrices is an absolute property (that is, it is independent of the base field), in the following sense.

Corollary 2.223 *Let k be a field and let K be a field extension of k. Let $M, M' \in \mathrm{Mat}_n(k)$. The following assertions are equivalent.*

(i) *M and M' are similar in $\mathrm{Mat}_n(k)$.*
(ii) *M and M' are similar in $\mathrm{Mat}_n(K)$.*

Proof It is an immediate consequence of the fact that the invariants of an element $M \in \mathrm{Mat}_n(k)$ are the invariants of M viewed as an element of $\mathrm{Mat}_n(K)$. □

2.3.5.3 Completely Reducible Endomorphisms

The following proposition-definition is an immediate application of Proposition 2.205.

Proposition–Definition 2.224 *Let ϕ be an endomorphism of a finite dimensional k-vector space V. The following properties are equivalent*:

(i) *the minimal polynomial of ϕ is not divisible by a square in $k[X]$,*
(ii) *whenever W is a subspace of V stable under ϕ, there is a complement of W in V which is stable under ϕ.*

In that case, we say that ϕ is completely reducible, or semisimple.

The proof of the next proposition is left as an exercise for the reader.

Proposition 2.225 *Let ϕ be an endomorphism of a finite dimensional k-vector space V. The following properties are equivalent*:

(i) *ϕ is diagonalizable,*

(ii) *ϕ is semisimple and its characteristic polynomial is a product of degree* 1 *factors over k.*

Examples 2.226

(1) Let V be a finite dimensional $\mathbb{R}$-vector space endowed with a Euclidean scalar product $(x, y) \mapsto \langle x, y\rangle$. Let ϕ be an endomorphism of V. The *adjoint endomorphism* ϕ^{ad} is defined by the condition

$$\big\langle \phi(x), y\big\rangle = \big\langle x, \phi^{\mathrm{ad}}(y)\big\rangle \quad \text{for all } x, y \in V.$$

One says that ϕ is *normal* if it commutes with its adjoint ϕ^{ad}.

Assume ϕ is normal. Exercise:

(a) Prove that ϕ is completely reducible.

HINT. Prove that if W is a ϕ-stable subspace of V, then its orthogonal $W^{\perp}$ is a ϕ-stable complement of W.

(b) Prove that there exists an orthonormal basis of V over which the matrix of ϕ is

$$\begin{pmatrix}
\lambda_1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & \cdots & \lambda_m & 0 & 0 & \cdots & 0 & 0 \\
0 & 0 & \cdots & 0 & a_1 & -b_1 & \cdots & 0 & 0 \\
0 & 0 & \cdots & 0 & b_1 & a_1 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & a_n & -b_n \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & b_n & a_n
\end{pmatrix}$$

(2) Exercise: State and prove analogous results where V is replaced by a finite dimensional $\mathbb{C}$-vector space endowed with a Hermitian scalar product.

More Exercises on Sect. 2.3

Exercise 2.227 Let $M = \mathbb{Z}^2$, and let N be the cyclic $\mathbb{Z}$-submodule of M generated by $(21, 77)$. Describe M/N.

Exercise 2.228 Let R be a Dedekind domain with only a finite number of prime ideals. Prove that R is a principal ideal domain.

Exercise 2.229 Let R be a Dedekind domain.

• We denote by $M = \bigoplus_{i=1}^{r} E_i$ a finitely generated projective R-module, where each E_i is a projective R-module of rank 1. We assume $E_i = \mathfrak{a}_i e_i$ for some $e_i \in M$

and some integral ideal $\mathfrak{a}_i$, so that

$$M \subset E := \bigoplus_{i=1}^{r} Re_i,$$

where E is a free module.

• Whenever X is a rank one submodule of M, we denote by $M^*(X)$ the ideal of R generated by $\{\varphi(m) \mid m \in X, \varphi \in M^*\}$. We assume $X = \mathfrak{a}x$ for some $x \in M$ and some fractional ideal $\mathfrak{a}$. We write $x = \lambda_1 e_1 + \cdots + \lambda_r e_r$ where $\lambda_i \in \mathfrak{a}_i$. The set $\{\varphi(x) \mid \varphi \in M^*\}$ is an ideal of R denoted by $M^*(x)$.

(1) Prove that

(a) $M^*(X) = \mathfrak{a}M^*(x)$ and $M^*(X) = R$ if and only if $M^*(x) = \mathfrak{a}^*$.
(b) $M^*(x) = \lambda_1\mathfrak{a}_1^* + \cdots + \lambda_r\mathfrak{a}_r^*$ so $M^*(X) = \lambda_1\mathfrak{a}\mathfrak{a}_1^* + \cdots + \lambda_r\mathfrak{a}\mathfrak{a}_r^*$.

(2) Let $\mathfrak{d}$ be an ideal of R. Prove that the following assertions are equivalent:

(i) $M^*(X) \subset \mathfrak{d}$, i.e., $\mathfrak{d}$ divides $M^*(X)$,
(ii) there exists a projective submodule Y of rank 1 of M such that $X = \mathfrak{d}Y$, i.e., $\mathfrak{d}$ divides X.

Exercise 2.230 Let R be a Dedekind domain, and let M_1, M_2, M be finitely generated torsion free R-modules.

(1) Assume that

$$M_1 \oplus M \cong M_2 \oplus M.$$

Prove that $M_1 \cong M_2$.

