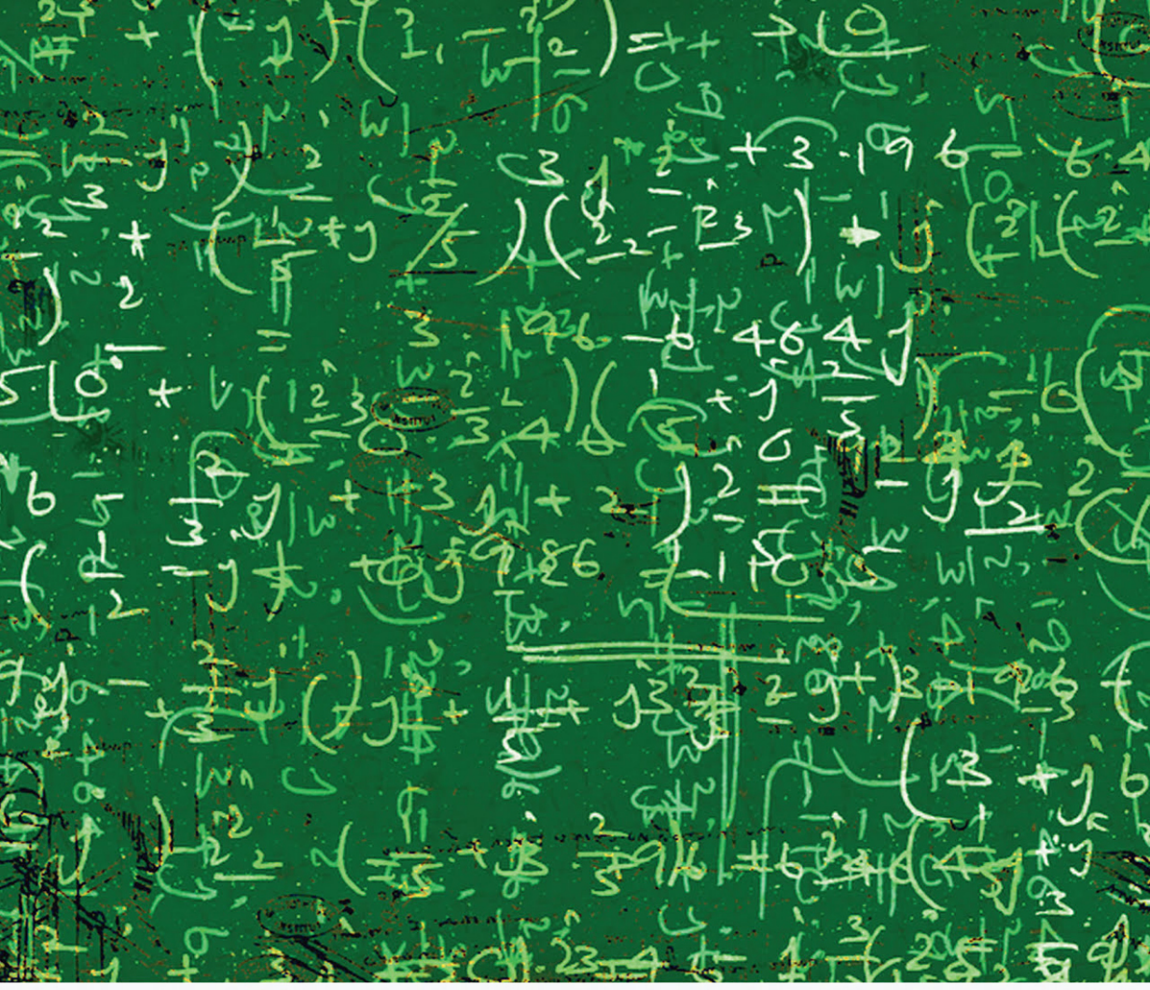


Fundamentals of Advanced Mathematics 1

Henri Bourlès

Categories, Algebraic Structures, Linear and Homological Algebra

iSTE PRESS

ELSEVIER

Fundamentals of Advanced Mathematics 1

New Mathematical Methods, Systems and Applications Set

coordinated by
Henri Bourlès

Fundamentals of Advanced Mathematics 1

Categories, Algebraic Structures, Linear and Homological Algebra

Henri Bourlès

iSTE PRESS

ELSEVIER

O récompense après une pensée.
Qu'un long regard sur le calme des dieux!

Paul VALÉRY

"When thought has had its hour, oh how rewarding
are the long vistas of celestial calm".

(Translation by Cecil DAY-LEWIS)

First published 2017 in Great Britain and the United States by ISTE Press Ltd and Elsevier Ltd

ISTE Press Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

Elsevier Ltd
The Boulevard, Langford Lane
Kidlington, Oxford, OX5 1GB
UK

www.elsevier.com

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
Library of Congress Cataloging in Publication Data
A catalog record for this book is available from the Library of Congress
ISBN 978-1-78548-173-4

Printed and bound in the UK and US

Preface

The objective of this Précis in three volumes, of which this is the first, is to present the mathematical objects that make up the "foundation" of certain methods, not only from modern Systems Theory, but also from Mathematics, Physics and many fields of Engineering. Viewed from this perspective, these mathematical concepts are "fundamental". They are "advanced" because they assume that the reader has mastered the most important parts of a Mathematics degree or the mathematical content taught in most advanced engineering courses. The reference works, *Algebra* by R. Godement [GOD 64] and *Foundations of Modern Analysis* by J. Dieudonné (first volume of his *Treatise on Analysis* [DIE 82]), together with a few notions of measure theory and integration [MAC 14], are amply sufficient as prerequisites. The original plan was only to write one single volume, and so this work could never have become an encyclopedia of mathematics. Such an endeavor would have exceeded the skills of the author by far, even excluding all mathematics discovered (or invented, according to your epistemological preference) during the last 50 years, as we shall do below - with a few exceptions. Presenting this more recent material would require too technical of a discussion. Moreover, one such encyclopedia already exists, at least in part. Although it does not cover every topic discussed between these pages, *Éléments de mathématique* by N. Bourbaki presents a great many others - this work represents a monumental milestone that we shall refer to abundantly. Nevertheless, it quickly became apparent that this Précis could not limit itself to being a simple formula booklet or collection of results (as had originally been imagined by the author), which would have been incapable of conveying any *understanding*. Hence, the decision was made to construct a coherent

presentation without attempting to prove *everything* in the usual manner of a Treatise. Long proofs are omitted, especially when they do not aid comprehension (at least in the opinion of the author) or where they exceed the scope of the discussion. Some results are simply justified by examples. Whenever a proof is omitted, a reference is given (chosen to be as accessible as possible). A number of easy proofs are given as **exercises**. Others, slightly more difficult but nonetheless within the reach of any reader (assuming pencil and paper at hand), are given as "starred exercises" (written as **exercise*** and supplemented by a reference). For some ideas, we refer to well-written Wikipedia articles (although we can only guarantee the quality of the French pages). Each volume is divided into chapters, paragraphs and items; section 3.2.4 is the fourth item of the second paragraph of the third chapter. To simplify these references, larger items are subdivided into smaller ones labeled by Roman numerals in parentheses. Throughout this Précis, the three volumes are respectively labeled by [P1], [P2] and [P3].

This volume begins with Category Theory (section 1.1). Considering the crucial role played by set theory, a few additional explanations are given (in a non-Bourbakian approach[1]) for the Zermelo-Fraenkel theory and the axiom of choice, as well as for the theory of ordinals and cardinals, used later to reason by transfinite induction and for cardinal arithmetic. Chapter 2 gives a fairly classical presentation of general algebraic structures (monoids, groups, rings, etc.) and a classification of rings according to the properties of their ideals (simple rings, Artinian rings, Noetherian rings, Bézout rings, unique factorization domains, principal ideal domains, etc.). Chapter 3, which goes into more detail, presents modules and algebras (the latter are a special case of the former). For the most part, the modules that we shall consider are defined over non-commutative rings. This is mostly because linear differential equations with variable coefficients are modeled using differential operators that do not commute (theory of $\mathcal{D}$-modules [KAS 95], [BJÖ 79], [MAI 93], [COU 95]). Mathematically, the non-commutative case includes the commutative case, and so we won't deprive ourselves of the opportunity to explore a few notions of Commutative Algebra (localization, primary decomposition, *Nullstellensatz*, etc.), noting their significance for Number

1 For Bourbaki, we might say that: "In the beginning there was Hilbert's operator", as discussed in [BKI 70] (Chap. I, section 1.1). This perspective is controversial: see section 1.1.2 [FRO 83] and (more polemically) [MAT 92].

Theory and Algebraic Geometry (sections 3.2.2 and 3.2.7). Finally, some fundamental concepts of Homological Algebra are presented (cogenerators and injective modules, complex modules, homotopy, derived functors, etc.), which will allow us to mention Algebraic Topology (section 3.3.8). The limited scope of this Précis prevents us from studying derived functors within the more general context of derived categories (see [GEL 03] or [KAS 06]). This volume ends with the non-commutative theory of invariant factors and the rational canonical form of matrices, as well as the (commutative) theory of elementary divisors and Jordan normal form; the final result is the structure theorem for modules over Dedekind domains. These notions from Homological Algebra and these structure theorems are essential in Algebraic Analysis (analytico-algebraic systems theory[2] of ordinary or partial linear differential equations), which has a great deal of overlap and contact with the methods of Algebraic Geometry (as well as the links with the $\mathcal{D}$-module theory mentioned above, see also [EHR 70], [PAL 70]). The elementary case of systems of ordinary linear differential equations with constant coefficients is discussed in section 3.4.4.

Henri BOURLÈS
April 2017

2 Here, we use the mathematical meaning of the term "system". In the field of automatic control, the existence of *concrete examples* of "multidimensional systems" (without boundary conditions and with distributed control variables) is not given and has been repeatedly reaffirmed, refuted and generally the subject of much controversy since 1990.

List of Notations

Standard notation

$:=$: equal by definition

$\mathbb{N}$: set of non-negative integers $\{0, 1, 2, ...\}$

$\mathbb{N}^{\times}$: set of natural integers $\{1, 2, ...\}$

$\mathbb{Z}$: set of relative integers $\{... - 2, -1, 0, 1, 2, ...\}$

$\mathbb{Q}$: set of rational numbers

$\mathbb{R}$: set of real numbers

$\bar{\mathbb{R}}$: extended real line $\mathbb{R} \cup \{-\infty, +\infty\}$ with $\forall x \in \mathbb{R}$:

$$-\infty < x < +\infty, x + (\pm\infty) = \pm\infty, (\pm\infty) + (\pm\infty) = \pm\infty,$$

$$1/(\pm\infty) = 0, x(\pm\infty) = \pm\infty \text{ if } x > 0$$

$\mathbb{R}_+$ and $\bar{\mathbb{R}}_+$: $\{x \in \mathbb{R} : x \geq 0\}$ and $\left\{x \in \bar{\mathbb{R}} : x \geq 0\right\}$

$\mathbb{C}$: set of complex numbers

$\bar{\mathbb{Z}}$: $\mathbb{Z} \cup \{-\infty, +\infty\}$ (same conventions as $\bar{\mathbb{R}}$)

$\mathfrak{P}(X)$: set of subsets of the set X

$\mathfrak{P}_f(X)$: set of finite subsets of the set X

$A - B = \complement_A B$: complement of B in A ($B \subset A$)

$\cup, \cap$: union, intersection

$\leq, \geq$: order relation, dual order relation

$<$: strict order relation

$\subset$, $\subsetneq$: inclusion, strict inclusion

$\mathrm{id}_X = 1_X$: identity mapping of X

can: canonical morphism

mod.: modulo

$f|_A$: restriction of $f : X \to Y$ to $A \subset Y$

δ_i^j: Kronecker delta ($\delta_i^j = 1$ if $i = j$, 0 otherwise)

$\det$: determinant

Tr: trace

I_n: $n \times n$ identity matrix

A^T: transpose of the matrix A

Categories (section 1.1)

$\mathrm{Ob}(\mathcal{C})$, $\mathrm{Mor}(\mathcal{C})$: class of objects, morphisms of the category $\mathcal{C}$, pp. 1–2

$\mathrm{Hom}_{\mathcal{C}}(X, Y)$: set of $\mathcal{C}$-morphisms from X to Y, p. 2

$\mathbf{Set}$, $\mathbf{Top}$: category of sets, topological spaces, p. 2

$\mathbf{Mon}$, $\mathbf{Grp}$, $\mathbf{Rng}$: category of monoids, groups, rings, p. 2

${}_{\mathbf{K}}\mathbf{Vec}$: category of left vector spaces over the division ring $\mathbf{K}$, p. 2

Functors (section 1.2)

$\mathbf{Ab}$: category of abelian groups, p. 14

$\mathbf{ComRng}$: category of commutative rings, p. 14

$\mathrm{Hom}\,(\mathcal{C},\mathcal{D})$: category of functors $\mathcal{C}\to\mathcal{D}$, p. 14

$\mathbf{t}:\mathfrak{F}\dot{\to}\mathfrak{G}$: functorial morphism, p. 15

$\mathbf{t}:\mathfrak{F}\tilde{\to}\mathfrak{G}$: functorial isomorphism, p. 15

$\mathfrak{F}\cong\mathfrak{G}$: isomorphic functors, p. 15

$\mathbf{j}_X=\mathrm{Hom}_{\mathcal{C}}\,(X,-)\,,\quad \mathbf{h}_Y=\mathrm{Hom}_{\mathcal{C}}\,(-,Y)$, p. 15

$\mathcal{C}^{\vee}=\mathrm{Hom}\,(\mathcal{C},\mathbf{Set})^{\mathrm{op}}\,,\mathcal{C}^{\wedge}=\mathrm{Hom}\,(\mathcal{C}^{\mathrm{op}},\mathbf{Set})$, p. 18

$\mathrm{pr}_i:\prod_{i\in I}X_i\to X_i$: canonical projection, p. 19

$X^I,X^{(I)}$: power, copower, p. 19

$\mathrm{inj}_i:X_i\to\coprod_{i\in I}X_i$: canonical injection, p. 19

$\biguplus_{i\in I}X_i$: disjoint union, p. 20

$X_1\times_Z X_2, X_1\coprod_Z X_2$: fibered product, fibered sum, p. 21

$\varinjlim X_i,\varprojlim Y_i$: inductive limit, projective limit, p. 22

Structures (section 1.3)

$(\mathcal{C},|.|\,,\mathcal{X})$: concrete category, p. 28

$|.|:\mathcal{C}\to\mathcal{X}$: forgetful functor, p. 28

$A\subseteq B$: subobject in a concrete category, p. 28

$A\subsetneq B$: proper subobject, p. 28

Monoids and ordered sets (section 2.1)

$\mathbf{U}(\mathbf{M})$: set of units of $\mathbf{M}$, p. 34

$\mathbf{M}^{\times}$: set of non-zero elements of $\mathbf{M}$, p. 34

$[S], [x_1, ..., x_n]$: monoid generated by S, generated by the elements $x_1, ..., x_n$, p. 34

$a \mid b, a \parallel b$: divisor, total divisor, pp. 35–36

$[a, b]$: interval, p. 36

$\bigwedge_{i \in I} a_i = \inf \{a_i : i \in I\}, \quad \bigvee_{i \in I} a_i = \sup \{a_i : i \in I\}$, p. 36

$x \mapsto x^{\perp}$: Galois connection, p. 36

$|C|, |P|$: length of the chain C, of the ordered set P, p. 37

$\mathfrak{d}(x), \mathfrak{h}(x)$: depth, height of x, p. 37

Groups (section 2.2)

$\mathfrak{S}_E, \mathfrak{S}_n$: symmetric group, p. 41

xH, Hx: left, right coset of x mod H, p. 41

$G/H, G\backslash H$: set of left cosets, right cosets mod H $(H \subseteq G)$, p. 41

$(G : 1)$: order of the group G, p. 41

$(G : H)$: index of H in G, p. 41

$\omega(g)$: order of $g \in G$, p. 41

$\varepsilon(G)$: exponent of the group G, p. 41

$N_G(H)$: normalizer of H, p. 41

$\divideontimes_{i \in I} G_i$: free product of the family of groups (G_i), p. 42

$F(I)$: free group on I, p. 42

Rings and algebras (section 2.3)

Additional concepts from linear algebra (section 3.1)

$R \in \mathbf{A}^{Q\times(K)}$: matrix of rows with finite support, p. 91

$\mathrm{rk}_{\mathbf{R}}(E)$: rank of the free $\mathbf{R}$-module E, p. 92

$R \sim R'$: equivalent matrices, p. 92

$\sim_l, \sim_r$: left-equivalence, right-equivalence of matrices, p. 92

$\dim_{\mathbf{K}}(V)$: dimension of the $\mathbf{K}$-vector space V, p. 93

$A \bigotimes_{\mathbf{R}} B$: tensor product, p. 97

$s \otimes t$: tensor product of linear mappings, p. 98

${}^{s}\bigotimes_{i\in I} \mathbf{A}_i$: skew tensor product, pp. 100–101

ρ^*, ρ_*: extension, restriction of the ring of scalars, p. 102

$\hat{\mathbf{R}}, \hat{M}$: $\mathfrak{m}$-adic completion, pp. 107–108

$S^{-1}\mathbf{A}, \mathbf{A}S^{-1}$: ring of left fractions, right fractions, p. 110

$\mathcal{T}_S(M)$: S-torsion submodule of M, p. 111

$\mathrm{Q}(\mathbf{A})$: field of fractions of $\mathbf{A}$, p. 112

$\mathbf{K}\left((X_i)_{i\in I}\right)$: field of rational functions, p. 112

$\mathbf{K}((X))$: field of Laurent series, p. 112

$\mathcal{T}(M)$: torsion submodule of M, p. 112

$\mathrm{rk}_{\mathbf{A}}(M)$: rank of an $\mathbf{A}$-module M, p. 113

$\mathrm{rk}(f)$: rank of an $\mathbf{A}$-homomorphism f, p. 113

$\mathbf{K}[X;\sigma,\delta], \mathbf{K}[X;\delta], \mathbf{K}[X;\sigma]$: ring of skew polynomials, p. 119

$\mathbf{K}\left[Y, Y^{-1};\sigma\right]$: ring of skew Laurent polynomials, p. 121

$A_1(\mathbf{k}), A_1'(\mathbf{k}), B_1(\mathbf{k})$, p. 121

Notions of Commutative Algebra (section 3.2)

$\mathbf{A}_{\mathfrak{p}}$: local ring of $\mathfrak{p}$, p. 122

$\kappa(\mathfrak{p})$: residue field of $\mathbf{A}_{\mathfrak{p}}$, p. 122

$\mathcal{Z}_A(\mathbf{K})$: zero set of A in $\mathbf{K}$, p. 125

$\tilde{x}$: Gelfand transform of x, p. 125

$\mathbb{Z}_p$: ring of p-adic integers, p. 127

$\mathbb{Q}_p$: field of p-adic numbers, p. 127

Γ, Γ_∞: order of a valuation, $\Gamma \bigcup \{+\infty\}$, p. 127

$\mathrm{Supp}(M)$: support of the module M, p. 128

$\mathrm{Ass}(M)$: set of prime ideals associated with M, p. 129

$\dim(X)$: Krull dimension, p. 143

$\mathbb{A}^n_{\mathbf{k}}$: affine space of dimension n over $\mathbf{k}$, p. 146

$\mathfrak{I}(E)$: ideal of the algebraic set E, p. 146

$\Gamma(E)$: algebra of regular functions over the algebraic set E, p. 148

$\mathbf{AlSet}$: category of algebraic sets, p. 148

Homological notions (section 3.3)

$E(M)$: injective envelope of the module M, p. 153

$C^\infty(\Omega)$: space of infinitely differentiable functions on Ω, p. 155

$[x, y]$: interval with endpoints x, y, p. 163

$\mathfrak{O}_{\mathbf{K}}$: ring of integers of the number field $\mathbf{K}$, p. 167

$\mathrm{pd}(M)$, $\mathrm{fd}(M)$, $\mathrm{id}(M)$: projective, flat, injective dimension, p. 170

$R^n(\mathfrak{G})$: n^{th} *right derived* functor of the contravariant functor $\mathfrak{G}$, p. 200

$\mathrm{Ext}^n_{\mathcal{A}}$, p. 201

Modules over principal ideal domains and related notions (section 3.4)

C_f: companion matrix, p. 215

$J_{\mu(\pi_i)}(\lambda_i)$: Jordan block, p. 220

1

Categories and Functors

Category theory was introduced by S. Eilenberg and S. MacLane in an article published in 1945 [EIL 45], which also axiomatized the notions of *functor* and *natural transformation*. MacLane [MCL 98, p. 18] wrote that the notion of category was defined in order to define the notion of functor, which was in turn defined in order to define the notion of natural transformation. The archetypal example of a *natural* (or *canonical*) *isomorphism* is the one that identifies finite-dimensional vector spaces with their biduals (see Theorem 3.12 and compare with Remark 3.13). The notion of structure gradually began to emerge at the end of the 19th Century, and was fully formalized in *Éléments de mathématique* by N. Bourbaki (vector space structures, topological spaces, etc.). A vector space, for example, is a *set* equipped with a vector space structure. This "structuralist" perspective adopted by Bourbaki is based on set theory. In the category theory, however, the *objects* of a category are not always sets, and consequently the *morphisms* are not always mappings. A *functor* $\mathfrak{F}$ is a "large function" from a category $\mathcal{C}$ to a category $\mathcal{D}$ that sends each object A in C to an object $\mathfrak{F}(A)$ in $\mathcal{D}$ and each morphism $f : A \to B$ in $\mathcal{C}$ to a morphism $\mathcal{F}(f) : \mathcal{F}(A) \to \mathcal{F}(B)$ in $\mathcal{D}$.

1.1. Categories

1.1.1. *General results about categories*

(I) A *category* $\mathcal{C}$ consists of:

1) a class $\mathrm{Ob}(\mathcal{C})$ whose elements are the objects of $\mathcal{C}$;

2) for all $X, Y \in \mathrm{Ob}(\mathcal{C})$, a set $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ whose elements are the morphisms (or arrows) from X to Y;

3) for all $X, Y, Z \in \mathrm{Ob}(\mathcal{C})$, a composition rule $\circ : \mathrm{Hom}_{\mathcal{C}}(X, Y) \times \mathrm{Hom}_{\mathcal{C}}(Y, Z) \to \mathrm{Hom}_{\mathcal{C}}(X, Z)$.

The class of morphisms of $\mathcal{C}$ is denoted by $\mathrm{Mor}(\mathcal{C})$. The composition

$$X \xrightarrow{f} Y \xrightarrow{g} Z \qquad [1.1]$$

of two morphisms f and g is denoted by $g \circ f$ or $g.f$ or gf. We call X the *domain* of f and Y the *codomain*. Composition is associative, and for each object X there exists a morphism $\mathrm{id}_X : X \to X$ such that, for each $f : X \to Y$, $f \circ \mathrm{id}_X = f$ and $\mathrm{id}_Y \circ f = f$.

The *opposite category* $\mathcal{C}^{\mathrm{op}}$ of $\mathcal{C}$ is defined as $\mathrm{Ob}(\mathcal{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathcal{C})$ and $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$ (the direction of the arrows is reversed). If $\mathcal{C}_1, \mathcal{C}_2$ are two categories, the product $\mathcal{C}_1 \times \mathcal{C}_2$ is defined as $\mathrm{Ob}(\mathcal{C}_1 \times \mathcal{C}_2) = \mathrm{Ob}(\mathcal{C}_1) \times \mathrm{Ob}(\mathcal{C}_2)$ and the morphisms of $\mathcal{C}_1 \times \mathcal{C}_2$ are the (f_1, f_2) such that f_1, f_2 are morphisms of $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively, with $(f_1', f_2') \circ (f_1, f_2) = (f_1' \circ f_1, f_2' \circ f_2)$.

(II) EXAMPLES. The objects of the category $\mathbf{Set}$ of sets are sets, and the morphisms of this category are mappings. As this example shows, it is always redundant to specify the objects of a category; however, it is necessary to state its morphisms. The morphisms of the category $\mathbf{Mon}$ of monoids (section 2.1.1**(I)**), the category $\mathbf{Grp}$ of groups (section 2.2), the category $\mathbf{Rng}$ of rings, the category ${}_{\mathbf{K}}\mathbf{Vec}$ of left vector spaces over a division ring $\mathbf{K}$, the category ${}_{\mathbf{R}}\mathbf{Mod}$ of left $\mathbf{R}$-modules over a ring $\mathbf{R}$ (section 2.3.1) and the category $\mathbf{Top}$ of topological spaces are respectively monoid homomorphisms, group homomorphisms, ring homomorphisms, $\mathbf{K}$-linear mappings, $\mathbf{R}$-linear mappings and continuous mappings.

(III) CLASSIFICATION OF MORPHISMS AND OBJECTS. A morphism $f : A \to B$ is a *monomorphism* (written as $f : A \hookrightarrow B$) if it is left-cancellable, i.e. for every pair of morphisms $s_1, s_2 : C \to A$, the relation $f \circ s_1 = f \circ s_2$ (in $\mathrm{Hom}_{\mathcal{C}}(C, B)$) implies $s_1 = s_2$ (in $\mathrm{Hom}_{\mathcal{C}}(C, A)$). The notion of *epimorphism* is *dual* to that of monomorphism, i.e. f is an *epimorphism* (written as $f : A \twoheadrightarrow B$) if it is a monomorphism in the opposite category; in other words, if it is a right-cancellable morphism, i.e. for all morphisms $r_1, r_2 : B \to C$, the relation

$r_1 \circ f = r_2 \circ f$ implies $r_1 = r_2$. A *bimorphism* is a monomorphism that is also an epimorphism.

A morphism $f : A \to B$ is *left-invertible* if there exists a morphism $r : B \to A$, called a *retraction* of f, such that $r \circ f = \mathrm{id}_A$; $f : A \to B$ is *right-invertible* if there exists a morphism $s : B \to A$, called a *section* of f, such that $f \circ s = \mathrm{id}_B$; the morphism f is invertible, or is an *isomorphism* (written as $f : A \tilde{\to} B$), if it is both right- and left-invertible, in which case it has a unique inverse f^{-1}. A retractable morphism (a section) is a monomorphism, a sectionable morphism (a retraction) is an epimorphism and an invertible morphism is a bimorphism, but the converse statements do not hold in general. For example, if A, B are topological spaces and $f : A \to B$ is a continuous bijection, the inverse bijection is not necessarily continuous.

The notions of source and sink generalize the notion of morphism: a *source* $\mathcal{S}$ of a category $\mathcal{C}$ is a family of morphisms $(f_i : A \to A_i)_{i \in I}$; its domain is the object A and its codomain is the family of objects $(A_i)_{i \in I}$. A *sink* $\mathcal{P}$ is the dual notion: it is a family of morphisms $(g_i : A \longleftarrow A_i)_{i \in I}$ whose domain is the family $(A_i)_{i \in I}$ and whose codomain is the object A. The notion of *monosource* generalizes the notion of monomorphism: a source $(f_i : A \to A_i)_{i \in I}$ is a monosource if the relation $f_i \circ s_1 = f_i \circ s_2$ for all $i \in I$ implies $s_1 = s_2$. The notion of *episink* is dual to the notion of monosource.

Recall that a *preorder relation* on a set I is a binary relation $\preceq$ such that, for all $i, j, k \in I$, we have: 1) $i \preceq j$ and $j \preceq k \Rightarrow i \preceq k$ and 2) $i \preceq i$. A preordered set I is a category whose objects are the elements i and whose morphisms $i \to j$ are the pairs (i, j) such that $i \preceq j$.

Let $X \in \mathrm{Ob}\,(\mathcal{C})$. We can define a preorder on the set P_X of all morphisms with codomain X as follows: write $u \preceq v$ if u factors through v, i.e. if there exists a morphism u' such that $u = v \circ u'$. Two morphisms $u, v \in P_X$ are said to be equivalent (written as $u \cong v$) if $u \preceq v$ and $v \preceq u$. Dually, the set Q^X of all morphisms with domain X can be preordered as follows: write $f \succeq g$ if g factors through f, i.e. if there exists a morphism g' such that $g = g' \circ f$. A *subobject* of X is an equivalence class of monomorphisms in P_X. Representatives of a subobject of X are therefore pairs (Y, can) where $\mathrm{can} : Y \to X$ is the so-called *canonical* monomorphism (also known as inclusion). If $\mathcal{C} = \mathbf{Set}$, we recover the usual notion of subsets $Y \subset X$ with canonical injection. Dually, a *quotient object* is an equivalence class of epimorphisms,

and representatives of this quotient object are pairs (Z, can) where $\text{can} : X \twoheadrightarrow Z$ is the so-called *canonical* epimorphism. If $\mathcal{C} = \mathbf{Set}$ and $\sim$ is an equivalence relation on the elements of X, we recover the usual notion of quotient sets $X/\sim$ and can is the canonical surjection (section 1.1.2**(VI)**).

Let (f, g) be a pair of morphisms $A \to B$ (this pair may be written as $A \underset{g}{\overset{f}{\rightrightarrows}} B$). An *equalizer* (or *generalized kernel*) of (f, g) is a morphism $\kappa : K \underset{g}{\overset{}{\to}} A$ (which is necessarily a monomorphism) such that $f \circ \kappa = g \circ \kappa$ and, for any morphism $\kappa' : K' \to A$ such that $f \circ \kappa' = g \circ \kappa'$, there exists a unique morphism $\lambda : K' \to K$ such that $\kappa' = \kappa \circ \lambda$:

$$\begin{array}{ccc} K & \overset{\kappa}{\longrightarrow} & A \underset{g}{\overset{f}{\rightrightarrows}} B \\ {\scriptstyle\lambda}\uparrow & \nearrow {\scriptstyle\kappa'} & \\ K' & & \end{array}$$

The morphism κ is written as $\text{eq}\,(f, g)$, and is a subobject of A, unique up to isomorphism. We say that the diagram $K \overset{\kappa}{\to} A \underset{g}{\overset{f}{\rightrightarrows}} B$ is *exact* if $\kappa = \text{eq}\,(f, g)$. If $\mathcal{C} = \mathbf{Set}$ and $f, g : A \to B$ are mappings, then $\text{eq}\,(f, g) = \kappa : K \to A$, where $K = \{x \in A : f(x) = g(x)\}$ and $\kappa = \text{can} : K \hookrightarrow A$ is the canonical injection. If $\mathcal{C} = {}_{\mathbf{K}}\mathbf{Vec}$ and $f, g : A \to B$ are $\mathbf{K}$-linear functions, we have $\text{eq}\,(f, 0) = \kappa : K \to A$ where $K = \ker(f) := f^{-1}(\{0\})$ is the usual definition of the kernel of f and $\kappa = \text{can}$ is the canonical injection.

Dually, a *coequalizer* (or *generalized cokernel*) of a pair of morphisms $A \underset{g}{\overset{f}{\leftleftarrows}} B$ is a morphism $\gamma : C \longleftarrow A$ (which is necessarily an epimorphism) such that $\gamma \circ f = \gamma \circ g$ and, for any morphism $\gamma' : C' \longleftarrow A$ such that $\gamma' \circ f' = \gamma \circ g$, there exists a unique morphism $\mu : C' \longleftarrow C$ such that $\gamma' = \mu \circ \gamma$:

$$\begin{array}{ccc} C & \overset{\gamma}{\longleftarrow} & A \underset{g}{\overset{f}{\leftleftarrows}} B \\ {\scriptstyle\mu}\downarrow & \swarrow {\scriptstyle\gamma'} & \\ C' & & \end{array}$$

The morphism γ is written as $\text{coeq}\,(f, g)$, and is a quotient object of A, unique up to isomorphism. We say that the diagram $C \overset{\gamma}{\longleftarrow} A \underset{g}{\overset{f}{\leftleftarrows}} B$ is *exact* if

$\gamma = \text{coeq}\,(f,g)$. If $A \overset{f}{\underset{g}{\rightrightarrows}} B$ is a double arrow, the diagram

$$K \overset{\text{eq}(f,g)}{\longrightarrow} A \overset{f}{\underset{g}{\rightrightarrows}} B \overset{\text{coeq}(f,g)}{\longrightarrow} C$$

is said to be exact. If $\mathcal{C} = \mathbf{Set}$ and $f, g : A \to B$ are mappings, we have that $\text{coeq}\,(f,g) = \gamma : B \longrightarrow B/\sim$, where $\sim$ is the coarsest equivalence relation whose graph $\mathfrak{G} := \{(y,y') \in B \times B : y \sim y'\}$ contains the set $\{(f(x), g(x)) : x \in X\}$, and $\gamma = \text{can} : B \twoheadrightarrow B/\sim$ is the canonical surjection (see section 1.1.2**(VI)**). If $\mathcal{C} = {}_{\mathbf{K}}\mathbf{Vec}$ and $f : A \longrightarrow B$ are a $\mathbf{K}$-linear mapping, we have that $\text{coeq}\,(f,0) = \gamma : B \longrightarrow C$, where $C = B/\text{im}\,(f)$ is the usual definition of the cokernel $\text{coker}\,(f)$ of f (with $\text{im}\,(f) = f(A)$, the *image* of A under f) and $\gamma = \text{can}$ is the canonical surjection.

(IV) An object I of $\mathcal{C}$ is said to be *initial* if for any object X there exists a unique morphism $I \to X$. The dual notion is the notion of *terminal* object. An initial or terminal object is necessarily unique up to isomorphism (**exercise**). A *zero object* (written as 0) is an object that is both initial and terminal. For example, in ${}_{\mathbf{K}}\mathbf{Vec}$, the zero object is the vector space $\{0\}$.

1.1.2. *The category of sets*

(I) Set theory, founded by G. Cantor at the end of the 19th Century, was at first highly protested by some mathematicians, but received the unconditional support of D. Hilbert, who coined the aphorism: "No one will drive us from the paradise which Cantor created for us." The category of sets $\mathbf{Set}$ is one of the most important categories. If $\text{Ob}\,(\mathbf{Set})$ denotes the class of all sets, it cannot be a set due to contradictions such as the well-known "Russell's paradox"[1]. However, we can talk about the *class* of all sets. This notion of class has a precise definition in the von Neumann-Bernays-Gödel Set Theory.

(II) Following the approach of A. Grothendieck and J.L. Verdier [GRO 72] (and the appendix to this text written by N. Bourbaki), we can also define categories in the more classical Zermelo-Fraenkel (**ZF**) set-theoretical framework[2], using the notion of *universe*. A universe is defined as a *set (sic)*

1 See *Russell's paradox* on Wikipedia.

2 The list of axioms used by Zermelo Set Theory, Zermelo-Fraenkel Set Theory and von Neumann-Bernays-Gödel Set Theory can be found on Wikipedia.

$\mathfrak{U}$ that satisfies the following conditions: 1) $x \in u$ and $u \in \mathfrak{U} \Rightarrow x \in \mathfrak{U}$; 2) $x, y \in \mathfrak{U} \Rightarrow \{x, y\} \in \mathfrak{U}$; 3) $x \in \mathfrak{U} \Rightarrow \mathfrak{P}(x) \in \mathfrak{U}$; 4) if $(x_i)_{i \in I}$ is a family of elements of $\mathfrak{U}$ and $I \in \mathfrak{U}$, then $\bigcup_{i \in I} x_i \in \mathfrak{U}$. It can be useful to add the following axiom **AU** (which is independent of the axioms of **ZF**) to the axioms of **ZF**: *for any set x, there exists a universe $\mathfrak{U}$ such that $x \in \mathfrak{U}$* (we say that x is a $\mathfrak{U}$-set). For a given universe $\mathfrak{U}$, $\mathrm{Ob}(\mathbf{Set})$ is the set of $\mathfrak{U}$-sets. A set is called $\mathfrak{U}$-small if it is isomorphic to a $\mathfrak{U}$-set. A category $\mathcal{C}$ is a $\mathfrak{U}$-category if the set $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ is $\mathfrak{U}$-small for all $X, Y \in \mathrm{Ob}(\mathcal{C})$, and is $\mathfrak{U}$-small if $\mathrm{Ob}(\mathcal{C})$ is $\mathfrak{U}$-small. From now on, there is no reason to use the word *class* rather than *set* in the definition of a category (section 1.1.1**(I)**). When adopting this perspective, given that choosing a specific universe *a priori* has no practical implications (except for set theorists), in the remainder of this presentation a universe $\mathfrak{U}$ should be considered to have been implicitly chosen and to lighten the notation we shall omit the prefix $\mathfrak{U}$. For example, we will say that a category is "small" to describe the property of being "$\mathfrak{U}$-small".

LEMMA 1.1.– *In* $\mathbf{Set}$*, a monomorphism $A \hookrightarrow B$, i.e. an injection, is retractable whenever $A \neq \varnothing$.*

PROOF.– If $f : A \to B$ is injective, then for all $y \in f(A)$ there exists a uniquely determined $x \in A$ such that $y = f(x)$, and there exists a unique element $r(y) \in A$ such that $r(f(x)) = x$; moreover, by choosing an element $x_0 \in A$ and setting $r(y) = x_0$ if $y \notin f(A)$, $r : B \to A$ is a retraction. ■

(III) THE AXIOM OF CHOICE AND ITS CONSEQUENCES. By adding the axiom of choice **AC** (introduced by Zermelo in 1904) to the axioms of **ZF**, we obtain the **ZFC** Set Theory. The relation [1.2] below shows that there exist other equivalent formulations of **AC**; nevertheless, it is traditionally emphasized in its following form:

Axiom of choice **AC**: *For any non-empty set X, there exists a choice function $\phi : \mathfrak{P}(X) - \varnothing \longrightarrow X$ such that $\forall A \in \mathfrak{P}(X) - \varnothing$, $\phi(A) \in A$.*

In **ZFC**, let $(X)_{i \in I}$ be a family of sets. The product $\prod_{i \in I} X_i$ is by definition the set of families $(x_i)_{i \in I}$ such that $x_i \in X_i, \forall i \in I$. The proof of the next corollary is an **exercise**.

COROLLARY 1.2.– *(i) Let $(X_i)_{i \in I}$ be a family of non-empty sets. Then $\prod_{i \in I} X_i \neq \varnothing$. (ii) Every epimorphism in* $\mathbf{Set}$*, i.e. every surjection, has a section.*

An *order relation* on a set X is a preorder relation (section 1.1.1 **(III)**) that is also antisymmetric: $\forall x, y \in X$, $x \leq y$ and $y \leq x \Rightarrow x = y$. We sometimes call this a *partial* order relation. We write $x < y$ if $x \leq y$ and $x \neq y$, and call $<$ a *strict order relation*. An order relation on X is a *total order relation* if $\forall x, y \in X$, $x \leq y$ or $y \leq x$. An ordered set X is said to be *inductive* if every *chain*, i.e. every *totally* ordered subset, has an upper bound.

Zorn's *lemma*, published in 1935 (but established in an equivalent form by K. Kutatowski in 1922), is an extremely important consequence of **AC**. To prove it, we need to introduce the following notation: we define an *upper set* of an ordered set E to be a subset S such that:

$$\forall x \in S, \forall y \in E : y \leq x \Longrightarrow y \in S.$$

Given a choice function $\phi : \mathfrak{P}(E) - \varnothing \longrightarrow E$ (whose existence follows from **AC**), we say that $C \subset E$ is a ϕ*-chain* if, for any upper set S of C not equal to C, the smallest element of the set $\complement_S C$ is $\phi(M_S)$, where $M_S \subset E$ is the set of strict upper bounds of S. It can be shown by contradiction (**exercise***; see [DOU 05], Prop. 1.3.5) that the union $\bar{C}$ of all ϕ-chains of E is a ϕ-chain without a strict upper bound. This result allows us to derive Zorn's lemma:

LEMMA 1.3.– *(Zorn) Every inductive set E has a maximal element.*

PROOF.– Since the set E is inductive, let ϕ be a choice function on E; the union $\bar{C}$ of all ϕ-chains of E has an upper bound m, which is not strict, thus is a maximal element of E. ■

Let E be a non-empty set and suppose that $X \subset \mathfrak{P}(E)$. We say that X is *of finite character* if, for any subset A of E, the following conditions are equivalent: (i) $A \in X$ and (ii) every finite subset B of A belongs to X.