(2) Let

$$0 \to M_1 \to M \to M_2 \to 0$$

be a short exact sequence. Prove that

$$M \cong M_1 \oplus M_2 \quad \text{and} \quad \mathrm{St}(M) = \mathrm{St}(M_1)\,\mathrm{St}(M_2).$$

Exercise 2.231 An example of a finitely generated torsion module M, with two isomorphic submodules N_1 and N_2 such that $M/N_1 \not\cong M/N_2$

For R a ring, $\mathfrak{a}$ an ideal of R, and M an R-module, we set

$$\mathrm{Ann}_M(\mathfrak{a}) := \{m \in M \mid \mathfrak{a}m = 0\}.$$

Assume that R is a Dedekind domain, and let $\mathfrak{p}$ and $\mathfrak{q}$ be two distinct prime ideals of R. Define

$$M_1 := R/\mathfrak{p}^2, \qquad M_2 := R/\mathfrak{p}\mathfrak{q}, \qquad M := M_1 \oplus M_2.$$

(1) Describe $N_1 := \mathrm{Ann}_{M_1}(\mathfrak{p})$, $N_2 := \mathrm{Ann}_{M_2}(\mathfrak{p})$.

(2) Prove that $N_1 \cong N_2$.
(3) Check that $M/N_1 \ncong M/N_2$.

Exercise 2.232 Let M be a free $\mathbb{Z}$-module of rank $n \geq 1$, and let N be a submodule of M of the same rank.

(1) Prove that the quotient M/N is a finite group. Its order (the *index* of N in M) will be denoted by $|M : N|$.
(2) Let $(e_1, \ldots, e_n)$ be a basis of M and let $(f_1, \ldots, f_n)$ be a basis of N. Let us denote by $\det_{(e_1,\ldots,e_n)}(f_1, \ldots, f_n)$ the determinant of the matrix of coefficients of $(f_1, \ldots, f_n)$ expressed in terms of $(e_1, \ldots, e_n)$. Prove that

$$\det_{(e_1,\ldots,e_n)}(f_1, \ldots, f_n) = |M : N|.$$

Exercise 2.233

(1) Are the matrices

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

similar?

What are their minimal polynomials? What are their invariants?
(2) Are the matrices

$$\begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

similar ?

What are their minimal polynomials? What are their invariants?

Exercise 2.234 Let k be a field. Let $M(X)$ and $C(X)$ in $k[X]$. Give a necessary and sufficient condition for the existence of a square matrix α with entries in k such that $M(X)$ and $C(X)$ are respectively the minimal and the characteristic polynomial of α.

Exercise 2.235 Let k be a field and let $P(X) \in k[X]$.

Give a necessary and sufficient condition for the multiplication by X in the (finite dimensional) vector space $k[X]/(P(X))$ to induce a diagonalizable endomorphism.

Exercise 2.236 What are the polynomial invariants, the minimal polynomial, the characteristic polynomial, of the matrix

$$\begin{pmatrix} 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}?$$

Exercise 2.237 We denote by u an endomorphism of a finite dimensional k-vector space V.

(1) (a) Prove that there exists an integer N such that

- for $n < N$, $\ker u^n \subsetneq \ker u^{n+1}$
- for $n \geq N$, $\ker u^n = \ker u^{n+1}$.

(b) Prove that $\ker u^N \oplus \operatorname{im} u^N = V$.

(2) Let $P(X) \in k[X]$, and let $\Delta(X)$ denote the gcd of $P(X)$ and the minimal polynomial of u.

(a) Prove that $\ker P(u) = \ker(\Delta(u))$.

(b) Prove that $\dim \ker P(u) \geq \deg \Delta(X)$.

HINT: One may reduce to the case where $P(X)$ is a power of an irreducible polynomial, then apply (1) above.

Exercise 2.238 We denote by u an endomorphism of a finite dimensional k-vector space V, and by $a_1(X), \ldots, a_m(X)$ its family of invariant polynomials, that is

- $a_m(X) \mid \cdots \mid a_1(X)$,
- $V = k[u]e_1 \oplus k[u]e_2 \oplus \cdots \oplus k[u]e_m$, where, for all j $(1 \leq j \leq m)$, the map $k[X] \to k[u]e_j$, $P(X) \mapsto P(u)e_j$, induces an isomorphism $k[X]/(a_j(X)) \xrightarrow{\sim} k[u]e_j$.

For each j, we set $a_1(X) = a_j(X)r_j(X)$.

(1) Prove that for each j there is a unique endomorphism π_j of V such that

$$\pi_j : \begin{cases} x \mapsto x & \text{for all } x \in k[u]e_i \text{ if } i \neq j, \\ P(u)e_j \mapsto P(u)r_j(u)e_j & \text{for all } P(X) \in k[X]. \end{cases}$$

(2) Prove that π_j commutes with u.

(3) Let us denote by $\operatorname{BiCom}(u)$ the "bicommutant" of u, that is, the space of endomorphisms ϕ of V which commute with the endomorphisms which commute with u. We shall prove that $\operatorname{BiCom}(u) = k[u]$.

(1) Prove that for all j $(1 \leq j \leq m)$, there is $P_j(X) \in k[X]$ such that $\phi(e_j) = P_j(u)e_j$.
(2) Prove that for all j $(1 \leq j \leq m)$, $a_j(X) \mid (P_j(X) - P_1(X))$, and deduce that $\phi = P_1(u)$.

Exercise 2.239

(1) Let G be a finite Abelian group. Prove that, for all divisor d of the order $|G|$ of G, there exists a subgroup of G of order d.
(2) State and prove the analogous statement for V_ϕ (with the usual meaning of V_ϕ).
(3) State and prove the analogous general statement for a finitely generated torsion module over a Dedekind domain.

Exercise 2.240 Let k be a commutative field, let V be a k-vector space of finite dimension r. For ψ an endomorphism of V, we let $C_\psi(X)$ denote its characteristic polynomial.

Let $\phi \in \operatorname{End}(V)$ and let $P(X) \in k[X]$ be nonzero, monic and of degree d.

(1) We assume that, in a splitting field K of $C_\phi(X)$ over k, we have

$$C_\phi(X) = \prod_{j=1}^{r} (X - \lambda_j).$$

Prove that

$$C_{P(\phi)}(X) = \prod_{j=1}^{r} \big(X - P(\lambda_j)\big).$$

(2) Deduce that

$$\det\big(P(\phi)\big) = \operatorname{Res}_{r,d}\big(C_\phi(X), P(X)\big),$$

(3) and that

$$\det\big(C'_\phi(\phi)\big) = (-1)^{\binom{r}{2}} \operatorname{Disc}\big(C_\phi(X)\big).$$

2.4 Complement on Dedekind Domains

2.4.1 Characterizations of Dedekind Domains

Theorem 2.241 *Let R be an integral domain. The following assertions are equivalent.*

(i) *R is a Dedekind domain.*
(ii) *R satisfies the following three properties*:

(1) *R is Noetherian*,

(2) *all nonzero prime ideals of R are maximal*,

(3) *R is integrally closed.*

(iii) *R satisfies the following two properties*:

(1) *R is Noetherian*,

(2) *for each nonzero prime ideal $\mathfrak{p}$ of R, the ring $R_{\mathfrak{p}}$ is a local principal ideal domain.*

Proof • (i)⇒(ii):

(1) is obvious, since all the ideals of R are finitely generated.

(2) is Corollary 2.171.

(3) is Corollary 2.172.

• (ii)⇒(iii):

Only (iii)(2) has to be proven.

Let $\mathfrak{p} \in \operatorname{Spec}(R)$. Then (ii) implies

$(1)_{\mathfrak{p}}$: $R_{\mathfrak{p}}$ is Noetherian (since the localization of a Noetherian domain is Noetherian),

$(2)_{\mathfrak{p}}$: $R_{\mathfrak{p}}$ has only one nonzero prime ideal (indeed, the prime ideals of $R_{\mathfrak{p}}$ are of the form $\mathfrak{q}_{\mathfrak{p}} = \mathfrak{q}R_{\mathfrak{p}}$ where $\mathfrak{q}$ is a prime ideal of R contained in $\mathfrak{p}$, hence $\mathfrak{q} = \mathfrak{p}$),

$(3)_{\mathfrak{p}}$: $R_{\mathfrak{p}}$ is integrally closed (by Proposition 2.86).

Thus, in order to prove (ii)⇒(iii), it suffices to prove the following proposition.

Proposition 2.242 *Let R be a Noetherian integrally closed local domain with only one nonzero prime ideal. Then R is a principal ideal domain.*

Proof We shall use two lemmas.

Lemma 2.243 *Let R be an integrally closed Noetherian domain, with field of fractions F.*

Let $\mathfrak{b}$ be a nonzero fractional ideal and let $x \in F$. The following assertions are equivalent:

(i) $x\mathfrak{b} \subset \mathfrak{b}$,

(ii) $x \in R$.

Proof of Lemma 2.243 Only (i)⇒(ii) needs to be proved. Since $x\mathfrak{b} \subset \mathfrak{b}$, for all integer $n \geq 1$ we have $x^n\mathfrak{b} \subset \mathfrak{b}$, hence $R[x]\mathfrak{b} \subset \mathfrak{b}$. Choosing a nonzero element $b \in \mathfrak{b}$, the multiplication by b provides an R-module isomorphism $R[x] \xrightarrow{\sim} R[x]b$ and $R[x]b$ is a submodule of $\mathfrak{b}$. Since R is Noetherian, this shows that $R[x]$ is a finitely generated R-module, hence (Proposition 2.74) that x is integral over R, so $x \in R$ since R is integrally closed. □

Lemma 2.244 *Let R be a Noetherian local domain with only one nonzero prime ideal. Let $\mathfrak{a}$ be a proper nonzero ideal of R. Then $R \subsetneq \mathfrak{a}^*$.*

Proof of Lemma 2.244 Let $\mathfrak{p}$ be the unique nonzero prime ideal of R. Thus $\mathfrak{a} \subset \mathfrak{p}$. Let $a \in \mathfrak{a}$, $a \neq 0$. By Lemma 2.108 there exists an integer $n \geq 1$ (which we may, and do, assume to be minimal) such that $\mathfrak{p}^n \subset Ra$. Let $x \in \mathfrak{p}^{n-1}$ such that $x \notin Ra$ hence $xa^{-1} \notin R$.

We have

$$xa^{-1}\mathfrak{a} \subset a^{-1}x\mathfrak{p} \subset a^{-1}\mathfrak{p}^n \subset a^{-1}Ra = R,$$

which proves that $xa^{-1} \in \mathfrak{a}^*$ and so $\mathfrak{a}^* \neq R$. □

Now we prove Proposition 2.242.