LEMMA 1.4.– *Every set X of finite character is inductive under the inclusion ordering. It follows that every set of finite character has a maximal element.*

PROOF.– Let $(A_i)_{i \in I}$ be a chain of X and suppose that $A = \bigcup_{i \in I} A_i$. Every finite subset B of A belongs to one of the A_i, so belongs to X; since X is of finite character, A belongs to X and is an upper bound of $(A_i)_{i \in I}$. ■

A *well-ordering relation* on a set X is an order relation $\preceq$ such that any non-empty subset of X has a smallest element. For example, the usual order

relation on the set $\mathbb{N}^{\times}$ of natural integers $\{1, 2, ...\}$ is a well-ordering relation by the Peano *axioms* **AP1**-**AP3**:

AP1: Each element n in $\mathbb{N}^{\times}$ has a successor $s(n) = n + 1$.

AP2: $s(n) \neq 1$ for all $n \in \mathbb{N}^{\times}$.

AP3: If $E \subset \mathbb{N}^{\times}$ satisfies $1 \in E$ and $s(E) \subset E$, then $E = \mathbb{N}^{\times}$.

We can equip $\mathbb{Z}$ with a well-ordering relation by arranging its elements as follows: $0, 1, -1, 2, -2, ...$ Similarly, we can equip $\mathbb{Q}^{+}$ with a well-ordering relation by arranging its elements as follows: $0, 1, 1/2, 2, 1/3, 2/3, 3/2, 3, ...$ By combining both methods, we can equip $\mathbb{Q}$ with a well-ordering relation. More generally, whenever the elements of a set are countable, we can equip this set with a well-ordering relation. But can $\mathbb{R}$ be well-ordered? Zermelo's *theorem*, which may be deduced from Zorn's lemma, affirms that this is indeed possible.

THEOREM 1.5.– *(Zermelo) Every set X has a well-ordering relation.*

PROOF.– Let X be a set. Let Ω be the set of pairs $(S, \preceq)$ such that $S \subset X$ and $\preceq$ is a well-ordering relation on S. Equip Ω with the following order relation: $(S, \preceq) \leq (S', \preceq')$ if S is an upper set of S' and $\preceq'$ extends $\preceq$. The ordered set Ω is inductive, since if $\mathfrak{S}$ is a chain of Ω, then $\bar{S} = \bigcup_{S \in \mathfrak{S}} S$ has an order relation $\bar{\preceq}$ that extends the order relation $\preceq$ for each $S \in \mathfrak{S}$. By Zorn's lemma, Ω has a maximal element $\left(\hat{S}, \hat{\preceq}\right)$. It remains to be shown that $\hat{S} = X$. If not, there exists $a \in \complement_X \hat{S}$. Let $\leqq$ be the order relation on $\hat{S} \cup \{a\}$ defined by $x \leqq y \Leftrightarrow x \hat{\preceq} y, \forall x, y \in \hat{S}$ and $a > x$. Then, $\left(\hat{S} \cup \{a\}, \leqq\right)$ is a strict upper bound of $\left(\hat{S}, \hat{\preceq}\right)$: contradiction. ■

Finally, Zermelo's theorem implies the *axiom of choice*. Indeed, let X be a well-ordered set and suppose $A \in \mathfrak{P}(X) - \varnothing$. Then, the smallest element $\phi(A)$ of X belongs to A. We therefore have:

$$\boxed{\textbf{AC} \Rightarrow \text{Zorn} \Rightarrow \text{Zermelo} \Rightarrow \textbf{AC}}. \qquad [1.2]$$

(IV) ORDINALS AND CARDINALS. These notions were introduced by Cantor. An *ordinal* is a set α such that: (i) the relation $x \in y$ $(x, y \in \alpha)$ is a strict

order relation $<$ that induces a well-ordering relation $\leq$; (ii) if $x \in \alpha$, then $x \subset \alpha$. Each ordinal is therefore the set of all preceding ordinals: for any ordinals α, β, $\alpha \leq \beta \Leftrightarrow \alpha \subset \beta$. In particular, $\varnothing \subset \alpha$ for any ordinal α, so $\varnothing$ is the smallest ordinal. We write $\alpha + 1$ the successor $\alpha \cup \{\alpha\}$ of α. Hence, the successor of $\varnothing$ is $\{\varnothing\}$, whose successor is $\{\varnothing, \{\varnothing\}\}$, whose successor is $\{\varnothing, \{\varnothing, \{\varnothing\}\}\}$, etc. These ordinals are respectively written as $0, 1, 2, 3$, etc. It can be shown that for any well-ordered set there exists precisely one order isomorphism from A to some ordinal ([KRI 98], Thm. 2.3).

DEFINITION 1.6.– *A* collection *is a relation* $\boldsymbol{R}(x)$ *with one single argument.*

For example, if X is a set, the relation "$x \in X$" identifies the set X. The relation "α is an ordinal" identifies the collection of ordinals, which *is not* a set **(exercise***: see [KRI 98], p. 21). In practice, the terms "collection" (Definition 1.6) and "class" (in the terminology of von Neumann-Bernays-Gödel) can be employed interchangeably. A class that is not a set is called a *proper class*.

An ordinal $n > 0$ is said to be *finite* if it has a predecessor m or, in other words, if $m < m+1$ and $m+1 = n$. The *axiom of infinity* **AI** (which is one of the axioms of **ZF**) states that the collection of all finite ordinals is a *set*, written as $\mathbb{N}$.

THEOREM 1.7.– *(*Principle of transfinite induction*) Given a set X equipped with a well-ordering relation $\leq$ (for example, an ordinal), let $\boldsymbol{R}$ be a relation such that, for each $x \in X$, the relation $\boldsymbol{R}(x)$ is true if the relation $\boldsymbol{R}(y)$ is true for all $y \in X$ such that $y < x$. Then, the relation $\boldsymbol{R}(x)$ is true for all $x \in X$.*

PROOF.– Let $Y = \{z \in X : \text{ not } \boldsymbol{R}(z)\}$ and suppose that $Y \neq \varnothing$. Since X is well-ordered, Y has a smallest element x. For all $y \in X$ such that $y < x$, the relation $\boldsymbol{R}(y)$ is therefore true. Therefore, $\boldsymbol{R}(x)$ is true: contradiction. ■

When $X = \mathbb{N}$, this principle reduces to classical induction (see the Peano axiom **AP3**). The results stated from the beginning of **(IV)** do not use **AC** nor any results that require it.

Two sets A, B are said to be *equipotent* (written as $\text{Eq}(A, B)$) if there exists a bijection from A onto B. The relation $\text{Eq}(A, B)$ is an equivalence relation. Let A be a set. By Zermelo's theorem (Theorem 1.5), which follows from **AC**, there exists a well-ordering on A, and therefore an isomorphism from A

equipped with this well-ordering onto some ordinal. We define the *cardinal* of A, written as $\text{Card}(A)$, to be the smallest ordinal equipotent to A. Hence, we have:

$$\boxed{\text{Eq}(A, B) \Leftrightarrow \text{Card}(A) = \text{Card}(B)}.$$

A cardinal $\mathfrak{a}$ is said to be *infinite* (or *transfinite*) if $\mathfrak{a} = \mathfrak{a} + 1$, and finite otherwise (we write $\mathfrak{a} < \infty$ to indicate that the cardinal $\mathfrak{a}$ is finite; this is an abuse of notation since ∞ is not a cardinal). It can be shown by induction that the finite cardinals are precisely the finite ordinals. For a set A with n elements, where n is an integer ≥ 0, we have $\text{Card}(A) = n$. The smallest infinite cardinal is $\aleph_0 := \text{Card}(\mathbb{N})$, the *cardinal of countable infinity*, and **AI** therefore implies the existence of an infinite cardinal. For any ordinal $\alpha \geq 0$, we write $\aleph_{\alpha+1}$ as the smallest cardinal $> \aleph_\alpha$, noting that the $\aleph_\alpha$ ("aleph α") are defined by transfinite induction. Consequently, every infinite cardinal is of the form $\aleph_\alpha$, where α is an ordinal. The collection of cardinals is not a set ([KRI 98], Thm. 2.15).

We can define the following preorder relation on the cardinals: $\text{Card}(A) \leq \text{Card}(B)$ if there exists an injection from A into B, or equivalently if A is equipotent to a subset of B. It can be shown (Schröder-Bernstein-Cantor *theorem*) that this is an order relation, and is in fact a well-ordering relation (**exercise***; see [BKI 70], Chap. III, section 3.2, Thm. 1).

We define cardinal addition and multiplication as follows: if $(X_i)_{i\in I}$ is a family of disjoint sets,

$$\begin{aligned} \text{Card}\left(\bigcup_{i\in I} X_i\right) &:= \sum_{i\in I} \text{Card}(X_i), \\ \text{Card}\left(\prod_{i\in I} X_i\right) &:= \prod_{i\in I} \text{Card}(X_i) \end{aligned} \qquad [1.3]$$

and we say that the family $(X_i)_{i\in I}$ is a *partition* of $X = \bigcup_{i\in I} X_i$. Cardinal addition and multiplication are commutative, and multiplication is distributive over addition, as is the case for the elements of $\mathbb{N}$.

We stated earlier that every countable set, such as $\mathbb{Q}$, has cardinal $\aleph_0$. Since $\mathbb{Q}$ is equipotent to $\mathbb{N} \times \mathbb{N}$, we have $\aleph_0^2 = \aleph_0$. More generally, we can show the following result ([BKI 70], Chap. III, section 6.3, Thm. 2):

LEMMA 1.8.– *For any infinite cardinal* $\mathfrak{a}$, *we have that* $\mathfrak{a}^2 = \mathfrak{a}$.

Hence, if $\mathfrak{a}, \mathfrak{b}$ are both cardinals and at least one of them is infinite, we have (**exercise**):

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{a}\mathfrak{b} = \max\{\mathfrak{a}, \mathfrak{b}\}. \qquad [1.4]$$

COROLLARY 1.9.– *If* $(\mathfrak{a}_i)_{i\in I}$ *is a family of cardinals such that* $1 \leq \mathfrak{a}_i \leq \aleph_0$ *and* I *is an infinite index set, then* $\sum_{i\in I} \mathfrak{a}_i = Card\,(I)$.

PROOF.– We have that $\text{Card}\,(I) \leq \sum_{i\in I} \mathfrak{a}_i \leq \aleph_0 \text{Card}\,(I)$, and it follows from [1.4] that $\aleph_0 \text{Card}\,(I) = \text{Card}\,(I)$. ■

By Corollary 1.2 (which uses **AC**), if X, Y are two sets and there exists a surjection from X onto Y, then $\text{Card}\,(Y) \leq \text{Card}\,(X)$.

If A and B are sets, the set of mappings from B into A is A^B. Let $\mathfrak{a} = \text{Card}\,(A)$ and $\mathfrak{b} = \text{Card}\,(B)$. Then, $\text{Card}\left(A^B\right)$ only depends on $\mathfrak{a}$ and $\mathfrak{b}$ and we set $\mathfrak{a}^{\mathfrak{b}} = \text{Card}\left(A^B\right)$.

LEMMA 1.10.– *Let* $\mathfrak{a} = \text{Card}\,(A)$. *Then,* $\text{Card}\,(\mathfrak{P}(A)) = 2^{\mathfrak{a}}$.

PROOF.– The set $\mathfrak{P}(A)$ is equipotent to $\{\varnothing, \{\varnothing\}\}^A$. Indeed, for any subset X of A, let $f_X : X \to \{\varnothing, \{\varnothing\}\}^A$ be the mapping defined by $f_X(x) = \varnothing$ for $x \in X$ and $f_X(x) = \{\varnothing\}$ for $x \in \complement_A X$. The mapping $X \mapsto f_X$ from $\mathfrak{P}(A)$ to $\{\varnothing, \{\varnothing\}\}^A$ is a bijection. ■

THEOREM 1.11.– *(Cantor) For any cardinal* $\mathfrak{a}$, *we have* $2^{\mathfrak{a}} > \mathfrak{a}$.

PROOF.– The mapping $A \to \mathfrak{P}(A) : x \mapsto \{x\}$ is injective, so $2^{\mathfrak{a}} \geq \mathfrak{a}$. It is sufficient to show that $2^{\mathfrak{a}} \neq \mathfrak{a}$, or alternatively that, for any mapping $f : \mathfrak{a} \to \mathfrak{P}(\mathfrak{a})$, we have $f(\mathfrak{a}) \neq \mathfrak{P}(\mathfrak{a})$. Let $X = \{x \in \mathfrak{a} : x \notin f(x)\}$. If we had $f(\mathfrak{a}) = \mathfrak{P}(\mathfrak{a})$, we would have $X \in f(\mathfrak{a})$. However, since $x \in X$, we have $x \notin f(x)$, so $f(x) \neq X$. Furthermore, if $x \in \complement_{\mathfrak{a}} X$, we have $x \in f(x)$ and $x \notin X$, so once again $f(x) \neq X$. Hence, $X \notin f(\mathfrak{a})$. ■

Another theorem by Cantor shows that $\text{Card}\,(\mathbb{R}) = 2^{\aleph_0}$ ([BKI 71], Chap. IV, section 8.6, Thm. 1). This cardinal is called the *power of the continuum*. Consider the question where $2^{\aleph_0}$ is situated within the well-ordered set of cardinals $\aleph_\alpha$. The *continuum hypothesis* (**CH**) proposed by Cantor states that $2^{\aleph_0} = \aleph_1$. The *generalized continuum hypothesis* (**GCH**) states that

$2^{\aleph_\alpha} = \aleph_{\alpha+1}$, for any ordinal α. K. Gödel showed in 1931 and 1938 that **AC** cannot be disproven within **ZF,** that **GCH** cannot be disproven within **ZFC** ([KRI 98], Thm. 8.8), and that the absence of contradiction within an axiomatic system sufficiently strong to include the usual rules of arithmetic, such as **ZF** is undecidable within this system ([KRI 98], Thm. 9.3). This last result prompted a great deal of epistemological thought. P. Cohen showed in 1963 that **AC** is undecidable in **ZF** and **CH** is undecidable in **ZFC** ([KRI 98], pp. 150, 162). **CH** and **GCH** are infrequently used in mathematics, unlike **AC**.

(V) HILBERT'S τ OPERATOR. This logical operator is not strictly speaking part of Set Theory. If $\boldsymbol{R}(x)$ is a relation depending on a variable x, $\tau_x \boldsymbol{R}(x)$ is a "value" x_0 of the variable such that the relation $\boldsymbol{R}(x_0)$ is true (Hilbert used the symbol ε to denote this operator τ [HIL 39]). In particular, with this formalism, the equivalences:

$$(\exists x)\, \boldsymbol{R}(x) \Leftrightarrow \boldsymbol{R}(\tau_x \boldsymbol{R}(x)), \quad (\forall x)\, \boldsymbol{R}(x) \Leftrightarrow R(\tau_x(\urcorner \boldsymbol{R}(x)))$$

(where $\urcorner \boldsymbol{R}$ means "not $\boldsymbol{R}$") respectively define the quantifiers $\exists$ and $\forall$. Observe that $\phi : \mathfrak{P}(X) - \varnothing \to X : A \mapsto \tau_x (x \in A)$ is a choice function for $X \neq \varnothing$. As is done in Bourbaki [BKI 70], Hilbert's operator allows us to define the cardinals without requiring the notion of ordinal: we can simply set $\mathrm{Card}(A) = \tau_A \mathrm{Eq}(A, B)$. The problem with this approach, despite its internal consistency, is that the "universal choice" operator τ used to select individuals from *collections* (Definition 1.6) and not just from *sets* is too general to be compatible with the work in Set Theory that has been done since Gödel (see note 1, p. x); nonetheless, the Bourbakian perspective can be justified *a posteriori* [FEL 71].

(VI) MISCELLANEOUS RESULTS (EXERCISE).

LEMMA 1.12.– *Let $f : X \to Y$ be a mapping. By setting $f^{-1}(B) := \{x \in X : f(x) \in B\}$ when $B \in \mathfrak{P}(Y)$ (*inverse image *of B under f), we have:*

1) $f^{-1}(f(A)) \supset A, \quad \forall A \in \mathfrak{P}(X)$;

2) $f\left(f^{-1}(B)\right) \subset B, \quad \forall B \in \mathfrak{P}(Y)$.

The inclusion in (1) is an equality if and only if f is injective. The inclusion in (2) is an equality if and only if f is surjective.

The operator $f^* : \mathfrak{P}(Y) \to \mathfrak{P}(X) : B \mapsto f^{-1}(B)$ conserves all relations of type $\subset, \supset, \cap, \cup$, as well as complements. The operator $f_* : \mathfrak{P}(X) \to \mathfrak{P}(Y) : A \mapsto f(A)$ conserves $\subset, \supset, \cup$. In the general case, we have $f(A \cap A') \subset f(A) \cap f(A')$, and this inclusion becomes equality for sets $A, A' \in \mathfrak{P}(X)$ if and only if f is injective.

Let E be a set and $x \sim y$ an equivalence relation on E $(x, y \in E)$. The class of x (mod. $\sim$) is $\bar{x} := \{y : x \sim y\}$; the set of equivalence classes, called the *quotient set*, is written as $E/\sim$, and the mapping can : $E \ni x \mapsto \bar{x} \in E/\sim$ is the *canonical surjection*. The equivalence classes mod. $\sim$ form a partition of E. If $\boldsymbol{R}_1, \boldsymbol{R}_2$ are two equivalence relations on E, $\boldsymbol{R}_1$ is *coarser* than $\boldsymbol{R}_2$ if $\boldsymbol{R}_2 \Rightarrow \boldsymbol{R}_1$. Let $f : E \to F$ be a mapping and $\sim$ be an equivalence relation on E. If $f(x) = f(y)$ whenever $x, y \in E$ are such that $x \sim y$, f induces a mapping $\bar{f} : E/\sim \to F$ which is said to be *well-defined*.

1.2. Functors

1.2.1. *Covariant functors and contravariant functors*

(I) Let $\mathcal{C}, \mathcal{D}$ be two categories. A *covariant functor* $\mathfrak{F} : \mathcal{C} \to \mathcal{D}$ consists of two mappings: (i) an "object-mapping" $\mathfrak{F}_{\mathrm{Ob}} : \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D})$ and (ii) an "arrow-mapping" $\mathfrak{F}_{\mathrm{Mor}} : \mathrm{Mor}(\mathcal{C}) \to \mathrm{Mor}(\mathcal{D})$ (usually both written as $\mathfrak{F}$) such that:

1) for all $X, Y \in \mathrm{Ob}(\mathcal{C})$,

$$\mathfrak{F}_{\mathrm{Mor}}(\mathrm{Hom}_{\mathcal{C}}(X, Y)) \subset \mathrm{Hom}_{\mathcal{D}}(\mathfrak{F}_{\mathrm{Ob}}(X), \mathfrak{F}_{\mathrm{Ob}}(Y));$$

2) for all $X \in \mathrm{Ob}(\mathcal{C})$, $\mathfrak{F}_{\mathrm{Mor}}(\mathrm{id}_X) = \mathrm{id}_{\mathfrak{F}_{\mathrm{Ob}}(X)}$;

3) the image under $\mathfrak{F}_{\mathrm{Mor}}$ of the composition $g \circ f$ is $\mathfrak{F}_{\mathrm{Mor}}(g) \circ \mathfrak{F}_{\mathrm{Mor}}(f)$.

(II) A *contravariant functor* $\mathfrak{C}$ from $\mathcal{C}$ to $\mathcal{D}$ is a covariant functor from $\mathcal{C}^{\mathrm{op}}$ to $\mathcal{D}$. These functors therefore reverse the direction of arrows. To state that a functor $\mathfrak{C}$ from $\mathcal{C}$ to $\mathcal{D}$ is contravariant, we typically write that it is a functor $\mathcal{C}^{\mathrm{op}} \to \mathcal{D}$. To avoid ambiguity, we will write this as: "$\mathfrak{C}$ is a (contravariant) functor $\mathcal{C}^{\mathrm{op}} \to \mathcal{D}$".

A covariant functor $\mathfrak{F} : \mathcal{C} \to \mathcal{D}$ canonically induces a covariant functor $\mathfrak{F}^{\mathrm{op}} : \mathcal{C}^{\mathrm{op}} \to \mathcal{D}^{\mathrm{op}}$ as follows: for each object $A \in \mathrm{Ob}(\mathcal{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathcal{C})$,

$\mathfrak{F}^{\mathrm{op}}(A) = \mathfrak{F}(A)$; for each morphism $A \longleftarrow B$ in $\mathcal{C}^{\mathrm{op}}$, $\mathfrak{F}^{\mathrm{op}}(A \longleftarrow B) = \mathfrak{F}^{\mathrm{op}}(A) \longleftarrow \mathfrak{F}^{\mathrm{op}}(B)$.

(III) A functor is said to be *injective* (respectively *surjective*) if the mapping $\mathfrak{F}_{\mathrm{Ob}}$ is injective (respectively surjective). (From now on, "respectively" is abbreviated as "resp.".) It is said to be *faithful* (resp. *full*) if the mapping $\mathfrak{F}_{\mathrm{Mor}}$ is injective (resp. surjective). It is said to be *essentially surjective* if, for any object Y in $\mathcal{D}$, there exists an object X in $\mathcal{C}$ such that $\mathfrak{F}_{\mathrm{Ob}}(X)$ is isomorphic to Y.

A *subcategory* $\mathcal{D}$ of $\mathcal{C}$ is a category such that $\mathrm{Ob}(\mathcal{D}) \subset \mathrm{Ob}(\mathcal{C})$ and, for all $X, Y \in \mathrm{Ob}(\mathcal{D})$, $\mathrm{Hom}_{\mathcal{D}}(X,Y) \subset \mathrm{Hom}_{\mathcal{C}}(X,Y)$. If the second inclusion is an equality, the subcategory $\mathcal{D}$ is said to be *full*, which is equivalent to saying that the inclusion functor $\mathcal{C} \to \mathcal{D}$ is full. The category $\mathbf{Ab}$ of abelian groups (named after the mathematician N. Abel; these are the commutative groups) is a full subcategory of $\mathbf{Grp}$; the category $\mathbf{ComRng}$ of commutative rings is a full subcategory of $\mathbf{Rng}$, etc.

A functor $\mathfrak{F} : \mathcal{C} \to \mathcal{D}$ is an *isomorphism* if $\mathfrak{F}_{\mathrm{Ob}}$ and $\mathfrak{F}_{\mathrm{Mor}}$ are both bijective. If so, there exists a functor $\mathfrak{G} : \mathcal{D} \to \mathcal{C}$ such that $\mathfrak{F} \circ \mathfrak{G} = \mathrm{id}_{\mathcal{D}}$ and $\mathfrak{G} \circ \mathfrak{F} = \mathrm{id}_{\mathcal{C}}$. (See also the notions of *equivalence* and *duality* at section 1.2.2.)

(IV) Let $\mathfrak{F} : \mathcal{C} \to \mathcal{D}$ be a functor. The *image* of $\mathfrak{F}$ is the pair $\mathfrak{F}(\mathcal{C})$ formed by the sets $\{\mathfrak{F}(X) : X \in \mathrm{Ob}(X)\}$ and $\{\mathfrak{F}(f) : f \in \mathrm{Mor}(\mathcal{C})\}$.

LEMMA 1.13.– *If $\mathfrak{F}$ is injective, then $\mathfrak{F}(\mathcal{C})$ is a subcategory of $\mathcal{D}$.*

PROOF.– Let $X, X' \in \mathrm{Ob}(\mathcal{C})$ and $f_1 : X_1 \to X, f_2 : X' \to X_2$ such that $\mathfrak{F}(f_2) \circ \mathfrak{F}(f_1)$ exists in $\mathrm{Mor}(\mathcal{D})$, i.e. $\mathfrak{F}(X) = \mathfrak{F}(X')$. If $\mathfrak{F}$ is injective, we have that $X = X'$, so $f_2 \circ f_1$ exists in $\mathcal{C}$, and $\mathfrak{F}(f_2) \circ \mathfrak{F}(f_1) = \mathfrak{F}(f_2 \circ f_1)$ is a morphism of $\mathfrak{F}(\mathcal{C})$, hence $\mathfrak{F}(\mathcal{C})$ is a category. ■

(V) Let $\mathfrak{F} : \mathcal{C} \to \mathcal{D}$ be a functor, let $\mathcal{C}'$ and $\mathcal{D}'$ be subcategories of $\mathcal{C}$ and $\mathcal{D}$ respectively, and suppose that, for all $X \in \mathrm{Ob}(\mathcal{C}')$, $\mathfrak{F}(X) \in \mathrm{Ob}(\mathcal{D}')$. Then, $\mathfrak{F}$ induces a *subfunctor* $\mathfrak{G} : \mathcal{C}' \to \mathcal{D}'$ (with the obvious definition).

1.2.2. *Functorial morphisms*

(I) Given two categories $\mathcal{C}$ and $\mathcal{D}$, we can define the category $\mathrm{Hom}(\mathcal{C},\mathcal{D})$ of functors from $\mathcal{C}$ to $\mathcal{D}$. The class $\mathrm{Ob}(\mathrm{Hom}(C,D))$ is the set of functors

$\mathcal{C} \to \mathcal{D}$. The elements of the class $\mathrm{Mor}(\mathrm{Hom}(C,D))$ are *functorial morphisms*, with the following meaning: a functorial morphism, also called a *natural transformation*, is a mapping $\mathbf{t} : \mathfrak{F} \longrightarrow \mathfrak{G}$ (which we can write as $\mathfrak{F} \dot{\longrightarrow} \mathfrak{G}$) where $\mathfrak{F}, \mathfrak{G} \in \mathrm{Hom}(\mathcal{C}, \mathcal{D})$. It sends each object in $X \in \mathrm{Ob}(\mathcal{C})$ to the morphism $\mathbf{t}(X) = \mathbf{t}_X \in \mathrm{Hom}_{\mathcal{D}}(\mathfrak{F}(X), \mathfrak{G}(X))$ in such a way that, for any morphism $f : X \to Y$ in $\mathcal{C}$, the following diagram commutes:

$$\begin{array}{ccc} \mathfrak{F}(X) & \xrightarrow{\mathfrak{F}(f)} & \mathfrak{F}(Y) \\ \downarrow \mathbf{t}_X & & \downarrow \mathbf{t}_Y \\ \mathfrak{G}(X) & \xrightarrow{\mathfrak{G}(f)} & \mathfrak{G}(Y) \end{array}$$

This morphism $\mathbf{t}$ is a functorial *isomorphism* (written as $\mathbf{t} : \mathfrak{F} \tilde{\longrightarrow} \mathfrak{G}$) if each $\mathbf{t}_X$ is an isomorphism. If so, there exists an inverse functorial isomorphism $\mathbf{u} = \mathbf{t}^{-1} : \mathfrak{G} \dot{\to} \mathfrak{F}$ such that, for all $X \in \mathrm{Ob}(\mathcal{C})$, $\mathbf{u}_X = (\mathbf{t}_X)^{-1}$. If the functors $\mathfrak{F}$ and $\mathfrak{G}$ are isomorphic, we write $\mathfrak{F} \cong \mathfrak{G}$.

(II) The notion of equivalence is less restrictive than that of isomorphism: a functor $\mathfrak{F} : \mathcal{C} \to \mathcal{D}$ is an *equivalence* if there exists a functor $\mathfrak{G} : \mathcal{D} \to \mathcal{C}$ such that $\mathfrak{F} \circ \mathfrak{G} \cong \mathrm{id}_{\mathcal{D}}$ and $\mathfrak{G} \circ \mathfrak{F} \cong \mathrm{id}_{\mathcal{C}}$. This functor $\mathfrak{G}$ exists if and only if $\mathfrak{F}$ is fully faithful, injective and essentially surjective. An *anti-isomorphism* is an isomorphism $C^{\mathrm{op}} \to \mathcal{D}$, and a *duality* is an equivalence $C^{\mathrm{op}} \to \mathcal{D}$.

1.2.3. *Bifunctor Hom*

Given three categories $\mathcal{C}, \mathcal{D}, \mathcal{E}$, a *bifunctor* from $\mathcal{C}$ and $\mathcal{D}$ to $\mathcal{E}$ is a functor $\mathfrak{B} : \mathcal{C} \times \mathcal{D} \to \mathcal{E}$. Multifunctors may be defined similarly.

Let $X \in \mathrm{Ob}(\mathcal{C})$ and write $\mathbf{j}_X = \mathrm{Hom}_{\mathcal{C}}(X, -) : \mathcal{C} \to \mathbf{Set}$ for the covariant functor defined as follows: for all $Y \in \mathrm{Ob}(C)$, $\mathbf{j}_X(Y)$ is the set $\mathrm{Hom}_{\mathcal{C}}(X,Y)$. For every $\mathcal{C}$-morphism $\delta : X' \to Y$, $\mathbf{j}_X(\delta) = \mathrm{Hom}_{\mathcal{C}}(X,\delta) : \mathrm{Hom}_{\mathcal{C}}(X,X') \to \mathrm{Hom}_{\mathcal{C}}(X,Y)$ is the composition $\delta\circ : \alpha \mapsto \delta \circ \alpha$, and hence $\mathbf{j}_X(\delta)(\alpha) = \delta \circ \alpha$. Writing this morphism as γ, the following diagram commutes:

$$\begin{array}{ccc} X & \xrightarrow{\alpha} & X' \\ & \gamma \searrow & \downarrow \delta \\ & & Y \end{array}$$

Moreover, let $Y \in \mathrm{Ob}(C)$ and write $\mathbf{h}_Y = \mathrm{Hom}_{\mathcal{C}}(-, Y)$ for the (contravariant) functor $\mathcal{C}^{\mathrm{op}} \to \mathbf{Set}$ defined as follows: for all $X \in \mathrm{Ob}(C)$, $\mathbf{h}_Y(X)$ is the set $\mathrm{Hom}_{\mathcal{C}}(X, Y)$. For every $\mathcal{C}$-morphism $\beta : X' \to X''$, $\mathrm{Hom}_{\mathcal{C}}(\beta, Y) : \mathrm{Hom}_{\mathcal{C}}(X'', Y) \to \mathrm{Hom}_{\mathcal{C}}(X', Y)$ is the composition $\circ\beta : \varepsilon \mapsto \varepsilon \circ \beta$, and hence $\mathbf{h}_Y(\beta)(\varepsilon) = \varepsilon \circ \beta$. Writing this morphism as δ, the follow diagram commutes:

$$\begin{array}{ccc} X' & \xrightarrow{\beta} & X'' \\ \delta \downarrow & \swarrow & \varepsilon \\ Y & & \end{array}$$

This diagram can be derived from the previous diagram by reversing the arrows and adjusting the notation correspondingly. Assembling these two commuting diagrams together, we obtain:

$$\begin{array}{ccccc} X & \xrightarrow{\alpha} & X' & \xrightarrow{\beta} & X'' \\ \gamma & \searrow & \downarrow \delta & \swarrow & \varepsilon \\ & & Y & & \end{array}$$

The covariance of $\mathbf{j}_X$ follows from the observation that $\gamma = \varepsilon \circ (\beta \circ \alpha) = \mathbf{j}_X(\varepsilon)(\beta \circ \alpha) = \mathbf{j}_X(\varepsilon)(\mathbf{j}_X(\beta)(\alpha)) = (\mathbf{j}_X(\varepsilon) \circ \mathbf{j}_X(\beta))(\alpha)$ and $\gamma = (\varepsilon \circ \beta) \circ \alpha = \mathbf{j}_X(\varepsilon \circ \beta)(\alpha)$, hence $\mathbf{j}_X(\varepsilon \circ \beta) = \mathbf{j}_X(\varepsilon) \circ \mathbf{j}_X(\beta)$.

The contravariance of $\mathbf{h}_Y$ follows from the observation that $\gamma = \delta \circ \alpha = \mathbf{h}_Y(\alpha)(\delta) = \mathbf{h}_Y(\alpha)((\mathbf{h}_Y(\beta)(\varepsilon))) = \mathbf{h}_Y(\alpha) \circ \mathbf{h}_Y(\beta)(\varepsilon)$ and $\gamma = \varepsilon \circ (\beta \circ \alpha) = \mathbf{h}_Y(\beta \circ \alpha)(\varepsilon)$, hence $\mathbf{h}_Y(\beta \circ \alpha) = \mathbf{h}_Y(\alpha) \circ \mathbf{h}_Y(\beta)$.

The bifunctor $\mathrm{Hom}_{\mathcal{C}} : \mathcal{C}^{\mathrm{op}} \times \mathcal{C} \to \mathbf{Set}$ sends $(X, Y) \in \mathrm{Ob}(\mathcal{C}^{\mathrm{op}} \times \mathcal{C})$ to the set $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ and sends the pair of $\mathcal{C}$-morphisms $(\varepsilon, \alpha), \varepsilon \in \mathrm{Hom}_{\mathcal{C}}(X'', Y)$, $\alpha \in \mathrm{Hom}_{\mathcal{C}}(X, X')$ to the composition $\mathrm{Hom}_{\mathcal{C}}(X', X'') \to \mathrm{Hom}_{\mathcal{C}}(X, Y) : \beta \mapsto \varepsilon \circ \beta \circ \alpha$.

1.2.4. *Universal arrows and universal elements*

DEFINITION 1.14.– *Let $\mathcal{C}, \mathcal{D}$ be two categories, $\mathfrak{F} : \mathcal{C} \to \mathcal{D}$ be a functor and $d \in \mathrm{Ob}(\mathcal{D})$. A* universal arrow *from d to $\mathfrak{F}$ is a pair $(c, \xi) \in \mathrm{Ob}(\mathcal{C}) \times \mathrm{Mor}(\mathcal{D})$,*

$\xi : d \to \mathfrak{F}(c)$, *such that for every pair* $(c', \xi') \in \mathrm{Ob}(\mathcal{C}) \times \mathrm{Mor}(\mathcal{D})$, $\xi' : d \to \mathfrak{F}(c')$, *there exists a unique morphism* $\upsilon : c \to c'$ *of* $\mathcal{C}$ *such that* $\mathfrak{F}(\upsilon) \circ \xi = \xi'$, *i.e. such that the following diagram commutes:*

$$\begin{array}{ccccc} d & \xrightarrow{\xi} & \mathfrak{F}(c) & \xleftarrow{\mathfrak{F}} & c \\ \| & & \downarrow \mathfrak{F}(\upsilon) & & \downarrow \upsilon \\ d & \xrightarrow{\xi'} & \mathfrak{F}(c') & \xleftarrow{\mathfrak{F}} & c' \end{array}$$

LEMMA 1.15.– *If* (c, ξ) *and* (c', ξ') *are two universal arrows from* d *to* $\mathfrak{F}$, *then* $\upsilon : c \to c'$ *is an isomorphism of* $\mathcal{C}$ (***exercise***).

If $\mathcal{D} = \mathbf{Set}$, X is an object of a category $\mathcal{C}$ and $\mathfrak{F}$ is a subfunctor of $\mathrm{Hom}_{\mathcal{C}}(X, -) = \mathbf{j}_X$, then every set $\xi \in \mathfrak{F}(\mathcal{C})$ is of the form $\mathrm{Hom}_{\mathcal{C}}(X, Y)$, where $Y \in \mathrm{Ob}(\mathcal{C})$ is uniquely determined by ξ. In addition, $\xi \in \mathfrak{F}(Y)$, so we are led to the following definition:

DEFINITION 1.16.– *Let* $\mathcal{C}$ *be a category and let* $\mathfrak{F} : \mathcal{C} \to \mathbf{Set}$ *be a functor. A* universal element *of* $\mathfrak{F}$ *is a pair* $(Y, \xi) \in \mathcal{C} \times \mathbf{Set}$ *consisting of an object* $Y \in \mathrm{Ob}(\mathcal{C})$ *and a set* $\xi \in \mathfrak{F}(Y)$ *with the following property (called a* universal property*): for each object* $Y' \in \mathrm{Ob}(\mathcal{C})$ *and each element* $\xi' \in \mathfrak{F}(Y')$, *there exists a unique morphism* $\upsilon : Y \to Y'$ *such that* $\mathfrak{F}(\upsilon)(\xi) = \xi'$ *(we sometimes simply write* ξ *instead of* (Y, ξ) *if there is no risk of ambiguity). A* universal problem *consists of finding a universal arrow or a universal element (see the following diagram):*

$$\begin{array}{ccc} Y & \xi \in & \mathfrak{F}(Y) \\ \upsilon \downarrow & \downarrow & \downarrow \mathfrak{F}(\upsilon) \\ Y' & \xi' \in & \mathfrak{F}(Y') \end{array}$$

The following result holds ([MCL 99], section IV.3, Thm 1 & 2):

THEOREM 1.17.– *If* $\xi \in \mathfrak{F}(Y)$ *is a universal element of the functor* $\mathfrak{F} : \mathcal{C} \to \mathbf{Set}$, *then for each* $Z \in \mathrm{Ob}(\mathcal{C})$ *there exists a bijection:*

$$\theta : \mathrm{Hom}_{\mathcal{C}}(Y, Z) \cong \mathfrak{F}(Z), \quad \upsilon \mapsto \mathfrak{F}(\upsilon)(\xi).$$

It follows from Lemma 1.15 and from this theorem that the solutions of a universal problem are "essentially identical" and may be identified with each other in practice.

1.2.5. *Representable functors*

(I) COVARIANT CASE. Let $\mathcal{C}$ be a category and let $u : X \to X'$ be a $\mathcal{C}$-morphism. For all $Y \in \mathrm{Ob}(\mathcal{C})$ and all $v \in \mathrm{Hom}_{\mathcal{C}}(X', Y') = \mathbf{h}_{X'}(Y')$, we have that $v \circ u \in \mathbf{j}_X(Y') := \mathrm{Hom}_{\mathcal{C}}(X, Y')$. Define $\mathbf{j}_u(X)$ as the mapping:

$$\circ u : \mathrm{Hom}_{\mathcal{C}}\left(X', Y'\right) \to \mathrm{Hom}_{\mathcal{C}}\left(X, Y'\right) : v \mapsto v \circ u.$$

For all $\mathcal{C}$-morphisms $w : Y \to Y'$ and $\delta : X' \to Y$, we have that $\mathbf{j}_{X'}(w)(\mathbf{j}_u(Y).\delta) = \mathbf{j}_{X'}(w).(\delta \circ u) = w \circ \delta \circ u$, and similarly that $\mathbf{j}_u(Y')((\mathbf{j}_{X'})(w).\delta) = \mathbf{j}_u(Y').(w \circ \delta) = w \circ \delta \circ u$:

$$X \xrightarrow{u} X' \xrightarrow{\delta} Y \xrightarrow{w} Y'. \qquad [1.5]$$

Therefore, the diagram

$$\begin{array}{ccc} \mathbf{j}_X(Y') & \xleftarrow{\mathbf{j}_X(w)} & \mathbf{j}_X(Y) \\ \mathbf{j}_u(Y') \uparrow & & \uparrow \mathbf{j}_u(Y) \\ \mathbf{j}_{X'}(Y') & \xleftarrow{\mathbf{j}_{X'}(w)} & \mathbf{j}_{X'}(Y) \end{array}$$

commutes, which implies that the definitions of $\mathbf{j}_X$ and $\mathbf{j}_u$ determine a canonical (contravariant) functor $\mathbf{j}_{\mathcal{C}} : \mathcal{C}^{\mathrm{op}} \to \mathrm{Hom}(\mathcal{C}, \mathbf{Set})$.

Let $\mathfrak{F} : \mathcal{C} \to \mathbf{Set}$ be a covariant functor. Specifying a functorial morphism $\mathbf{t} : \mathbf{j}_X \dot{\to} \mathfrak{F}$ (section 1.2.2**(I)**) is equivalent to specifying an element $\xi \in \mathfrak{F}(X)$, and $\mathbf{t}$ is a functorial isomorphism if and only if (X, ξ) is a universal element of $\mathfrak{F}$ (section 1.2.4) or, in other words, for all $Y \in \mathrm{Ob}(\mathcal{C})$, the mapping $\theta : v \mapsto (\mathfrak{F}(v))(\xi)$ from $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ to $\mathfrak{F}(Y)$ is bijective. If so, we say that (X, ξ) *represents* the functor $\mathfrak{F}$ and that this functor is *representable*. We also say that:

$$\boxed{X \in \mathrm{Ob}(\mathcal{C}) \text{ represents } \mathfrak{F} \text{ if } \mathfrak{F} \cong \mathbf{j}_X = \mathrm{Hom}_{\mathcal{C}}(X, -)}.$$

We set $\mathcal{C}^{\vee} := \mathrm{Hom}(\mathcal{C}, \mathbf{Set})^{\mathrm{op}} \cong \mathrm{Hom}(\mathcal{C}^{\mathrm{op}}, \mathbf{Set}^{\mathrm{op}})$.