Since R is local, it suffices to prove that every fractional ideal $\mathfrak{a}$ of R is a finitely generated projective R-module, i.e., that $\mathfrak{a}^*\mathfrak{a} = R$.

Let $\mathfrak{b} := \mathfrak{a}^*\mathfrak{a}$. We have $\mathfrak{b} \subset R$. Since $\mathfrak{b}\mathfrak{b}^* \subset R$, we have $\mathfrak{a}^*\mathfrak{b}^* \subset \mathfrak{a}^*$, which in turn (by Lemma 2.243) implies $\mathfrak{b}^* \subset R$. It follows then from Lemma 2.244 that $\mathfrak{b} = R$. □

- (iii)⇒(i): follows from Proposition 2.138. □

2.4.2 *Rings of Integers of Number Fields Are Dedekind*

2.4.2.1 Complements on Field Extensions in Characteristic Zero

The following result is, in a sense, an improvement of Corollary 1.77.

Proposition 2.245 *Let k be a characteristic zero field, and let K be a finite extension of k.*

Let L be a finite normal extension of k containing K.

Then there are $[K : k]$ distinct morphisms

$$\begin{tikzcd} K \arrow[rr] & & L \\ & k \arrow[ul] \arrow[ur] & \end{tikzcd}$$

from K into L which are trivial on k.

Proof As in Theorem 1.76, it is easier to prove a slightly more general result.

Proposition 2.246 *Assume given fields $k \subset K$ and $\widetilde{k} \subset \widetilde{K} \subset \widetilde{L}$ with a commutative diagram*

$$\begin{tikzcd}
 & \widetilde{L} \\
K \arrow[r, "\sim"] & \widetilde{K} \arrow[u] \\
k \arrow[u] \arrow[r, "\phi"] & \widetilde{k} \arrow[u]
\end{tikzcd}$$

and assume that $\widetilde{L}$ is a normal (finite) extension of $\widetilde{k}$.

Then if k has characteristic zero, there are exactly $[K : k]$ morphisms Φ from K into $\widetilde{L}$ which extend ϕ.

$$\begin{tikzcd}
 & \widetilde{L} \\
K \arrow[ur, "\Phi"] & \\
k \arrow[u] \arrow[r, "\phi"] & \widetilde{k} \arrow[uu]
\end{tikzcd}$$

Proof of Proposition 2.246 The proof is by induction on $[K : k]$.

If $[K : k] = 1$, the assertion is trivially true. So we assume $k \subsetneq K$ and we choose $x \in K \setminus k$. Let $M(X)$ be its minimal polynomial, of degree > 1. Set $\widetilde{M}(X) := \phi(M(X))$. The image of x in $\widetilde{K}$ under the given isomorphism $K \xrightarrow{\sim} \widetilde{K}$ is a root of $\widetilde{M}(X)$.

Since $\widetilde{L}$ is a normal extension of $\widetilde{k}$, it follows from the characterization of normal extensions (see Proposition 1.78) that $\widetilde{M}(X)$ splits into a product of degree one factors over $\widetilde{L}$.

Moreover, since all these fields have characteristic 0, we know by Proposition 1.184 that $\widetilde{M}(X)$ has exactly $\deg M(X) = [k(x) : k]$ distinct roots. Let us set $n := [k(x) : k]$ and let us denote by $y_1, \ldots, y_n$ the roots of $\widetilde{M}(X)$ in $\widetilde{L}$.

The receipe

$$\phi_j : k(x) \to \widetilde{L}, \qquad x \mapsto y_j,$$

induces a bijection between this set of roots and the set of morphisms $\phi_j : k(x) \to \widetilde{L}$ which extend ϕ.

$$\begin{tikzcd}
 & \widetilde{L} \\
K \arrow[ur, "\Phi"] & \\
k(x) \arrow[u] \arrow[r, "\phi_j"] & \widetilde{k}(y_j) \arrow[uu] \\
k \arrow[u] \arrow[r, "\phi"] & \widetilde{k} \arrow[u]
\end{tikzcd}$$

Now, by the induction hypothesis, for each $j = 1, \dots, n$ there are exactly $[K : k(x)]$ extensions of ϕ_j to a morphism $K \to \widetilde{L}$.

Since $[K : k] = [K : k(x)]n$, that proves Proposition 2.246. □

□

For K a finite extension of k, and for $x \in K$, we denote by

- $m_{K/k,x}$ the k-linear endomorphism of K defined by the multiplication by x,
- $\mathit{\Gamma}_{K/k,x}(X)$ the characteristic polynomial of $m_{K/k,x}$,
- $\mathrm{Tr}_{K/k}(x)$ the trace of $m_{K/k,x}$,
- $N_{K/k}(x)$ the determinant of $m_{K/k,x}$, called the *norm* of x relative to the extension K/k.

Proposition 2.247 *Let k be a field of characteristic zero, let K be a finite extension of k and let L be a normal extension of k which contains K. Let $\mathrm{Mor}_k(K, L)$ denote the set of all morphisms from K into L which induce the identity on k (thus $|\mathrm{Mor}_k(K, L)| = [K : k]$).*

Let $x \in K$. Then

(1) $\mathit{\Gamma}_{K/k,x}(X) = \prod_{\sigma \in \mathrm{Mor}_k(K,L)} (X - \sigma(x))$,
(2) $\mathrm{Tr}_{K/k}(x) = \sum_{\sigma \in \mathrm{Mor}_k(K,L)} \sigma(x)$,
(3) $N_{K/k}(x) = \prod_{\sigma \in \mathrm{Mor}_k(K,L)} \sigma(x)$.