(II) CONTRAVARIANT CASE. The contravariant case is handled analogously by reversing the arrows ([GRO 70], Chap. 0, section 1.1, 2nd ed.). We thus obtain a canonical covariant functor:

$$\mathbf{h}_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}^{\wedge} := \mathrm{Hom}(\mathcal{C}^{\mathrm{op}}, \mathbf{Set}).$$

Given a (contravariant) functor $\mathfrak{C} : \mathcal{C}^{\mathrm{op}} \to \mathbf{Set}$, specifying a functorial morphism $\mathbf{t} : \mathbf{h}_Y \dot{\to} \mathfrak{C}$ is equivalent to specifying an element $\upsilon \in \mathfrak{C}(Y)$, and $\mathbf{t}$ is a functorial isomorphism if and only if, for all $X \in \mathrm{Ob}(\mathcal{C})$, the mapping $\vartheta : w \mapsto (\mathfrak{C}(w))(\upsilon)$ from $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ to $\mathfrak{C}(X)$ is bijective or, in other words, (Y, υ) is a universal element of $\mathcal{C}$. If so, we say that (Y, υ) *represents* the contravariant functor $\mathfrak{C}$ and that this functor is representable. We also say that:

$$\boxed{Y \in \mathrm{Ob}(\mathcal{C}) \text{ represents } \mathfrak{C} \text{ if } \mathfrak{C} \cong \mathbf{h}_Y = \mathrm{Hom}_{\mathcal{C}}(-, Y)}.$$

LEMMA 1.18.– *(Yoneda) The functors* $\mathbf{j}_{\mathcal{C}} : \mathcal{C}^{op} \to \mathcal{C}^{\wedge op}$ *and* $\mathbf{h}_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}^{\wedge}$ *are fully faithful.*

The functor $\mathbf{j}_{\mathcal{C}}$ allows $\mathcal{C}^{\mathrm{op}}$ to be embedded in $C^{\vee \mathrm{op}}$ by identifying $\mathcal{C}^{\mathrm{op}}$ with the full subcategory of $\mathcal{C}^{\vee \mathrm{op}} = \mathrm{Hom}(\mathcal{C}, \mathbf{Set})$ whose objects are given by the representable covariant functors taking values in $\mathbf{Set}$; furthermore, $\mathbf{j}_{\mathcal{C}}^{\mathrm{op}} : \mathcal{C} \to \mathcal{C}^{\vee}$ allows $\mathcal{C}$ to be embedded in $C^{\vee}$. Similarly, the functor $\mathbf{h}_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}^{\wedge}$ allows $\mathcal{C}$ to be embedded in $\mathcal{C}^{\wedge}$ by identifying it with the full subcategory of $\mathcal{C}^{\wedge}$ whose objects are given by the representable contravariant functors taking values in $\mathbf{Set}$. The two embeddings $\mathbf{j}_{\mathcal{C}}^{\mathrm{op}} : \mathcal{C} \hookrightarrow \mathcal{C}^{\vee}$ (or $\mathbf{j}_{\mathcal{C}} : \mathcal{C}^{\mathrm{op}} \to \mathrm{Hom}(\mathcal{C}, \mathbf{Set})$) and $\mathbf{h}_{\mathcal{C}} : \mathcal{C} \hookrightarrow \mathcal{C}^{\wedge}$ are called Yoneda embeddings. In summary:

$$\boxed{\mathbf{j}_{\mathcal{C}} : \mathcal{C}^{\mathrm{op}} \hookrightarrow \mathrm{Hom}(\mathcal{C}, \mathbf{Set}), \quad \mathbf{h}_{\mathcal{C}} : \mathcal{C} \hookrightarrow \mathrm{Hom}(\mathcal{C}^{\mathrm{op}}, \mathbf{Set})}.$$

1.2.6. *Products and coproducts*

(I) Let $(X_i)_{i \in I}$ be a family of objects in a category $\mathcal{C}$. A *product* of this family, when it exists, is a source $(\mathrm{pr}_i : X \to X_i)_{i \in I}$ with the universal property (section 1.2.4) that, for any family of morphisms $(\alpha_i)_{i \in I}$, $\alpha_i : X' \to X_i$, there exists a unique morphism $\alpha : X' \to X$ such that $\mathrm{pr}_i \circ \alpha = \alpha_i$ for all $i \in I$. This product is written as $\prod_{i \in I} X_i$ and the morphism $\mathrm{pr}_i : \prod_{i \in I} X_i \to X_i$ is called the *canonical projection* of index i. By definition, the product therefore makes the following diagram commute:

$$\begin{array}{ccc} X' & \xrightarrow{\alpha_i} & X_i \\ \alpha & \searrow & \uparrow \mathrm{pr}_i \\ & & \prod_{i \in I} X_i \end{array}$$

If, for all $i \in I$, $X_i = X$, then $\prod_{i \in I} X_i$ is written as X^I and is a called a *power* of X. If $I = \{1, ..., n\}$, we write X^n instead of X^I. The product of X_1

and X_2 is written as $X_1 \times X_2$. In **Set**, as we saw earlier (section 1.1.2**(III)**), the existence of products (with arbitrary index sets) is guaranteed by the *axiom of choice* (Corollary 1.2).

(II) The *coproduct* (or *sum*) of a family $(X_i)_{i\in I}$ of objects in $\mathcal{C}$ is the product of this family in the opposite category $\mathcal{C}^{\mathrm{op}}$. When it exists, this coproduct is a sink $(\mathrm{inj}_i : X_i \to X)_{i\in I}$ with the universal property that, for any family of morphisms $(\beta_i)_{i\in I}$, $\beta_i : X_i \to X'$, there exists a unique morphism $\beta : X \to X'$ such that $\beta \circ \mathrm{inj}_i = \beta_i$ for all $i \in I$. The object X is written as $\coprod_{i\in I} X_i$ and the morphism $\mathrm{inj}_i : X_i \to \coprod_{i\in I} X_i$ is called the *canonical injection* of index i. By definition, the coproduct therefore makes the following diagram commute:

$$\begin{array}{ccc} X' & \xleftarrow{\beta_i} & X_i \\ \beta & \nwarrow & \downarrow \mathrm{inj}_i \\ & & \coprod_{i\in I} X_i \end{array}$$

If, for all $i \in I$, $X_i = X$, then $\coprod_{i\in I} X_i$ is written as $X^{(I)}$ and is called a *copower* of X. Coproducts (with arbitrary index sets) exist in **Set** and are called disjoint unions (or sums of sets). They are constructed as follows: if $(X_i)_{i\in I}$ is a family of sets, their *disjoint union* is:

$$X = \biguplus_{i\in I} X_i := \bigcup_{i\in I} \{i\} \times X_i.$$

(III) If every source $(\mathrm{pr}_i : X \to X_i)_{i\in I}$ in a category $\mathcal{C}$ has a product, we say that $\mathcal{C}$ admits arbitrary products (or that $\mathcal{C}$ admits products). If every sink $(\mathrm{inj}_i : X_i \to X)_{i\in I}$ in $\mathcal{C}$ has a coproduct, we say that $\mathcal{C}$ admits arbitrary coproducts (or that $\mathcal{C}$ admits coproducts). We can similarly define categories that admit finite products (when I is finite), etc.

1.2.7. *Fibered products and fibered coproducts*

Fibered products and coproducts are other examples of universal arrows:

LEMMA-DEFINITION 1.19.– *Let $\mathcal{C}$ be a category. The* fibered product *of two morphisms $f_1 : X_1 \to Z$ and $f_2 : X_2 \to Z$ over Z, if it exists, is a source $(h_i : P \to X_i)_{i=1,2}$ where $f_1 \circ h_1 = f_2 \circ h_2$ for which the following universal property is satisfied:*

Given an object S and two morphisms $u_1 : S \to X_1$ and $u_2 : S \to X_2$ such that $f_1 \circ u_1 = f_2 \circ u_2$, there exists a unique morphism $u : S \to P$ for which the following diagram commutes:

$$\begin{array}{ccccc} & & S & & \\ & {\scriptstyle u_1}\swarrow & \downarrow u & \searrow{\scriptstyle u_2} & \\ X_1 & \xleftarrow{h_1} & P & \xrightarrow{h_2} & X_2 \\ & {\scriptstyle f_1}\searrow & & \swarrow{\scriptstyle f_2} & \\ & & Z & & \end{array}$$

The triple (P, h_1, h_2) is uniquely determined up to isomorphism, and P is written as $X_1 \times_Z X$.

The notion of *fibered coproduct* (also called *fibered sum* or *amalgamated sum*[3] of a pair of morphisms $f_1 : X_1 \longleftarrow Z$ and $f_2 : X_2 \longleftarrow Z$ "over Z", written as $X_1 \coprod_Z X_2$, is dual to the notion of fibered product. In other words, it is a fibered product in the opposite category (remember to reverse the arrows!).

1.2.8. *Inductive limits and projective limits*

(I) INDUCTIVE LIMITS. Let I be a preordered index set (section 1.1.1**(III)**). This set is said to be *filtrant* if every couple $(i, j) \in I \times I$ has an upper bound, i.e. an element $k \in I$ such that $i \preceq k$ and $j \preceq k$. A filtrant set I is, much like a preordered set, a category whose objects are the elements i and whose morphisms $i \to j$ are the pairs (i, j) where $i \preceq j$.

Let $\mathcal{C}$ be a category, and let $(X_i)_{i \in I}$ be a family of objects of $\mathcal{C}$ indexed by a preordered or filtrant set I, and, for every pair $(i, j) \in I \times I$ such that $i \preceq j$, let $\varphi_j^i : X_i \to X_j$ be a morphism such that: 1) $\varphi_i^i = \mathrm{id}_{X_i}, \forall i \in I$ and 2) $i \preceq j \preceq k \Rightarrow \varphi_k^i = \varphi_k^j \circ \varphi_j^i$, which gives the commuting diagram:

$$\begin{array}{ccc} X_i & \xrightarrow{\varphi_j^i} & X_j \\ {\scriptstyle \varphi_k^i}\searrow & & \downarrow{\scriptstyle \varphi_k^j} \\ & & X_k \end{array}$$

3 The terms *pullback* and *pushout* are also respectively used for the fibered product and the fibered coproduct.

We call $\mathfrak{D} = \left\{X_i, \varphi_j^i; I\right\}$ a *direct system* (or an *inductive system*) in $\mathcal{C}$, with the index set I. Any such direct system is a covariant functor $\mathfrak{D}$ from I to $\mathcal{C}$, where $\mathfrak{D}(i) = X_i$ and $\mathfrak{D}(i \to j) = \varphi_j^i$.

DEFINITION 1.20.– *Let $\mathfrak{D} = \left\{X_i, \varphi_j^i; I\right\}$ be a direct system in $\mathcal{C}$, where I is a preordered set. The* inductive limit *(or* direct limit*) of this system, if it exists, is a functor $\mathcal{C} \to \mathcal{C}$ consisting of an object $X = \varinjlim X_i$ and a family of morphisms $\varphi_i : X_i \to X$ satisfying the condition $\varphi_i = \varphi_j \circ \varphi_i^j$ for $j \succeq i$ such that, for any object Y and all morphisms $f_i : X_i \to Y$, there exists a unique morphism $f : X \to Y$ such that $f_i = f \circ \varphi_i$. If I is a filtrant set, this inductive limit is said to be* filtrant *. The following diagram commutes:*

$$\begin{array}{ccccc}
\varinjlim X_i & & \xrightarrow{f} & & Y \\
\uparrow & \varphi_i \nwarrow & & \nearrow f_i & \uparrow \\
\downarrow & & X_i & & \downarrow \\
\varinjlim X_i & & \downarrow \varphi_j^i & & Y \\
 & \varphi_j \nwarrow & & \nearrow f_j & \\
 & & X_j & &
\end{array}$$

The inductive limit, if it exists, is a universal arrow (section 1.2.4) written as $\left(\varphi_i : X_i \to \varinjlim X_i\right)_{i \in I}$ ([MCL 98], Chap. III, section 3). For every object Y of $\mathcal{C}$, we then have the canonical isomorphism:

$$\mathrm{Hom}_C\left(\varinjlim X_i, Y\right) \cong \varprojlim \mathrm{Hom}_C\left(X_i, Y\right) \qquad [1.6]$$

which makes $Y \mapsto \mathrm{Hom}_C\left(\varinjlim F_i, Y\right)$ a representable functor (section 1.2.5(**I**)).

(II) PROJECTIVE LIMITS. A *projective limit* (or *inverse limit*) in the category $\mathcal{C}$, if it exists, is an inductive limit in the opposite category $\mathcal{C}^{\mathrm{op}}$. We say that $\mathfrak{I} = \left\{Y_i, \psi_i^j; I\right\}$ is an *inverse system* (or *projective system*) if, for any $(i, j) \in I \times I$ such that $i \preceq j$, we have that $\psi_i^j : Y_i \longleftarrow Y_j$ and these morphisms satisfy: 1) $\psi_i^i = \mathrm{id}_{Y_i}, \forall i \in I$ and 2) $\psi_i^k = \psi_i^j \circ \psi_j^k$ for $i \preceq j \preceq k$. An inverse system is a contravariant functor $\mathfrak{C}$ from I to $\mathcal{C}$ where $\mathfrak{C}(i) = X_i$ and (with

$i \to j = (i,j))\ \mathfrak{C}(i \to j) = \psi_i^j$; so the following diagram commutes:

$$\begin{array}{ccc} Y_i & \xleftarrow{\psi_i^j} & Y_j \\ \psi_i^k & \nwarrow & \uparrow \psi_j^k \\ & & Y_k \end{array}$$

DEFINITION 1.21.– *Let* $\mathfrak{I} = \left\{Y_i, \psi_i^j; I\right\}$ *be an inverse system in* $\mathcal{C}$*, where* I *is a preordered set. The* projective limit *(or* inverse limit*) of this system, if it exists, is a functor* $\mathcal{C} \to \mathcal{C}$ *consisting of an object* $Y = \varprojlim Y_i$ *and a family of morphisms* $\psi_i : Y_i \longleftarrow Y$ *satisfying* $\psi_i = \psi_i^j \circ \psi_j$ *for* $j \succeq i$ *such that, for any object* X *and all morphisms* $f_i : Y_i \longleftarrow X$*, there exists a unique morphism* $f : Y \longleftarrow X$ *such that* $f_i = \psi_i \circ f$*. If* I *is a filtrant set, this projective limit is said to be* filtrant*. The following diagram commutes:*

$$\begin{array}{ccccc} \varprojlim Y_i & & \xleftarrow{f} & & X \\ \uparrow & \psi_i \searrow & & \swarrow f_i & \uparrow \\ \downarrow & & Y_i & & \downarrow \\ \varprojlim Y_i & & \uparrow \psi_i^j & & X \\ & \psi_j \searrow & & \swarrow f_j & \\ & & Y_j & & \end{array}$$

The projective limit of this system, if it exists, is written as $\psi_i : \varprojlim Y_i \to Y_i$. Then, for every object X of $\mathcal{C}$, we have the canonical isomorphism:

$$\mathrm{Hom}_C\left(X, \varprojlim Y_i\right) \cong \varprojlim \mathrm{Hom}_C\left(X, Y_i\right) \qquad [1.7]$$

and $X \mapsto \mathrm{Hom}_C\left(X, \varprojlim Y_i\right)$ is a representable functor.

PROPOSITION 1.22.– *Let* $\mathfrak{a} \geq 3$ *be a cardinal.* The following conditions are equivalent*:*

1) Every projective system indexed by a preordered set I *of cardinal* $\mathrm{Card}\,(I) \leq \mathfrak{a}$ *admits a projective limit.*

2) Every family $(X_i)_{i \in I}$ *where* $\mathrm{Card}\,(I) \leq \mathfrak{a}$ *admits a product in* $\mathcal{C}$ *and every double arrow* $A \underset{g}{\overset{f}{\leftleftarrows}} B$ *admits an equalizer.*

3) Every family $(X_i)_{i\in I}$ *where* $\mathrm{Card}\,(I) \leq \mathfrak{a}$ *admits a product in* $\mathcal{C}$ *and every pair of morphisms* $f_1 : X_1 \to Z$ *and* $f_2 : X_2 \to Z$ *admits a fibered product over* Z. Dually, the following conditions are equivalent*:*

1') Every injective system indexed by a preordered set I *of cardinal* $\mathrm{Card}\,(I) \leq \mathfrak{a}$ *admits an injective limit.*

2') Every family $(X_i)_{i\in I}$ *where* $\mathrm{Card}\,(I) \leq \mathfrak{a}$ *admits a coproduct in* $\mathcal{C}$ *and every double arrow* $A \underset{g}{\overset{f}{\rightrightarrows}} B$ *admits a coequalizer.*

3') Every family $(X_i)_{i\in I}$ *where* $\mathrm{Card}\,(I) \leq \mathfrak{a}$ *admits a coproduct in* $\mathcal{C}$ *and every pair of morphisms* $f_1 : X_1 \longleftarrow Z$, $f_2 : X_2 \longleftarrow Z$ *admits a fibered coproduct over* Z.

PROOF.–

(2) $\Rightarrow$(1): For $i \preceq j$, set $Y_{ij} = Y_i$, $\alpha_{ij} = \mathrm{pr}_i$, where $\mathrm{pr}_i : \prod_{i\in I} Y_i \to Y_i$ is the canonical projection and $\beta_{ij} = \psi_i^j \circ \mathrm{pr}_j$. Then, $\alpha = (\alpha_{ij})_{i\in I, i\preceq j}$ and $\beta = (\beta_{ij})_{i,j\in I, i\preceq j}$ are morphisms from $\prod_{i\in I} Y_i$ to $\prod_{i,j\in I, i\preceq j} Y_{ij}$, and the equalizer of the double arrow $\underset{\beta}{\overset{\alpha}{\rightrightarrows}}$ is the projective limit $Y := \varprojlim Y_i \to Y_i$ as required:

$$\begin{array}{ccccc} Y & \to & \prod\limits_{i\in I} Y_i & \underset{\beta}{\overset{\alpha}{\rightrightarrows}} & \prod\limits_{i,j\in I, i\preceq j} Y_{ij} \\ & \beta_i \searrow & \mathrm{pr}_i \downarrow & & \\ & & Y_i & & \end{array}$$

(1) $\Rightarrow$(3): When $I = \{1, 2, 3\}$ with $1 \preceq 2$ and $1 \preceq 3$, the projective limit of the inverse system

$$\begin{array}{ccccc} Y_2 & \overset{\psi_2}{\dashleftarrow} & P & \overset{\psi_1}{\dashrightarrow} & Y_3 \\ & \psi_1^2 \searrow & & \swarrow \psi_1^3 & \\ & & Y_1 & & \end{array}$$

is the fibered product $P = Y_2 \times_{Y_1} Y_3$. Let I be a set such that $\mathrm{Card}\,(I) \leq \mathfrak{a}$, equipped with the discrete order relation, namely $i \preceq j$ if and only if $i = j$. Then, $\varprojlim Y_i = \prod_{i\in I} Y_i$.

(3) $\Longrightarrow$(2): Consider the double arrow $X_1 \underset{g_2}{\overset{g_1}{\rightrightarrows}} X_2$, the morphism $f_1 : X_1 \to P := X_1 \times X_2$ with components (g_1, g_2) and the morphism $f_2 : X_2 \to P$ with

components $(\mathrm{id}_{X_2}, \mathrm{id}_{X_2})$. The fibered product $X_1 \times_P X_2$ of f_1, f_2 over P is the equalizer of (g_1, g_2). ■

COROLLARY 1.23.– *Equalizers, products and fibered products are projective limits. Coequalizers, coproducts and fibered sums are inductive limits.*

(III) A category $\mathcal{C}$ is said to be *complete* (resp. *cocomplete*) if, for any preordered index set I, every projective (resp. inductive) system indexed by I has a limit in $\mathcal{C}$.

1.2.9. *Exact functors and adjoint functors*

(I) EXACT FUNCTORS. A covariant functor $\mathfrak{F} : \mathcal{C} \to \mathcal{D}$, where $\mathcal{C}$ and $\mathcal{D}$ are categories admitting finite projective (resp. inductive) limits (i.e. with finite index set I), is said to be *left-exact* (resp. *right-exact*) if it commutes with *finite* projective (resp. inductive) limits. This functor is said to be *exact* if it is both left-exact and right-exact (assuming that $\mathcal{C}$ and $\mathcal{D}$ admit finite projective and inductive limits). More intuitively, $\mathfrak{F}$ is left-exact (resp. right-exact) if, for every inverse system $\mathfrak{I} = \left\{Y_i, \psi_i^j; I\right\}$ (resp. any direct system $\mathfrak{D} = \left\{X_i, \varphi_j^i; I\right\}$) where I is finite,

$$\mathfrak{F}\left(\varprojlim_{i\in I} Y_i\right) = \varprojlim_{i\in I} \mathfrak{F}(Y_i) \quad \left(\text{resp. } \mathfrak{F}\left(\varinjlim_{i\in I} Y_i\right) = \varinjlim_{i\in I} \mathfrak{F}(Y_i)\right).$$

A (contravariant) functor $\mathfrak{F} : \mathcal{C}^{\mathrm{op}} \to \mathcal{D}$ is said to be left-exact (resp. right-exact) if (for finite I)

$$\mathfrak{F}\left(\varinjlim_{i\in I} Y_i\right) = \varprojlim_{i\in I} \mathfrak{F}(Y_i) \quad \left(\text{resp. } \mathfrak{F}\left(\varprojlim_{i\in I} Y_i\right) = \varinjlim_{i\in I} \mathfrak{F}(Y_i)\right).$$

In particular, [1.7] and [1.6] imply that the functors $\mathrm{Hom}_{\mathcal{C}}(X, -)$ and $\mathrm{Hom}_{\mathcal{C}}(-, Y)$ are left-exact.

(II) ADJOINT FUNCTORS. Let $\mathfrak{D} : \mathcal{C} \to \mathcal{D}$ and $\mathfrak{G} : \mathcal{D} \to \mathcal{C}$ be two functors. The pair $(\mathfrak{G}, \mathfrak{D})$ is said to be *adjoint* if there exists a functorial isomorphism (section 1.2.2(**I**))

$$\mathfrak{t} : \mathrm{Hom}_{\mathcal{C}}(\mathfrak{G}(-), -) \cong \mathrm{Hom}_{\mathcal{D}}(-, \mathfrak{D}(-))$$

or, more intuitively, writing $\langle -,- \rangle = \mathrm{Hom}\,(-,-)$, which serves as the "duality bracket" (section 3.1.2)

$$\boxed{\mathbf{t} : \langle \mathfrak{G}\,(-)\,,- \rangle \cong \langle -, \mathfrak{D}\,(-) \rangle}.$$

This defines the following relation, for all $C \in \mathrm{Ob}\,(\mathcal{C})$ and all $D \in \mathrm{Ob}\,(\mathcal{D})$,

$$\mathbf{t}_{C,D} : \mathrm{Hom}_{\mathcal{C}}\,(\mathfrak{G}\,(C)\,, D) \cong \mathrm{Hom}_{\mathcal{D}}\,(C, \mathfrak{D}\,(D))$$

which is a natural bijection in each variable. We say that $\mathfrak{G}$ admits the right adjoint $\mathfrak{D}$ and that $\mathfrak{D}$ admits the left adjoint $\mathfrak{G}$. If so, it can be shown that every left adjoint $\mathfrak{G}'$ of $\mathfrak{D}$ is canonically isomorphic to $\mathfrak{G}$ and that every right adjoint $\mathfrak{D}'$ of $\mathfrak{G}$ is canonically isomorphic to $\mathfrak{D}$ (i.e. there exists a *unique* functorial isomorphism $\mathfrak{D} \tilde{\to} \mathfrak{D}'$). It follows from the definitions that $\mathfrak{G} : \mathcal{D} \to \mathcal{C}$ admits a right adjoint if and only if the (contravariant) functor $C^{\mathrm{op}} \mapsto \mathrm{Hom}_{\mathcal{C}}\,(\mathfrak{G}\,(C)\,, D)$ is representable, and that $\mathfrak{D} : \mathcal{C} \to \mathcal{D}$ admits a left adjoint if and only if the covariant functor $D \mapsto \mathrm{Hom}_{\mathcal{D}}\,(C, \mathfrak{D}\,(D))$ is representable ([KAS 06], Thm. 1.5.3). The following result also holds ([KAS 06], Prop. 2.1.10):

PROPOSITION 1.24.– *Let $\mathcal{C}$ and $\mathcal{D}$ be two categories.*

i) Suppose that every projective system indexed by a preordered set I admits a projective limit in $\mathcal{C}$. Then, if $\mathfrak{D} : \mathcal{C} \to \mathcal{D}$ admits a left adjoint, this functor commutes with projective limits indexed by I.

ii) Suppose that every injective system indexed by a preordered set I admits an injective limit in $\mathcal{C}$. Then, if $\mathfrak{G} : \mathcal{D} \to \mathcal{C}$ admits a right adjoint, this functor commutes with injective limits indexed by I.

1.2.10. *Projective objects and injective objects*

(I) PROJECTIVE OBJECTS. Let $\mathcal{C}$ be a category. An object P of $\mathcal{C}$ is said to be *projective* if the covariant functor $\mathbf{j}_P = \mathrm{Hom}_{\mathcal{C}}\,(P,-) : \mathcal{C} \to \mathbf{Set}$ conserves epimorphisms, i.e. for every epimorphism $f : X \twoheadrightarrow Y$ in $\mathcal{C}$, $\mathbf{j}_P\,(f) : \mathrm{Hom}_{\mathcal{C}}\,(P,X) \to \mathrm{Hom}_{\mathcal{C}}\,(P,Y)$ is surjective, or alternatively if for every $\beta : P \to Y$ there exists $\alpha : P \to X$ such that $\mathbf{j}_P\,(f)\,(\alpha) = \beta$, where

$\mathbf{j}_P(f)(\alpha) := f \circ \alpha$:

$$\begin{array}{ccc} & P & \\ & \downarrow \beta & \\ X & \overset{f}{\twoheadrightarrow} & Y \end{array} \Longrightarrow \exists \alpha : \quad \begin{array}{ccc} & & P \\ & \overset{\alpha}{\swarrow} & \downarrow \beta \\ X & \overset{f}{\twoheadrightarrow} & Y \end{array}$$

If $\mathcal{C}$ has coproducts indexed by I, it follows from [1.6] that, for any object Y,

$$\mathrm{Hom}_{\mathcal{C}}\left(\coprod_{i\in I} P_i, Y\right) = \coprod_{i\in I} \mathrm{Hom}_{\mathcal{C}}(P_i, Y) \qquad [1.8]$$

and consequently $\coprod_{i\in I} P_i$ is projective if each P_i is projective; conversely, if $\mathcal{C}$ admits a zero object (section 1.1.1(**IV**)) and $\coprod_{i\in I} P_i$ is projective, then each P_i is projective ([MIT 65], Chap. II, Prop. 14.3).

A category $\mathcal{C}$ is said to have *sufficiently many projectives* if for any object A there exists an epimorphism $P \twoheadrightarrow A$, where P is projective. If $r : A \twoheadrightarrow P$ is an epimorphism and P is projective, then r is a retraction (section 1.1.1(**III**)); conversely, if P has the property that every epimorphism $A \twoheadrightarrow P$ is a retraction and $\mathcal{C}$ has sufficiently many projectives, then P is projective ([MIT 65], Chap. II, Prop. 14.2).

Let $f : X \twoheadrightarrow Y$ be an epimorphism in $\mathbf{Set}$. From Corollary 1.2, f admits a section $\alpha : Y \to X$, so $\mathbf{j}_Y(f)(\alpha) = \mathrm{id}_Y$, and hence Y is projective. Consequently, every object in $\mathbf{Set}$ is projective.

(II) INJECTIVE OBJECTS. An object I of $\mathcal{C}$ is *injective* if it is projective in $\mathcal{C}^{\mathrm{op}}$; in other words, if $\mathbf{h}_I = \mathrm{Hom}_{\mathcal{C}}(-, I) : \mathcal{C} \to \mathbf{Set}$ conserves monomorphisms or, alternatively, if for any monomorphism $f : X \hookrightarrow Y$ and any morphism $\beta : X \to I$ there exists a morphism $\alpha : Y \to I$ such that $\beta = \alpha \circ f$:

$$\begin{array}{ccc} X & \overset{f}{\hookrightarrow} & Y \\ \beta \downarrow & & \\ I & & \end{array} \Longrightarrow \exists \alpha : \quad \begin{array}{ccc} X & \overset{f}{\hookrightarrow} & Y \\ \beta \downarrow & \overset{\alpha}{\swarrow} & \\ I & & \end{array}$$

Readers should carefully "dualize" the properties of the projective objects listed above to obtain "translations" for injective objects. In particular, a category $\mathcal{C}$ is said to have *sufficiently many injectives* if for any object A there exists a monomorphism $A \hookrightarrow I$, where I is injective. It follows from Lemma 1.1 that every non-empty object in $\mathbf{Set}$ is injective.

1.2.11. *Generators and cogenerators*

Let $\mathcal{C}$ be a category. An object U of $\mathcal{C}$ is said to be a *generator* of $\mathcal{C}$ if the functor $\mathbf{j}_U : \mathcal{C} \to \mathbf{Set}$ is faithful. An object W of $\mathcal{C}$ is a *cogenerator* if it is a generator of $\mathcal{C}^{\mathrm{op}}$ or, in other words, if the functor $\mathbf{h}_W : \mathcal{C}^{\mathrm{op}} \to \mathbf{Set}$ is faithful.

PROPOSITION 1.25.– *1) If the category $\mathcal{C}$ admits arbitrary coproducts (section 1.2.6**(II)**), an object U is a generator of $\mathcal{C}$ if and only if for all $A \in \mathrm{Ob}(\mathcal{C})$ there exists a set I and an epimorphism $\beta : U^{(I)} \twoheadrightarrow A$.*

2) Dually, *if the category $\mathcal{C}$ admits arbitrary products (section 1.2.6**(I)**), an object W is a cogenerator of $\mathcal{C}$ if and only if for all $A \in \mathrm{Ob}(\mathcal{C})$ there exists a set I and a monomorphism $\beta : A \hookrightarrow W^I$.*

PROOF.– It is sufficient to prove (1). The functor $\mathbf{j}_U$ is faithful if and only if for any objects A, B and any morphisms $\delta_1, \delta_2 : B \to A$, the equality $\mathbf{j}_U(\delta_1) = \mathbf{j}_U(\delta_2)$ implies that $\delta_1 = \delta_2$ (section 1.2.1(**III**)). But $\mathbf{j}_U(\delta_2) = \mathbf{j}_U(\delta_1)$ if and only if for every morphism $i : U \to A$, $\delta_1 \circ i = \delta_2 \circ i$ (section 1.2.3). Let $I = \mathrm{Hom}_{\mathcal{C}}(U, A)$ and $\beta : U^{(I)} \to A : \beta_i = i, \forall i \in I$. The above condition is satisfied if and only if β is an epimorphism (section 1.1.1(**III**)). ■

1.3. Structures

1.3.1. *Concrete categories*

(I) In algebra, we work with the structures of groups, rings, fields, vector spaces, etc. In analysis, we work with the structures of topological spaces, metric spaces, etc. Let $\mathcal{X}$ be a category. A *concrete category* with base $\mathcal{X}$ is a category $\mathcal{C}$ equipped with a faithful functor $|.| : \mathcal{C} \to \mathcal{X}$, called the *forgetful functor*. This concrete category is written as $(\mathcal{C}, |.|, \mathcal{X})$; often, $\mathcal{X} = \mathbf{Set}$ and the category $\mathcal{X}$ is implied. For example, the category $\mathbf{Grp}$ is a concrete category with base $\mathbf{Set}$; for any group G, $|G|$ is the underlying set and, for any group morphism $f : G \to H$, $|f|$ is the *function* f. Given a category $\mathcal{C}$ with base $\mathbf{Set}$, we will henceforth write $A \subseteq B$ when $\mathrm{can} : A \to B$ is a subobject of B in $\mathcal{C}$, and we will write $A \subset B$ when $|A| \subset |B|$. We will also write $A \subsetneq B$ when $\mathrm{can} : A \to B$ is a subobject of B such that $|A| \subsetneq |B|$. We then say that $\mathrm{can} : A \to B$ is a *proper subobject* of B. We say that the $\mathcal{X}$-morphism $f : |B| \to |A|$ is a $\mathcal{C}$-morphism if there exists a $\mathcal{C}$-morphism $B \to A$ (necessarily unique, also written as f) such that $|B \to A| = |B| \to |A|$. A *structured arrow* is a pair (f, A), where $A \in \mathcal{C}$ and

$f : X \to |A|$ is a $\mathcal{X}$-morphism. Given a concrete category $(\mathcal{C}, |.|, \mathcal{X})$, the *opposite* concrete category is $(\mathcal{C}^{\mathrm{op}}, |.|^{\mathrm{op}}, \mathcal{X}^{\mathrm{op}})$ where $|A|^{\mathrm{op}} = |A|$ and $|B \longleftarrow A|^{\mathrm{op}} = |B \longleftarrow A|$, using the obvious notation.

(II) Two objects A and B of the concrete category $(\mathcal{C}, |.|, \mathcal{X})$ are said to be *equivalent* if $|A| = |B|$ and if there exists an isomorphism $A \to B$. We thus define an equivalence relation on the objects of $(\mathcal{C}, |.|, \mathcal{X})$, and the equivalence class of A, written as $\bar{A}$, is called the *structure* of A in $(\mathcal{C}, |.|, \mathcal{X})$. We say that A has a *finer* structure than B (or that B has a coarser structure than A) in $(\mathcal{C}, |.|, \mathcal{X})$, writing $\bar{A} \preceq \bar{B}$ (or $\bar{B} \succeq \bar{A}$), if $|A| = |B|$ and there exists a morphism $A \to B$ (necessarily unique) such that $|A \to B| = \mathrm{id}_{|A|}$. For example, let $\mathfrak{T}_1, \mathfrak{T}_2$ be topologies on a set X; the topology $\mathfrak{T}_1$ is finer than $\mathfrak{T}_2$ if and only if id_X is continuous from the topological space $(X, \mathfrak{T}_1)$ to the topological space $(X, \mathfrak{T}_2)$ ([P2], section 2.3.4). The relation $\bar{A} \preceq \bar{B}$ is an order relation on the structures of $(\mathcal{C}, |.|, \mathcal{X})$. We have that $\bar{A} \preceq \bar{B}$ in $(\mathcal{C}, |.|, \mathcal{X})$ if and only if $\bar{A} \succeq \bar{B}$ in the opposite concrete category.

1.3.2. *Initial structures and terminal structures*

(I) A source $\mathcal{S} = (f_i : A \to A_i)_{i \in I}$ of $(\mathcal{C}, |.|, \mathcal{X})$ is said to be *initial* if the following condition is satisfied: for any object B of $\mathcal{C}$, the relation "$f : |B| \to |A|$ is a $\mathcal{C}$-morphism" is equivalent to the relation "for any $i \in I$, $f_i \circ f : |B| \to |A_i|$ is a $\mathcal{C}$-morphism". We then say that the structure of A is *initial* for the family of $\mathcal{X}$-morphisms $(f_i : |A| \to |A_i|)_{i \in I}$. If A has an initial structure for the family of $\mathcal{X}$-morphisms $(f_i : |A| \to |A_i|)_{i \in I}$, A has the coarsest structure of all structures for which the $\mathcal{X}$-morphisms $f_i : |A| \to |A_i|$ are $\mathcal{C}$-morphisms (**exercise**). This structure is therefore unique.

Let $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ be three categories, let $\mathfrak{O}_1 : \mathcal{C}_1 \to \mathcal{C}_2$ and $\mathfrak{O}_2 : \mathcal{C}_2 \to \mathcal{C}_3$ be forgetful functors and let $\mathcal{S} = (f_i : \mathfrak{O}_1(A) \to \mathfrak{O}_1(A_i))_{i \in I}$ and $\mathcal{T}_i = (g_{ij} : \mathfrak{O}_2(A_i) \to \mathfrak{O}_2(A_{ij}))_{j \in J}$ be sources of $(\mathcal{C}_1, \mathfrak{O}_1, \mathcal{C}_2)$ and $(\mathcal{C}_2, \mathfrak{O}_2, \mathcal{C}_3)$ respectively for all $i \in I$. Then, $\mathcal{U} = (g_{ij} \circ f_i : \mathfrak{O}_2 \circ \mathfrak{O}_1(A) \to \mathfrak{O}_2 \circ \mathfrak{O}_1(A_{ij}))_{(i,j) \in I \times J}$ is a source of $(\mathcal{C}_1, \mathfrak{O}_2 \circ \mathfrak{O}_1, \mathcal{C}_3)$. Suppose that for any $i \in I$, there exists an initial structure of A_i for $\mathcal{T}_i$ equip A_i with this structure. Then, there exists an initial structure of A for $\mathcal{U}$ if and only if there exists an initial structure of A for $\mathcal{S}$, and these initial structures coincide (*transitivity of initial structures*) ([BKI 70], Chap. IV, section 2.3).

(II) The notions of *initial source* and *initial structure* are dual to the notions of terminal source and terminal structure. The above results still hold with the arrows reversed. In particular, if A has a terminal structure for the family of $\mathcal{X}$-morphisms $(f_i : |A| \longleftarrow |A_i|)_{i\in I}$, A has the finest structure of all structures for which all $f_i : |A| \longleftarrow |A_i|$ are $\mathcal{C}$-morphisms, and so this structure is unique. Readers may wish to derive a theorem for the transitivity of terminal structures from **(I)** by reversing the arrows.

1.3.3. *Concrete functors*

(I) Products (with arrbitrary index sets) exist in $\mathbf{Set}$ (Corollary 1.2), as well as in $\mathbf{Grp}$, $\mathbf{Ab}$, $\mathbf{Rng}$, $\mathbf{ComRng}$, $\mathbf{Top}$, ${}_{\mathbf{K}}\mathbf{Vect}$ and ${}_{\mathbf{K}}\mathbf{Mod}$ (section 3.1.3) where they commute with forgetful functors that take values in $\mathbf{Set}$; in other words, by viewing these categories as concrete categories with base $\mathbf{Set}$, we obtain $\left|\mathrm{pr}_i : \prod_{j\in I} X_j \to X_i\right| = \prod_{j\in I} |X_j| \to |X|$ in each case. In these concrete categories, the product of a family $(X_i)_{i\in I}$ therefore has the initial structure for the family $\left(\mathrm{pr}_i : \prod_{j\in I} |X_j| \to |X|\right)_{i\in I}$. Consequently, we say that these categories admit *concrete products* (with arbitrary index sets).

(II) The notion of concrete coproduct is dual to the notion of concrete product. Concrete coproducts (with arbitrary index sets) exist in the categories $\mathbf{Ab}$, $\mathbf{Rng}$, $\mathbf{ComRng}$, $\mathbf{Top}$, ${}_{\mathbf{K}}\mathbf{Vect}$ and ${}_{\mathbf{K}}\mathbf{Mod}$. In the category $\mathbf{Grp}$, there exist coproducts (called free products: see section 2.2.1), but they are not concrete. We can similarly define *concrete* fibered products and coproducts, *concrete* projective and inductive limits, etc. They exist in $\mathbf{Ab}$, $\mathbf{Rng}$, $\mathbf{ComRng}$, $\mathbf{Top}$, ${}_{\mathbf{K}}\mathbf{Vect}$ and ${}_{\mathbf{K}}\mathbf{Mod}$. More generally, a functor between concrete categories $\mathfrak{F} : (\mathcal{C}, |.|, \mathcal{X}) \to (\mathcal{D}, |.|, \mathcal{X})$ with the same base $\mathcal{X}$ is said to be *concrete* if it commutes with the forgetful functor.

1.3.4. *Free objects, free functor*

Let $(\mathcal{C}, |.|, \mathbf{Set})$ be a concrete category and let X be a set. Suppose that there exists an object $A \in \mathcal{C}$ and a structured arrow (section 1.3.1**(I)**) (υ_X, A), $\upsilon_X : X \to |A|$ for which the following condition is satisfied:

(**F**) For any object $B \in \mathcal{C}$, and any structured arrow $f : X \to |B|$, there exists a uniquely determined $\mathcal{C}$-morphism $\hat{f} : A \to B$ such that $f = \left|\hat{f}\right| \circ \upsilon_X$.

Then, (υ_X, A) is called a *universal arrow* on X (compare with section 1.2.4). A *free object* on X is an object A for which there exists a universal arrow (υ_X, A) on X. For example, a $\mathbf{K}$-vector space V (where $\mathbf{K}$ is a field) is a free object on any basis of V (**exercise**). If for every set X there exists a free object $\mathfrak{F}(X)$ on X, we say that $(\mathcal{C}, |.|, \mathbf{Set})$ *admits free objects*. Let $\mathfrak{F}$ be the functor $\mathbf{Set} \to \mathcal{C} : X \mapsto \mathfrak{F}(X), f \mapsto \hat{f}$. The condition (**F**) then means that the mapping

$$\mathrm{Hom}_{\mathcal{C}}(\mathfrak{F}(X), Y) \to \mathrm{Hom}_{\mathbf{Set}}(X, |Y|)$$

is bijective, or alternatively that the functor $\mathfrak{F}$ is a left adjoint of the forgetful functor $|.|$ (section 1.2.9**(II)**). The functor $\mathfrak{F}$ is called the *free functor*.

2

Elementary Algebraic Structures

The elementary algebraic structures gradually emerged throughout the 19th Century. The first such structures were groups, which were already implicit in the work performed by C.F. Gauss, J.-L. Lagrange and A.-L. Cauchy but only truly initiated by E. Galois, and fields, which were formalized by the successors of Gauss. Lattices and fields were introduced by R. Dedekind (1871), and commutative rings were introduced by D. Hilbert (1897). Division rings, the first example of which was given by W. Hamilton (1843), were not systematically studied until E. Steinitz (1910). The work performed on these topics was summarized in the classical book by B.L. van der Waerden [VAN 31] following the lectures given by E. Noether and E. Artin between 1926 and 1928. This book was regularly updated until 1967 over the course of seven editions. Many mathematicians (including Ø. Ore, N. Jacobson, I. Kaplansky and P.M. Cohn) later contributed to the development of the theory of non-commutative rings. The theory of determinants (section 2.3.11) gradually began to emerge during the second half of the 18th Century, with G. Cramer, E. Bézout and P.-S. Laplace, well before the concept of matrices was introduced. Methods for calculating these determinants were systematically developed around 1815 by Cauchy, with further progress around 1850 by J. Sylvester and A. Cayley. However, a definitive formalization (Definition 2.63) was not found until L. Kronecker and K. Weierstrass in 1870–1880, even though the notion of matrix was introduced in 1850 by J. Sylvester and the notion of the rank of a matrix was proposed by F. Frobenius shortly thereafter.

2.1. Monoids and ordered sets

2.1.1. *Monoids and divisibility*

(I) MONOIDS. A *monoid* $\mathbf{M}$ is a non-empty set equipped with an associative internal binary operation $(x, y) \mapsto xy$ (i.e. $x(yz) = (xy)z, \forall x, y, z \in \mathbf{M}$) and a neutral element e ($ex = xe = x, \forall x \in \mathbf{M}$), also called the *unit element* of $\mathbf{M}$, written as 1. The morphisms of the category of monoids are the mappings $f : \mathbf{M} \to \mathbf{N}$ such that $f(xy) = f(x) f(y), \forall x, y \in \mathbf{M}$, which implies that $f(1) = 1$. An element $x \in \mathbf{M}$ is said to be *left-invertible* (resp. *right-invertible*) if there exists $y \in \mathbf{M}$ such that $yx = 1$ (resp. $xy = 1$) and *invertible* if it is both left- and right-invertible. If so, the inverse of x is necessarily unique and is written as x^{-1}. The set of invertible elements (or *units*) of a monoid $\mathbf{M}$ is a submonoid and is a group, written as $\mathbf{U}(\mathbf{M})$. If x, y are two elements such that $x = uy$ (resp. $x = yu$) with $u \in \mathbf{U}(\mathbf{M})$, then x and y are said to be *left-associated* (resp. *right-associated*) and x and y are said to be *associated* if there exist $u, v \in \mathbf{U}(\mathbf{M})$ such that $x = uyv$.

A zero of $\mathbf{M}$, if it exists, is an absorbing element ($x.0 = 0.x = 0$). Any such element is a zero in the category of monoids with zero (section 1.1.1**(IV)**). If $\mathbf{M}$ is a monoid with zero, we write $\mathbf{M}^{\times}$ for the submonoid $\complement_{\mathbf{M}}\{0\}$. One example of a monoid is $(\mathbb{N}, \times)$, where $\mathbb{N} = \{0, 1, 2, ...\}$. This monoid has a zero, and $\mathbb{N}^{\times} = \{1, 2, ...\}$ is the set of natural integers.

The internal binary operation of commutative monoids is sometimes written additively; in this case, the neutral element is written as 0 but is not a zero in the sense defined above. For example, $(\mathbb{N}, +)$ is a commutative monoid with neutral element 0, but $n + 0 \neq 0, \forall n \geq 1$.

Let $\mathbf{M}$ be a monoid and $S \subset \mathbf{M}$. The set S is called a *generator* of $\mathbf{M}$ if $\mathbf{M}$ is the smallest monoid containing S, i.e. the intersection of all monoids containing S. If so, we write $\mathbf{M} = [S]$. A monoid is said to be *finitely generated* if it is generated by a finite set and *monogenous* if it generated by a singleton $\{x\}$. We have that $[\{x\}] = \{x^n : n \geq 0\}$, and so monogenous monoids are commutative. The monoid generated by the elements $x_1, ..., x_n$ is typically written $[x_1, ..., x_n]$ rather than $[\{x_1, ..., x_n\}]$.

(II) DIVISIBILITY. In the rest of this subsection, monoids are written multiplicatively and have zeros.

An element $x \in \mathbf{M}^{\times}$ is said to be *left-cancellable* (resp. *right-cancellable*) if $xy = xz \Rightarrow y = z$ (resp. $yx = zx \Rightarrow y = z$) and *cancellable* if it is both left- and right-cancellable. A monoid $\mathbf{M}$ with the property, that every element of $\mathbf{M}^{\times}$ is cancellable, is said to be a *cancellation monoid*.

Let $a, b \in \mathbf{M}$. We say that b is a right multiple of a, or that a is a left divisor of b, if there exists $c \in \mathbf{M}$ such $b = ac$ or, in other words, $b \in a\mathbf{M}$. If a is both a left divisor and a right divisor of b, or in other words if $b \in a\mathbf{M} \cap \mathbf{M}a$, we write $a \mid b$. This is an order relation.

An element $a \in \mathbf{M}$ is said to be *right-regular* if it is not a left zero-divisor (i.e. $ab \neq 0, \forall b \in \mathbf{M}^{\times}$); we similarly define the notion of *left-regular* elements, and we say that an element is *regular* if it is both left- and right-regular.

EXAMPLE 2.1.– *The set $\mathfrak{M}_n(\mathbb{Z})$ of $n \times n$ square matrices with elements in $\mathbb{Z}$ is a non-commutative monoid under multiplication that contains both left and right zero-divisors. Let $A_1, ..., A_n$ be matrices with elements in $\mathbb{Z}$ such that the number of columns of A_i is equal to the number of rows of A_{i+1} $(i = 1, ..., n-1)$. Then, padding these matrices with rows of zeros on the bottom and columns of zeros on the right, we can reduce to the case where the matrices A_i are in the monoid $\mathfrak{M}_n(\mathbb{Z})$ for some sufficiently large n.*

An *atom* (or *irreducible element*) of $\mathbf{M}$ is a regular element that cannot be written in the form uv with $u, v \in \complement_{\mathbf{M}}\mathbf{U}(\mathbf{M})$. Let $a \in \mathbf{M}$ and let $a = a_1....a_n$ be a factorization such that each a_i is an atom. Then, this factorization is said to be *complete*. An element a with a complete factorization is said to be *atomic*. A monoid in which every element $\neq 0$ is atomic is called an *atomic monoid*.

An element c of a monoid $\mathbf{M}$ is said to be *invariant* if it is regular and $c\mathbf{M} = \mathbf{M}c$; this means that the set of right divisors of c is equal to the set of its left divisors. The monoid $\mathbf{M}$ is said to be *invariant* if every element of $\mathbf{M}^{\times}$ is invariant. Commutative cancellation monoids are invariant. A regular element p in a monoid $\mathbf{M}$ is said to be *prime* if $p \mid ab \Longrightarrow p \mid a$ or $p \mid b$.

LEMMA 2.2.– *Every prime element in an invariant monoid is an atom.*

PROOF.– If $p = ab$ is prime, then $p \mid a$ or $p \mid b$; for example $a = pq$, so $p = pqb$, and hence $qb = 1$ since p is regular. Therefore $\mathbf{M}b = \mathbf{M}$, and since

$\mathbf{M}$ is invariant, $b\mathbf{M} = \mathbf{M}$. Consequently, b is left- and right-invertible, and so is invertible. It follows that p is an atom. ■

Let $a, b \in \mathbf{M}^\times$. We say that a is a *total divisor* of b, writing $a \parallel b$, if there exists an invariant element c such that $a \mid c$ and $c \mid b$. The relation $a \parallel b$ is a preorder relation (section 1.1.1**(III)**). We have that $c \parallel c$ if and only if c is invariant, so the relation $a \parallel b$ is only an order relation if the monoid $\mathbf{M}$ is invariant.

2.1.2. *Ordered sets*

(I) Let $(P, \leq)$ be an ordered set (section 1.1.2**(III)**). We write $[a, b] \subset P$ for the (closed) *interval* of elements $x \in P$ such that $a \leq x \leq b$. Setting $a \geq b$ if and only if $b \leq a$, $(P, \geq)$ is again an ordered set, called the *dual* of $(P, \leq)$. The morphisms of the category of ordered sets are the monotone mappings, which are called *isotone* if they are increasing, and *antitone* if they are decreasing. The infimum of a family of elements $(a_i)_{i\in I}$, if it exists, is the greatest lower bound of the set $\{a_i : i \in I\}$ and is written as $\bigwedge_{i\in I} a_i$ or $\inf\{a_i : i \in I\}$. The supremum of this family, if it exists, is the least upper bound and is written as $\bigvee_{i\in I} a_i$ or $\sup\{a_i : i \in I\}$.

(II) GALOIS CONNECTIONS. A Galois *connection* between two ordered sets $(P, \leq)$ and $(Q, \leq)$ consists of two antitone mappings, written as $P \ni x \mapsto x^\perp \in Q$ and $Q \ni y \mapsto y^\perp \in P$, such that:

$$\boxed{y \leq x^\perp \Leftrightarrow x \leq y^\perp \quad (x \in P, y \in Q)}. \qquad [2.1]$$

THEOREM 2.3.– *Let $P \ni x \mapsto x^\perp \in Q$ and $Q \ni y \mapsto y^\perp \in P$ be two antitone mappings, where $(P, \leq)$ and $(Q, \leq)$ are two ordered sets.*

1) If these mappings form a Galois connection, the following conditions are satisfied for all $x \in P, y \in Q$:

i) $x \leq x^{\perp\perp}$, $y \leq y^{\perp\perp}$.

ii) $x^\perp = x^{\perp\perp\perp}$, $y^\perp = y^{\perp\perp\perp}$.

2) Conversely, if condition (i) is satisfied, then these two mappings form a Galois connection.

PROOF.–

1): By symmetry, it suffices to prove the properties (i) and (ii) for the variable x.

i) Let $y = x^{\perp}$. Then $y \leq x^{\perp}$, so $x \leq y^{\perp}$ from [2.1], and hence $x \leq x^{\perp\perp}$.

ii) By (i), $x^{\perp\perp\perp} = \left(x^{\perp\perp}\right)^{\perp} \leq x^{\perp}$, since $y \mapsto y^{\perp}$ is antitone. Replacing y by $x^{\perp}$ in the second equality of (i), we obtain $x^{\perp} \leq x^{\perp\perp\perp}$. Therefore, $x^{\perp} = x^{\perp\perp\perp}$.

2): If $y \leq x^{\perp}$, we have $y^{\perp} \geq x^{\perp\perp}$ since $y \mapsto y^{\perp}$ is antitone. Then, (i) implies $x^{\perp\perp} \geq x$, so $y^{\perp} \geq x$. The reverse implication is also true by symmetry. ■

We call $x^{\perp\perp}$ the Galois *closure* of x and $y^{\perp\perp}$ the Galois *closure* of y. We say that a *covers* b (or that a is a *cover* of b) if $b < a$ (section 1.1.2**(III)**) and there is no element $x \in P$ such that $b < x < a$.

(III) CHAINS. Recall that a chain C of an ordered set $(P, \leq)$ is a totally ordered subset. The *length* of C is $|C| := \text{Card}\,(C) - 1$. The length of P is $|P| = \sup\{|C| : C \text{ chain of } P\}$. A chain C' is called a *refinement* of C if it has the same endpoints as C, and $C \subset C'$. We then say that C' is *finer* than C. A chain $C = \{a_0, ..., a_m\}$ is said to be *connected* if a_{i+1} covers a_i for all $i \in \{0, ..., m-1\}$, thus if $C = C'$ for any refinement C' of C.

Let $(P, \leq)$ be an ordered set with greatest element 1. The *depth* of an element $x \in P$ is $\mathfrak{d}(x) = \sup(|C|)$, where C denotes the set of chains with endpoints x and 1. In a set with smallest element 0, we can similarly define the *height* $\mathfrak{h}(x) = \sup(|C|)$, where C denotes the set of chains with endpoints 0 and x.

2.1.3. *Lattice*

(I) A *lattice* is a set equipped with an order relation $\leq$ in which every pair (a, b) has an infimum (or greatest lower bound) $a \wedge b$ and a supremum (or least upper bound) $a \vee b$. The *dual lattice* may be obtained by reversing the order relation.

EXAMPLE 2.4.– *1) In $\mathfrak{P}(E)$ ($E \neq \varnothing$) ordered by the relation $\subset$, $a \vee b = a \cup b$ and $a \wedge b = a \cap b$.*

2) In $\mathbb{N}^{\times}$*, ordered by the relation "*$a \geq b$ *if* $a \mid b$*", which is equivalent to "*$a \geq b$ *if* $\mathbb{N}^{\times} a \supset \mathbb{N}^{\times} b$*", $a \vee b$ and $a \wedge b$ are, respectively, the greatest common divisor (*gcd*) and the least common multiple (*lcm*) of a and b. This lattice has the greatest element* 1*, since* $\mathbb{N}^{\times} 1 = \mathbb{N}^{\times} \supset \mathbb{N}^{\times} b$ *for any* $b \in \mathbb{N}^{\times}$*. In particular, we have that* $a \vee b = 1$ *if and only if* a, b *are coprime.*

The morphisms of the category of lattices are the mappings $\varphi : L \to M$ such that $\varphi(a \vee b) = \varphi(a) \vee \varphi(b)$ and $\varphi(a \wedge b) = \varphi(a) \wedge \varphi(b)$, $\forall a, b \in L$. A *complete lattice* is an ordered set in which every family of elements $\{a_i : i \in I\}$ has a supremum and an infimum. The ordered sets $(\mathfrak{P}(E), \subset)$ and $(\mathbb{N}^{\times}, |)$ are complete lattices.

In every lattice L, the *modular inequality* [2.2] holds ([MCL 99], Chap. XIV), as well as the following *distributive inequalities* [2.3], [2.4]:

$$a \vee (b \wedge c) \leq (a \vee b) \wedge c \text{ for all } a, b, c \in L \text{ such that } a \leq c, \qquad [2.2]$$

$$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c), \qquad [2.3]$$

$$a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c). \qquad [2.4]$$

(II) A lattice L is said to be *modular* if there is an equality in [2.2] (for all $a, b, c \in L$ such that $a \leq c$). It is said to be *distributive* if [2.3] (or equivalently [2.4] (**exercise**)) is an equality for all $a, b, c \in L$. Distributive lattices are modular. This claim and the proof of the following result are left as an **exercise*** ([MCL 99], Chap. XIV, Thm. 10).

LEMMA 2.5.– *Let M be a modular lattice and suppose that $a, b \in M$. The mapping $x \mapsto a \wedge x$ is a lattice isomorphism $\varphi_a : [b, a \vee b] \tilde{\to} [a \wedge b, a]$ with inverse isomorphism $\psi_b : y \mapsto b \vee y$.*

DEFINITION 2.6.– *In a modular lattice M:*

1) Two intervals of the form $[b, a \vee b]$ and $[a \wedge b, a]$ are said to be transposes.

2) Two intervals $[a, b]$ and $[a^*, b^*]$ are said to be projective *if there exists a finite sequence of intervals $[a_k, b_k]$, $0 \leq k \leq n$, such that 1) $[a_0, b_0] = [a, b]$, 2) $[a_n, b_n] = [a^*, b^*]$ and 3) $[a_{k-1}, b_{k-1}]$ and $[a_k, b_k]$ are transposes for all $k = 1, ..., n$.*

3) Two finite chains with the same endpoints are said to be isomorphic *if their intervals can be paired off in such as a way that each pair is projective.*

DEFINITION 2.7.– *In a modular lattice with the greatest element* 1*, the elements* $a_1, ..., a_n$ *are said to be* independent *if* $a_i \vee \left(\bigwedge_{1 \leq j \leq n, j \neq i} a_i \right) = 1$.

It can be shown that if $a_1, ..., a_n \neq 1$, all have finite depth (section 2.1.2(**III**)), we have that $\mathfrak{d}\left(\bigwedge_{1 \leq i \leq n} a_i\right) \leq \sum_{1 \leq i \leq n} \mathfrak{d}(a_i)$ with equality if and only if $a_1, ..., a_n$ are independent ([COH 81], Prop. 4.9).

DEFINITION 2.8.– *A finite decomposition* $a = \bigwedge_{1 \leq i \leq n} a_i$ *is said to be* irredundant *if none of the* a_i *can be omitted,* independent *if the* $a_1, ..., a_n$ *are independent and* irreducible *if the* a_i *are all irreducible (section 2.1.1(**II**)), i.e. have depth equal to 1.*

Proofs of the following results may be found in ([MCL 99], Chap. XIV; [COH 81], section II.4):

THEOREM 2.9.– *1) Schreier* refinement theorem*: In a modular lattice, any two chains with the same endpoints have isomorphic refinements.*

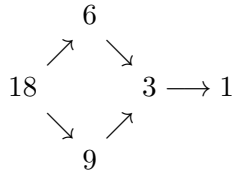
2) Jordan-Hölder-Dedekind theorem: *In a modular lattice of finite length, every chain has a maximal refinement, and any two chains with the same endpoints are isomorphic and have the same length.*

3) Krull-Remak-Schmidt theorem: *In a modular lattice with greatest element* 1*, let* $a \neq 1$ *be an element of finite depth and let* $a = \bigwedge_{1 \leq i \leq n} a_i = \bigwedge_{1 \leq i \leq m} b_i$ *be two* independent *representations of* a*. Then,* $n = m$ *and there exists a permutation* $i \mapsto i'$ *of* $\{1, ..., n\}$ *such that* $[a_i, 1]$ *and* $[b_{i'}, 1]$ *are projective.*

EXAMPLE 2.10.– *Consider the monoid* $(\mathbb{N}^{\times}, \times)$ *(Example 2.4(2)). Checking the following claims is left as an* ***exercise****. The integer* a *covers* b *if and only if* $a \mid b$ *and* b/a *is a prime number. A chain* $\{a_0, ..., a_m\}$ *is connected if and only if for each* $i \in \{1, ..., m\}$ *there exists a prime number* p_i *such that* $a_{i-1} = p_i a_i$*. Let* $a = \prod_i p_i^{\alpha_i}$, $b = \prod_i p_i^{\beta_i}$ *and* $c = \prod_i p_i^{\gamma_i}$ $(\alpha_i, \beta_i, \gamma_i \in \mathbb{N})$ *be the decomposition of* a, b, c *into prime factors. Then* $b \vee c = \prod_i p_i^{\inf(\beta_i, \gamma_i)}$, $a \wedge b = \prod_i p_i^{\sup(\alpha_i, \beta_i)}$ *and* $a \wedge (b \vee c) = \prod_i p_i^{\delta_i}$*, where* $\delta_i = \sup(\alpha_i, \inf(\beta_i, \gamma_i))$*, and similarly* $(a \wedge b) \vee (a \wedge c) = \prod_i p_i^{\varepsilon_i}$*, where* $\varepsilon_i = \inf(\sup(\alpha_i, \beta_i), \sup(\alpha_i, \gamma_i))$*. Since* $\delta_i = \varepsilon_i$ *is the median of the three*

numbers $\alpha_i, \beta_i, \gamma_i$, $(\mathbb{N}^{\times}, \times)$ *is a distributive lattice. We have that* $(a \vee b)(a \wedge b) = ab$.

Consider the number 18 *with divisors* $\{1, 2, 3, 6, 9, 18\}$ *and two chains with endpoints* 18 *and* 1*; for example* $\{1, 2, 18\}$ *and* $\{1, 3, 18\}$. *It follows from the Schreier* refinement theorem *and the Jordan-Hölder-Dedekind* theorem *that these chains have refinements that are isomorphic maximal chains, namely* $\{1, 2, 6, 18\}$ *and* $\{1, 3, 9, 18\}$, *both of which have length* 3. *Consider the sublattice of these two chains, shown below:*



The transpose intervals are the parallel arrows: $[18, 6]$ *and* $[9, 3]$ *are transposes because (using the notation of Lemma 2.5)* $[18, 6] = \varphi_6([9, 3])$ *and* $[9, 3] = \psi_9([6, 18])$*; similarly,* $[6, 3]$ *and* $[18, 9]$ *are transposes because* $[18, 9] = \varphi_9([6, 3])$ *and* $[6, 3] = \psi_6([18, 9])$.

The numbers $a_1, ..., a_n$ *are* independent *if and only if they are pairwise coprime. The Krull-Remak-Schmidt* theorem *states that an integer may be written as the product of pairwise coprime factors, and that this representation is unique. For example,* $180 = 4 \times 9 \times 5$.

2.2. Groups

2.2.1. *Groups and subgroups*

(I) A *group* is a monoid in which every element is invertible. In the rest of this subsection, we will write the neutral element of the group G as 1 whenever its internal binary operation is written multiplicatively (which is always the case when G is not commutative), and as 0 when this operation is written additively (in which case the considered group is $(G, +)$; these groups are said to be *additive*). A group morphism (or homomorphism) is defined as a monoid morphism (section 2.1.1**(I)**). If G is a group, its *order*, written as $(G : 1)$, is Card (G). For example, $(\mathbb{Z}, +)$ is a group of infinite order (and since the binary

operation is written additively, inverses with respect to this operation are called opposites). Another classical example of a group is the set $\mathfrak{S}_E$ of permutations of the set E (called the *symmetric group* of E), i.e. bijections $E \to E$. If E has a finite cardinal n, then $\mathfrak{S}_E$ is written as $\mathfrak{S}_n$ and its order is $n! := 1.2...n$. Recall that $H \subseteq G$ means that H is a subgroup of G, and $H \subsetneq G$ means that H is a *proper subgroup* (meaning $\neq G$) of G (section 1.3.1**(I)**). If $H \subseteq G$, the relations $x^{-1}y \in H$ and $yx^{-1} \in H$ $(x, y \in G)$ are equivalence relations; their equivalence classes are written as xH and Hx respectively, and called the left and right cosets of x mod.H. The set of left (resp. right) cosets mod.H is written as G/H (resp. $G\backslash H$). We have that $\mathrm{Card}\,(xH) = \mathrm{Card}\,(H) = \mathrm{Card}\,(Hx)$ for any $x \in G$; this cardinal is called the *index* of H in G, and is written as $(G : H)$. Since the xH and the Hx $(x \in G)$ form partitions of G, by [1.3], we have Lagrange's *theorem*:

$$\boxed{(G : 1) = (G : H)\,(H : 1)}. \qquad [2.5]$$

Let $g \in G$. The order of the subgroup $\langle g \rangle$ generated by g is called the *order* of g and is written as $\omega\,(g)$. If the order of G is finite, then by [2.5] the order of g divides the order of G. We say that G has a finite exponent if there exists an integer $n > 0$ such that $g^n = 1, \forall g \in G$, and the smallest integer $\varepsilon\,(G)$ satisfying this condition is called the *exponent* of G: this is the lcm (Example 2.4(2)) of the orders of the elements of G. The exponent of a finite group G is finite and divides $(G : 1)$.

(II) Let $H \subseteq G$. We say that $x \in G$ *normalizes* H if $xH = Hx$. The set of these elements x is called the *normalizer* $N_G\,(H)$.

(III) If $(G_i)_{i \in I}$ is a family of groups, the product $\prod_{i \in I} G_i$ of the *sets* G_i (section 1.1.2**(III)**) may be endowed with a canonical group structure by setting $(x_i)_{i \in I}\,(y_i)_{i \in I} = (x_i y_i)_{i \in I}$. Consequently, products (section 1.2.6**(I)**) exist in $\mathbf{Grp}$. Let $G \underset{g}{\overset{f}{\rightrightarrows}} G'$ be a double arrow in $\mathbf{Grp}$; then $H = \{x \in G : f\,(x) = g\,(x)\}$ is a subgroup of G (**exercise**), the equalizer $\mathrm{eq}\,(f, g)$. By Proposition 1.22, $\mathbf{Grp}$ therefore admits projective limits and fibered products.

(IV) The category $\mathbf{Grp}$ also admits coproducts, often called *free products* ([BKI 12], Chap. I, section 7.3)[1]. Let $(G_i)_{i\in I}$ be a family of groups. Each element of the free product $\divideontimes_{i\in I} G_i$ has a unique expression of the form $g_{i_1}\cdots g_{i_p}$, $g_{i_j} \notin G_{i_{j+1}}$. There exists (by definition) a canonical monomorphism $G_i \hookrightarrow \divideontimes_{j\in I} G_j$ for each $i \in I$. If $G_i = \mathbb{Z}$ for all $i \in I$, $\divideontimes_{i\in I} G_i$ is called the *free group* on I, and is written as $F(I)$; it has the following universal property (**exercise***: see [BKI 12], Chap. I, section 7.5, Prop. 8): for any group G and any function $f : I \to G$, there exists a unique homomorphism $\bar{f} : F(I) \to G$ extending f. A free group is therefore a free object in $\mathbf{Grp}$ (section 1.3.4). In $\mathbf{Ab}$, $\divideontimes_{i\in I} G_i$ is written as $\bigoplus_{i\in I} G_i$ and is called the *direct sum* of the G_i; the *support* of the family $(g_i)_{i\in I} \in (G_i)_{i\in I}$ is the set $\operatorname{supp}\left((g_i)_{i\in I}\right)$ of indices i such that $g_i \neq 0$, and $\bigoplus_{i\in I} G_i$ is the subgroup of $\prod_{i\in I} G_i$ consisting of the families $(g_i)_{i\in I}$ with finite support.

2.2.2. Normal subgroups

(I) The sets G/H and $G\backslash H$ are in turn groups if and only if for all $x \in G$ $xH = Hx$ or, in other words, if $N_G(H) = G$. We say that H is a *normal* subgroup of G, written as $H \lhd G$. Thus $(G/H, \text{can})$, where $\text{can} : G \to G/H$ is the canonical surjection (section 1.1.2**(VI)**), is a quotient object (section 1.1.1**(III)**) of G in $\mathbf{Grp}$ if and only if $H \lhd G$. If the group G is abelian, every subgroup of G is normal.

Let G, H be two groups and let $f : G \to H$ be a morphism. Its kernel is $\ker(f) = f^{-1}(\{1\})$ and we have that:

$$x^{-1}y \in \ker(f) \Leftrightarrow f\left(x^{-1}y\right) = 1 \Leftrightarrow f\left(x^{-1}\right) f(y) = 1 \Leftrightarrow f\left(x^{-1}\right) = f(y)^{-1}.$$

The symmetry in the final equality implies that $x^{-1}y \in \ker(f)$ if and only if $yx^{-1} \in \ker(f)$, and hence $\ker(f)$ is a normal subgroup of G. However, $\operatorname{im}(f) := f(G)$ is typically not a normal subgroup of H.

The relation $\lhd$ is not transitive: we can have that $K \lhd H$ and $H \lhd G$ without having $K \lhd G$ ([BKI 12], Chap. I, section 5, Exerc. 10). However, if $H \lhd G$, $K \lhd G$ and $K \subseteq H$, then $K \lhd H$ (**exercise**).

1 This is not the same as the notion of direct product defined in ([VAN 31], section 7.6).

If H, K are subgroups of G, then their intersection $H \cap K$ is a subgroup; the same is true for $H.K := \{hk : h \in H, k \in K\}$ if $H \lhd G$ or $K \lhd G$; if $H \lhd G$ and $K \lhd G$, then $H.K \lhd G$ (**exercise**).

(II) We say that a sequence:

$$... \longrightarrow G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \longrightarrow ..., \qquad [2.6]$$

where I is an interval of $\mathbb{Z}$, $(G_i)_{i\in I}$ is a family of groups and $(f_i : G_i \to G_{i+1})_{i\in I}$ is a family of homomorphisms (both of these families are indexed by I) is *exact at* G_i if $\mathrm{im}\,(f_{i-1}) = \ker(f_i)$. The sequence is said to be *exact* if it is exact at each G_i $(i \in I)$. If the sequence

$$\{1\} \longrightarrow G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \longrightarrow \{1\}, \qquad [2.7]$$

is exact, it is said to be a *short exact sequence*. This means that f_1 is injective, $\mathrm{im}\,(f_1) = \ker(f_2)$ and f_2 is surjective; this implies that $\mathrm{im}\,(f_1) \cong G_1$ is a normal subgroup of G_2, and that $G_3 \cong \mathrm{coker}\,(f_1) := G_2/\mathrm{im}\,(f_1)$. We then say that G_2 is an *extension* of G_3 by G_1[2]; in particular, $G_1 \times G_3$ is an extension of G_3 by G_1 when $f_1 = \mathrm{inj}_1$ is taken to be the canonical injection and $f_2 = \mathrm{pr}_2$ is the canonical projection (section 1.2.6). Conversely, if $H \lhd G$, we have the short exact sequence $\{1\} \longrightarrow H \xrightarrow{\iota} G \xrightarrow{\pi} G/H \longrightarrow \{1\}$, where ι and π are the canonical monomorphism and the canonical epimorphism, respectively.

(III) We write $\mathrm{Aut}\,(G)$ for the group of *automorphisms* of G, i.e. the isomorphisms from G onto G; $\mathrm{Aut}\,(G)$ is a subgroup of $\mathfrak{S}_G$. A subgroup H of G is said to be *characteristic* if it is invariant under every automorphism of G. Characteristic subgroups are normal (**exercise**), but the converse is not true. The mapping $\gamma_x : G \to G : y \mapsto xyx^{-1}$ is an automorphism, called an *inner automorphism*. The mapping $\gamma : G \to \mathrm{Aut}\,(G) : x \mapsto \gamma_x$ is a homomorphism, and we have the following exact sequence:

$$\{1\} \to \mathfrak{Z}(G) \xrightarrow{\text{can}} G \xrightarrow{\gamma} \mathrm{Aut}\,(G) \xrightarrow{\text{can}} \mathrm{Aut}\,(G)/\mathrm{Int}\,(G) \to \{1\},$$

where $\mathfrak{Z}(G) = \{x \in G : \gamma_x = \mathrm{id}_G\}$ is the *center* of G and $\mathrm{Int}\,(G) := \mathrm{im}\,(\gamma)$ is a normal subgroup of $\mathrm{Aut}\,(G)$. We write $y^x = \gamma_{x^{-1}}(y)$, so that $y^x z^x = \left(x^{-1}yx\right)\left(x^{-1}zx\right) = (yz)^x$ and $(y^x)^z = z^{-1}\left(x^{-1}yx\right)z = (xz)^{-1}\, y\, (xz) = y^{xz}$. Two subsets A, B of G (or two elements A, B of G) are said to be *conjugate* if there exists $x \in G$ such that $B = xAx^{-1}$.

2 Some authors prefer to say that G_2 is an extension of G_1 by G_3.

2.2.3. *Fundamental isomorphisms*

(I) INDUCED HOMOMORPHISMS.

THEOREM-DEFINITION 2.11.– *Let G_1, G_2 be groups, $H_1 \lhd G_1, H_2 \lhd G_2$ and let $f : G_1 \to G_2$ be a homomorphism.*

1) The following conditions are equivalent*: (a) $f(H_1) \subseteq H_2$. (b) There exists a homomorphism $\bar{f} : G_1/H_1 \to G_2/H_2$ that makes the following diagram commute:*

$$\begin{array}{ccc} G_1 & \xrightarrow{f} & G_2 \\ \varphi_1 \downarrow & & \downarrow \varphi_2 \\ G_1/H_1 & \xrightarrow{\bar{f}} & G_2/H_2 \end{array}$$

where φ_1 and φ_2 are the canonical epimorphisms.

2) If these conditions are satisfied*, we have that* $\ker\left(\bar{f}\right) = \varphi_1\left(f^{-1}(H_2)\right)$ *and* $\text{im}\left(\bar{f}\right) = \varphi_2(f(G_1))$*. The homomorphism $\bar{f}$ is said to be* induced *by f.*

PROOF.– (1) may be shown as follows: if (a) is true, let $x, x' \in G_1$ be such that $xx'^{-1} \in H_1$. Then $f\left(xx'^{-1}\right) = f(x) f(x')^{-1} \in H_2$, so $\varphi_2(f(x))$ only depends on $\bar{x} = \varphi_1(x)$ and $\bar{f} : \bar{x} \mapsto \varphi_2(f(x))$ is a homomorphism. Conversely, if (b) is true, let $x \in H_1$, i.e. $\varphi_1(x) = 1$. Then $\varphi_2(f(x)) = \bar{f}(1)$, i.e. $f(x) \in H_2$. (2): **exercise**. ■

(II) NOETHER'S ISOMORPHISM THEOREMS. Noether's three isomorphism theorems for groups may be stated as follows ([BKI 12], Chap. I, section 4.6, Thm. 4):

THEOREM 2.12.– *(E. Noether)*

1) Let $f : G \to H$ be a group homomorphism. Then:

$$G/\ker(f) \cong im(f). \qquad [2.8]$$

2) If $N \lhd G$ and $H \subseteq G$, we have that $N \lhd H.N$, $H \cap N \lhd H$, as well as the group isomorphism:

$$(H.N)/N \cong H/(H \cap N). \qquad [2.9]$$

3) If $N \lhd G$ and $H \subseteq G$ are such that $N \subseteq H$, then $H/N \lhd G/N$ if and only if $H \lhd G$, in which case we have the group isomorphism:

$$G/H \cong (G/N) \,/\, (H/N)\,. \qquad [2.10]$$

PROOF.– We will prove these results for additive groups, which simplifies the reasoning slightly, as every subgroup is normal. Readers may wish to rewrite the general case as an **exercise**.

1): For each $x \in G$, $f(x)$ only depends on the canonical image $\bar{x}$ of x in $G/\ker(f)$ and $\bar{f} : G/\ker(f) \to \text{im}(f) : \bar{x} \mapsto f(x)$ is an isomorphism.

2): We need to show that if $M_1, M_2 \subset M$ are three abelian groups, then:

$$(M_1 + M_2)\,/M_2 \cong M_1/\,(M_1 \cap M_2)\,. \qquad [2.11]$$

Let $\varphi : M \twoheadrightarrow M/M_2$ be the canonical epimorphism and let $f = \varphi\,|_{M_1}$ be the restriction of φ to M_1. We have that $\ker(f) = M_1 \cap M_2$ and $\text{im}(f) = (M_1 + M_2)\,/M_2$, hence [2.11] by (1).

3): We need to show that if $M_1 \subseteq M_2 \subseteq M_3$ are three abelian groups, then:

$$M_3/M_2 \cong (M_3/M_1) \,/\, (M_2/M_1)\,. \qquad [2.12]$$

Let $\varphi : G \twoheadrightarrow M_3/M_2$ be the canonical epimorphism. Then for all $x \in M_3, \varphi(x)$ only depends on the canonical image $\bar{x}$ of x in M_3/M_1 and thus determines an epimorphism $\bar{\varphi} : M_3/M_1 \to M_3/M_2$, said to be *derived from φ by passing to the quotients*. We have that $\ker(\bar{\varphi}) = \{\bar{x} \in M_3/M_1 : x \in M_2\} = M_2/M_1$, and hence [2.12] by (1). ■

(III) CORRESPONDENCE THEOREM. Let G be a group and $N \lhd G$. There exists a bijection between the subgroups H of G containing N and the subgroups of G/N, namely $H \mapsto H/N$.

PROOF.– Let $\mathcal{S}$ be the set of groups H such that $N \subseteq H \subseteq G$ and let $\mathcal{Q}$ be the set of subgroups of G/N. For each $H \in \mathcal{S}$, we have that $N \lhd H$ (Theorem 2.12(2)) and that $\varphi : \mathcal{S} \to \mathcal{Q} : H \mapsto H/N$ is isotone with respect to inclusion (section 2.1.2**(I)**). This mapping φ is surjective, since if $H^* \in \mathcal{Q}$, there exists some uniquely determined $H \in \mathcal{S}$ such that $H^* = H/N$. ■

(IV) PRODUCT ISOMORPHISM. Let $(G_i)_{i\in I}$ and $(N_i)_{i\in I}$ be families of groups such that $N_i \lhd G_i$. There is a canonical group isomorphism:

$$\left(\prod\nolimits_{i\in I} G_i\right) / \left(\prod\nolimits_{i\in I} N_i\right) \cong \prod\nolimits_{i\in I} (G_i/N_i)\,. \qquad [2.13]$$

PROOF.– Let $\pi_i : G_i \twoheadrightarrow G_i/N_i$ be the canonical epimorphism and let $\pi : \prod_{i\in I} G_i \to \prod_{i\in I} (G_i/N_i)$ be the homomorphism defined by $\pi\left((x_i)_{i\in I}\right) = (\pi_i(x_i))_{i\in I}$. Then, π is an epimorphism and $\ker(\psi) = \prod_{i\in I} N_i$. We deduce [2.13] by Noether's first isomorphism theorem. ■

(V) ISOMORPHISM OF DIRECT SUMS. This may be deduced from the product isomorphism: let $(G_i)_{i\in I}$ and $(N_i)_{i\in I}$ be families of *abelian* groups such that $N_i \subseteq G_i$. There exists a canonical isomorphism:

$$\left(\bigoplus\nolimits_{i\in I} G_i\right) / \left(\bigoplus\nolimits_{i\in I} N_i\right) \cong \bigoplus\nolimits_{i\in I} (G_i/N_i)\,. \qquad [2.14]$$

2.2.4. *Cyclic groups and simple groups*

(I) A group G is said to be *generated* by a set S (we also say that S is a generator of G) if G is the smallest group containing S, in which case we write $G = \langle S\rangle$. A group that is generated by a single element g is written as $\langle g\rangle$, and is said to be *monogenous*. A monogenous group of finite order is said to be *cyclic*[3]. Let G be a group and $g \in G$; then $(\langle g\rangle : 1)$ is called the *order* of g. A group is said to be *simple* if its only normal subgroups are G and $\{1\}$.

The proofs of the following claims are left as an **exercise**: we have that $\langle g\rangle = \{g^n : n \in \mathbb{Z}\}$ and there exists an integer $n \in \mathbb{N}$ such that $\langle g\rangle \cong (\mathbb{Z}/n\mathbb{Z}, +)$. The quotient of a monogenous group G by a subgroup H is monogenous. If $\langle g\rangle$ has order n, then for any divisor $d \geq 1$ of n there exists a subgroup H of order d in G, and $H = \langle g^{n/d}\rangle$. A finite abelian group is simple if and only if it is cyclic and has prime order. If G is a finite abelian group, there exists an element g in G whose order $\omega(g)$ is equal to the exponent $\varepsilon(G)$ of G (section 2.2.1**(I)**), since if $\prod_{i=1}^{s} p_i^{r_i}$ is the prime factor decomposition of $\varepsilon(G)$, there exists $g_i \in G$ such that $p_i^{m_i} \mid \omega(g_i) \Rightarrow \omega(g_i) = p_i^{m_i} q_i$ and $\prod_{i=1}^{s} g_i^{q_i} \in G$ has order ε.

3 For some authors, "cyclic" and "monogenous" are synonymous, although, for example, there is no cycle in the additive group $\mathbb{Z}$, unlike what happens in $\mathbb{Z}/(n)$ for $n \in \mathbb{N}^{\times}$.