Proof It is enough to prove (1).

Let $M_x(X)$ be the (monic) minimal polynomial of x over k. It is clear that $M_x(X)$ is also the minimal polynomial of the endomorphism $m_{K/k,x}$.

Lemma 2.248 *Let K be a finite extension of k and let $x \in K$. Then*

$$\mathit{\Gamma}_{K/k,x}(X) = M_x(X)^{[K:k(x)]}.$$

Proof of Lemma 2.248 If $(e_i)_{1\le i\le d}$ is a basis of K over $k(x)$, and if $(f_j)_{1\le j\le m}$ is a basis of $k(x)$ over k, then $(e_i f_j)_{1\le i\le d, 1\le j\le m}$ is a basis of K over k, and the matrix of the multiplication by x in that basis has the shape

$$\begin{pmatrix} M & 0 & \cdots & 0 \\ 0 & M & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ddots & M \end{pmatrix}$$

where M is the matrix of the k-linear endomorphism of $k(x)$ defined by the multiplication by x on the basis $(f_j)_{1\le j\le m}$.

It is an easy exercise (see Exercise 1.1!) to check that $M_x(X)$ is the characteristic polynomial of the multiplication by x in $k(x)$, since $k(x)\cong k[X]/(M_x(X))$. This proves Lemma 2.248. □

Let us set $[k(x):k]=:n$, and let us denote by $x_1, x_2, \ldots, x_n$ the n distinct roots of $M_x(X)$ in L.

For each $j=1,\ldots,n$, let $\phi_j : k(x) \xrightarrow{\sim} k(x_j)$ the isomorphism which sends x to x_j and induces the identity on k. By Proposition 2.246, we know that there exist exactly $[K:k(x)]$ morphisms $K\to L$ which extend ϕ_j. Let us denote by $\mathrm{Mor}_k(K,L)_j$ the set of such morphisms. Thus

$$\mathrm{Mor}_k(K,L) = \bigsqcup_{j=1}^{n} \mathrm{Mor}_k(K,L)_j ,$$

hence

$$\begin{aligned}\prod_{\sigma\in\mathrm{Mor}_k(K,L)} \big(X-\sigma(x)\big) &= \prod_{j=1}^{n} \prod_{\sigma\in\mathrm{Mor}_k(K,L)_j} \big(X-\sigma(x)\big) \\ &= \prod_{j=1}^{n} (X-x_j)^{[K:k(x)]} = M_x(X)^{[K:k(x)]} \\ &= \Gamma_{K/k,x}(X)\end{aligned}$$

by Lemma 2.248. □

Proposition 2.249 *Let k be a characteristic zero field and let K be a finite extension of k. The k-bilinear form on K*

$$K\times K\to k, \qquad (x,y)\mapsto \mathrm{Tr}_{K/k}(xy),$$

is non-degenerate.

Proof Let $(e_1, \dots, e_n)$ be a basis of K as k-vector space. We must check that $\det(\mathrm{Tr}_{K/k}(e_i e_j)) \neq 0$.

Let us choose a normal extension L of k which contains K (which is possible: why?). By Proposition 2.247, we know that

$$\mathrm{Tr}_{K/k}(e_i e_j) = \sum_{\sigma \in \mathrm{Mor}_k(K,L)} \sigma(e_i e_j) = \sum_{\sigma \in \mathrm{Mor}_k(K,L)} \sigma(e_i)\sigma(e_j),$$

which can be expressed as the following equality between matrices:

$$\big(\mathrm{Tr}_{K/k}(e_i e_j)\big)_{i,j} = \det\big(\sigma(e_j)\big)^2_{\sigma \in \mathrm{Mor}_k(K,L), 1 \leq j \leq n}.$$

So it suffices to prove that $\det(\sigma(e_j))_{\substack{\sigma \in \mathrm{Mor}_k(K,L) \\ 1 \leq j \leq n}} \neq 0$. If this is not the case, there is a dependence relation

$$\sum_{\sigma \in \mathrm{Mor}_k(K,L)} \lambda_\sigma \sigma(e_j) = 0 \quad \text{for all } j = 1, \dots n,$$

hence, since $(e_j)_{1 \leq j \leq n}$ is a basis of K over k,

$$\sum_{\sigma \in \mathrm{Mor}_k(K,L)} \lambda_\sigma \sigma = 0,$$

with $\lambda_\sigma \in L$, and the λ_σ's not all zero.

But that is a contradiction to the following lemma.

Lemma 2.250 (Dedekind lemma)

Let G be a group, let L be a field, and let (σ) be a finite family of distinct group morphisms from G to $L^\times$. Then the family (σ) is linearly independent over L.