(II) The *symmetric group* $\mathfrak{S}_n$ (section 2.2.1**(I)**) is generated by the *transpositions*, i.e. the cycles of order 2 $[ij] : i \mapsto j \mapsto i$. There exists a unique homomorphism $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ such that $\varepsilon(\tau) = -1$ for any transposition τ; $\varepsilon(\sigma)$ is called the *signature* of the permutation $\sigma \in \mathfrak{S}_n$. We call $\mathfrak{A}_n = \ker(\varepsilon)$ the *alternating group* on $\{1, ..., n\}$. The sequence

$$\{1\} \longrightarrow \mathfrak{A}_n \xrightarrow{\text{can}} \mathfrak{S}_n \xrightarrow{\text{can}} \{-1, 1\} \longrightarrow \{1\} \qquad [2.15]$$

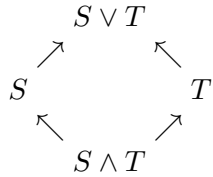
is exact, and hence $(\mathfrak{A}_n : 1) = n!/2$ by Lagrange's *theorem* [2.5]. See Theorem 2.18.

2.2.5. *Lattice of normal subgroups*

(I) The proof of the following result is an **exercise*** ([MCL 99], Sect. XIV.4, Thm. 7):

LEMMA 2.13.– *The set $\mathcal{N}(G)$ of all normal subgroups of G is a complete lattice (section 2.1.3**(I)**) with $H \vee K := H.K$ and $H \wedge K := H \cap K$; this lattice is modular, with greatest element G.*

Let $S, T \in \mathcal{N}(G)$, and consider the following "diamond":



The sides of the diamond are the parallel intervals $[S, S \vee T]$ // $[S \wedge T, T]$ and $[S \wedge T, S]$ // $[T, S \vee T]$. As in Example 2.10, the parallel intervals are transposes (Definition 2.6(1)) and, by Noether's *second isomorphism theorem* (Theorem 2.12(2)), these transpositions correspond to the isomorphisms $S.T/S \cong T/(S \cap T)$ and $S.T/T \cong S/(S \cap T)$. By transitivity, projective intervals (Definition 2.6(2)) also correspond to isomorphisms, which leads to the following result:

LEMMA 2.14.– (diamond lemma)*: In the modular lattice $\mathcal{N}(G)$, projective intervals $[K_1, H_1]$ and $[K_2, H_2]$ $(K_1 \lhd H_1, K_2 \lhd H_2)$ correspond to group isomorphisms $H_1/K_1 \cong H_2/K_2$.*

(II) JORDAN-HÖLDER THEOREM. Lemmas 2.13 and 2.14 allow us to translate the terminology of lattices into the language of groups. A chain of length r in $\mathcal{N}(G)$, with endpoints G and $\{1\}$ of the form

$$G = G_0 \rhd G_1 \rhd ... \rhd G_r = \{1\} \qquad [2.16]$$

is called a *normal series* or a *composition series* of G. Another normal series of G

$$G = H_0 \rhd H_1 \rhd ... \rhd H_s = \{1\}$$

is *isomorphic* to it (Definition 2.6(3)) if and only if $r = s$ and there exists a permutation $i \mapsto i'$ of $\{0, ..., r-1\}$ such that $G_i/G_{i+1} \cong H_{i'}/H_{i'+1}$, $\forall i \in \{0, ..., r-1\}$. The Schreier-Zassenhaus *theorem* directly follows from Schreier's *theorem* (Theorem 2.9(1)): *Any two normal series of G have isomorphic refinements*.

A normal series Σ of G is called a Jordan-Hölder *series* of G if it is *strictly decreasing* and does not have any refinement distinct from Σ. The normal series [2.16] is therefore a Jordan-Hölder series if and only if each quotient G_i/G_{i+1} is simple. The Jordan-Hölder-Dedekind *theorem* (Theorem 2.9(2)) implies the Jordan-Hölder *theorem* for groups:

THEOREM 2.15.– *(Jordan-Hölder) Any two Jordan-Hölder series of G are isomorphic.*

If [2.16] is a Jordan-Hölder *series* Σ, the integer $r = |\Sigma|$ is called the *length* of G and is written as $|G|$. If [2.16] is an arbitrary normal series, then $|G| = \sum_{0 \leq i \leq n} |G_i/G_{i+1}|$ (**exercise***; see [BKI 12], Chap. I, section 4.7, Cor. of Prop. 10).

2.2.6. *Derived subgroup*

Let G be a group and $x, y \in G$. Write $(x, y) := (yx)^{-1} xy$. Then $(x, y) = 1$ if and only if x and y commute, and (x, y) is called the *commutator* of x and y. If $H, K \subseteq G$, the subgroup of G generated by the commutators $(h, k) \in H \times K$ is written as (H, K). If H and K are normal (resp. characteristic), then so is (H, K) (**exercise**). The *derived subgroup* of G (also known as the *commutator subgroup* of G) is $G' = (G, G)$. Checking the following claims is an **exercise*** ([BKI 12], Chap. I, section 6.2):

We have that $G' \lhd G$ and the quotient group G/G' is commutative. $G' = \{1\}$ if and only if G is commutative. For any *abelian* group H and any morphism $f : G \to H$, there exists a unique morphism $\bar{f} : G/G' \to H$ such that the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \text{can}\downarrow & \nearrow & \bar{f} \\ G/G' & & \end{array}$$

If $H \subseteq G$, the following conditions are equivalent: 1) $G' \subseteq H$ and 2) $H \lhd G$ and G/H is abelian. The derived subgroup G' is *characteristic*.

DEFINITION 2.16.– *The group $G^{ab} = G/G'$ is called the* abelianization *of the group G.*

Let G, H be two groups and let $f : G \to H$ be a homomorphism. The image of the restriction $f' = f|_{G'}$ is in H' (**exercise**) and may therefore be viewed as a homomorphism $G' \to H'$. Hence, $\mathfrak{D} : G \longmapsto G', f \longmapsto f'$ is a functor.

2.2.7. Solvable groups and nilpotent groups

(I) SOLVABLE GROUPS. By iterating the above functor $\mathfrak{D}$, we obtain the k-th derived subgroup $G^{(k)}$ and a decreasing series $G \rhd G' \rhd ... \rhd G^{(k)} \rhd ...$ We therefore have that:

$$G^{(0)} = G, \quad G^{(k+1)} = \mathfrak{D}\left(G^{(k)}\right), k \geq 0. \qquad [2.17]$$

The group G is said to be *solvable* if there exists an integer $k \geq 0$ such that $G^{(k)} = \{1\}$. If so, the smallest integer $k \geq 0$ satisfying this condition is called the *solvability class* of G. A group G is solvable with solvability class 0 (resp. solvability class ≤ 1) if and only if $G = \{1\}$ (resp. G is commutative). The following claims can be shown as an **exercise*** ([MCL 99], Sect. XII.7): every commutative group is solvable. Every subgroup and every quotient group of a solvable group with solvability class n is solvable with solvability class $\leq n$. The class of solvable groups is *closed under extension* (section 2.2.2(**II**)). Hence, given a *normal series* [2.16], if each quotient group G_i/G_{i+1} $(i = 1, ..., r-1)$ is solvable, then G is solvable.

THEOREM 2.17.– *(Galois) The group $\mathfrak{S}_n$ is solvable if and only if $n \leq 4$.*

PROOF.– It is easy to check that $\mathfrak{S}_n$ is solvable if $n \leq 4$. We will show the converse. (1) If $N \lhd \mathfrak{S}_n$ $(n \geq 5)$ contains all 3-cycles $[ijk] : i \mapsto j \mapsto k \mapsto i$, $H \lhd N$, and N/H is abelian, then H contains all 3-cycles. Indeed, let i, j, k, r, s be five symbols and $[kjs]$ an arbitrary 3-cycle in N. Let $x = [ijk]$ and $y = [krs]$ be two 3-cycles in N, and let $\bar{x}, \bar{y}$ be the canonical images of x and y in N/H. Since N/H is abelian, we have that $\bar{x}^{-1}\bar{y}^{-1}\bar{x}\bar{y} = 1$, so $x^{-1}y^{-1}xy \in H$. But $x^{-1}y^{-1}xy = [kji] \circ [srk] \circ [ijk] \circ [krs] = [kjs]$ (**exercise**). (2) For all $n \geq 3$, $\mathfrak{S}_n$ contains all 3-cycles. Hence, by (1), for all $n \geq 5$, $\mathfrak{S}'_n$ contains all 3-cycles, and so by induction $\mathfrak{S}_n^{(k)}$ contains all 3-cycles for all $k \geq 1$. Hence, $\mathfrak{S}_n$ is not solvable. ■

Since the sequence [2.15] is exact, $\mathfrak{S}_n$ is an extension of $\{-1, 1\}$ by $\mathfrak{A}_n$, and so $\mathfrak{A}_n$ is not solvable for any $n \geq 5$. É. Galois showed the following stronger result ([MCL 99], Sect. XII.9):

THEOREM 2.18.– *(Galois) The group $\mathfrak{A}_n$ is simple if and only if $n \geq 5$.*

LEMMA 2.19.– *Let G be a group and let [2.16] be a Jordan-Hölder* series *of G. Then, G is solvable if and only if the quotients G_i/G_{i+1} $(i = 1, ..., r-1)$ are all cyclic with prime order.*

PROOF.– If the quotients of a Jordan-Hölder series of G are cyclic, then they are commutative, so G is solvable. Conversely, if G is solvable, each group G_i/G_{i+1} is solvable and simple. But every solvable simple group H is cyclic with prime order, since $H' \lhd H$ and $H' \neq H$ (otherwise, $H^{(k)} = H$ for all k and H would not be solvable), so $H' = \{1\}$. Therefore H is commutative, and since it is simple, we have that $H \cong \mathbb{Z}/p\mathbb{Z}$, where p is prime. ■

The Feit-Thompson *theorem*, established in 1963, whose proof spans 254 pages (we will therefore refrain from setting it as an exercise!), shows that *every finite group of odd order is solvable*.

(II) NILPOTENT GROUPS. Let G be a group. We define the *central descending* series of G to be the series $(\mathbf{C}^n(G))_{n\geq 0}$ defined by the recurrence

$$\mathbf{C}^0(G) = \{1\}, \qquad \mathbf{C}^{n+1}(G) = (G, \mathbf{C}^n(G))$$

(with the notation introduced in section 2.2.6). We say that a group is *nilpotent* if there exists an integer $n \geq 0$ such that $\mathbf{C}^n(G) = \{1\}$, and the smallest

integer n satisfying this condition is called the *nilpotency class* of G. A group is nilpotent with class 0 (resp. with class ≤ 1) if and only if $G = \{1\}$ (resp. G is commutative). Every subgroup and every quotient group of a nilpotent group of class n is nilpotent of class $\leq n$, and every finite product of nilpotent groups is nilpotent (**exercise**). It can be shown that a nilpotent group of class $\leq 2^n - 1$ is solvable with class $\leq n$ ([BKI 12], Chap. I, section 6.4, Example 2), and in particular *nilpotent groups are solvable*.

(III) Let $p \geq 2$ be a prime number. A *p-group* is a group G whose order is a power of p. Every subgroup and quotient group of a p-group is a p-group, and the class of p-groups is closed under extension (**exercise**). It can be shown ([BKI 12], Chap. I, section 6.7, Thm. 4) that a finite group is nilpotent if and only if it is a product of p-groups (typically with different values of p). Every p-group is solvable. Let G be a group; a Sylow p-subgroup of G is a p-group $P \subseteq G$ such that $(G : P)$ is not a multiple of p. The first Sylow theorem states that every finite group contains a Sylow p-subgroup ([BKI 12], Chap. I, section 6.6, Thm. 2); consequently, if $(G : 1)$ is a multiple of p, G contains an element of order p (section 2.2.4**(I)**).

2.2.8. *Action of a group on a set*

(I) ORBIT-STABILIZER FORMULA. Let G be a group and E a set. An action of G on E is a homomorphism $\pi : G \to \mathfrak{S}_E$. If $g \in G$ and $x \in E$, the element $\pi(g)(x)$ is written as $g.x$. The *orbit* of x is $G.x$. Since distinct orbits are disjoint, the orbits G_i $(i \in I)$ form a partition of E (section 1.1.2**(VI)**) and $E = \bigcup_{i \in I} G.x_i$, where $x_i \in G_i$. The *stabilizer* of $x \in E$ is the subgroup G_x of G such that $G_x.x = \{x\}$. The relation $g.x = h.x$ is equivalent to $h^{-1}g \in G_x$, and so the mapping $G \ni g \mapsto g.x \in G.x$ factorizes into $G \xrightarrow{\text{can}} G/G_x \xrightarrow{\varphi_x} G.x$, where φ_x is a bijection, which implies that (section 2.2.1**(I)**) $(G : G_x) = \text{Card}(G.x)$ and, by [1.3], the *orbit-stabilizer formula*:

$$\boxed{\text{Card}(E) = \textstyle\sum_{i \in I} (G : G_{x_i})}.$$

(II) HOMOGENEOUS SETS. An action of G on E is said to be *transitive* (resp. *free*, resp. *simply transitive*) if, for any $x \in E$, the mapping $g \mapsto g.x$ from G into E is surjective (resp. injective, resp. bijective). If the action of G on X is transitive, the set E consists of a single orbit (i.e. $E = G.\,x$ for all $x \in E$) and

is said to be *homogeneous*. Then, φ_x is a bijection $G/G_x \tilde{\to} E$. Conversely, if H is a subgroup of G, then G acts transitively on G/H in the obvious way, and so the set of left cosets of G/H is homogeneous. The group G acts freely on E if and only if, for all $x \in G$, $G_x = \{1\}$, or alternatively if the mapping $g \mapsto g.x$ from G into $G.x$ is bijective.

2.3. Rings and algebras

2.3.1. *Rings and modules*

(I) RINGS. A ring $\mathbf{R}$ is a set equipped with two operations $+, \times$ such that $(\mathbf{R}, +)$ is an additive group (section 2.2.1**(I)**) and $(\mathbf{R}, \times)$ is a monoid with zero (section 2.1.1**(I)**), with the stipulation that multiplication must be distributive over addition, i.e. $(x+y)\,z = xz+yz$ and $z\,(x+y) = zx+zy$, $\forall x, y, z \in \mathbf{R}$. Ring *morphisms* are the mappings $f : \mathbf{R} \to \mathbf{A}$ such that $f\,(x+y) = f\,(x) + f\,(y)$, $f\,(xy) = f\,(x)\,f\,(y)$, $f\,(1) = 1$, $\forall x, y \in \mathbf{R}$.

In the following, unless otherwise stated, rings are $\neq \{0\}$. The notions of divisibility defined above for monoids (section 2.1.1**(II)**) are applicable to a ring $\mathbf{R}$ viewed as a monoid $(\mathbf{R}^{\times}, \times)$. In particular, the set of *units* of $\mathbf{R}$ (its invertible elements) is the multiplicative group denoted by $\mathbf{U}\,(\mathbf{R})$. The opposite ring $\mathbf{R}^{\mathrm{op}}$ of $\mathbf{R}$ has the same elements as $\mathbf{R}$, but is equipped with the opposite internal binary operation $(\lambda, \mu) \mapsto \mu.\lambda$.

The ring $\mathbf{R}$ is said to be *commutative* if multiplication is commutative, and *entire* (or is said to be an *integral domain* or a *domain*)[4] if the monoid $(\mathbf{R}, \times)$ is a cancellation monoid (section 2.1.1**(II)**). For example, $\mathbb{Z}$ is a commutative entire ring. The set $\mathfrak{M}_2\,(\mathbb{Z})$ of matrices of dimension 2×2 with coefficients in $\mathbb{Z}$ is neither commutative nor entire.

(II) MODULES. An abelian group M is a left $\mathbf{R}$-*module* if there exists an action of $\mathbf{R}$ on $M : \mathbf{R} \times M \to M : (\lambda, x) \mapsto \lambda.x$ such that, for all $\lambda, \mu \in \mathbf{R}$, $x, y \in M$,

$$\lambda.\,(x+y) = \lambda.x + \lambda.y, \quad (\lambda+\mu)\,.x = \lambda.x + \mu.x,$$
$$(\lambda\mu)\,.x = \lambda.\,(\mu.x)\,, \quad 1.x = x.$$

4 For certain authors (but not in this book), (integral) domains are always commutative.

We can similarly define a right $\mathbf{R}$-module M by writing the "scalars" (the elements of $\mathbf{R}$) to the right of the "vectors" (the elements of M). The *morphisms* of the category ${}_{\mathbf{R}}\mathbf{Mod}$ of left $\mathbf{R}$-modules and the category $\mathbf{Mod}_{\mathbf{R}}$ of right $\mathbf{R}$-modules are the $\mathbf{R}$-linear mappings (also called $\mathbf{R}$-homomorphisms). A morphism of left $\mathbf{R}$-modules is therefore a mapping $f : M \to N$ such that $\forall \lambda, \mu \in \mathbf{R}, \forall x, y \in M, f(\lambda.x + \mu.y) = \lambda.f(x) + \mu.f(y)$.

An abelian group is a $\mathbb{Z}$-module. The set of morphisms from M into N (where M and N are both either left or right $\mathbf{R}$-modules) is the abelian group denoted by $\mathrm{Hom}_{\mathbf{R}}(M, N)$. Each right $\mathbf{R}$-module may be identified with a left $\mathbf{R}^{\mathrm{op}}$-module; more precisely, the category ${}_{\mathbf{R}^{\mathrm{op}}}\mathbf{Mod}$ of left $\mathbf{R}^{\mathrm{op}}$-modules coincides with the category $\mathbf{Mod}_{\mathbf{R}}$ of right $\mathbf{R}$-modules. To keep track, it can be helpful to write ${}_{\mathbf{R}}M$ for a left $\mathbf{R}$-module M and $N_{\mathbf{R}}$ for a right $\mathbf{R}$-module N. If $\mathbf{R}$ is commutative, there is no need to distinguish left and right $\mathbf{R}$-modules. The module with the underlying set (section 1.3.1(**I**)) $\{0\}$ is written as 0. Recall that $N \subseteq M$ means that N is a *submodule* of the $\mathbf{R}$-module M (section 1.3.1(**I**)), i.e. an $\mathbf{R}$-module such that $N \subset M$. This submodule N is said to be *proper* if $N \neq M$, and *trivial* if $N = 0$. Let M be a left or right $\mathbf{R}$-module and suppose that $S \subset M$. We write $[S]_{\mathbf{R}}$ for the submodule of M generated by S, i.e. the smallest submodule containing S, or alternatively the intersection of all submodules containing S. We say that S is a *generator* of $M = [S]_{\mathbf{R}}$, or that $(x_i)_{i \in I}$ is a *generating family* of M, when $S = \{x_i : i \in I\}$. An $\mathbf{R}$-module is said to be *finitely generated* if it is generated by finitely many elements, and *monogenous* if it is generated by a single element[5]. A subset L of a $\mathbf{R}$-module M is said to be *free* if, for any family $(e_i)_{i \in I}$ in L and any family $(\lambda^i)_{i \in I}$ of elements in $\mathbf{R}$ with finite support, the equality $\sum_{i \in I} \lambda^i.e_i = 0$ implies that $\lambda^i = 0, \forall i \in I$. If so, we say that the family $(e_i)_{i \in I}$ is *free*. A set that is not free is said to be *related*. The family $(e_i)_{i \in I}$ is called a *basis* of M if it is free and generates M. In this case, the set $\{e_i : i \in I\}$ is also called a basis of M. We say that a module M is *free* if it has a *basis*, and so is a free object on its basis (section 1.3.4); we say that M is *finite free* if it has a basis with a finite cardinal.

5 We will mirror the terminology that is used in particular within French-speaking circles. "Monogenous modules" are more often called "cyclic modules" in English (compare with Definition 3.206, and see footnote 3, p. 46).

LEMMA 2.20.– *Let E and F be two left $\mathbf{R}$-modules. Suppose that E is a free module with basis $(a_i)_{i\in I}$ and let $(b_i)_{i\in I}$ be a family of elements of F. Then, there exists a unique $\mathbf{R}$-homomorphism $f : E \to F$ such that $f(a_i) = b_i$, $\forall i \in I$.*

PROOF.– Let $x = \sum_{i\in I} \lambda^i.a_i$ be an arbitrary element of E. Then, $f(x) = \sum_{i\in I} \lambda^i.b_i$. ■

Free modules are studied in more detail in section 3.1.3.

(III) The categories ${}_{\mathbf{R}}\mathbf{Mod}$ and $\mathbf{Mod}_{\mathbf{R}}$ admit products and coproducts with the same definitions as in $\mathbf{Ab}$ (section 2.2.1**(IV),(V)**). Coproducts are more commonly referred to as *direct sums*. A ring $\mathbf{R}$ may be viewed as a left $\mathbf{R}$-module ${}_{\mathbf{R}}\mathbf{R}$ or as a right $\mathbf{R}$-module $\mathbf{R}_{\mathbf{R}}$. As in section 1.2.6, we define the *power* $\mathbf{R}^I = \prod_{i\in I} \mathbf{R}_i$ and the *copower* $\mathbf{R}^{(I)} = \bigoplus_{i\in I} \mathbf{R}_i$, where $\mathbf{R}_i = \mathbf{R}$ for each $i \in I$. If $M = M_1 \oplus M_2$, we say that that the modules M_1 and M_2 are supplementary (in M); if so, we have that $M_2 \cong M/M_1$ by [2.14]. If $M_1 \subseteq M$ has a supplementary module M_2 in M, we say that M_1 is a *direct factor* or a *direct summand* of M.

Let M be an $\mathbf{R}$-module and $N \subseteq M$. The relation $x - y \in N$ $(x, y \in M)$ is an equivalence relation $\sim$. The quotient set $M/\sim$ has an $\mathbf{R}$-module structure; it is denoted by M/N and is called the quotient module of M by N. If can : $M \twoheadrightarrow M/N$ is the mapping $x \mapsto \bar{x}$, where $\bar{x} := x + N$ is the class of x (mod. $\sim$), $(M/N, \text{can})$ is a quotient object (section 1.1.1**(III)**) of M in ${}_{\mathbf{R}}\mathbf{Mod}$, and we call can the canonical epimorphism. The fundamental isomorphisms in section 2.2.3, which hold for abelian groups, also hold for left and right $\mathbf{R}$-modules.

2.3.2. *Ideals*

(I) A *left* (resp. *right*) *ideal* is a submodule of ${}_{\mathbf{R}}\mathbf{R}$ (resp. $\mathbf{R}_{\mathbf{R}}$). We write $\mathfrak{a} \lhd_l \mathbf{R}$ (resp. $\mathfrak{a} \lhd_r \mathbf{R}$) to indicate that $\mathfrak{a}$ is a left (resp. right) ideal in $\mathbf{R}$. An *ideal* (or *two-sided ideal*) in $\mathbf{R}$ is a left ideal that is also a right ideal, in which case we write $\mathfrak{a} \lhd \mathbf{R}$. In commutative rings, every ideal is two-sided. A left or right ideal $\mathfrak{a}$ in the ring $\mathbf{R}$ is said to be *proper* if $\mathfrak{a} \subsetneq \mathbf{R}$. Let $S \subset \mathbf{R}$. The left ideal (resp. right ideal, resp. two-sided ideal) generated by S is the smallest left ideal (resp. right ideal, resp. two-sided ideal) that contains S. We write (S) for the two-sided ideal generated by S. When $S = \{a\}$, $(a \in \mathbf{R})$, the left ideal (resp.

right ideal, resp. two-sided ideal) $\mathbf{R}a$ (resp. $a\mathbf{R}$, resp. $(a) = \mathbf{R}a\mathbf{R}$), is said to be *principal*. If S is finite, the left ideal (resp. right ideal, resp. two-sided ideal) generated by S is said to be *finitely generated*.

LEMMA 2.21.– *Let* $\mathbf{R}$ *be a ring.*

i) Let $a, b \in \mathbf{R}$. *If* a, b *are left-associated, then* $\mathbf{R}a = \mathbf{R}b$. *Conversely, if* a, b *are right-regular and* $\mathbf{R}a = \mathbf{R}b$, *then* a, b *are left-associated.*

ii) Suppose that $\mathbf{R}$ *is entire. If* $\mathfrak{a} \neq 0$ *is both a principal left ideal and a principal right ideal, then it is generated by an invariant element* a, *so* $\mathfrak{a} = \mathbf{R}a\mathbf{R}$.

PROOF.– i) If there exists $u \in \mathbf{U}(\mathbf{R})$ such that $a = ub$, then $\mathbf{R}a = \mathbf{R}ub$ and $\mathbf{R}u = \mathbf{R}$, so $\mathbf{R}a = \mathbf{R}b$. Conversely, if $\mathbf{R}a = \mathbf{R}b$, then $a \in \mathbf{R}b$, so there exists $c \in \mathbf{R}$ such that $a = cb$. Moreover, we have that $b \in \mathbf{R}a$, so there exists $d \in \mathbf{R}$ such that $b = da$. Hence, $a(1 - cd) = 0$, and since a is right-regular, $cd = 1$. By symmetry, $dc = 1$, so c and d are two units and are inverses of each other.

ii) Write $\mathfrak{a} = a\mathbf{R} = b\mathbf{R}$. Then, $a \in b\mathbf{R}$ and there exists $c \neq 0$ such that $a = bc$. Similarly, there exists $d \neq 0$ such that $b = ad$, so $a = adc$ and we conclude as above that $c, d \in \mathbf{U}(\mathbf{R})$. Hence, $a\mathbf{R} = \mathbf{R}a$. ■

(II) It follows from Lemma 2.13 that the set $\mathrm{Lat}(M)$ of submodules of an $\mathbf{R}$-module M is a complete modular lattice, with $N_1 \vee N_2 = N_1 + N_2$ and $N_1 \wedge N_2 = N_1 \cap N_2$ if $N_1, N_2 \subseteq M$.

(III) Let M be a left $\mathbf{R}$-module and $m \in M$. The *annihilator* of m (resp. of M) is written as $\mathrm{Ann}_l^{\mathbf{R}}(m)$ (resp. $\mathrm{Ann}_l^{\mathbf{R}}(M)$), and is the left ideal defined by:

$$\mathrm{Ann}_l^{\mathbf{R}}(m) := \{\lambda \in \mathbf{R} : \lambda.m = 0\} \quad (\text{resp. } \mathrm{Ann}_l^{\mathbf{R}}(M) = \bigcap_{m \in M} \mathrm{Ann}_l^{\mathbf{R}}(m)\,).$$

A left $\mathbf{R}$-module is said to be *faithful* if $\mathrm{Ann}_l^{\mathbf{R}}(M) = \{0\}$, and *bounded* if there exists a regular element $c \in \mathrm{Ann}_l^{\mathbf{R}}(M)$ (a faithful module is therefore not bounded, and, if $\mathbf{R}$ is an entire ring, an $\mathbf{R}$-module is faithful if and only if it is not bounded).

LEMMA 2.22.– *An* $\mathbf{R}$*-module* M *is monogenous (section 2.3.1(**II**)) if and only if there exists a left ideal* $\mathfrak{a}$ *such that* $M \cong \mathbf{R}/\mathfrak{a}$. *If so,* $\mathrm{Ann}_l^{\mathbf{R}}(M)$ *is a two-sided ideal.*

PROOF.– Suppose that $M = [m]_{\mathbf{A}}$. Then, by Noether's first isomorphism theorem (Theorem 2.12(1)), $M \cong \mathbf{R}/\mathfrak{a}$, where $\mathfrak{a} = \mathrm{Ann}_l^{\mathbf{R}}(m)$. Conversely, if there exists an isomorphism $\psi : M \tilde{\to} \mathbf{R}/\mathfrak{a}$, M is generated by $m = \psi^{-1}(\bar{1})$, where $\bar{1}$ is the canonical image of 1. Then $\lambda \in \mathrm{Ann}_l^{\mathbf{R}}(M) \Leftrightarrow \lambda.\mathbf{R}/\mathfrak{a} = 0 \Leftrightarrow \lambda\mathbf{R} \subset \mathfrak{a}$, which implies that $\lambda\mu\mathbf{R} \subset \mathfrak{a}$ for all $\mu \in \mathbf{R}$, so $\lambda\mu \in \mathrm{Ann}_l^{\mathbf{R}}(M)$. It follows that $\mathrm{Ann}_l^{\mathbf{R}}(M)$ is a right ideal. Since it is obviously a left ideal, it is in fact two-sided. ■

(IV) Let $\mathfrak{a}$ be a two-sided ideal in the ring $\mathbf{R}$. Then, the quotient module $\mathbf{R}/\mathfrak{a}$ may be equipped with a canonical ring structure by setting $(x+\mathfrak{a})(y+\mathfrak{a}) = x.y + \mathfrak{a}$.

LEMMA 2.23.– *Let $\mathbf{R}$ be a ring and suppose that $\mathfrak{a}$ is a two-sided ideal in $\mathbf{R}$. Every left ideal (resp. two-sided ideal) in $\mathbf{R}/\mathfrak{a}$ may be written uniquely in the form $\mathfrak{b}/\mathfrak{a}$, where $\mathfrak{b}$ is a left ideal (resp. two-sided ideal) in $\mathbf{R}$ such that $\mathfrak{b} \supset \mathfrak{a}$.*

PROOF.– Let $\varphi : \mathbf{R} \twoheadrightarrow \mathbf{R}/\mathfrak{a}$ be the canonical epimorphism. Let $\mathfrak{i}$ be a left ideal in $\mathbf{R}/\mathfrak{a}$ and $\mathfrak{b} = \varphi^{-1}(\mathfrak{i})$. Then $\mathfrak{b}$ is a left ideal in $\mathbf{R}$, $\mathfrak{b} \supset \mathfrak{a}$, and $\varphi(\mathfrak{b}) = \mathfrak{b}/\mathfrak{a}$; hence $\mathfrak{i} = \mathfrak{b}/\mathfrak{a}$ (Lemma 1.12). The converse is obvious. ■

(V) If $\mathfrak{a}, \mathfrak{b} \subset \mathbf{R}$, we write $\mathfrak{ab}$ for the $\mathbb{Z}$-module generated by the products ab, $a \in \mathfrak{a}, b \in \mathfrak{b}$. This satisfies the following properties (**exercise**): if $\mathfrak{a} \lhd_l \mathbf{R}$, then $\mathfrak{ab} \lhd_l \mathbf{R}$; if $\mathfrak{b} \lhd_r \mathbf{R}$, then $\mathfrak{ab} \lhd_r \mathbf{R}$; and in both cases $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$ (this inclusion is usually strict). In particular, if $\mathfrak{a} \lhd \mathbf{R}$ and $\mathfrak{b} \lhd \mathbf{R}$, then $\mathfrak{ab} \lhd \mathbf{R}$. If $\mathfrak{b},\mathfrak{c} \lhd_r \mathbf{R}$ and $\mathfrak{a} \subset \mathbf{R}$, then $\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{ab} + \mathfrak{ac}$; if $\mathfrak{a}, \mathfrak{c} \lhd_l \mathbf{R}$ and $\mathfrak{b} \subset \mathbf{R}$, then $(\mathfrak{a}+\mathfrak{c})\mathfrak{b} = \mathfrak{ab} + \mathfrak{cb}$. If $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \lhd_l \mathbf{R}$, then $(\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc})$.

LEMMA 2.24.– *If $\mathfrak{b}_1, ..., \mathfrak{b}_n \lhd \mathbf{R}$ satisfy $\mathfrak{b}_i + \mathfrak{b}_j = \mathbf{R}$ for $i \neq j$, then:*

$$\bigcap\nolimits_{1\leq i\leq n} \mathfrak{b}_i = \sum_{\sigma\in\mathfrak{S}(n)} \prod\nolimits_{i=1}^{n} \mathfrak{b}_{\sigma(i)}.$$

In particular, if $\mathbf{R}$ is commutative, $\bigcap\limits_{1\leq i\leq n} \mathfrak{b}_i = \prod\limits_{i=1}^{n} \mathfrak{b}_i$.

PROOF.– When $n = 2$, there exist $a_1 \in \mathfrak{b}_1, a_2 \in \mathfrak{b}_2$ such that $a_1 + a_2 = 1$. If $x \in \mathfrak{b}_1 \cap \mathfrak{b}_2$, we have that $x = x(a_1 + a_2) = xa_1 + xa_2 \in \mathfrak{b}_2\mathfrak{b}_1 + \mathfrak{b}_1\mathfrak{b}_2$, so $\mathfrak{b}_1 \cap \mathfrak{b}_2 = \mathfrak{b}_2\mathfrak{b}_1 + \mathfrak{b}_1\mathfrak{b}_2$. We can now simply argue by induction (**exercise**) using the result (**Res**) stated below, which may also be shown by induction (**exercise***: see [BKI 12], Chap. I, section 8.9, Prop. 6): ■

(**Res**) Let $\mathfrak{a}, \mathfrak{b}_1, ..., \mathfrak{b}_n \lhd \mathbf{R}$ be such that $\mathbf{R} = \mathfrak{a} + \mathfrak{b}_i$ for all $i \in \{1, ..., n\}$. Then:

$$\mathbf{R} = \mathfrak{a} + \prod_{i=1}^{n} \mathfrak{b}_i = \mathfrak{a} + \bigcap\nolimits_{1 \leq i \leq n} \mathfrak{b}_i.$$

THEOREM 2.25.– *(*Chinese remainder theorem*): Let* $\mathbf{R}$ *be a ring and let* $\mathfrak{b}_i$ $(1 \leq i \leq n)$ *and* $\mathfrak{c}$ *be left ideals in* $\mathbf{R}$*.*

1) There exists a homomorphism:

$$\bar{f} : \mathbf{R}/\mathfrak{c} \to \prod_{i=1}^{n} \mathbf{R}/\mathfrak{b}_i,$$

if and only if $\mathfrak{c} \subset \bigcap_{i=1}^{n} \mathfrak{b}_i$*. This homomorphism is injective if and only if* $\mathfrak{c} = \bigcap_{i=1}^{n} \mathfrak{b}_i$*.*

2) The canonical homomorphism from $\mathbf{R}$ *to* $\prod_{i=1}^{n} \mathbf{R}/\mathfrak{b}_i$ *with kernel* $\bigcap_{i=1}^{n} \mathfrak{b}_i$ *is surjective if one of the following two conditions holds:*

i) $\mathfrak{b}_i + \bigcap_{j \neq i} \mathfrak{b}_j = \mathbf{R} \quad (i = 1, ..., n)$.

ii) The ideals $\mathfrak{b}_i$ $(1 \leq i \leq n)$ *are* two-sided *and* $\mathfrak{b}_i + \mathfrak{b}_j = \mathbf{R}$ $(i, j = 1, ..., n; i \neq j)$.

PROOF.– (1) The homomorphism $\bar{f}$, if it exits, is induced by the ring homomorphism $f : \mathbf{R} \to \prod_{i=1}^{n} \mathbf{R} : x \mapsto (x, ..., x)$. We can then simply apply Theorem-definition 2.11. (2) We must show that for any family $(x_i)_{1 \leq i \leq n}$ of elements of $\mathbf{R}$ there exists $x \in \mathbf{R}$ such that $x + \mathfrak{b}_i = x_i + \mathfrak{b}_i$ $(i = 1, ..., n)$. We proceed by induction. The result is trivial for $n = 1$. By the induction hypothesis on n, there exists $y \in \mathbf{R}$ such that $y + \mathfrak{b}_i = x_i + \mathfrak{b}_i$ $(i = 1, ..., n-1)$. We must find x of the form $y + z, z \in \mathbf{R}$. We need $z + \mathfrak{b}_i = \mathfrak{b}_i$ $(i = 1, ..., n-1)$, i.e. $z \in \mathfrak{b} := \bigcap_{i=1}^{n-1} \mathfrak{b}_i$, and also $z + \mathfrak{b}_n = x_n - y + \mathfrak{b}_n$. In case (i) we have that $\mathfrak{b}_n + \mathfrak{b} = \mathbf{R}$, and this also holds in case (ii) by the result (**Res**) stated in the proof of Lemma 2.24. ■

In the following, whenever a condition is only satisfied on the left or on the right, this will be stated. Otherwise, we implicitly assume that it is satisfied on both sides. (For example, we will simply say *ideal* for a *two-sided ideal*. A *principal ideal domain* (section 2.3.8(**IV**)) is a *principal left ideal domain that is also a principal right ideal domain*, etc.).

2.3.3. *Maximal ideals and prime ideals. Spectrum*

(I) MAXIMAL IDEALS A submodule that is maximal (with respect to inclusion) among the proper submodules of an $\mathbf{R}$-module M (section 2.3.1**(II)**) is called a *maximal submodule* of M.

DEFINITION 2.26.– *Let* $\mathbf{R}$ *be a ring. A* maximal left ideal *in* $\mathbf{R}$ *is a maximal submodule of* ${}_{\mathbf{R}}\mathbf{R}$. *If* $\mathbf{R}$ *is commutative, the set of maximal ideals in* $\mathbf{R}$ *is called the* maximal spectrum *of* $\mathbf{R}$ *and is written as Spm* $(\mathbf{R})$.

THEOREM 2.27.– *(Krull): 1) Let* $M \neq 0$ *be a finitely generated left* $\mathbf{R}$*-module and let* N *be a proper submodule of* M. *Then, there exists a maximal submodule of* M *that contains* N. *2) In particular, every proper left ideal in* $\mathbf{R} \neq 0$ *belongs to some maximal left ideal.*

PROOF.– (1) Let X be a generating set of M, $\mathcal{P}$ the set of proper submodules of M that contain N, and C a chain of $\mathcal{P}$ ordered by inclusion. The union A of the elements of C is a submodule of M. If $A = M$, then $A \supset X$ and since X is finite, all the elements of X must belong to some element of $\mathcal{P}$, which is impossible. Hence, A is a proper submodule of M, which implies that $\mathcal{P}$ is inductive, and so must have a maximal element by Zorn's lemma (Lemma 1.3). (2) is a special case of (1). ■

The following result, whose proof is an **exercise*** ([COH 03a], Thm. 10.2.4), establishes a useful generalization of Krull's theorem:

LEMMA 2.28.– *Let* $\mathbf{R}$ *be a commutative ring,* $S \subset \mathbf{R}$ *a* multiplicative monoid *and* $\mathfrak{a} \neq \mathbf{R}$ *an ideal disjoint from* S. *Then, there exists an ideal* $\mathfrak{m}$ *that is maximal among the ideals that contain* $\mathfrak{a}$ *and are disjoint from* S *and* $\mathfrak{m}$ *is a prime ideal.*

(II) PRIME SPECTRUM OF A RING.

DEFINITION 2.29.– *A proper ideal* $\mathfrak{p} \lhd \mathbf{R}$ *is said to be* prime *if, for all ideals* $\mathfrak{a}, \mathfrak{b} \lhd \mathbf{R}$,

$$\mathfrak{a}\mathfrak{b} \subset \mathfrak{p} \implies \mathfrak{a} \subset \mathfrak{p} \text{ or } \mathfrak{b} \subset \mathfrak{p}.$$

The set of all prime ideals in $\mathbf{R}$ *is called the* prime spectrum *of* $\mathbf{R}$ *and is written as Spec* $(\mathbf{R})$.

The ideals in $\mathbb{Z}$ are principal, so are of the form (n). These ideals are proper if and only if $n \neq 1$, and maximal if and only if $n > 0$ is a prime number. The ideal (0) is prime but is not maximal.

By Krull's theorem (Theorem 2.27), Spec $(\mathbf{R}) \neq \varnothing$ if $\mathbf{R} \neq \{0\}$. The proof of the following result is left as an **exercise*** ([LAM 01], Prop. (10.2)):

LEMMA 2.30.– *For a proper ideal* $\mathfrak{p} \lhd \mathbf{R}$, *the following conditions are equivalent:*

i) $\mathfrak{p}$ *is prime;*

ii) For $a, b \in \mathbf{R}$, $(a)(b) \subset \mathfrak{p}$ *implies that* $a \in \mathfrak{p}$ *or* $b \in \mathfrak{p}$;

iii) For $a, b \in \mathbf{R}$, $a\mathbf{R}b \subset \mathfrak{p}$ *implies that* $a \in \mathfrak{p}$ *or* $b \in \mathfrak{p}$;

iv) For $\mathfrak{a}, \mathfrak{b} \lhd_l \mathbf{R}$, $\mathfrak{ab} \subset \mathfrak{p}$ *implies that* $\mathfrak{a} \subset \mathfrak{p}$ *or* $\mathfrak{b} \subset \mathfrak{p}$;

v) For $\mathfrak{a}, \mathfrak{b} \lhd_r \mathbf{R}$, $\mathfrak{ab} \subset \mathfrak{p}$ *implies that* $\mathfrak{a} \subset \mathfrak{p}$ *or* $\mathfrak{b} \subset \mathfrak{p}$.

An ideal $\mathfrak{p} \lhd \mathbf{R}$ is said to be *completely prime* (or *strongly prime*) if the ring $\mathbf{R}/\mathfrak{p}$ is entire. This condition is satisfied if and only if $\mathfrak{p} \neq \mathbf{R}$ and, for all $a, b \in \complement_{\mathbf{R}}\mathfrak{p}$, $ab \in \complement_{\mathbf{R}}\mathfrak{p}$, or alternatively if and only if $\mathfrak{p} \neq \mathbf{R}$ and $ab \in \mathfrak{p} \Longrightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. A completely prime ideal is prime, and the converse holds *if* $\mathbf{R}$ *is commutative*.

LEMMA 2.31.– *Let* $p \in \complement_{\mathbf{R}}\mathbf{U}(\mathbf{R})$ *be a regular and invariant element. Then,* p *is prime in* $\mathbf{R}$ *(section 2.1.1**(II)**) if and only if the principal ideal* (p) *is completely prime.*

PROOF.– Let $c \in \mathbf{R}$. We have that $p \mid c$ if and only if $c \in (p)$, so $c \notin (p)$ if and only if $p \nmid c$. But p is prime if and only if $(p \nmid a$ and $p \nmid b) \Longrightarrow p \nmid ab$; in other words $a, b \in \complement_{\mathbf{R}}(p) \Longrightarrow ab \in \complement_{\mathbf{R}}(p)$. ■

By applying Zorn's lemma (Lemma 1.3), it can be shown that every completely prime ideal $\mathfrak{p}$ in a ring $\mathbf{R}$ contains a *minimal* completely prime ideal in $\mathbf{R}$ (**exercise**).

(III) ZARISKI TOPOLOGY. A *topology* $\mathfrak{T}$ on a set X is a subset of $\mathfrak{P}(X)$ such that $\varnothing \in \mathfrak{T}$; $X \in \mathfrak{T}$; if $(O_{i\in I})$ is a family of elements of $\mathfrak{T}$, then $\cup_{i\in I} O_i \in \mathfrak{T}$; if $O_1, ..., O_n$ are (a finite number of) elements of $\mathfrak{T}$, then their intersection is in $\mathfrak{T}$. The elements of $\mathfrak{T}$ are called the *open sets* of the topological space $(X, \mathfrak{T})$

(or of X whenever $\mathfrak{T}$ is implicit); the complement of an open set is called a *closed set*. A neighborhood of a point x is a set $\mathcal{V}$ that contains an open set containing x.

Let $\mathbf{R}$ be a commutative ring, let $\mathfrak{I}(\mathbf{R})$ be the set of ideals of $\mathbf{R}$ and, given an ideal $\mathfrak{a}$, let $\mathrm{V}(\mathfrak{a})$ be the set of prime ideals containing $\mathfrak{a}$. If $\mathfrak{I}(\mathbf{R})$ and $\mathrm{Spec}(\mathbf{R})$ are ordered by inclusion, the mapping $\mathfrak{I}(\mathbf{R}) \to \mathrm{Spec}(\mathbf{R}) : \mathfrak{a} \mapsto \mathrm{V}(\mathfrak{a})$ is decreasing. For any index set I, we also have that:

$$\mathrm{V}\left(\sum\nolimits_{i\in I}\mathfrak{a}_i\right) = \bigcap_{i\in I}\mathrm{V}(\mathfrak{a}_i), \quad \mathrm{V}(\mathfrak{a}_1\cap\mathfrak{a}_2) = \mathrm{V}(\mathfrak{a}_1\mathfrak{a}_2) = \mathrm{V}(\mathfrak{a}_1)\cup\mathrm{V}(\mathfrak{a}_2),$$
$$\mathrm{V}((0)) = \mathrm{Spec}(\mathbf{R}), \quad \mathrm{V}(\mathbf{R}) = \varnothing,$$

so the $\mathrm{V}(\mathfrak{a})$ satisfy the axioms of the closed sets of a topology on $\mathrm{Spec}(\mathbf{R})$, called the Zariski topology on $\mathrm{Spec}(\mathbf{R})$. This is a Kolmogorov space, which means that, given two distinct points in $\mathrm{Spec}(\mathbf{R})$, there exists a neighborhood of one that does not contain the other ([BKI 98], Chap. II, section 4, Exerc. 9); however, it is not Hausdorff (the Hausdorff separation axiom, stating that any two distinct points have disjoint neighborhoods, is stronger than the Kolmogorov separation axiom)[6]. A point $\mathfrak{a}$ is closed in $\mathrm{Spec}(\mathbf{R})$ if and only if $\mathfrak{a}$ is a maximal ideal in $\mathbf{R}$ (**exercise**).

2.3.4. *Noetherian rings and Artinian rings*

(I) We say that the ring $\mathbf{R}$ is *left Noetherian* (after E. Noether) if every left ideal in $\mathbf{R}$ is finitely generated, or equivalently (**exercise**) if every ascending sequence of left ideals $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_r \subset \ldots$ is *stationary*, i.e. there exists a rank r such that $\mathfrak{a}_n = \mathfrak{a}_r, \forall n \geq r$. A ring $\mathbf{R}$ is said to be *left Artinian* (after E. Artin) if every descending sequence of left ideals $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \ldots \supset \mathfrak{a}_r \supset \ldots$ is stationary. Every left Artinian ring is left Noetherian (Hopkins' *theorem*: see [COH 03a], Cor. 5.3.10). The ring $\mathbb{Z}$ is Noetherian (since it is principal), but is not Artinian since, if $q > 1$, the sequence of ideals $(q) \supset \left(q^2\right) \supset \ldots \supset (q^r) \supset \ldots$ is *strictly* descending.

6 Unless otherwise stated, the separation axiom of a topological space is always the Hausdorff axiom.

(II) Let $\mathfrak{p} \in \text{Spec}(\mathbf{R})$. The set of prime ideals $\mathfrak{p}' \subseteq \mathfrak{p}$ is an ordered set under inclusion and the height $\mathfrak{h}(\mathfrak{p})$ of $\mathfrak{p}$ is defined as in section 2.1.2**(III)**, i.e. is the maximal length r of chains of prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset ... \subset \mathfrak{p}_r = \mathfrak{p}$. Let $\mathfrak{a}$ be a proper ideal in a commutative ring $\mathbf{R}$. We say that a prime ideal $\mathfrak{p}$ is *minimal* over $\mathfrak{a}$ if $\mathfrak{p}$ is minimal in $V(\mathfrak{a})$ (ordered by inclusion). The *generalized theorem of principal ideals* ([ROT 02], Thm. 11.162) states that:

THEOREM 2.32.– *Let* $\mathbf{R}$ *be a commutative Noetherian ring and let* $\mathfrak{a} = (a_1, ..., a_n)$ *be a proper ideal in* $\mathbf{R}$. *If* $\mathfrak{p} \in \text{Spec}(\mathbf{R})$ *is minimal over* $\mathfrak{a}$, *then* $\mathfrak{h}(\mathfrak{p}) \leq n$ *(and in particular, if* $\mathfrak{a}$ *is principal, then* $\mathfrak{h}(\mathfrak{p}) \leq 1$*).*

2.3.5. *Division rings. Simple modules and simple Artinian rings. Radical*

(I) DIVISION RINGS. A ring $\mathbf{K} \neq \{0\}$ is a *division ring* (or a *skew field*) if every non-zero element is invertible. This is equivalent to saying that the only proper left or right ideal of the ring $\mathbf{K}$ is (0), so a division ring is a Noetherian ring. A *field* is a commutative division ring. By the correspondence theorem (section 2.2.3**(III)**), whenever $\mathbf{R}$ is a ring and $\mathfrak{m} \lhd \mathbf{R}$, $\mathbf{R}/\mathfrak{m}$ is a division ring if and only if the ideal $\mathfrak{m}$ is a maximal left ideal or a maximal right ideal. Let $\mathbf{K}$ be a division ring. A left $\mathbf{K}$-module (resp. right $\mathbf{K}$-module) is called a left $\mathbf{K}$-vector space (resp. right $\mathbf{K}$-vector space). Let $\varphi : \mathbb{Z} \to \mathbf{K}$ be the homomorphism defined by $\varphi(n) = 1 + 1... + 1$ (sum of n terms in $\mathbf{K}$). If φ is injective, then $\mathbb{Z} \subset \mathbf{K}$ and we say that $\mathbf{K}$ has the characteristic 0. If φ is not injective, Noether's first isomorphism theorem (Theorem 2.12(1)) implies that $\mathbb{Z}/\ker(\varphi) \cong F$, where F is a sub-division ring of $\mathbf{K}$ (and is a field). The ideal $\ker(\varphi)$ in $\mathbb{Z}$ is maximal and $\neq (0)$, so is of the form (p), where p is a prime number (by Lemma 2.31 and Theorem 2.38), written as $\text{Char}(\mathbf{K})$ and called the *characteristic* of $\mathbf{K}$. A division ring is said to be *prime* if it does not contain a proper sub-division ring; any such division ring is a field. If $\text{Char}(\mathbf{K}) = 0$, its prime field is $\mathbb{Q}$; if $\text{Char}(\mathbf{K}) = p > 0$, its prime field is $\mathbb{Z}/p\mathbb{Z}$.

LEMMA 2.33.– *If* $\mathbf{R}$ *is a ring* $\neq 0$ *and* $f : \mathbf{K} \to \mathbf{R}$ *is a ring homomorphism, then* f *is injective (**exercise**).*

It can be shown that every non-commutative division ring is infinite (Wedderburn's theorem: see [BKI 12], Chap. VIII, section 18, section 2, Thm. 2), and similarly that in any such division ring, every element belongs to some infinite subfield ([COH 95], Thm. 3.4.8).

(II) DIVISION RING EXTENSIONS. If two division rings $\mathbf{K}, \mathbf{L}$ are such that $\mathbf{K} \subset \mathbf{L}$, we say that $\mathbf{L}$ is an *extension* of $\mathbf{K}$, often written as $\mathbf{L}/\mathbf{K}$. If so, $\mathbf{L}$ and $\mathbf{K}$ have the same characteristic. For example, if a division ring $\mathbf{L}$ has characteristic 0, the field $\mathbb{Q}$ of rational numbers is isomorphic to a field $\mathbf{K} \subset \mathbf{L}$, and by identification $\mathbf{L}$ is an extension of $\mathbb{Q}$. Let $\mathbf{K}$ be a field and let $\mathbf{L}$ be an extension of $\mathbf{K}$. We say that $x \in \mathbf{L}$ is *algebraic* over $\mathbf{K}$ if there exists a non-zero polynomial $f \in \mathbf{K}[X]$ (where $\mathbf{K}[X]$ denotes the ring of polynomials in the indeterminate X with coefficients in $\mathbf{K}$) such that x is a root of f. In the set of *unitary polynomials* (polynomials for which the coefficient of the highest degree term is 1) such that $f(x) = 0$, there is a unique polynomial of minimal degree called the *minimal polynomial* of x. This polynomial is necessarily irreducible in $\mathbf{K}[X]$ (and conversely, a polynomial that is irreducible in $\mathbf{K}[X]$ is the minimal polynomial of some algebraic element x). The degree of this polynomial is called the *degree* of x and is written as $d^{\circ}(x)$. If every element of $\mathbf{L} \supset \mathbf{K}$ is algebraic over $\mathbf{K}$, we say that $\mathbf{L}$ is an *algebraic extension* of $\mathbf{K}$. An extension that is not algebraic is called *transcendental*. A field extension $\mathbf{L}/\mathbf{K}$ is said to be *finite* if the dimension $[\mathbf{L} : \mathbf{K}]$ of the $\mathbf{K}$-vector space $\mathbf{L}$, called the *degree of the extension* $\mathbf{L}/\mathbf{K}$, is finite. Finite field extensions $\mathbf{L}/\mathbf{K}$ are necessarily algebraic, since if $x \in \mathbf{L}$ is not algebraic over $\mathbf{K}$, the sequence (V_m) of subspaces $V_m = \bigcup_{0 \leq n \leq m} \mathbf{K}x^n$ of $\mathbf{L}$ is strictly ascending. A field $\mathbf{K}$ is said to be *algebraically closed* if every polynomial $f \in \mathbf{K}[X]$ of degree ≥ 1 has a root in $\mathbf{K}$. An *algebraic closure* of $\mathbf{K}$ is an algebraic extension that is algebraically closed. The set $\bar{\mathbb{Q}}$ of all the roots of the polynomials $f \in \mathbb{Q}[X]$ is the *field of algebraic numbers*, which is therefore algebraically closed. Similarly, $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$ (*fundamental theorem of algebra*, see [P2], section 1.1.4) - we sometimes say, by abuse of language, that it is *the* algebraic closure, because of the following theorem by E. Steinitz (see [P2], section 1.1.4): *let* $\mathbf{K}$ *be a field. Then there exists an algebraic closure of* $\mathbf{K}$. *If* Ω *and* Ω' *are two algebraic closures of* $\mathbf{K}$, *then there exists a* $\mathbf{K}$*-isomorphism* $\Omega \xrightarrow{\sim} \Omega'$, i.e. an isomorphism that leaves each element of $\mathbf{K}$ *fixed.*

LEMMA 2.34.– *Every algebraically closed field is infinite.*

PROOF.– Suppose that $\mathbf{K}$ is finite. Then, $f(X) = 1 + \prod_{a \in \mathbf{K}} (X - a)$ does not have a root in $\mathbf{K}$. ■

(III) SIMPLE ARTINIAN RINGS AND SEMI-SIMPLE RINGS. An $\mathbf{R}$-module is said to be *simple* if its only proper submodule is 0, and *semi-simple* if it is a

direct sum of simple modules. By the correspondence theorem (section 2.2.3(**III**)), if M is an $\mathbf{R}$-module and $N \subseteq M$, M/N is simple if and only if N is a maximal submodule. Theorem 2.27 therefore implies:

COROLLARY 2.35.– *Every module $M \neq 0$ has a quotient S that is a simple module.*

A ring is said to be *simple* if its only proper two-sided ideal is (0). Any division ring is a simple Artinian ring. A ring $\mathbf{R}$ is said to be *left semi-simple* if the module ${}_{\mathbf{R}}\mathbf{R}$ is semi-simple. The ring $\mathbf{R}$ is left semi-simple if and only if every left $\mathbf{R}$-module is semi-simple ([BKI 12], Chap. VIII, section 8.2, Prop. 4). All left semi-simple rings can be shown to be left Artinian ([LAM 01], Chap. 1, Cor. (2.6)), and a ring is left semi-simple if and only if it is right semi-simple ([LAM 01], Chap. 1, Cor. (3.7)), so such a ring is said to be semi-simple.

LEMMA 2.36.– *Let $\mathbf{K}$ be a division ring, V a $\mathbf{K}$-vector space of dimension $n \geq 1$ and $\mathrm{End}(V)$ the ring of endomorphisms of V. Then, $\mathrm{End}(V)$ is a simple Artinian ring.*

PROOF.– Let $0 \neq f \in \mathrm{End}(V)$, $0 \neq e_1 \in \ker(f)$, $a = f(e_1)$ and let $e_i, 2 \leq i \leq n$ be vectors such that $(e_i)_{1 \leq i \leq n}$ is a basis of V (these vectors exist by the basis extension theorem: see Theorem 3.10). Let $(p_j)_{1 \leq j \leq n}$ and $(q_i)_{1 \leq i \leq n}$ be sequences of elements in $\mathrm{End}(V)$ such that $p_j(e_i) = e_1$ if $i = j$, $p_j(e_i) = 0$ and $i \neq j$, $q_i(a) = e_i$. Then $(q_i \circ f \circ p_j)(e_1) = e_i \delta_i^j$, and so the family $(q_i \circ f \circ p_j)_{i,j \in \{1,\ldots,n\}} \in (f)$ generates $\mathrm{End}(V)$, hence the latter is a simple ring. Furthermore, $\mathrm{End}(V)$ is a $\mathbf{K}$-vector space of dimension n^2, so each left or right ideal in $\mathrm{End}(V)$ is a vector space of dimension $\leq n^2$, from which it follows that the ring $\mathrm{End}(V)$ is Artinian. ■

The ring $\mathrm{End}(V)$ is isomorphic to the ring $\mathfrak{M}_n(\mathbf{K})$ of $n \times n$ matrices with elements in $\mathbf{K}$. Therefore, if $\mathbf{K}$ is an arbitrary division ring, the ring $\mathfrak{M}_n(\mathbf{K})$ is simple Artinian. The converse of this result was established by J. Wedderburn ([BKI 12], Chap. VIII, section 7.1, Thm. 1 & section 8.1, Thm. 1), who also fully clarified the structure of semi-simple rings:

THEOREM 2.37.– *(Wedderburn-Artin* structure theorem*):*

1) A ring is simple left Artinian if and only if it is simple right Artinian, and for this condition to be satisfied, it is necessary and sufficient for it to be isomorphic to a ring of matrices $\mathfrak{M}_n(\mathbf{K}), n \geq 1$, where $\mathbf{K}$ is a division ring;

2) A ring is semi-simple if and only if it is a finite product of simple Artinian rings.

The relationship between simple modules and quotients by maximal submodules is made explicit by the following theorem:

THEOREM 2.38.– *1) Any simple* $\mathbf{R}$*-module* S *is isomorphic to a quotient* $\mathbf{R}/\mathfrak{m}$*, where* $\mathfrak{m}$ *is a maximal left ideal;*

2) If M *is an* $\mathbf{R}$*-module and* $N \subseteq M$*, the quotient module* M/N *is simple if and only if* N *is a maximal submodule of* M;

3) Every finitely generated $\mathbf{R}$*-module has a quotient that is a simple module;*

4) Let $\mathfrak{m}$ *be a* two-sided *ideal in* $\mathbf{R} \neq \{0\}$*. Then, the quotient ring* $\mathbf{R}/\mathfrak{m}$ *is a division ring if and only if* $\mathfrak{m}$ *is a maximal left ideal. Consequently, a two-sided ideal that is also a maximal left ideal is completely prime.*

PROOF.– (1) If the module S is simple, then it is monogenous, so it is isomorphic to a quotient $\mathbf{R}/\mathfrak{m}$, where $\mathfrak{m}$ is a left ideal in $\mathbf{R}$ (Lemma 2.22). The *correspondence theorem* (section 2.2.3**(III)**) implies that the submodules of $\mathbf{R}/\mathfrak{m}$ are the quotients $\mathfrak{n}/\mathfrak{m}$ where $\mathfrak{n} \supseteq \mathfrak{m}$, so since $\mathbf{R}/\mathfrak{m}$ is simple, $\mathfrak{n} = \mathbf{R}$ or $\mathfrak{n} = \mathfrak{m}$, which implies that $\mathfrak{m}$ is a maximal left ideal. (2) may be shown using the same reasoning and (3) follows from (2) and Krull's theorem (Theorem 2.27(2)). (4) is a consequence of (1). ■

(IV) RADICAL.

LEMMA 2.39.– *(N. Jacobson): Let* $\mathbf{R}$ *be a ring and let* $\mathfrak{J}$ *be a left ideal in* $\mathbf{R}$*. The following conditions are equivalent:*

i) $\mathfrak{J}$ *is the intersection of all maximal left ideals in* $\mathbf{R}$*;*

ii) An element x *belongs to* $\mathfrak{J}$ *if and only if, for each* $y \in \mathbf{R}$, $1 - yx$ *is left-invertible;*

iii) $\mathfrak{J} = \bigcap Ann_l^{\mathbf{R}}(S)$ *(section 2.3.2**(III)**), where* S *ranges over the set of simple left* $\mathbf{R}$*-modules;*

iv) An element x *belongs to* $\mathfrak{J}$ *if and only if, for all* $y, z \in \mathbf{R}$, $1 - yxz$ *is invertible;*

v) $\mathfrak{J}$ *is the largest left ideal (and in particular the largest two-sided ideal)* $\mathfrak{a}$ *such that* $1 - x$ *is invertible for every* $x \in \mathfrak{a}$;

vi) $\mathfrak{J}$ *is the intersection of all maximal right ideals in* $\mathbf{R}$*.*

PROOF.– (i)⇒(ii)⇒(iii)⇒(i): assume that (i) holds and let $x \in \mathfrak{J}$. If there exists $y \in \mathbf{R}$ such that $1 - yx$ is not left-invertible, then $\mathbf{R}(1 - yx)$ is contained in a maximal left ideal $\mathfrak{m}$ in $\mathbf{R}$. Hence, $1 - yx \in \mathfrak{m}$ and $x \in \mathfrak{m}$. This implies that $1 \in \mathfrak{m}$, contradiction. Therefore, $\mathfrak{J} \subset \mathfrak{J}_0$ where $\mathfrak{J}_0$ is the set of $x \in \mathbf{R}$ such that $1 - yx$ is left-invertible for all $y \in \mathbf{R}$. Let $x \in \mathfrak{J}_0$, let S be a simple left $\mathbf{R}$-module, $s \in S$, and suppose that $xs \neq 0$. The module $[xs]_{\mathbf{R}}$ is contained in S, so is equal to S. Hence, there exists $y \in \mathbf{R}$ such that $s = yxs$, from which it follows that $(1 - yx)\, s = 0$, contradiction. So, $\mathfrak{J}_0 \subset \bigcap \mathrm{Ann}_l^{\mathbf{R}}(S)$. But the maximal left ideals are the $\mathrm{Ann}_l^{\mathbf{R}}(S)$ such that S is a simple left $\mathbf{R}$-module, so $\bigcap \mathrm{Ann}_l^{\mathbf{R}}(S) = \mathfrak{J}$.

((ii),(iii))⇔(iv): let $x \in \mathfrak{J}$ and $y, z \in \mathbf{R}$. By (iii) and Lemma 2.22, $xz \in \mathfrak{J}$, so by (ii) there exists u (which clearly must be right-invertible) such that $u(1 - yxz) = 1$, which by (ii) implies that $yxz \in \mathfrak{J}$, so by (ii) $1 + uyxz$ is left-invertible, and thus $u = 1 + uyxz$ is left-invertible. Since u is both left- and right-invertible, it is invertible, and so $1 - yxz$ is invertible. Hence $\mathfrak{J} \subset \mathfrak{J}_1$, where $\mathfrak{J}_1$ is the set of $x \in \mathbf{R}$ such that $1 - yxz$ is invertible for all $y, z \in \mathbf{R}$. By setting $z = 1$, we find that $\mathfrak{J} = \mathfrak{J}_1$.

((ii),(iv)⇔(v)): this is clear. (v) is left/right symmetric and so is equivalent to (vi). ■

DEFINITION 2.40.– *The ideal $\mathfrak{J}$ that satisfies the conditions of Lemma 2.39 is called the Jacobson* radical *(or just the* radical*) of the ring $\mathbf{R}$ and is written as* $\mathrm{rad}(\mathbf{R})$. *The ring $\mathbf{R}$ is said to be* radical-free *if* $\mathrm{rad}(\mathbf{R}) = 0$.

The intersection of the maximal ideals in $\mathbb{Z}$ is $\mathrm{rad}(\mathbb{Z}) = 0$: the ring $\mathbb{Z}$ is radical-free. If $\mathbf{R}$ is a ring and $\mathfrak{a} \subset \mathrm{rad}(\mathbf{R})$ is a two-sided ideal in $\mathbf{R}$, then the maximal left ideals in $\mathbf{R}/\mathfrak{a}$ are the ideals of the form $\mathfrak{m}/\mathfrak{a}$, where $\mathfrak{m}$ is a maximal left ideal in $\mathbf{R}$ containing $\mathfrak{a}$, so $\mathrm{rad}(\mathbf{R}/\mathfrak{a}) = \mathrm{rad}(\mathbf{R})/\mathfrak{a}$.

LEMMA 2.41.– *(Nakayama): Let M be a finitely generated $\mathbf{R}$-module and let $\mathfrak{a} \subset \mathrm{rad}(\mathbf{R})$ be a two-sided ideal in $\mathbf{R}$. If $N \subseteq M$ and $M = N + \mathfrak{a}.M$, then $M = N$. In particular, if $M \neq 0$, then $M \neq \mathfrak{a}.M$.*

PROOF.– (1) We will show the special case first. Suppose that $M = \mathfrak{a}.M$ with $\mathfrak{a} \subset \mathrm{rad}(\mathbf{R})$. Let $(x_i)_{1 \leq i \leq n}$ be a generating family of M. There exists a family $\left(a_i^j\right)_{1 \leq i,j \leq n}$ of $\mathfrak{a}$ such that, for all $i \in \{1, ..., n\}$, $x_i = \sum_{j=1}^n a_i^j x_j$. Writing A

for the matrix $\left(a_i^j\right)$, Cramer's rule (see [2.31]) implies that $\det(I_n - A)\, x_i = 0$ for all $i \in \{1, ..., n\}$, and there exists $z \in \mathfrak{a}$ such that $\det(I_n - A) = 1 + z$ by the Cayley-Hamilton theorem (see [2.33]). By Lemma 2.39, $1 + z$ is invertible, so $x_i = 0$ for all $i \in \{1, ..., n\}$ and $M = 0$. (2) If $N \subseteq M$ and $M = N + \mathfrak{a}.M$, we have that $M/N = \mathfrak{a}.M/N$ which reduces the claim to the previous result. ■

2.3.6. *Nilradical. Radical ideal*

LEMMA 2.42.– *Let* $\mathbf{R}$ *be a commutative ring. The set* $\mathfrak{N}(\mathbf{R})$ *of nilpotent elements (the elements* x *for which there exists an integer* $n > 0$ *such that* $x^n = 0$*) is an ideal, and is the intersection of all prime ideals in* $\mathbf{R}$*. This set* $\mathfrak{N}(\mathbf{R})$ *is also the intersection of all* minimal *prime ideals in* $\mathbf{R}$*.*

PROOF.– The set of prime ideals in $\mathbf{R}$ is $\mathrm{Spec}(\mathbf{R})$ (Definition 2.29). If $x \in \mathfrak{N}(\mathbf{R})$, there exists an integer $n > 0$ such that $x^n = 0$, so for all $\mathfrak{p} \in \mathrm{Spec}(\mathbf{R})$, $x^n \in \mathfrak{p}$, and hence $\mathfrak{N}(\mathbf{R}) \subset \bigcap_{\mathfrak{p} \in \mathrm{Spec}(\mathbf{R})} \mathfrak{p}$. If $x \notin \mathfrak{N}(\mathbf{R})$, then $x^n \neq 0, \forall n > 0$, so $0 \notin S$ where $S = \left\{1, x, x^2, ...\right\}$, and by Lemma 2.28 there exists a prime ideal disjoint from S. Hence, $x \notin \bigcap_{\mathfrak{p} \in \mathrm{Spec}(\mathbf{R})} \mathfrak{p}$. Finally, every prime ideal in a commutative ring contains a minimal prime ideal (section 2.3.3(**II**)). ■

DEFINITION 2.43.– *The ideal* $\mathfrak{N}(\mathbf{R})$ *is called the* nilradical *of* $\mathbf{R}$*. The ring* $\mathbf{R}$ *is said to be* reduced *if* $\mathfrak{N}(\mathbf{R}) = (0)$.

If $\mathbf{R}$ is a commutative ring, it follows from Lemmas 2.30 and 2.42 that $\mathfrak{N}(\mathbf{R}) \subseteq \mathrm{rad}(\mathbf{R})$.

DEFINITION 2.44.– *Let* $\mathfrak{a}$ *be an ideal in a commutative ring* $\mathbf{A}$*. Its* radical *is the ideal:*

$$\sqrt{\mathfrak{a}} := \{x \in \mathbf{R} : \exists n \geq 1, x^n \in \mathfrak{a}\}.$$

THEOREM 2.45.– *Let* $\mathbf{R}$ *be a commutative ring and let* $\mathfrak{a}$ *be an ideal in* $\mathbf{R}$*. Then,* $\sqrt{\mathfrak{a}}$ *is the intersection of all the prime ideals containing* $\mathfrak{a}$*. Hence (with the notation of section 2.3.3(**III**)),* $V\left(\sqrt{\mathfrak{a}}\right) = V(\mathfrak{a})$.

PROOF.– By the correspondence theorem (section 2.2.3(**III**)), the canonical epimorphism $\varphi : \mathbf{R} \twoheadrightarrow \mathbf{R}/\mathfrak{a}$ gives a bijection between the ideals of $\mathbf{R}$

containing $\mathfrak{a}$ and the ideals in $\mathbf{R}/\mathfrak{a}$. We have that $\sqrt{\mathfrak{a}} = \varphi^{-1}(\mathfrak{N}(\mathbf{R}/\mathfrak{a}))$ and the prime ideals in $\mathbf{R}/\mathfrak{a}$ are the $\varphi(\mathfrak{p}), \mathfrak{p} \in \mathrm{V}(\mathfrak{a})$. By Lemma 2.42, $\mathfrak{N}(\mathbf{R}/\mathfrak{a}) = \bigcap_{\mathfrak{p}\in\mathrm{V}(\mathfrak{a})} \varphi(\mathfrak{p})$ and therefore $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p}\in\mathrm{V}(\mathfrak{a})} \mathfrak{p}$. ■

Clearly $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$, which leads to the following definition:

DEFINITION 2.46.– *An ideal* $\mathfrak{a}$ *in a commutative ring* $\mathbf{R}$ *is called a* radical ideal *if* $\sqrt{\mathfrak{a}} = \mathfrak{a}$.

In $\mathbb{Z}$, $\sqrt{(n)} = \bigcap_{p|n}(p)$ where the p are distinct prime numbers; for example $\sqrt{(504)} = \sqrt{(2^3 \times 3^2 \times 7)} = (2 \times 3 \times 7) = (42)$. If $p_1, ..., p_k$ are distinct prime numbers and $\mathfrak{a} = \left(\prod_{i=1}^{k} p_i\right)$, then $\mathfrak{a}$ is a radical ideal.

2.3.7. *Local rings*

The proof of the following result is an **exercise:**

LEMMA 2.47.– *Let* $\mathbf{R}$ *be a ring. The following conditions are equivalent:*

i) $\mathbf{R}$ *has a unique maximal left ideal (equal to* $\mathrm{rad}(\mathbf{R})$*);*

ii) $\mathbf{R}$ *has a unique maximal right ideal (equal to* $\mathrm{rad}(\mathbf{R})$*);*

iii) $\mathbf{R}/\mathrm{rad}(\mathbf{R})$ *is a division ring;*

iv) $\complement_{\mathbf{R}}\mathbf{U}(\mathbf{R})$ *is a two-sided ideal in* $\mathbf{R}$*, where* $\mathbf{U}(\mathbf{R})$ *is the set of units of* $\mathbf{R}$*. This ideal is* $\mathrm{rad}(\mathbf{R})$.

DEFINITION 2.48.– *A ring* $\mathbf{R}$ *is said to be* local *if one of the above equivalent conditions is satisfied, and* $\mathbf{R}/\mathrm{rad}(\mathbf{R})$ *is called the* residue class division ring *(in the commutative case, the* residue class field*) of* $\mathbf{R}$*, written as* $\kappa_{\mathbf{R}}$.

Later, in section 2.3.9**(II)**, we will encounter an important class of examples of local rings, namely formal power series rings with coefficients in a field.

2.3.8. *Principal ideal domains and related notions*

(I) GCD DOMAINS. Let $\mathbf{R}$ be an entire ring and suppose that $c \in \mathbf{R}$. The set $\mathbf{L}(\mathbf{R}c, \mathbf{R})$ of principal left ideals containing c is an ordered set with $\mathbf{R}a \leq \mathbf{R}b$ if $\mathbf{R}a \subseteq \mathbf{R}b$; it has a maximal element $\mathbf{R}$. If $\mathbf{L}(\mathbf{R}c, \mathbf{R})$ is a lattice, then

$\mathbf{R}a \wedge \mathbf{R}b = \mathbf{R}a \cap \mathbf{R}b \in \mathbf{L}(\mathbf{R}c, \mathbf{R})$, and $\mathbf{R}a \vee \mathbf{R}b = \mathbf{R}a + \mathbf{R}b$. If so, the lattice $\mathbf{L}(\mathbf{R}c, \mathbf{R})$ is modular (**exercise**). If $\mathbf{L}(\mathbf{R}c, \mathbf{R})$ is a lattice for every $c \in \mathbf{R}$, $\mathbf{R}$ is called a *right GCD domain*. In this case, writing $\mathbf{R}a \wedge \mathbf{R}b = \mathbf{R}m$, m is a left multiple of a and b, and every left multiple of a and b is a left multiple of m, so m is a *least common left multiple* (lclm) of a and b. Furthermore, setting $\mathbf{R}a \vee \mathbf{R}b = \mathbf{R}d$, d is a right divisor of a and b (section 2.1.1**(II)**), and every right divisor of a and b is a right divisor of d, so d is a *greatest common right divisor* (gcrd) of a and b. We can similarly define the notions of *least common right multiple* (lcrm) and *greatest common left divisor* (gcld). These notions generalize the classical notions of the gcd and the lcm of two integers (Example 2.4(2)). An entire ring is called a *right GCD domain* if any two elements $a, b \in \mathbf{R}$ have a gcrd. We can similarly define the notion of *left GCD domain*. A commutative GCD domain is also called a *pseudo-Bézout domain* ([BKI 98], Chap. VII, section 1, Exerc. 21). In the following, whenever $\mathbf{R}$ is commutative, as in Example 2.10, we write $a \wedge b$ and $a \vee b$ respectively for an lcm and a gcd of $a, b \in \mathbf{R}$ if they exist (in which case they are unique up to multiplication by units in $\mathbf{R}$). The proof of the following results is an **exercise*** ([AND 00], section 1.3):

LEMMA 2.49.– *Let* $\mathbf{R}$ *be a* commutative *entire ring.*

1) If $\mathbf{R}$ *is a GCD domain and* $a, b, c \in \mathbf{R}^\times$ *are such that* $a \mid bc$ *and* $a \vee b = 1$, *then* $a \mid c$ *(Euclid-Gauss* lemma*). Every atom in* $\mathbf{R}$ *is prime.*

2) Two elements $a, b \in \mathbf{R}^\times$ *have an lcm* m *if and only if* $(a) \cap (b) = (m)$, *in which case* $(m) = (a \wedge b)$. *This implies that* $((a) + (b))_v := \bigcap \{(x) : (x) \supseteq (a) + (b)\}$ *is a principal ideal* $(d) = (a \vee b)$, *and* $md = uab$ *where* $u \in \mathbf{U}(\mathbf{R})$. *Hence, if* $a, b \in \mathbf{R}^\times$ *have an lcm, then they also have a gcd.*

3) If $\mathbf{R}$ *is a GCD domain, any two elements* $a, b \in \mathbf{R}$ *have an lcm.*

(II) UNIQUE FACTORIZATION DOMAINS. Let $\mathbf{R}$ be a ring. Two *regular* elements $a, b \in \mathbf{R}$ are said to be *similar* (written as $a \simeq b$) if $\mathbf{R}/a\mathbf{R} \cong \mathbf{R}/b\mathbf{R}$. *Similarity* $\simeq$ of two regular elements is clearly an equivalence relation and it will be shown in Corollary 3.25 that it is left/right symmetric. We also say that two left ideals or two right ideals $\mathfrak{a}, \mathfrak{b}$ in $\mathbf{R}$ are *similar*, writing $\mathfrak{a} \simeq \mathfrak{b}$, if $\mathbf{A}/\mathfrak{a} \cong \mathbf{A}/\mathfrak{b}$. An explicit similarity condition for two regular elements is stated in Corollary 3.25. The proof of the following result is an **exercise*** ([COH 85], Sect. 3.2, Prop. 2.1):

LEMMA 2.50.– *Let* $\mathfrak{a}, \mathfrak{a}'$ *be two right ideals in* $\mathbf{R}$*. Then,* $\mathfrak{a} \simeq \mathfrak{a}'$ *if and only if there exists an element* $b \in \mathbf{R}$ *such that 1)* $\mathfrak{a} + b\mathbf{R} = \mathbf{R}$ *and 2)* $\mathfrak{a}' = \{x \in \mathbf{R} : bx \in \mathfrak{a}\}$ *(using shorthand notation,* $\mathfrak{a}' = b^{-1}\mathfrak{a}$*).*

By Lemma 2.21, any two left-associated or right-associated regular elements are similar. Conversely:

LEMMA 2.51.– *Let* $\mathbf{R}$ *be a* commutative *ring and let* a, b *be two regular elements of* $\mathbf{R}$*. If they are similar, they are associated (equivalently, if the principal ideals that they generate are similar, they are equal).*

PROOF.– Let $\psi : \mathbf{R}/\mathbf{R}a \tilde{\to} \mathbf{R}/\mathbf{R}b$. Then $\psi(b + \mathbf{R}a) = 0$, so $b \in \mathbf{R}a$, and hence $\mathbf{R}b \subseteq \mathbf{R}a$. By symmetry, $\mathbf{R}a \subseteq \mathbf{R}b$, so $\mathbf{R}a = \mathbf{R}b$, and a, b are left-associated, and therefore associated, since $\mathbf{R}$ is commutative. ■

Let $\mathbf{R}$ be an *entire* ring and $c \in \mathbf{R}^{\times}$. Consider a *complete factorization* (section 2.1.1**(II)**) $c = a_1....a_r$ corresponding to the decreasing chain of principal right ideals from $\mathbf{R}$ to $c\mathbf{R}$:

$$\mathbf{R} \supseteq a_1\mathbf{R} \supseteq a_1a_2\mathbf{R} \supseteq ... \supseteq a_1a_2...a_r\mathbf{R} = c\mathbf{R}. \qquad [2.18]$$

The mapping $\varphi : \mathbf{R}/a_2\mathbf{R} \to a_1\mathbf{R}/a_1a_2\mathbf{R} : x + a_2\mathbf{R} \mapsto a_1x + a_1a_2\mathbf{R}$ is surjective and $\ker(\varphi) = \{x + a_2\mathbf{R} : a_1x \in a_1a_2\mathbf{R}\} = 0$, since $a_1 \neq 0$ and $\mathbf{R}$ is entire. Hence, $a_1\mathbf{R}/a_1a_2\mathbf{R} \cong \mathbf{R}/a_2\mathbf{R}$ and, as in 2.2.5**(II)**, the chain [2.18] corresponds to the quotients:

$$\mathbf{R}/a_1\mathbf{R}, \quad a_1\mathbf{R}/a_1a_2\mathbf{R} \cong \mathbf{R}/a_2\mathbf{R}, ..., \quad \mathbf{R}/a_r\mathbf{R}.$$

The following definition, which is classically familiar in its commutative version, was established by P.M. Cohn [COH 63] in the non-commutative case: an entire ring $\mathbf{R}$ is said to be a *unique factorization domain* (UFD, for short) if it is *atomic* (in other words, for all $c \in \mathbf{R}^{\times}$, the lattice $\mathbf{L}(\mathbf{R}c, \mathbf{R})$, or equivalently the lattice $\mathbf{L}(c\mathbf{R}, \mathbf{R})$, has *finite length*: see section 2.1.2**(III)**) *and if*, for all $c \in \mathbf{R}^{\times}$, any two complete factorizations

$$c = a_1...a_r = b_1...b_s$$

are isomorphic in the sense that $r = s$ and there exists a permutation $i \mapsto i'$ of $\{1, ..., r\}$ such that $a_i \simeq b_{i'}$, $\forall i \in \{1, ..., r\}$. This condition is satisfied if

the finite-length lattice $\mathbf{L}(\mathbf{R}c, \mathbf{R})$ is *modular*, by Theorem 2.9(3), the Krull-Remak-Schmidt theorem. The length of $\mathbf{L}(\mathbf{R}c, \mathbf{R})$ is the *depth* $\mathfrak{d}(c) = r$ of c (section 2.1.2(**III**)).