Proof of Lemma 2.250 Assume that there is a dependence relation, and choose one where the number of nonzero coefficients is minimal. Write that relation

$$\lambda_1 \sigma_1 + \cdots + \lambda_m \sigma_m = 0.$$

Notice that at least two of the λ_j's are nonzero. For all $g, h \in G$, we have

$$\lambda_1\sigma_1(gh) + \cdots + \lambda_m\sigma_m(gh) = \lambda_1\sigma_1(g)\sigma_1(h) + \cdots + \lambda_m\sigma_m(g)\sigma_m(h) = 0.$$

Multiplying the equation $\lambda_1\sigma_1(g) + \cdots + \lambda_m\sigma_m(g) = 0$ by $\sigma(g)$ and subtracting from the preceding equation gives

$$\lambda_2\bigl(\sigma_1(h) - \sigma_2(h)\bigr)\sigma_2(g) + \cdots + \lambda_m\bigl(\sigma_1(h) - \sigma_m(h)\bigr)\sigma_m(g) = 0,$$

an equality which holds for all $g, h \in G$, hence in particular is equivalent to the relation

$$\lambda_2\bigl(\sigma_1(h) - \sigma_2(h)\bigr)\sigma_2 + \cdots + \lambda_m\bigl(\sigma_1(h) - \sigma_m(h)\bigr)\sigma_m = 0, \quad \text{for all } h \in G.$$

By the minimality of m, and since there is $j \geq 2$ such that $\lambda_j \neq 0$, we deduce that

$$\forall h \in G, \quad \sigma_1(h) = \sigma_j(h) \quad \text{hence} \quad \sigma_1 = \sigma_j,$$

a contradiction to the fact that the σ_j's are all distinct. □

□

2.4.2.2 On Integral Closures of Noetherian Rings

Let R be an integral domain, with field of fractions F. Let K be a finite field extension of F.

We shall see that many properties of R transfer to its integral closure in K, which we denote by R_K.

Proposition 2.251 *Assume R is a Noetherian domain.*

(1) *R_K is a finitely generated R-module,*
(2) *R_K is a Noetherian domain.*

Proof We use the following lemma.

Lemma 2.252 *There exists a basis $(e_j)_{1\leq j\leq n}$ of K as an F-vector space such that*

$$R_K \subset \bigoplus_{j=1}^{n} Re_j.$$

Proof of Lemma 2.252 By Proposition 2.87, we know that for each j there exists $\lambda_j \in R$, $\lambda_j \neq 0$, such that $\lambda_j x_j \in R_K$. We set $y_j := \lambda_j x_j$. By Proposition 2.249 above, there is a basis $(e_j)_{1\leq j\leq n}$ of K as an F-vector space such that $\mathrm{Tr}_{K/F}(y_i e_j) = \delta_{i,j}$. We shall check that

$$R_K \subset \bigoplus_{1\leq j\leq n} Re_j.$$

Let $x \in R_K$. We have $x = \sum_{j=1}^{n} \mathrm{Tr}_{K/F}(y_j x) e_j$. Since for all $j = 1, \dots, n$, we have $y_j \in R_K$, it follows that $y_j x \in R_K$, hence by Proposition 2.88 that $\mathrm{Tr}_{K/F}(y_j x) \in R$. □

Lemma 2.252 shows that R_K is an R-submodule of a finitely generated (free) R-module. Since R is Noetherian, it follows that R_K is a finitely generated R-module and a Noetherian ring. □

2.4.2.3 Integral Closures of Dedekind Domains

Theorem 2.253 *Let R be a Dedekind domain with field of fractions F. Let K be a finite field extension of F and let R_K be the integral closure of R in K.*

Then R_K is a Dedekind domain.

Proof We shall use the characterization of Dedekind domains given in Theorem 2.241, (ii).

(1) R_K is a Noetherian domain by the previous Proposition 2.251.

(2) We shall prove now that any nonzero prime ideal $\mathfrak{P}$ of R_K is maximal. Let $\mathfrak{p} := R \cap \mathfrak{P}$. Then $\mathfrak{p}$ is a prime ideal in R.

• Let us prove that $\mathfrak{p} \neq 0$. Let $x \in \mathfrak{P}$, $x \neq 0$. The multiplication by x induces an automorphism

$$m_x : K \to K, \qquad y \mapsto xy,$$

of the F-vector space K. We recall that $N_{K/F}(x)$ denotes the determinant of m_x (hence $N_{K/F}(x) \neq 0$), and $C(X)$ its characteristic polynomial. By the Cayley–Hamilton theorem, we have $C(x) = 0$, which implies that $N_{K/F}(x)$ belongs to the principal ideal generated by x, hence belongs to $\mathfrak{P}$.

Moreover, by Proposition 2.88, we know that $N_{K/F}(x) \in R$.

Thus $N_{K/F}(x)$ is a nonzero element of $R \cap \mathfrak{P} = \mathfrak{p}$, which proves that $\mathfrak{p} \neq 0$.

• Since R is a Dedekind domain and $\mathfrak{p} \neq 0$, $\mathfrak{p}$ is a maximal ideal of R. Now $R_K/\mathfrak{P}$ is a finitely generated $R/\mathfrak{p}$-vector space. It follows for example from Proposition 2.83 that $R_K/\mathfrak{P}$ is also a field, hence that $\mathfrak{P}$ is a maximal ideal of R_K.