THEOREM 2.52.– *Let* $\mathbf{R}$ *be an* atomic entire commutative *ring. Then, the following conditions are equivalent:*

i) $\mathbf{R}$ *is a UFD.*

ii) Every atom is prime (compare with Lemma 2.2).

iii) $\mathbf{R}$ *is a GCD domain.*

PROOF.– (i)⇒(iii): let $a = up_1^{\alpha_1}...p_r^{\alpha_r}$ and $b = vp_1^{\beta_1}...p_r^{\beta_r}$ be complete factorizations such that $a, b \neq 0$, $u, v \in \mathbf{U}(\mathbf{R})$, where the $p_1, ..., p_r$ are pairwise distinct atoms, and suppose that $\alpha_i, \beta_i \geq 0$. Then, as in Example 2.10, $\prod_{i=1}^{r} p_i^{\sup(\alpha_i,\beta_i)}$ and $\prod_{i=1}^{r} p_i^{\inf(\alpha_i,\beta_i)}$ are respectively an lcm and a gcd of a, b. (iii)⇒(ii): by Lemma 2.49(1). (ii)⇒(i): consider two complete factorizations $a = p_1...p_n = uq_1...q_m$, where $u \in \mathbf{U}(\mathbf{R})$. Since p_1 is prime, it divides one of the q_i, namely $q_{\sigma(1)}$, which is prime, so $p_1 = u_1 q_{\sigma(1)}$, where $u_1 \in \mathbf{U}(\mathbf{R})$. We can now simply argue by induction to show that the factorization is unique up to multiplication by a unit of $\mathbf{R}$. ■

DEFINITION 2.53.– *Let* $\mathbf{R}$ *be a commutative UFD. We say that* $P \subset \mathbf{R}$ *is a* representative system of prime elements *for* $\mathbf{R}$ *if every prime element of* $\mathbf{R}$ *is associated with exactly one* $p \in P$.

With this notation, we immediately obtain the result:

THEOREM 2.54.– *(Gauss): Let* $\mathbf{A}$ *be a commutative UFD and* $0 \neq a \in \mathbf{A}$. *Then, there exist a uniquely determined unit* u *and a uniquely determined family* $(n_p(a))_{p\in P}$ *of integers* ≥ 0 *with only finitely many non-zero members such that:*

$$a = u \prod\nolimits_{p\in P} p^{n_p(a)}. \qquad [2.19]$$

(III) BÉZOUT DOMAINS. An entire ring $\mathbf{R}$ is said to be a left Bézout domain (after the mathematician É. Bézout) if every *finitely generated* left ideal in $\mathbf{R}$ is principal. If $\mathbf{R}$ is a left Bézout domain and $a, b \in \mathbf{R}^{\times}$, then $\mathbf{R}a + \mathbf{R}b$ is a

principal ideal domain $\mathbf{R}d$ and d is a gcrd of a and b. A left Bézout domain is therefore a right GCD domain. In a left Bézout domain $\mathbf{R}$, an element d is a gcrd of a, b if and only if there exist x, y such that $xa + yb = d$ (Bézout's identity).

EXAMPLE 2.55.– *An entire function f in the complex plane is defined as the sum of a power series $f(z) = \sum_{n=0}^{+\infty} a_n z^n$, where (a_n) is a sequence of complex numbers such that $\limsup_{n\to\infty} |a_n|^{1/n} = 0$. The power series converges in the full complex plane $\mathbb{C}$. The ring $\mathcal{O}(\mathbb{C})$ of entire functions is a Bézout domain but is not a unique factorization domain. Indeed, let $f_1, f_2 \in \mathcal{O}(\mathbb{C})$. By the Weierstrass factorization theorem ([RUD 87], p. 306, Thm. 15.10), there exist a sequence $(a_j)_{j\geq 0}$ of isolated points, two functions $g_1, g_2 \in \mathcal{O}(\mathbb{C})$ and integers $n_{ij} \geq 0$ $(1 \leq i \leq 2, j \geq 0)$ such that:*

$$f_i(z) = \prod_{j=0}^{+\infty} (z - a_j)^{n_{ij}} e^{g_i(z)},$$

where $n_{ij} > 0$ if and only if a_j is a zero of order n_{ij} of f_i. The units of $\mathcal{O}(\mathbb{C})$ are the entire functions without zeros. Let $n_j = \min\{n_{ij} : 1 \leq i \leq 2\}$. Then, $f(z) = \prod_{j=0}^{+\infty} (z - a_j)^{n_j}$ is a gcd of f_1, f_2, so $\mathcal{O}(\mathbb{C})$ is a GCD domain. To show that the ring $\mathcal{O}(\mathbb{C})$ is a Bézout domain, we now simply need to prove that if f_1, f_2 do not have a zero in common, then $(f_1, f_2) = (1)$. This result was established by Wedderburn in 1915 ([REM 98], Lem. 6.3.2). The prime elements of $\mathcal{O}(\mathbb{C})$ are the entire functions of the form $u(z)(z - a)$ $(a \in \mathbb{C})$, where u is a unit of $\mathcal{O}(\mathbb{C})$. An entire function with infinitely many zeros, for example $z \mapsto \sin(\pi z)$, cannot therefore be written as a (finite) product of prime factors.

(IV) PRINCIPAL IDEAL DOMAINS. A ring $\mathbf{R}$ is said to be a *principal left ideal ring* if every left ideal in $\mathbf{R}$ is principal. A *principal left ideal domain* is an entire principal left ideal ring. We can similarly define the notions of principal right ideal rings and domains.

THEOREM 2.56.– *Let $\mathbf{R} \neq \{0\}$ be a ring. The following conditions are equivalent:*

i) $\mathbf{R}$ *is a principal right ideal domain;*

ii) $\mathbf{R}$ *is a right Bézout atomic domain;*

iii) $\mathbf{R}$ *is a right Bézout UFD;*

iv) $\mathbf{R}$ *is a right Noetherian ring and a right Bézout domain.*

PROOF.– (i)⇔(ii): any principal right ideal domain is clearly right Bézout. Let a be a non-zero element of $\mathbf{R}$. If $a \notin \mathbf{U}(\mathbf{R})$, $a\mathbf{R}$ is a proper right ideal in $\mathbf{R}$ and so, by Krull's theorem (Theorem 2.27(2)), there exists a maximal right ideal $\mathfrak{m}_1$ that contains it. This right ideal $\mathfrak{m}_1$ is principal, so is of the form $a_1\mathbf{R}$ where a_1 is an atom. Since $a\mathbf{R} \subseteq a_1\mathbf{R}$, there exists $c_1 \neq 0$ such that $a = a_1c_1$. If $c_1 \notin \mathbf{U}(\mathbf{R})$, we have that $a\mathbf{R} \subsetneq a_1\mathbf{R}$ and the same reasoning shows that there exist an atom a_2 and $c_2 \neq 0$ such that $c_1 = a_2c_2$, from which it follows that $a = a_1a_2c_2$ and $a\mathbf{R} \subsetneq a_1a_2\mathbf{R}$. We thus obtain a strictly ascending sequence of right ideals:

$$a\mathbf{R} \subsetneq a_1\mathbf{R} \subsetneq a_1a_2\mathbf{R}... \subsetneq a_1a_2...a_s\mathbf{R} \subsetneq ...$$

Since the right ideal $a\mathbf{R}$ is principal, it is finitely generated and there exists an integer $r > 0$ such that the sequence terminates at $s = r$. Therefore, $\mathbf{R}$ is atomic. We have therefore shown that (i)⇒(ii) and the converse may be shown in the same way, except arguing by contradiction.

((i),(ii))⇒(iii): the set $\mathbf{L}(a\mathbf{R}, \mathbf{R})$ is the set of principal right ideals containing a. If the ring $\mathbf{R}$ is a principal right ideal domain, $\mathbf{L}(a\mathbf{R}, \mathbf{R})$ is the set of all right ideals containing a and is therefore a modular lattice. By (ii), it has finite length, so $\mathbf{R}$ is a UFD. (i)⇔(iv): clear. ■

THEOREM 2.57.– *Let $\mathbf{R}$ be a principal ideal domain and let $p \neq 0$ be an invariant element that is not a unit. Then, p is prime (section 2.1.1(**II**)) if and only if the ideal (p) is a maximal right ideal and a maximal left ideal.*

PROOF.– If (p) is both a maximal left ideal and a maximal right ideal, then (p) is completely prime by Theorem 2.38(4). Conversely, if $p \neq 0$ is an invariant element that is not a unit, the ideal (p) is completely prime by Lemma 2.31. We will show by contradiction that (p) is a maximal left ideal. If not, there exists a left ideal $\mathfrak{a} \neq \mathbf{R}$ such that $(p) \subsetneq \mathfrak{a}$. Then, $\mathfrak{a}$ is generated by an invariant element a by Lemma 2.21(ii), so $(p) \subsetneq (a)$. Therefore, there exists an element b that is not a unit such that $p = ab$. Then $a, b \notin (p)$ and $ab \in (p)$, so (p) is not completely prime: contradiction. ■

(V) EUCLIDEAN DOMAINS. Let $\mathbf{R}$ be an entire ring. A function $\theta : \mathbf{R} \to \mathbb{N} \cup \{-\infty\}$ (*see standard notation*) is called a *left Euclidean function* if

(**E1**) $\theta(0) = -\infty$;

(**E2**) $\forall a, b \in \mathbf{R}^{\times}, \theta(ab) \geq \theta(a) > -\infty$;

(**E3**) For all $a, b \in \mathbf{R}$ such that $b \neq 0$, there exist $q, r \in \mathbf{R}$ such that:

$$a = qb + r, \quad \theta(r) < \theta(b). \qquad [2.20]$$

The last of these conditions is known as the *right Euclidean division algorithm* (which performs the *right* Euclidean division of a by b). An entire ring $\mathbf{R}$ on which a left Euclidean function is defined is called a *left Euclidean domain*. We can similarly define the left Euclidean division algorithm (changing qb to bq in [2.20]), and thus the notions of right Euclidean domain, and Euclidean domain (= a left Euclidean domain that is also a right Euclidean domain).

A *strictly* left Euclidean function is a function $\theta : \mathbf{R} \to \mathbb{N} \cup \{-\infty\}$ that satisfies conditions (**E1**), (**E2**) as well as the following condition, which is stronger than (**E2**):

(**E2'**): $\forall a, b \in \mathbf{R}^{\times}, \theta(a-b) \leq \max\{\theta(a), \theta(b)\}$ and $\theta(ab) = \theta(a) + \theta(b)$.

The proof of the following result is an **exercise*** ([COH 85], Sect. 2.1, Prop. 1.3):

LEMMA 2.58.–

i) In a left Euclidean domain $\mathbf{R}$, $\theta(b) \geq \theta(1)$ *if* $b \neq 0$ *and* $\theta(b) = \theta(1)$ *if and only if* $b \in \mathbf{U}(\mathbf{R})$.

*ii) The condition (**E3**) is equivalent to the condition (**E3'**) below:*

*(**E3'**) For all* $a, b \in \mathbf{R}$ *such that* $b \neq 0$ *and* $\theta(a) \geq \theta(b)$, *there exists* $c \in \mathbf{R}$ *such that* $\theta(a - cb) < \theta(a)$.

iii) The remainder r *of Euclidean division [2.20] is unique for all* $a, b \in \mathbf{R}$ *such that* $b \neq 0$, *if and only if the function* θ *is* strictly *Euclidean, in which case the quotient* q *is also unique.*

For example, $\mathbb{Z}$ is a Euclidean domain with $\theta(a) = |a|$ if $a \neq 0, \theta(0) = -\infty$. This Euclidean function θ is not strict and $9 = 4 \times 2 + 1, 9 = 5 \times 2 - 1$ are two Euclidean divisions of 9 by 2.

THEOREM 2.59.– *Every left Euclidean domain is a principal left ideal domain.*

PROOF.– Let $\mathfrak{a} \neq (0)$ be a left ideal in a ring $\mathbf{R}$ equipped with the left Euclidean function θ. Let $b \in \mathfrak{a}$ be an element such that $\theta(b)$ is minimal in the set $\{\theta(x) : x \in \mathfrak{a}, \theta(x) > -\infty\}$. Let $a \in \mathfrak{a}$ and let $a = qb + r$ be its right Euclidean division by b. We have that $\theta(r) < \theta(b)$ and $r = a - qb \in \mathfrak{a}$. Hence, $a = qb$ and $\mathfrak{a} = \mathbf{R}b$. ■

2.3.9. *Polynomial rings and formal power series rings*

(I) POLYNOMIAL RINGS. Given a commutative ring $\mathbf{K}$, consider the usual ring $\mathbf{K}[X]$ of polynomials in a single indeterminate X with coefficients in $\mathbf{K}$. Each element f in $\mathbf{K}[X]$ is of the form $f(X) = a_0X^n + a_1X^{n-1} + ...a_n$, $a_i \in \mathbf{K}$, $a_0 \neq 0$ if $f \neq 0$, in which case $n = d^\circ(f)$. The following is called Gauss's lemma [AND 00], ([LAN 99], Chap. IV, Thm. 2.3)[7]:

LEMMA 2.60.– *(Gauss) If* $\mathbf{K}$ *is a GCD domain (resp. a UFD), then the ring* $\mathbf{K}[X]$ *is a GCD domain (resp. a UFD).*

If $\mathbf{K}$ is a field, $\mathbf{K}[X]$ is a Euclidean domain with $\theta(f) = d^\circ(f)$ if $f \in \mathbf{K}[X]^\times$ and $\theta(0) = -\infty$. This Euclidean function θ is strict (**exercise**). Consequently, $\mathbf{K}[X]$ is a principal ideal domain (for a generalization, see section 3.1.11).

The ring $\mathbf{K}[X_1, ..., X_n]$ of polynomials in n indeterminates $X_1, ..., X_n$ may be defined inductively as $\mathbf{K}[X_1, ..., X_n] = \mathbf{K}[X_1, ..., X_{n-1}][X_n]$ for each integer $n \geq 2$. If I is an arbitrary set, as above, we define the polynomial ring $\mathbf{K}\left[(X_i)_{i\in J}\right]$, $J \in \mathfrak{P}_f(I)$ (where $\mathfrak{P}_f(I)$ is the set of finite subsets of I). If $K, J \in \mathfrak{P}_f(I)$ and $K \supset J$, there is a canonical injection $\varphi_K^J : \mathbf{K}\left[(X_i)_{i\in J}\right] \hookrightarrow \mathbf{K}\left[(X_i)_{i\in K}\right]$, which determines a direct system $\left\{\mathbf{K}\left[(X_i)_{i\in J}\right], \varphi_K^J; \mathfrak{P}_f(I)\right\}$. The inductive limit of this direct system is written as $\mathbf{K}\left[(X_i)_{i\in I}\right]$. One immediate consequence is that if $\mathbf{K}$ is an entire ring, then $\mathbf{K}[X]$ is an entire ring, and so by induction $\mathbf{K}[X_1, ..., X_n]$ is an entire ring, and by transfinite induction (Theorem 1.7) $\mathbf{K}\left[(X_i)_{i\in I}\right]$ is an entire ring. If $\mathbf{K}$ is a GCD domain (resp. a UFD), it follows from Gauss's lemma (by induction) that the same is true for $\mathbf{K}[X_1, ..., X_n]$. In particular, if $\mathbf{K}$ is a field, it is a UFD, since the only ideals are (0) and $\mathbf{K}$, and so $\mathbf{K}[X_1, ..., X_n]$ is a UFD. By transfinite induction, it can be shown that if $\mathbf{K}$ is a UFD, then $\mathbf{K}\left[(X_i)_{i\in I}\right]$ is also a UFD ([DOU 05], Thm. 3.7.9).

7 See the WIKIPEDIA article *Gauss's lemma (polynomial)*.

The elements of $\mathbf{K}[X_1, ..., X_n]$ are of the form:

$$a = \sum_{0 \leq i_1, ..., i_n < \infty} a_{i_1, ..., i_n} X_1^{i_1} ... X_n^{i_n}. \qquad [2.21]$$

It is useful to introduce the *multi-indices* $i = (i_1, ..., i_n) \in \mathbb{N}^n$, writing $|i| := \sum_{k=1}^n i_k$, $X^i = X_1^{i_1} ... X_n^{i_n}$. The terms $a_i X^i$ such that $|i| = p$ in [2.21] are called the *terms of degree* p and the polynomial $a_p = \sum_{|i|=p} a_i X^i$ is called the *homogeneous component* of degree p of the polynomial a. The component of degree 0 is the constant term. The *total degree* of a is $-\infty$ if $a = 0$, and is equal to the largest integer p for which the homogeneous part of degree p is non-zero otherwise.

(II) FORMAL POWER SERIES RINGS. Let $\mathbf{K}[[X]]$ be the abelian group of *formal power series* $a = \sum_{i=0}^{+\infty} a_i X^i$ in a single indeterminate X with coefficients in the commutative ring $\mathbf{K}$. By definition, a is the family $(a_i)_{i \in \mathbb{N}}$. If $b = \sum_{i=0}^{+\infty} b_i X^i$, we define the product $ab = \sum_{k=0}^{\infty} c_k X^k$ by the relation:

$$c_k = \sum_{i+j=k} a_i b_j. \qquad [2.22]$$

This equips $\mathbf{K}[[X]]$ with a ring structure, and $\mathbf{K}[X]$ is the subring of $\mathbf{K}[[X]]$ consisting of the set of formal power series with finitely many non-zero coefficients. If $\mathbf{K}$ is a field, the formal power series ring $\mathbf{K}[[X]]$ is a principal ideal domain since its only proper ideals are (0) and the $(X^n), n \geq 1$.

We define the formal power series ring $\mathbf{K}[[X_1, ..., X_n]]$ in n indeterminates $X_1, ..., X_n$ by induction as $\mathbf{K}[[X_1, ..., X_n]] = \mathbf{K}[[X_1, ..., X_{n-1}]][[X_n]]$ for each integer $n \geq 2$. If I is an arbitrary set, we define $\mathbf{K}\left[\left[(X_i)_{i \in I}\right]\right]$ as we did for polynomials. This ring is entire if $\mathbf{K}$ is entire.

Each formal power series is of the form:

$$a = \sum_{0 \leq i_1, ..., i_n} a_{i_1, ..., i_n} X_1^{i_1} ... X_n^{i_n}, \qquad [2.23]$$

similar to [2.21] except with unbounded indices. As we did for the polynomials, we define multi-indices, the terms of total degree p, and the homogeneous component a_p of degree p of the formal power series a. With

these conventions, if $a, b \in \mathbf{K}[[X_1, ..., X_n]]$ and $c = ab$, the equality [2.22] once again holds, where a_i, b_j, c_k are the homogeneous components of a, b, c of degree i, j, k, respectively.

The *order* of a non-zero formal power series $a \in \mathbf{K}\left[\left[(X_i)_{i\in I}\right]\right]$ is the smallest integer p such that $a_p \neq 0$ (where a_p is the homogeneous component of degree p) and this order is written as $\omega(a)$. In $\overline{\mathbb{Z}}$ (see standard notation), we set $\omega(0) = +\infty$. We have that (**exercise**) $\omega(a+b) \geq \min\{\omega(a), \omega(b)\}$ with equality if $\omega(a) \neq \omega(b)$, and $\omega(ab) \geq \omega(a) + \omega(b)$.

LEMMA 2.61.– *An element is invertible in* $\mathbf{K}\left[\left[(X)_{i\in I}\right]\right]$ *if and only if its constant term is invertible in* $\mathbf{K}$.

PROOF.– 1) First, consider the case with a single indeterminate. The polynomial $1 - X$ is invertible in $\mathbf{K}[[X]]$ since $(1-X)^{-1} = \sum_{i=0}^{\infty} X^i$. Indeed, $\left(\sum_{i=0}^{\infty} X^i\right)(1-X) = \sum_{i=0}^{\infty} X^i - \sum_{i=0}^{\infty} X^{i+1} = 1$. 2) If $a, b \in \mathbf{K}\left[\left[(X_i)_{i\in I}\right]\right]$ satisfy $ab = 1$, their constant terms a_0, b_0 satisfy $a_0 b_0 = 1$, and are therefore invertible. Conversely, if $a \in \mathbf{K}\left[\left[(X_i)_{i\in I}\right]\right]$ is a formal power series whose constant term a_0 is invertible, then there exists a power series $c \in \mathbf{K}\left[\left[(X_i)_{i\in I}\right]\right]$ such that $a - a_0 = -a_0 c \Leftrightarrow a = a_0(1-c)$ and c has a non-zero constant term. As in (1), we then have that $(1-c)^{-1}\sum_{i=0}^{\infty} c^i = 1$, so $1 - c$ is invertible, and a is too. ■

If $\mathbf{K}$ is a *field*, the ideal $\mathfrak{m} = \left((X_i)_{i\in I}\right)$ generated by the family of indeterminates $(X_i)_{i\in I}$ is the only maximal ideal of $\mathbf{S} = \mathbf{K}\left[\left[(X_i)_{i\in I}\right]\right]$ and is the radical of this ring. We then have that $\mathbf{S}/\mathfrak{m} \cong \mathbf{K}$, $\mathbf{U}(\mathbf{S}) = \mathbf{K}^{\times}$ and $\complement_{\mathbf{S}}\mathbf{K}^{\times} = \mathfrak{m}$. More generally:

LEMMA 2.62.– *If* $\mathfrak{o}$ *is a commutative local ring and* $\mathfrak{m}$ *is its radical, the ring* $\mathbf{T} = \mathfrak{o}\left[\left[(X_i)_{i\in I}\right]\right]$ *is local and has the radical* $\left(\mathfrak{m}, \left((X_i)_{i\in I}\right)\right)$.

PROOF.– Lemma 2.61 shows that the non-invertible elements of $\mathbf{T}$ are precisely the formal power series with non-invertible constant terms in $\mathfrak{o}$, which therefore belong to $\mathfrak{m}$. ■

If $\mathbf{K}$ is a field, the local ring $\mathbf{K}[[X_1, ..., X_n]]$ (section 2.3.7) is a UFD ([LAN 99], Chap. IV, Thm. 9.3) and by transfinite induction it follows that $\mathbf{K}\left[\left[(X_i)_{i\in I}\right]\right]$ is a UFD. (There is no equivalent of Gauss's theorem for power series, since there exist commutative UFDs $\mathbf{K}$ for which $\mathbf{K}[[X]]$ *is not*

a UFD ([LAN 99], p. 209), but the reasoning by transfinite induction given above is based on a result given in ([BKI 98], Chap. VII, section 3, Exerc. 2).)

2.3.10. *General notions relating to algebras*

(I) Let $\mathbf{K}$ be a *commutative* ring. A $\mathbf{K}$-module $\mathbf{A}$ is called a $\mathbf{K}$-algebra if there exists a $\mathbf{K}$-bilinear mapping $(x, y) \mapsto x.y$ from $\mathbf{A} \times \mathbf{A}$ to $\mathbf{A}$. This $\mathbf{K}$-algebra is said to be *associative* if the binary operation $(x, y) \mapsto x.y$ is associative, and *unitary* if there exists an unit element in $\mathbf{A}$ for this operation. If $\mathbf{A}$ is associative and unitary, then it is a ring. Every ring is a $\mathbb{Z}$-algebra. The algebra $\mathbf{A}$ is said to be commutative if $x.y = y.x$, and anticommutative if $x.y = -y.x, \forall x, y \in \mathbf{A}$. Given a $\mathbf{K}$-algebra $\mathbf{A}$, we can define the notions of *left ideal*, *right ideal* and *two-sided ideal* in $\mathbf{A}$, and *left* and *right* $\mathbf{A}$*-modules* as we did when $\mathbf{A}$ is a ring (section 2.3.1(**II**)).

The *morphisms* of $\mathbf{K}$-algebras are the morphisms $f : \mathbf{A} \to \mathbf{B}$ of $\mathbf{K}$-modules (where $\mathbf{A}, \mathbf{B}$ are $\mathbf{K}$-algebras) such that $f(xy) = f(x) f(y), \forall x, y \in \mathbf{A}$. We thus define the category $\mathbf{K}$-Alg of $\mathbf{K}$-algebras. A *morphism of unitary* $\mathbf{K}$*-algebras* is a morphism of $\mathbf{K}$-algebras such that $f(1) = 1$.

(II) The properties of rings can be extended to algebras. In particular, if $f : \mathbf{A} \to \mathbf{B}$ is a morphism of $\mathbf{K}$-algebras, $\mathfrak{a} = \ker(f) = f^{-1}(0)$ is a two-sided ideal, and f has the canonical decomposition:

$$\mathbf{A} \overset{\varphi}{\to} \mathbf{A}/\mathfrak{a} \overset{\bar{f}}{\to} f(\mathbf{A}) \overset{\iota}{\to} \mathbf{B},$$

where φ and ι are respectively canonical injection and surjection and $\bar{f}$ is an isomorphism. A $\mathbf{K}$-algebra $\mathbf{A}$ is said to be *generated* over $\mathbf{K}$ by a family $(x_i)_{i \in I}$ if $\mathbf{A}$ is the smallest $\mathbf{K}$-algebra that contains the x_i (we say that $(x_i)_{i \in I}$ is a generating family of the $\mathbf{K}$-algebra $\mathbf{A}$). This algebra $\mathbf{A}$ is said to be *finitely generated* if it is generated over $\mathbf{K}$ by finitely many elements $x_1, ..., x_n$.

(III) We write $\mathbf{K}$-Alga for the category of associative and unitary $\mathbf{K}$-algebras (whose morphisms are the morphisms of unitary algebras). Consider one such algebra $\mathbf{A}$, and suppose that it is a *free* $\mathbf{K}$-module (section 2.3.1(**II**)) with the basis $(x_i)_{i \in I}$. Suppose also that $\mathbf{K} \subset \mathfrak{Z}(\mathbf{A})$ where $\mathfrak{Z}(\mathbf{A})$ is the center of $\mathbf{A}$, i.e. the subset of $\mathbf{A}$ consisting of the elements that commute with every element of

$\mathbf{A}$. The *structure constants* of $\mathbf{A}$ with respect to the basis $x = (x_i)_{i\in I}$ are the uniquely determined elements $c_{ij}^k \in \mathbf{K}$ $(i, j, k \in I)$ such that:

$$x_i.x_j = \sum_{k\in I} c_{ij}^k x_k, \qquad [2.24]$$

where, for all $i, j \in I$, all except finitely many of the c_{ij}^k are zero. Arbitrary elements of $\mathbf{A}$ may be obtained from a polynomial $f \in \mathbf{K}\left[(X_i)_{i\in I}\right]$ (section 2.3.9(**I**)) by substituting x_i for the indeterminate X_i $(i \in I)$, and writing $f(x)$ $\left(x = (x_i)_{i\in I}\right)$ for the element of $\mathbf{A}$ thus obtained. The ring structure of $\mathbf{A}$ is entirely determined by the ring structure of $\mathbf{K}\left[(X_i)_{i\in I}\right]$ and the *multiplication table* [2.24]. We therefore write $\mathbf{A} = \mathbf{K}\left[(x_i)_{i\in I}\right]$.

For example, the n^{th} Weyl *algebra* over a field $\mathbf{K}$ is the $\mathbf{K}$-algebra $A_n(\mathbf{K}) := \mathbf{K}[x_1, ..., x_n, y_1, ..., y_n]$ where $y_i x_j - x_j y_i = \delta_i^j$ and $x_i x_j - x_j x_i = y_i y_j - y_j y_i = 0$.

Similarly, if $(x_i)_{i\in I}$ is a (not necessarily free) family of elements of an associative $\mathbf{K}$-algebra $\mathbf{B}$ with the property that these elements are pairwise permutable (i.e. $x_i.x_j = x_j.x_i, \forall i, j \in I$), it can be substituted for the family of indeterminates $(X_i)_{i\in I}$ and generates the algebra $\mathbf{K}\left[(x_i)_{i\in I}\right] \subseteq \mathbf{B}$.

(IV) We write $\mathbf{K}$-Algc for the full subcategory of $\mathbf{K}$-Alga whose objects are the associative, unitary and commutative $\mathbf{K}$-algebras. Let $\mathbf{A}$ be one such algebra, and let $(x_i)_{i\in I}$ be a family of elements of $\mathbf{A}$. Consider the morphism of algebras:

$$f : \mathbf{K}\left[(X_i)_{i\in I}\right] \to \mathbf{A} : X_i \mapsto x_i. \qquad [2.25]$$

If the family $(x_i)_{i\in I}$ is a generating family, this morphism is surjective, so $\bar{f} : \mathbf{K}\left[(X_i)_{i\in I}\right] \to \mathbf{A} : \bar{X}_i \mapsto x_i$ is an isomorphism of $\mathbf{K}$-Algc, where $\bar{X}_i$ is the canonical image of X_i in $\mathbf{K}\left[(X_i)_{i\in I}\right]/\mathfrak{a}$ with $\mathfrak{a} = f^{-1}(\{0\})$, and hence

$$\boxed{\mathbf{A} \cong \mathbf{K}\left[(X_i)_{i\in I}\right]/\mathfrak{a}} \qquad [2.26]$$

(universal property of polynomial rings with coefficients in $\mathbf{K}$). In particular, a finitely generated associative and commutative $\mathbf{K}$-algebra is isomorphic to a

$\mathbf{K}$-algebra of the form $\mathbf{K}[X_1, ..., X_n]/\mathfrak{a}$, where $\mathfrak{a}$ is an ideal in $\mathbf{K}[X_1, ..., X_n]$ and $\bar{X}_i$ is the canonical image of X_i. The family $(x_i)_{i\in I}$ is said to be *algebraically free* over $\mathbf{K}$, and the elements x_i $(i \in I)$ are said to be *algebraically independent* over $\mathbf{K}$, if the morphism [2.25] is injective. If $\mathbf{K}$ is a field and $\mathbf{A}$ is a $\mathbf{K}$-algebra, we say, as in section 2.3.5**(II)**, that an element $x \in \mathbf{A}$ is *algebraic* over $\mathbf{K}$ if there exists a polynomial $f \in \mathbf{K}[X]^{\times}$ such that $f(x) = 0$; the definitions of the *minimal polynomial* and the *degree* of x established in that section also apply here.

2.3.11. *Matrix algebras and determinants*

(I) Let $\mathbf{R}$ be a commutative ring. The ring $\mathfrak{M}_n(\mathbf{R})$ of square matrices of order n (i.e. of dimension $n \times n$) with elements in $\mathbf{R}$ is an associative $\mathbf{R}$-algebra. The *determinant* $\det(A)$ of a matrix $A = \left(a_i^j\right) \in \mathfrak{M}_n(\mathbf{R})$ is defined and calculated as in the classical case when $\mathbf{R}$ is a field[8]. We write $\mathrm{GL}_n(\mathbf{R})$ for the *general linear group* of degree n over $\mathbf{R}$, namely the submonoid of invertible matrices in the multiplicative monoid $\mathfrak{M}_n(\mathbf{R})$ (this notation is also used if $\mathbf{R}$ is not commutative).

DEFINITION 2.63.– *The mapping* $\det : \mathfrak{M}_n(\mathbf{R}) \to \mathbf{R} : A \mapsto \det(A)$ *is the unique alternating* n*-linear form on the* columns *of* A *such that* $\det(I_n) = 1$*, where* I_n *is the identity matrix.*

It can be shown that $\det$ is also the unique alternating n-linear form on the *rows* of A such that $\det(I_n) = 1$. A *minor* of order p of a matrix $B \in \mathbf{R}^{m\times n}$, with $p \leq \min(m, n)$, is the determinant of one of the submatrices $M \in \mathfrak{M}_p(\mathbf{R})$ obtained by deleting some of the rows and columns of B. The *rank* of B is the highest order of the non-zero minors of B. A *principal minor* of $A \in \mathfrak{M}_n(\mathbf{R})$ is a minor obtained by deleting rows and columns with the same indices.

(II) CALCULATING DETERMINANTS. The determinant of A can be calculated from the determinants of its submatrices using the Laplace *expansion* ([BKI 12], Chap. III, section 8.6, (21)). The most useful special case in practice is to expand along a row or a column. Write m_i^j for the minor of order $n-1$ obtained by deleting the i-th row and the j-th column. The

8 See the Wikipedia articles *Determinant*, *Multilinear map* and *Multilinear form*.

cofactor of index (i,j) is $\alpha_i^j := (-1)^{i+j} m_i^j$. We have that:

$$\det(A) = \sum_{i=1}^{n} a_i^j \alpha_i^j = \sum_{j=1}^{n} a_i^j \alpha_i^j.$$

The middle term is the expansion of $\det(A)$ along the j-th column, and the last term is the expansion along the i-th row. The following conditions are equivalent:

a) the rows of A are $\mathbf{R}$-linearly independent;

b) the columns of A are $\mathbf{R}$-linearly independent;

c) $\det(A)$ is a regular element of $\mathbf{R}$.

Elementary operations. We define the *elementary operations* on the *rows* l_i of a matrix $A \in \mathbf{R}^{q\times k}$, where $\mathbf{R}$ is a *not necessarily commutative* ring, as follows:

i) replacing a row l_i with $l_i + \lambda l_j$ $(i \neq j, \lambda \in \mathbf{R})$; this is equivalent to left-multiplying R by the matrix $B_{ij}(\lambda) = I_q + \lambda E_{ij}$, where $E_{ij} \in \mathfrak{M}_q(\mathbf{R})$ is the matrix of dimension $q \times q$ with 1 at indices i, j and zeros everywhere else.

ii) replacing a row l_i with ul_i, where $u \in \mathbf{U}(\mathbf{R})$; this is equivalent to left-multiplying R by $\Delta_i(u) = \operatorname{diag}(1, ..., 1, u, 1, ..., 1)$, where u is the i-th entry.

iii) exchanging l_i and l_j $(i \neq j)$; this is equivalent to left-multiplying R by a permutation matrix $P_{ij} \in \mathfrak{M}_q(\mathbf{A})$.

The matrices $B_{ij}(\lambda), \Delta_i(u), P_{ij}$ are said to be *elementary*.

We similarly define three elementary operations (i'), (ii'), (iii') on the *columns* c_i:

i') replacing a column c_i with $c_i + c_j\lambda$ $(i \neq j, \lambda \in \mathbf{R})$;

ii') replacing a column c_i with $c_i u$ where $u \in \mathbf{U}(\mathbf{R})$;

iii') exchanging c_i and c_j $(i \neq j)$.

It is immediately clear that $B_{ij}(\lambda) B_{ij}(\mu) = B_{ij}(\lambda + \mu), \forall \lambda, \mu \in \mathbf{R}$, so the matrices $B_{ij}(\lambda)$ form a subgroup $\mathrm{E}_q(\mathbf{R})$ of $\mathrm{GL}_q(\mathbf{R})$. Let $\mathrm{D}_q(\mathbf{R})$ be the

subset of $\mathfrak{M}_q(\mathbf{R})$ consisting of all matrices $\Delta_q(u)$, $u \in \mathbf{U}(\mathbf{R})$. We have that $\mathrm{D}_q(\mathbf{R}) \cong \mathbf{U}(\mathbf{R})$, so $\mathrm{D}_q(\mathbf{R})$ is a subgroup of $\mathrm{GL}_q(\mathbf{R})$.

(III) The following result may be shown by induction analogously to Theorem 2.65(a); in the case where $\mathbf{K}$ is a *field*, it is a classical result (the proof is the same).

THEOREM-DEFINITION 2.64.– *Let $X \in \mathbf{K}^{q\times k}$, where $\mathbf{K}$ is a division ring. There exist $P \in \mathrm{E}_q(\mathbf{K})$, $Q \in \mathrm{E}_k(\mathbf{K})$ such that:*

$$PXQ = \mathrm{diag}(1, ..., 1, \delta_r, 0, ..., 0),$$

where the right-hand side is a matrix (η_{ij}) whose terms are all zero except η_{ii} for $1 \leq i \leq r$, which have the values $\eta_{ii} = 1$ $(1 \leq i < r)$ and $\eta_{rr} = \delta_r \neq 0$. The integer $r \geq 0$ depends solely on the matrix X; it is called the rank *of X and is written as* $\mathrm{rk}(X)$; *we have that* $\mathrm{rk}(X) = 0$ *if and only if $X = 0$ (see Remark 3.39).*

THEOREM 2.65.– *Let $\mathbf{K}$ be a field. The following results hold:*

a) $\mathrm{GL}_n(\mathbf{K}) = \mathrm{E}_n(\mathbf{K})\,\mathrm{D}_n(\mathbf{K}) = \mathrm{D}_n(\mathbf{K})\,\mathrm{E}_n(\mathbf{K})$*;*

b) $\mathrm{E}_n(\mathbf{K}) \lhd \mathrm{GL}_n(\mathbf{K})$*;*

c) $\mathrm{GL}_n(\mathbf{K})/\mathrm{E}_n(\mathbf{K})$ *is abelian;*

d) Except when $n = 2$ and $\mathbf{K} = \mathbb{Z}/2\mathbb{Z}$, $\mathrm{E}_n(\mathbf{K}) = \mathrm{GL}_n(\mathbf{K})'$ (the derived subgroup of $\mathrm{GL}_n(\mathbf{K})$*), and the abelianization of* $\mathrm{GL}_n(\mathbf{K})$ *(section 2.2.6) is given by* $\mathrm{GL}_n(\mathbf{K})^{ab} = \mathrm{GL}_n(\mathbf{K})/\mathrm{E}_n(\mathbf{K}) \cong \mathrm{D}_n(\mathbf{K})^{ab} \cong \mathbf{K}^{ab}$.

PROOF.–

a) In everything that follows, we write equally a_{ij} for a_i^j. Let $Q_{ij} = B_{ij}(1)\,B_{ji}(-1)\,B_{ij}(1) \in \mathrm{E}_n(\mathbf{K})$ $(i \neq j)$. If $A \in \mathbf{K}^{n\times m}$, the matrix $Q_{ij}A$ is obtained by replacing the j-th row of X by the i-th row, and the i-th row by the j-th row with opposite sign. Let $A \in \mathrm{GL}_n(\mathbf{K})$; at least one element in the first column is non-zero, and by left-multiplying A if necessary by a matrix Q_{ij} we can assume that $a_{21} \neq 0$. Now, by left-multiplying by a suitable matrix $B_{21}(\lambda)$, we obtain a matrix (b_{ij}) where $b_{11} = 1$. Applying other type (i) elementary operations, we obtain a matrix (c_{ij}) whose elements are all zero in the first column except at indices $(1, 1)$; this first column is therefore $\mathrm{diag}(1)$. Proceeding similarly for the second column if $n > 2$, we reduce to the case of a

matrix whose first two columns are diag $(1,1)$. Finally, there exist $P \in \mathrm{E}_n(\mathbf{K})$ and $\Delta_n(u) \in \mathrm{D}_n(\mathbf{K})$ such that $A = P\Delta_n(u)$. Repeating this procedure for the rows, we see that there exist $P' \in \mathrm{E}_n(\mathbf{K})$ and $\Delta_n(u') \in \mathrm{D}_n(\mathbf{K})$ such that $A = \Delta_n(u')P'$.

b) To show that $\mathrm{E}_n(\mathbf{K}) \lhd \mathrm{GL}_n(\mathbf{K})$, we need to show that, for any matrix $B_{ij}(\lambda) \in \mathrm{E}_n(\mathbf{K})$ and any matrix $P \in \mathrm{GL}_n(\mathbf{K})$, we have $PB_{ij}(\lambda)P^{-1} \in \mathrm{E}_n(\mathbf{K})$. By (i), we only need to show this in the case where $P = \Delta_n(u) \in \mathrm{D}_n(\mathbf{K})$. But it is simple to check that $\Delta_n(u)B_{ij}(\lambda)\Delta_n^{-1}(u)$ is equal to: $B_{ij}(\lambda)$ if $i,j \neq n$; $B_{in}(\mu\lambda)$ if $j = n$; $B_{nj}\left(\lambda\mu^{-1}\right)$ if $i = n$.

c) We need to show that $\Delta_n(u)\Delta_n(v) \equiv \Delta_n(v)\Delta_n(u)$ (mod. $\mathrm{E}_n(\mathbf{K})$), which is equivalent to $\Delta_n(uv) \equiv \Delta_n(vu)$ (mod. $\mathrm{E}_n(\mathbf{K})$). Everything reduces to the case $n = 2$ and, by elementary operations of type (i), these two matrices are equivalent (mod. $\mathrm{E}_2(\mathbf{K})$) to diag (λ,μ).

d) See ([COH 03b], Prop. 9.2.4). ■

If $\mathbf{K}$ is a field, $\mathrm{E}_n(\mathbf{K})$ is the subgroup of $\mathrm{GL}_n(\mathbf{K})$ generated by the matrices with determinant 1; it is called the *special linear group* of degree n over $\mathbf{K}$ and is written as $\mathrm{SL}_n(\mathbf{K})$. Writing $A = P\Delta_n(u)$, where $P \in \mathrm{SL}_n(\mathbf{K})$, we have that $\det(A) = \det(P)\det(\Delta_n(u)) = u$, and so u is uniquely determined by A and we have the following exact sequence of groups:

$$\{1\} \to \mathrm{SL}_n(\mathbf{K}) \to \mathrm{GL}_n(\mathbf{K}) \overset{\det}{\to} \mathbf{K} \to \{1\}. \qquad [2.27]$$

The permutation matrices P_{ij} have determinant -1.