(3) It remains to prove that R_K is integrally closed. This follows from Proposition 2.87. □

ERRATUM

Erratum to: Rings and Polynomial Algebras

Erratum to: M. Broué, *Rings and Polynomial Algebras*, pp. 1–85
DOI 10.1007/978-3-642-41269-1_1
© Springer-Verlag Berlin Heidelberg 2014

Theorem 1.158 page 51 must be replaced by the following statement:

Theorem 1.158

(1) *For $d \geq 1$ not divisible by a square, the ring of integers of $\mathbb{Q}[\sqrt{-d}]$ $(d > 0)$ is a principal ideal domain if and only if*

$$d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

(2) *For $d \geq 1$ not divisible by a square, the ring of integers of $\mathbb{Q}[\sqrt{-d}]$ $(d > 0)$ is a Euclidean ring if and only if*

$$d \in \{1, 2, 3, 7, 11\},$$

and it is Euclidean for the map $N(a + b\sqrt{-d}) := a^2 + db^2$.

(3) *For $m \in \mathbb{Z} \setminus \{0\}$, m not divisible by a square, the ring of integers of $\mathbb{Q}[\sqrt{m}]$ is Euclidean for the map $N(a + b\sqrt{m}) := |a^2 - mb^2|$ if and only if*

$$m \in \{-1, \pm 2, \pm 3, 5, 6, \pm 7, \pm 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

There are other quadratic real extensions of $\mathbb{Q}$ whose ring of integers is Euclidean, but not for the function N defined above.

The online version of the original chapter can be found at doi: 10.1007/978-3-642-41269-1_1.

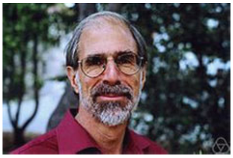
M. Broué, *Some Topics in Algebra*, Mathematical Lectures from Peking University,
DOI 10.1007/978-3-642-41269-1_3, © Springer-Verlag Berlin Heidelberg 2014

References

1. Atiyah, M., MacDonald, I.G.: Introduction to Commutative Algebra. Addison–Wesley, Reading (1969)

2. Bourbaki, N.: Commutative Algebra. Springer, Berlin (2006), Chaps. 5–7
3. Cohen, H.: Advanced Topics in Computational Number Theory. Graduate Texts in Mathematics, vol. 193. Springer, Berlin (2000)

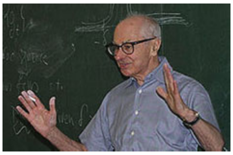
4. Eisenbud, D.: Commutative Algebra with a View Toward Algebraic Geometry. Graduate Texts in Mathematics, vol. 150. Springer, Berlin (1999)



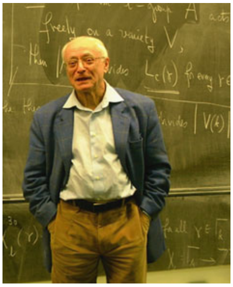
5. Jacobson, N.: Basic Algebra II. Freeman, San Francisco (1980)

M. Broué, *Some Topics in Algebra*, Mathematical Lectures from Peking University,
DOI 10.1007/978-3-642-41269-1, © Springer-Verlag Berlin Heidelberg 2014

6. Lang, S.: Algebra. Graduate Texts in Mathematics, vol. 211. Springer, Berlin (2002). Revised Third edn.



7. Samuel, P.: In: Algebraic Theory of Numbers. Dover Books in Mathematics (2008)
8. Serre, J.-P.: Faisceaux algébriques cohérents. Ann. Math. **61**(2), 197–278 (1955)



9. Serre, J.-P.: Local Fields. Graduate Texts in Mathematics, vol. 67. Springer, Berlin (1979)
10. Serre, J.-P.: Lectures on $N_X(p)$. Lectures at NCTS Taiwan (2012)

Index

A

$\mathfrak{a}\mathfrak{b}$, 12

$\mathfrak{a}^{-1}$, 151

$\mathrm{Ann}_R(E)$, 97

$\mathrm{Ann}_R(m)$, 96

A^{op}, 4

$\mathfrak{a}^{(\mathfrak{p})}$, 154

$\mathfrak{a}+\mathfrak{b}$, 12

$\mathfrak{a}^{(\mathfrak{p}')}$, 154

$A^{\times}$, 2

$A[X]$, 4

$A[\![X]\!]$, 5

Algebra, 15

Algebraic element, 16, 119

Algebraic extension, 119

Algebraically closed field, 22

Antisymmetric polynomial, 76

Associated elements, 47

B

Basis, 99

C

$\mathrm{Com}(N)$, 8

$c(P)$, 58

Center of a ring, 3

Characteristic ideal, 164

Chinese lemma, 14

Class group, 156

Complement of a submodule, 95

Completely reducible module, 168

Content, 58

Coprime fractional ideals, 153

$\mathrm{Coprod}(M_i)$, 102

Coproduct of modules, 102

Cyclic module, 91

Cyclotomic polynomial, 18

D

$\deg(P)$, 5

Discr $P(X)$, 82

Dedekind domain, 149

Degree of a nonzero polynomial, 5

Derivative, 9

Diagram chasing, 132

Direct sum, 102

Discrete valuation ring, 150

Discriminant, 82

Divisibility in Dedekind domains, 151

Division ring, 2

Dual morphism, 88

Dual of a module, 88

E

$\exp(G)$, 179

Eisenstein criterion, 61

Elementary symmetric polynomials, 73

Elementary tensors, 105

Euclidean ring, 49

Euler function, 18

Evaluation morphism, 11, 68

Exact sequence, 94

Exponent (of a group), 179

F

$\mathrm{Frac}(R)$, 43

Factorial ring, 48

Field, 2

Field extension, 21

Field of fractions, 42

Field to rational fractions in X, 43

Finite extension, 21

Finite ring extension, 118

Finitely generated R-algebra, 118

Finitely presented module, 132

M. Broué, *Some Topics in Algebra*, Mathematical Lectures from Peking University,
DOI 10.1007/978-3-642-41269-1, © Springer-Verlag Berlin Heidelberg 2014

$\mathbb{F}_q$, 29
Fractional ideal, 147
Fractional module, 147
Free module, 99
Free system, 99
Frobenius endomorphism, 10

G
Gauß's Lemma, 48
Gcd, 51
Generalized Jordan blocks, 178
Generated by $\varOmega$: $\langle \varOmega \rangle$, 90
Generator, 99
Generic matrix, 66
Generic polynomial, 73

H
$\mathrm{Hom}_R^{\mathrm{pr}}(X, Y)$, 139
$\mathrm{Hom}_R(\phi, X)$, 108
$\mathrm{Hom}_R(X, \phi)$, 108
$\mathbb{H}(R)$, 31
Hilbert's Basis Theorem, 129
Hilbert's Nullstellensatz, 125
$\mathrm{Hom}_R(\cdot, \cdot)$ is left exact, 109

I
Ideal, 12
Ideal generated by, 12
Ideal group, 151
Indecomposable module, 92
Infinite extension, 21
Integral, 116
Integral closure, 118
Integral domain, 2
Integral fractional ideal, 151
Integral over, 118
Integrally closed, 118
Invariant polynomials of a matrix, 181
Invariants, 164, 169
Invariants of M' in M, 169
Invertible fractional ideal, 151
Irr R, 55
Irreducible element, 48
Irreducible module, 167

J
Jacobson rings, 122
Jordan block, 177

K
$k[x]$, 16
$k(x)$, 22
$[K : k]$, 21

L
Laurent series, 45
Lcm, 51
Left ideal, 12
Legendre symbol, 35
Local commutative ring, 40
Local properties, 112
Localization of a ring, 44

M
$\mathrm{Mat}_n(R)$, 2
$M_{\mathfrak{p}}$, 147
M^*, 88
$\boldsymbol{\mu}(\mathbb{C})$, 17
$\boldsymbol{\mu}_n$, 17
$\mu(n)$, 33
Maximal ideal, 36
Maximal spectrum, 36
Minimal ideal, 164
Minimal polynomial, 16
Minimal polynomial of ϕ at v, 179
Möbius function, 33
Morphism of R-modules, 88
Multiple root, 9

N
$\mathrm{Nil\,Rad}(R)$, 39
$N_{K/k}(x)$, 190
$(\frac{n}{p})$, 35
Nilradical of a ring, 39
Noetherian module, 127
Noetherian ring, 129
Norm (for a field extension), 190
Normal extension, 28

O
Opposite ring, 4

P
$\varphi(n)$, 18
$\varPhi_n(X)$, 18
ϕ^*, 88
Prim $R[X]$, 54
$\mathrm{Prod}(M_i)$, 102
$\mathrm{pr}(P)$, 58
Polynomial function, 11, 68
Power series, 5
$\mathfrak{p}$-primary component, 159
Primary component, 159
Primary module, 160
Prime ideal, 36
Prime subfield, 44
Prime subring, 3
Primitive part, 58
Primitive polynomial, 54

Principal ideal, 12
Product of modules, 102
Projective module, 101
Projective morphism, 139
Proper, viii
Pseudo basis, 156
Pseudo basis adapted to (a submodule), 169

Q
Quadratic reciprocity, 80

R
Rad(R), 39
Res$_{m,n}(P, Q)$, 77
$R_{\mathfrak{p}}$, 45
$R((X))$, 45
Radical of a ring, 39
Radical of an ideal, 126
Rank of a finitely generated projective module, 146
Rank of a finitely generated torsion free module, 146
Rank of a projective module, 146
Reciprocity formula, 78
Relatively prime elements, 48
Relatively prime fractional ideals, 153
Remarkable identity, 66
Resultant, 77
Right ideal, 12
Ring, 1
Ring of integers, 50
Rings of quaternions, 31
R-module morphism, 88

S
$\Sigma_j(X)$, 73
$S^{-1}R$, 44
$S^{-1}M$, 110
$\mathfrak{S}_n$, 71
Spec(R), 36
Spec$_{\max}(R)$, 36
Spec$^*(R)$, 122
Short exact sequence, 94
Signature, 75
Similar matrices, 181
Spectrum, 36
Split exact sequence, 104
Splitting field, 25
Steinitz class, 157
Subalgebra, 16
Submodule generated by, 90
Subring, 2
Subring generated by, 3
Summand, 95
Symmetric polynomial, 72
Symmetric rational fractions, 75

T
tor(M), 97
Tr$_{K/k}(x)$, 190
$(\cdot \otimes_R \cdot)$ is right exact, 110
Tensor product, 105
Torsion element, 97
Torsion free, 97
Torsion free module, 98
Torsion module, 98
Torsion submodule, 98
Transcendental element, 16
Transpose, 109

U
UFD, 48
Unique factorization domain, 48
Units, 2

V
val(P), 5
Valuation at a prime, 153
Valuation of a nonzero polynomial, 5

Z
$Z(A)$, 3
$\mathbb{Z}_{(p)}$, 45