(IV) DIEUDONNÉ DETERMINANT. When $\mathbf{K}$ is non-commutative, Theorem 2.65(d) shows that we still have an exact sequence:

$$\{1\} \to \mathrm{E}_n(\mathbf{K}) \to \mathrm{GL}_n(\mathbf{K}) \overset{\delta}{\to} \mathbf{K}^{ab} \to \{1\}$$

where the group homomorphism $\delta : \mathrm{GL}_n(\mathbf{K}) \to \mathbf{K}^{ab}$ has the following universal property: for each abelian group Γ, every group homomorphism $\mathrm{GL}_n(\mathbf{K}) \to \Gamma$ factorizes as follows:

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbf{K}) & \overset{\delta}{\to} & \mathbf{K}^{ab} \\ & \searrow & \downarrow \\ & & \Gamma \end{array}$$

This homomorphism δ is called the Dieudonné determinant. If $A \in \mathfrak{M}_n(\mathbf{K})$ is not invertible, we set $\delta(A) = 0$. If $P \in \mathrm{GL}_n(\mathbf{K})$, we have $\delta\left(PAP^{-1}\right) = \delta(A)$. The Dieudonné determinant is usually written as $\det$, as it coincides with the usual determinant in the commutative case. In the non-commutative case, $\det(A)$ *is not* an alternating multilinear form with respect to the rows and columns of A. Furthermore, the Dieudonné determinant cannot be extended to matrices defined over *non-commutative rings* since $\det(A)$ is a rational function (and not a polynomial function) in the elements of A.

(V) PROPERTIES OF DETERMINANTS. In the rest of this subsection, unless otherwise stated, $\mathbf{R}$ is a *commutative* ring. Let $A \in \mathfrak{M}_n(\mathbf{R})$; elementary operations of types (i) and (i') do not change $\det(A)$, elementary operations of types (ii) and (ii') cause $\det(A)$ to be multiplied by u and elementary operations of types (iii) and (iii') cause $\det(A)$ to be multiplied by -1.

Writing α for the matrix of cofactors α_{ij}, the *adjugate matrix* of A is the transpose α^T of α and

$$\boxed{\alpha^T A = A\alpha^T = \det(A)\, I_n}. \qquad [2.28]$$

In particular, $A \in \mathrm{GL}_n(\mathbf{R})$ if and only if $\det(A) \in \mathbf{U}(\mathbf{R})$. The mapping $\det : \mathfrak{M}_n(\mathbf{R}) \to \mathbf{R}$ is an epimorphism of multiplicative monoids, and $\det(AB) = \det(A)\det(B) = \det(B)\det(A) = \det(BA)$. We have that $\det(A) = \det\left(A^T\right)$, since:

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{1 \le i \le n} a_{\sigma(i),i} = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{1 \le i \le n} a_{i,\sigma(i)},$$

where $\varepsilon(\sigma)$ is the signature of $\sigma \in \mathfrak{S}_n$ (section 2.2.4(**II**)). If

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \qquad [2.29]$$

where A_{11} and A_{22} are square submatrices, and if $A_{21} = 0$ or $A_{12} = 0$, we have that $\det(A) = \det(A_{11})\det(A_{22})$. If A_{11} is invertible, we have that $\det(A) = \det(A_{11})\det\left(A_{22} - A_{21}A_{11}^{-1}A_{12}\right)$.

(VI) CRAMER'S RULE. It may be stated as follows for a commutative ring $\mathbf{R}$ ([BKI 12], Chap. III, section 8.7): let $A_1, ..., A_n, B$ be elements of $\mathbf{R}^n$ let

$A \in \mathfrak{M}_n(\mathbf{R})$ be the matrix with columns $A_1, ..., A_n$, and suppose that:

$$Ax = B, \tag{2.30}$$

where $x \in \mathbf{R}^n$ is the column with elements $x_i \in \mathbf{R}$ $(i = 1, ..., n)$. The equality [2.30] implies that, for all $i \in \{1, ..., n\}$,

$$\det(A)\, x_i = \det(A_1, ..., A_{i-1}, B, A_{i+1}, ..., A_n). \tag{2.31}$$

Conversely, if $\det(A)$ is regular in $\mathbf{R}$, and if there exists a column x whose elements x_i satisfy [2.31], this column is unique and is a solution of [2.30]. In order for this column x to exist, it is sufficient for $\det(A)$ to be a unit of $\mathbf{R}$, since then $A \in \mathrm{GL}_n(\mathbf{R})$.

REMARK 2.66.– *Suppose that we replace the assumption of a commutative ring* $\mathbf{R}$ *with that of a division ring* $\mathbf{K}$. *Consider once again [2.30]. Then [2.31] still holds when* det *is the Dieudonné determinant, provided that we replace* x_i *with its canonical image* $\bar{x}_i$ *in* $\mathbf{K}^{ab} = \mathbf{K}/\mathbf{K}'$. *The calculation of the Dieudonné determinant of the matrix [2.29] still holds as stated above.*

(VII) CAYLEY-HAMILTON THEOREM. Let $A \in \mathfrak{M}_n(\mathbf{R})$ and let $P_A = \det(X.I_n - A) \in \mathbf{R}[X]$ be its characteristic polynomial. We have that:

$$P_A(X) = X^n + \sum\nolimits_{k=1}^{n} (-1)^k \Delta_k X^{n-k} \tag{2.32}$$

where Δ_k $(1 \leq k \leq n)$ is the sum of the principal minors of order k, and in particular $\Delta_1 = \mathrm{Tr}(A)$ is the *trace* of A (the sum of the diagonal elements) and $\Delta_n = \det(A)$. Setting $A^0 = I_n$, the Cayley-Hamilton theorem ([BKI 12], chap. III, section 8.11, Prop. 20) states that :

$$\boxed{P_A(A) = 0}. \tag{2.33}$$

2.3.12. *Graded algebras and graded modules*

Let $\mathbf{K}$ be a commutative ring, and let $\mathbf{A}$ be a $\mathbf{K}$-algebra. Suppose that $\mathbf{A}$ is the direct sum of a countable family $(\mathbf{A}_n)$ of $\mathbf{K}$-submodules such that:

$$\mathbf{A}_n \mathbf{A}_m \subset \mathbf{A}_{n+m},$$

for all integers $n, m \in \mathbb{Z}$, and that $\mathbf{A}$ has a unit element $1 \in \mathbf{A}_0$. Then,

DEFINITION 2.67.– *The algebra* $\mathbf{A}$ *defined above is said to be* graded. *The elements of* $\mathbf{A}_n$ *are said to be* homogeneous *of degree* n. *Each element* $x \neq 0$ *belongs to exactly one* $\mathbf{A}_n$ *and the integer* n *is called its degree, written as* $\deg(x)$. *If* $\mathbf{A}_n = 0$ *for* $n < 0$, *the family of* $\mathbf{A}_n$ *is written as* $(\mathbf{A}_n)_{n\in\mathbb{N}}$. *The* trivial gradation *is the one for which* $\mathbf{A}_0 = \mathbf{A}$ *and* $\mathbf{A}_n = 0$ *for* $n \neq 0$.

Any $\mathbf{K}$-algebra $\mathbf{A}$ may be viewed as a graded algebra $(\mathbf{A}_n)$ with the trivial gradation. The algebra of polynomials $\mathbf{K}[X_1, ..., X_n]$ is one typical example of a graded algebra.

Let $\mathbf{A}$ be a graded $\mathbf{K}$-algebra and M be a left $\mathbf{A}$-module. We say that M is *graded* if M is the direct sum of a sequence (M_n) of submodules such that $\mathbf{A}_n M_m \subset M_{m+n}$ for all integers $n, m \in \mathbb{Z}$. A *graded ideal* of a graded algebra $\mathbf{A}$ is a graded submodule of this algebra. Let $p \in \mathbb{Z}$ and M, N be graded $\mathbf{A}$-modules; we say that $f : M \to N$ is a *graded homomorphism* of degree p if $\forall n$, $f(M_n) \subseteq N_{n+p}$.

DEFINITION 2.68.– *Let* $\mathbf{A}$ *be a graded* $\mathbf{K}$*-algebra and let* M *be a graded* $\mathbf{A}$*-module.*

i) A derivation d *of* $\mathbf{A}$ *in* M *of degree* $r \in \mathbb{Z}$ *is a* $\mathbf{K}$*-linear mapping* $d : \mathbf{A} \to M$, *such that* $d(\mathbf{A}_n) \subset M_{n+r}$ *for every integer* n, *and for all* $f, g \in \mathbf{A}$, $d(fg) = (df)\, g + f\,(dg)$. *A derivation of degree 1 is simply called a* derivation.

ii) An antiderivation d *of* $\mathbf{A}$ *in* M *of degree* $r \in \mathbb{Z}$ *is a* $\mathbf{K}$*-linear mapping* $d : \mathbf{A} \to M$, *such that* $d(\mathbf{A}_n) \subset M_{n+r}$ *for every integer* n, *and for all* $f_m \in \mathbf{A}_m, g_n \in \mathbf{A}_n$, $d(f_m g_n) = (df_m)\, g_n + (-1)^{mr} f_m\,(dg_n)$.

3

Modules and Algebras

It is a well-known fact that modern linear algebra (section 3.1) is the fruit of the labor of countless different authors. The notion of *vector*, characterized by n components with respect to a given basis, was proposed by A. Cayley (1850), while during the same period H. Grassmann and W. Hamilton developed a more "geometric" perspective, avoiding the use of coordinates (see, for example, Grassmann's relation [3.14] in section 3.1.7).

The notion of *tensor product* (section 3.1.5) can be traced back to L. Kronecker, but its modern definition was given by H. Whitney (1938). *Exact sequences* (section 3.1.4) were introduced by J. Kelley and A. Pitcher (1947).

The development of *Commutative Algebra* (section 3.2) was primarily motivated by number theory (and especially by the work performed by E. Kummer (1847) on Fermat's last theorem, whose "ideal numbers" were precursors of ideals in the ring of integers of number fields, which were introduced by R. Dedekind in 1871) and (over the course of a period ranging from 1890 until ca. 1960) algebraic geometry (D. Hilbert, E. Noether, W. Krull, O. Zariski, A. Weil, J.P. Serre, A. Grothendieck, etc.): section 3.2.2, 3.2.7. It was E. Noether who axiomatized Dedekind's notion of a ring in 1927 in the form we shall encounter in theorem-definition 3.134(1).

The first notions of *Homological Algebra* (section 3.3) appeared between 1940 and 1955, derived from the work in algebraic topology that had gradually taken place between H. Poincaré's *Analysis Situs* (1892) and the seminal book by S. Eilenberg and N. Steenrod [EIL 52] (1952): see section 3.3.8. The notion of injective module (section 3.3.1) was informally

referenced in an article by R. Baer (1940) and was formally defined, together with the notion of injective envelope, by B. Eckmann and A. Schopf (1953). Cartan and Eilenberg [CAR 56] introduced the concepts of projective module, global dimension, injective and projective resolutions, etc., thus laying the foundations of modern homological algebra. In the appendix of this book, D. Buchsbaum gathered together the most essential parts of the work on what A. Grothendieck would later name *Abelian Categories* (section 3.3.7). A. Grothendieck developed the homological algebra of abelian categories in depth in an article published in 1957 [GRO 57], which defined the notions of generator and cogenerator (sections 1.2.11 and 3.3.3), and many others.

The theory of modules over non-commutative rings was established by many different authors, some of whom we already mentioned at the beginning of Chapter 2. The "homological" definition of a Dedekind domain (theorem-definition 3.134(6)), as given by H. Cartan and S. Eilenberg in their book mentioned just above, was extended to the non-commutative case in 1967 by J.C. Robson.

Pseudo-linear transformations, the natural generalization of vector space endomorphisms to the non-commutative case, were introduced by N. Jacobson in 1937 [JAC 37] and have recently been studied in more depth [LER 95], leading to the results stated in section 3.4.3. The structure of finitely generated modules over principal ideal domains (section 3.4.2) was determined thanks to the contributions of J. Sylvester, H. Smith, K. Weierstrass and F. Frobenius from 1851 to 1879 in the commutative case, then the work by J. Wedderburn, N. Jacobson, O. Teichmüller and T. Nakayama toward the end of the 1930s in the non-commutative case. The structure of finitely generated modules over Dedekind domains (section 3.4.5) was clarified most notably by E. Steinitz in 1911 in the commutative case, and by D. Eisenbud and J.C. Robson in 1970 in the general case. The notion of an elementary divisor ring was proposed by I. Kaplansky (1949).

When we consider *right* vector spaces, matrix computations are only compatible with the linear algebra on division rings if the vectors are represented as *columns*. To work with *left* vector spaces, we must represent vectors by *rows*, and the same is true for free left modules over a non-commutative ring (section 3.1.6). We will therefore adopt the latter convention for this chapter[1].

1 This convention is also used by mathematicians working on $\mathcal{D}$-modules (see p. x).

3.1. Additional concepts from linear algebra

3.1.1. *Bimodules*

Let $\mathbf{R}$ and $\mathbf{S}$ be two rings. An $(\mathbf{R},\mathbf{S})$-*bimodule* ${}_{\mathbf{R}}M_{\mathbf{S}}$ is a left $\mathbf{R}$-module that is also a right $\mathbf{S}$-module with the compatibility relation $(r.x).s = r.(x.s)$ for all $r \in \mathbf{R}, s \in \mathbf{S}, x \in M$. Every left $\mathbf{R}$-module is an $(\mathbf{R},\mathbb{Z})$-bimodule and every right $\mathbf{S}$-module is a $(\mathbb{Z},\mathbf{S})$-bimodule. The morphisms of the category of $(\mathbf{R},\mathbf{S})$-bimodules ${}_{\mathbf{R}}\mathbf{Mod}_{\mathbf{S}}$ are $\mathbb{Z}$-bilinear mappings that are morphisms of both ${}_{\mathbf{R}}\mathbf{Mod}$ and $\mathbf{Mod}_{\mathbf{S}}$. In particular, the ring $\mathbf{R}$ can be canonically equipped with an $(\mathbf{R},\mathbf{R})$-bimodule structure written ${}_{\mathbf{R}}\mathbf{R}_{\mathbf{R}}$ (which we will simply write as $\mathbf{R}$ unless doing so is ambiguous).

Let ${}_{\mathbf{R}}M_{\mathbf{T}}$, ${}_{\mathbf{S}}N_{\mathbf{T}}$ be bimodules; then the abelian group $\mathrm{Hom}_{\mathbf{T}}(M,N)$, where $M = M_{\mathbf{T}}$ and $N = N_{\mathbf{T}}$, has a canonical $(\mathbf{S},\mathbf{R})$-bimodule structure given by $s.f : M \ni x \mapsto s.f(x) \in N$ and $f.r : x \mapsto f(r.x)$ $(r \in \mathbf{R}, s \in \mathbf{S})$. Dually, let ${}_{\mathbf{R}}M_{\mathbf{S}}$, ${}_{\mathbf{R}}N_{\mathbf{T}}$ be bimodules; then $\mathrm{Hom}_{\mathbf{R}}(M,N)$, where $M = {}_{\mathbf{R}}M$ and $N = {}_{\mathbf{R}}N$, may be equipped with a canonical $(\mathbf{S},\mathbf{T})$-bimodule structure by setting $s.f : M \ni x \mapsto f(x.s)$ and $(f.t)(x) = f(x).t$. The following mnemonic device can be helpful:

$$\boxed{{}_{\mathbf{R}}\mathrm{Hom}_{\mathbf{T}}({}_{\mathbf{R}}M_{\mathbf{T}},{}_{\mathbf{S}}N_{\mathbf{T}})_{\mathbf{S}}\,, \qquad {}_{\mathbf{S}}\mathrm{Hom}_{\mathbf{R}}({}_{\mathbf{R}}M_{\mathbf{S}},{}_{\mathbf{R}}N_{\mathbf{T}})_{\mathbf{T}}}\,.$$

Given any left $\mathbf{R}$-module M, $\mathrm{Hom}_{\mathbf{R}}({}_{\mathbf{R}}\mathbf{R}_{\mathbf{R}}, M)$ is therefore a left $\mathbf{R}$-module and is isomorphic to M under the isomorphism

$$\theta : M \to \mathrm{Hom}_{\mathbf{R}}({}_{\mathbf{R}}\mathbf{R}_{\mathbf{R}}, M) : x \mapsto (\theta_x : {}_{\mathbf{R}}\mathbf{R}_{\mathbf{R}} \to M : r \mapsto r.x)\,. \quad [3.1]$$

3.1.2. *Duality*

(I) The *algebraic dual* of a left (resp. right) $\mathbf{R}$-module M is $M^* = \mathrm{Hom}_{\mathbf{R}}(M,\mathbf{R})$, the set of linear forms on M, which is a right (resp. left) $\mathbf{R}$-module. If $x^* \in M^*$ and $x \in M$, we write $x^*(x) = \langle x, x^*\rangle$ if M is a left $\mathbf{R}$-module, and $x^*(x) = \langle x^*, x\rangle$ if M is a right $\mathbf{R}$-module. We call $\langle -,-\rangle$ the *duality bracket*.

Let A, B be two right $\mathbf{R}$-modules and let $f : M \to N$ be a morphism of right $\mathbf{R}$-modules. The (algebraic) *transpose* of f is the morphism of left

$\mathbf{R}$-modules ${}^t f : N^* \to M^* : y^* \mapsto y^* \circ f$, which therefore satisfies, for all $x \in M$, $y^* \in N^*$,

$$\boxed{\langle y^*, f(x)\rangle = \langle {}^t f(y^*), x\rangle}.$$

(II) Let M be a right $\mathbf{R}$-module. For $x \in M$, consider the mapping $\mathrm{can}_M(x) : M^* \ni y^* \mapsto \langle y^*, x\rangle \in \mathbf{R}$. This mapping is $\mathbf{R}$-linear, so $\mathrm{can}_M(x) \in M^{**} := (M^*)^*$; M^{**} is the *bidual* of M and is again a right $\mathbf{R}$-module. Let $f : M \to N$ be a morphism of right $\mathbf{R}$-modules, ${}^t f : N^* \to M^*$ and $f^{**} := {}^t({}^t f) : M^{**} \to N^{**}$. The diagram

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \mathrm{can}_M \downarrow & & \downarrow \mathrm{can}_N \\ M^{**} & \xrightarrow{f^{**}} & N^{**} \end{array}$$

commutes, so can is a *functorial morphism* (section 1.2.2(**I**)) $\mathrm{id} \dot{\to} (-)^{**}$, where $(-)^{**}$ is the "bidual" functor. The mapping $\mathrm{can}_M : M \to M^{**}$, called the *canonical homomorphism*, is in general neither injective nor surjective; a module M is said to be *reflexive* if can_M is bijective (see theorem 3.12 below, as well as section 3.3.1).

3.1.3. *Free modules*

(I) In the following, unless otherwise stated, all modules are left modules.

LEMMA 3.1.– *Let* $(M_i)_{i\in I}$ *be an* infinite *family of* non-zero $\mathbf{R}$*-modules and suppose that* $M = \bigoplus_{i\in I} M_i$; *let* S *be a generating set of* M. *Then,* $\mathrm{Card}(S) \geq \mathrm{Card}(I)$.

PROOF.– For $m \in S$, write $m = \sum_{i\in I} \lambda^i . m_i$, where $m_i \in M_i$ and $\lambda^i \in \mathbf{R}$. Let C_m be the finite set of $i \in I$ such that $\lambda^i \neq 0$, and let $C = \bigcup_{m\in S} C_m$. We have that $m \in \bigoplus_{i\in C} M_i$, so $S \subset \bigoplus_{i\in C} M_i$, and so $M = [S]_{\mathbf{R}} = \bigoplus_{i\in C} M_i$, which implies that $C = I$. If S were finite, $C = \bigcup_{m\in S} C_m$ would be finite; hence, S is infinite and $\mathrm{Card}(S) \geq \mathrm{Card}(I)$ by corollary 1.9. ■

(II) Recall that a module M is said to be free if it has a basis $(e_i)_{i\in I}$ (section 2.3.1(**II**)). This is equivalent to saying that, for all $x \in M$, there exists a *uniquely determined* family $(x^i)_{i\in I}$ of elements of $\mathbf{R}$ with finite support such

that $x = \sum_{i\in I} x^i.e_i$. It is useful to represent x with respect to the basis $(e_i)_{i\in I}$ as the *row* $\mathbf{x}$ with i-th element x^i. This gives a (non-canonical) isomorphism of $\mathbf{R}$-modules $M \cong \mathbf{R}^{1\times(I)}$ where $\mathbf{R}^{1\times(I)}$ is the free left $\mathbf{R}$-module of rows with Card (I) elements, only finitely many of which are non-zero. We have that $\mathbf{R}^{1\times(I)} = \bigoplus_{i\in I} \mathbf{R}_i$, where $\mathbf{R}_i = {}_{\mathbf{R}}\mathbf{R}, \forall i \in I$.

Let $\mathbf{A}$ be a ring and let E, F be two free $\mathbf{A}$-modules with bases $(a_i)_{i\in Q}$ and $(b_j)_{j\in K}$, respectively. Let $f : E \to F$ be an $\mathbf{A}$-linear mapping. The element $f(a_i) \in E$ may be uniquely written in the form $\sum_{j\in K} r_i^j.b_j$, where $R = \left(r_i^j\right)$ is a matrix of dimension Card $(Q) \times$ Card (K) such that, for all $i \in I$, the family $\left(r_i^j\right)_{j\in K}$ (i.e. the row with index i) has finite support, which we will write as $R \in \mathbf{A}^{Q\times(K)}$.

DEFINITION 3.2.– *The matrix* $R =$ Mat (f) *is called the* representative matrix *of* f *with respect to the bases* $(a_i)_{i\in Q}$, $(b_j)_{j\in K}$.

(III) The equality $y = f(x)$ may be represented *with respect to the bases* $(a_i)_{i\in Q}$, $(b_j)_{j\in K}$ by the matrix equation $\mathbf{y} = \mathbf{x}.R$, where $\mathbf{x}$ and $\mathbf{y}$ are the *rows* with components x^i and y^j, respectively, which are uniquely determined by the equalities $x = \sum_{i\in Q} x^i a_i$ and $y = \sum_{j\in K} y^j b_j$.

Let $(a'_i)_{i\in Q'}$, $\left(b'_j\right)_{j\in K'}$ be alternative bases of E and F, respectively. We have that $a_i = \sum_{k\in Q'} s_i^k a'_k$ and $b_j = \sum_{l\in K'} t_j^l b'_l$, where $S = \left(s_i^k\right) \in \mathbf{A}^{Q\times(Q')}$, $T = \left(t_j^l\right) \in \mathbf{A}^{K\times(K')}$ are the change-of-basis matrices (which must therefore be invertible). Writing a for the *column* of the a_i's and b for the *column* of the b_j's, we obtain

$$x = \mathbf{x}a, \quad y = \mathbf{y}b, \quad a = Sa', \quad b = Tb', \quad x = \mathbf{x}'a', \quad y = \mathbf{y}'b'$$

using the obvious notation, and so $\mathbf{y}' = \mathbf{y}T$, $\mathbf{x}' = \mathbf{x}S$, hence $\mathbf{y}T = \mathbf{x}SS^{-1}RT$ and, finally, $\mathbf{y}' = \mathbf{x}'S^{-1}RT$. This allows us to state

COROLLARY 3.3.– *With respect to the new bases* $(a'_i)_{i\in Q'}$, $\left(b'_j\right)_{j\in K'}$, *the representative matrix of* f *is* $R' = S^{-1}RT$.

DEFINITION 3.4.– *Two matrices* $R \in \mathbf{A}^{Q\times(K)}$, $R' \in \mathbf{A}^{Q'\times(K')}$ *are* equivalent *(resp.* left-equivalent*, resp.* right-equivalent*), which we write as* $R \sim R'$ *(resp.*

$R \sim_l R'$, resp. $R \sim_r R'$), if there exist invertible matrices $S \in \mathbf{A}^{Q\times(Q')}$, $T \in \mathbf{A}^{K\times(K')}$ such that $R' = S^{-1}RT$ (resp. $R' = S^{-1}R$, resp. $R' = RT$).

(IV) If $M \cong \mathbf{R}^{1\times(I)} \cong \mathbf{R}^{1\times(J)}$ and Card (I) is *infinite*, then I and J are equipotent by lemma 3.1. This does not hold in general when Card (I) is finite (see theorem 3.28), at least in the non-commutative case (see theorem 3.8).

DEFINITION 3.5.– *A ring $\mathbf{R}$ is said to have the* invariant basis number (IBN) *property if $\mathbf{R}^{1\times n} \cong \mathbf{R}^{1\times m} \Rightarrow n = m$. A ring is said to be* weakly finite *if, for any integer n and any $\mathbf{R}$-module H, $\mathbf{R}^{1\times n} \cong \mathbf{R}^{1\times n} \oplus H \Rightarrow H = 0$.*

A weakly finite ring $\mathbf{R} \neq \{0\}$ has the IBN property (**exercise**). Non-weakly finite rings are "pathological"!

LEMMA 3.6.– *Let $\mathbf{R}$ be a ring. The following conditions are equivalent:*

i) $\mathbf{R}$ is weakly finite;

ii) For any integer $n \geq 1$ and any matrices $A, B \in \mathfrak{M}_n(\mathbf{R})$, if $AB = I_n$ then $BA = I_n$.

PROOF.– (ii)⇒(i) is obvious. (i)⇒(ii): consider the split exact sequence (see below, section 3.1.4(**I**))

$$0 \to H \xrightarrow{f_1} \mathbf{R}^{1\times n} \xrightarrow{f_2} \mathbf{R}^{1\times n} \to 0.$$

Let s be a linear section of f_2. With respect to the canonical basis in $\mathbf{R}^{1\times n}$, f_2 and s are represented by the matrices B and A, respectively. Since $f_2 \circ s = \mathrm{id}_n$, and $f_2 = \bullet B$, $s = \bullet A$, we have that $AB = I_n$. Note that $H = 0$ if and only if s is the inverse isomorphism of f_2, so $BA = I_n$. ■

LEMMA-DEFINITION 3.7.– *If E is a free $\mathbf{R}$-module and $\mathbf{R}$ has the IBN property, there exists a unique cardinal $\mathfrak{r}$ such that $E \cong \mathbf{R}^{1\times(I)}$ and* Card $(I) = \mathfrak{r}$. *This cardinal $\mathfrak{r}$ is called the* rank *of E and is written* $\mathrm{rk}_{\mathbf{R}}(E)$.

THEOREM 3.8.– *Every commutative ring $\mathbf{R}$ is weakly finite.*

PROOF.– This follows from lemma 3.6 and [2.28]. ■

LEMMA 3.9.– *Let $\mathbf{R}$ be a ring, M an $\mathbf{R}$-module, G a generating set of M and $L \subset \Gamma$ a free subset. The set $\mathcal{F}$ of all free sets F such that $L \subset F \subset G$ has a maximal element.*

PROOF.– A set $F \subset M$ is free if and only if every finite subset of F is free. Therefore, the set $\mathcal{F}$ is of finite character, and so has a maximal element (lemma 1.4). ■

THEOREM 3.10.– *(*basis extension theorem*) Let* $\mathbf{K}$ *be a division ring and* V *a* $\mathbf{K}$*-vector space. For every generator* G *of* V *and every free set* $L \subset G$*, there exists a basis* B *such that* $L \subset B \subset G$*. In particular, every* $\mathbf{K}$*-vector space* V *has a basis, and so is a free* $\mathbf{K}$*-module.*

PROOF.– 1) Let $F \subset V$ be a free subset of the $\mathbf{K}$-vector space V. If $b \in V$ does not belong to the vector subspace W generated by F, the set $F \cup \{b\}$ is free. Indeed, if there existed a relation $\mu.b + \sum_{i\in I} \lambda_i.f_i = 0$, with $f_i \in F$ and finite supp $\left((\lambda_i)_{i\in I}\right)$, we would have either $\mu \neq 0$ and $b = -\sum_{i\in I} \left(\mu^{-1}\lambda_i\right).f_i \in W$, or $\sum_{i\in I} \lambda_i.f_i = 0$. Both cases are impossible. 2) Let G be a generating set of V and let $\mathcal{F}$ be the set of all free sets F such that $L \subset F \subset G$. By lemma 3.9, $\mathcal{F}$ has a maximal element B, and so by (1) B generates V. ■

We will see later (theorem 3.28) that any two bases of the same $\mathbf{K}$-vector space V are equipotent, which motivates

DEFINITION 3.11.– *The cardinal of a basis of a* $\mathbf{K}$*-vector space* V *is called the* dimension *of* V *and is written* $\dim_{\mathbf{K}}(V)$.

It immediately follows (**exercise**) that

$$\dim_{\mathbf{K}}(V \oplus W) = \dim_{\mathbf{K}}(V) + \dim_{\mathbf{K}}(W). \qquad [3.2]$$

(V) The statement of theorem 3.10 can fail if $\mathbf{K}$ is a ring and V is a $\mathbf{K}$-module. For example, the $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ does not have a basis, since every element $m \in \mathbb{Z}/2\mathbb{Z}$ satisfies $2m = 0$, so is related.

(VI) If F is a finite free (section 2.3.1(**II**)) left $\mathbf{R}$-module with basis $(e_i)_{1\leq i\leq n}$, its dual F^* (section 3.1.2(**I**)) is also free with basis given by the family $\left(e^{*i}\right)_{1\leq i\leq n}$ defined by $\left\langle e_i, e^{*j}\right\rangle = \delta_i^j$. We call $\left(e^{*i}\right)_{1\leq i\leq n}$ the *dual basis* of $(e_i)_{1\leq i\leq n}$. If $x = \sum_{1\leq i\leq n} x^i.e_i \in F$ and $y^* = \sum_{1\leq i\leq n} e^{*i}.y_i \in F^*$, then $\langle x, y^*\rangle = \sum_{i=1}^n x^i y_i$. Hence, if F is finite free, then the canonical homomorphism $c_F : F \to F^{**}$ (section 3.1.2(**II**)) is bijective, since F^{**} is free and has basis $(\tilde{e}_i)_{1\leq i\leq n}$, where $\tilde{e}_i$ is the linear form on F^* such that $\left\langle \tilde{e}_i, e^{*j}\right\rangle = \delta_i^j$. Hence, in this case, the modules F and F^{**} are *canonically*

(or *naturally*) *isomorphic*. If M, N are two finite free $\mathbf{R}$-modules identified with their biduals and if $f : M \to N$ is $\mathbf{R}$-linear, then $f^{**} = f$. We therefore obtain the following result:

THEOREM 3.12.– *Let ${}_{\mathbf{R}}\mathcal{F}^f$ be the category of finite free left $\mathbf{R}$-modules. The functorial morphism ${}_{\mathbf{R}}\mathcal{F}^f \dot{\to}\ {}_{\mathbf{R}}\mathcal{F}^f$: id $\to (-)^{**}$ (section 3.1.2(**II**)) is a functorial* isomorphism.

REMARK 3.13.– *Let ${}_{\mathbf{R}}\mathcal{F}^f_{\mathfrak{b}}$ (resp. ${}_{\mathfrak{b}}\mathcal{F}^f_{\mathbf{R}}$) be the category of finite free left (resp. right) $\mathbf{R}$-modules* with a given basis. *Consider the "dual functor"* $(-)^* : {}_{\mathbf{R}}\mathcal{F}^f_{\mathfrak{b}} \to {}_{\mathfrak{b}}\mathcal{F}^f_{\mathbf{R}}$ *defined as follows: if $(F, \mathfrak{B})$ is an object of ${}_{\mathbf{R}}\mathcal{F}^f_{\mathfrak{b}}$, where $\mathfrak{B} = (e_i)_{1\leq i\leq n}$ is a basis of F, then $(F, \mathfrak{B})^* = (F^*, \mathfrak{B}^*)$, where F^* is the dual of F and $\mathfrak{B}^*$ is the dual basis of $\mathfrak{B}$. If M, N are two finite free left $\mathbf{R}$-modules and $f : M \to N$ is $\mathbf{R}$-linear, then $f^* = {}^t f$. If $\mathbf{R}$ is commutative, we have that ${}_{\mathbf{R}}\mathcal{F}_{\mathfrak{b}} = {}_{\mathfrak{b}}\mathcal{F}^f_{\mathbf{R}}$ and the mapping $F \to F^* : \sum_{1\leq i\leq n} x^i.e_i \mapsto \sum_{1\leq i\leq n} x^i.e_i^*$ is an isomorphism of finite free $\mathbf{R}$-modules. This isomorphism* is not *canonical (or natural), as it depends on the choice of basis $\mathfrak{B}$ in F.*

THEOREM-DEFINITION 3.14.– *([COH 03b], Thm. 8.7.1)*

1) Let $\mathbf{A}$ be a ring. The following conditions are equivalent:

i) Every finitely generated left ideal in $\mathbf{A}$ is free, with a unique rank.

ii) $\mathbf{A}$ has the IBN property and every finitely generated submodule of a free left $\mathbf{A}$-module is free.

2) A ring satisfying these conditions is called a semifir[2].

3) Semifirs are entire and weakly finite ([COH 85], section 1.1, Cor. 1.3).

3.1.4. *Exact sequences*

(I) Let (E_n) be an exact sequence of $\mathbf{R}$-modules and let (f_n) be a sequence of $\mathbf{R}$-linear mappings $f_n : E_{n-1} \to E_n$. We say that

$$\ldots \longrightarrow E_{n-1} \xrightarrow{f_n} E_n \xrightarrow{f_{n+1}} E_{n+1} \longrightarrow \qquad [3.3]$$

is an *exact sequence* at E_n in ${}_{\mathbf{R}}\mathbf{Mod}$ if $\mathrm{im}\,(f_n) = \ker(f_{n+1})$ where $\mathrm{im}\,(f_n) := f_n(E_{n-1})$ and $\ker(f_{n+1}) := f_{n+1}^{-1}(0)$ (section 2.2.2). The

2 *fir*: free ideal ring.

cokernel of f_n is $\operatorname{coker}(f_n) := E_n/\operatorname{im}(f_n)$. An exact sequence is a sequence that is exact at each point. An exact sequence

$$0 \to E_0 \overset{f_1}{\to} E_1 \overset{f_2}{\to} E_2 \to 0 \qquad [3.4]$$

is said to be *short*. Then, $f_1(E_0)$ is a submodule of E_1 isomorphic to E_0, and E_2 is isomorphic to $\operatorname{coker}(f_1)$ by Noether's first isomorphism theorem (theorem 2.12(1)), E_1 is an extension of E_2 by E_0, and we have ([BKI 12], Chap. II, section 1.9, Prop. 15):

LEMMA-DEFINITION 3.15.–

1) The following conditions are equivalent:

i) $f_1(E_0)$ *is a* direct factor *of* E_1*, i.e. there exists a submodule* E_2' *of* E_1 *(which is necessarily isomorphic to* E_2*) such that* $E_1 = f_1(E_0) \oplus E_2'$.

ii) There exists a linear retraction r *of* f_1*, i.e. an* $\mathbf{R}$*-linear surjection* $r : E_1 \twoheadrightarrow E_0$ *such that* $r \circ f_1 = \mathrm{id}_{E_0}$.

iii) There exists a linear section s *of* f_2*, i.e. an* $\mathbf{R}$*-linear injection* $s : E_2 \hookrightarrow E_1$ *such that* $f_2 \circ s = \mathrm{id}_{E_2}$.

2) If one of the equivalent conditions above is satisfied, $f_1 + s : E_0 \oplus E_2 \to E_1$ *is an isomorphism, the short exact sequence [3.4] is said to* split *and the monomorphism* f_1 *is also said to* split.

PROOF.– (iii)⇒(i) & (2): Let $x \in E_1$. Then $x - s(f_2(x)) \in \ker(f_2)$, hence $E_1 = \ker(f_2) + \operatorname{im}(s)$. The sum is exact since if $x = y + z$ with $y \in \ker(f_2)$ and $z \in \operatorname{im}(s)$, there exists $w \in E_2$ such that $z = s(w)$, thus $f_2(x) = w$ and z is uniquely determined by x, and so y is too. Since $E_1 = \ker(f_2) \oplus \operatorname{im}(s)$, $f_1 + s : E_0 \oplus E_2 \to E_1$ is an isomorphism. Reversing the arrows, (ii)⇒(i).

(i)⇒(ii): If $E_1 = f_1(E_0) \oplus E_2'$, for every $\xi \in E_0$ and $x \in E_2'$, let $r : f_1(\xi) \mapsto \xi, x \mapsto 0$. Then, $r : E_1 \to E_0$ is a linear retraction of f_1.

(i)⇒(iii): If $E_1 = \ker(f_2) \oplus E_2'$, for every $x = x_1 + x_2 \in E_1$, with $x_1 \in \ker(f_2)$ and $x_2 \in E_2'$, let $s : f_2(x) \mapsto x_2$. Then, s is a linear section of f_2. ■

COROLLARY 3.16.– *Consider an exact sequence of* $\mathbf{R}$*-modules*

$$0 \to G \overset{g}{\to} E \overset{f}{\to} F \to 0 \qquad [3.5]$$

where F *is free. Then, this exact sequence splits and* $E \cong g(G) \oplus F$.

PROOF.– Let $(b_\lambda)_{\lambda\in L}$ be a basis of F. Since f is surjective, there exists a family $(a_\lambda)_{\lambda\in L}$ of elements of E such that $f(a_\lambda) = b_\lambda$. Hence, there exists a unique homomorphism $s : F \to E$ such that $s(b_\lambda) = a_\lambda$ for all $\lambda \in L$ (lemma 2.20). It is clear that s is a linear section of f, so the exact sequence [3.5] splits and $E \cong g(G) \oplus F$. ■

(II) A functor $\mathfrak{F} : {}_{\mathbf{R}}\mathbf{Mod} \to \mathbf{Ab}$ is said to be *additive* if, for any two left $\mathbf{R}$-modules M, N, the mapping $\mathrm{Hom}_{\mathbf{R}}(M,N) \to \mathrm{Hom}_{\mathbb{Z}}(\mathfrak{F}(M), \mathfrak{F}(N))$ is $\mathbb{Z}$-linear. By corollary 1.23, a covariant additive functor $\mathfrak{F} : {}_{\mathbf{R}}\mathbf{Mod} \to \mathbf{Ab}$ is left-exact, resp. right-exact (section 1.2.9), if and only if it transforms every short exact sequence [3.4] into an exact sequence

$$0 \to \mathfrak{F}(E_0) \overset{\mathfrak{F}(f_1)}{\to} \mathfrak{F}(E_1) \overset{\mathfrak{F}(f_2)}{\to} \mathfrak{F}(E_2),$$

$$\text{resp. } \mathfrak{F}(E_0) \overset{\mathfrak{F}(f_1)}{\to} \mathfrak{F}(E_1) \overset{\mathfrak{F}(f_2)}{\to} \mathfrak{F}(E_2) \to 0.$$

(For contravariant functors, reverse the arrows in [3.4].)

LEMMA 3.17.– *If the additive functor $\mathfrak{F} : {}_{\mathbf{R}}\mathbf{Mod} \to \mathbf{Ab}$ is faithful, then it is injective, so $\mathfrak{F}({}_{\mathbf{R}}\mathbf{Mod})$ is a subcategory of $\mathbf{Ab}$.*

PROOF.– For any $\mathbf{R}$-module M, let $0_M : M \to M : x \mapsto 0$. If $\mathfrak{F}(M) = \mathfrak{F}(M')$, then $\mathfrak{F}(0_M) = \mathfrak{F}(0_{M'})$, so if $\mathfrak{F}$ is faithful, $0_M = 0_{M'}$, and $M = M'$, thus $\mathfrak{F}$ is injective. Hence, $\mathfrak{F}({}_{\mathbf{R}}\mathbf{Mod})$ is a subcategory of $\mathbf{Ab}$ by lemma 1.13. ■

3.1.5. *Tensor products*

(I) TENSOR PRODUCTS OF MODULES. Let $\mathbf{R}$ be a ring, $A_{\mathbf{R}}$ a right $\mathbf{R}$-module, ${}_{\mathbf{R}}B$ a left $\mathbf{R}$-module and C an abelian group. A function $f : A \times B \to C$ is said to be $\mathbf{R}$-biadditive if 1) it is $\mathbb{Z}$-bilinear and 2) for any $r \in \mathbf{R}$, $f(a.r, b) = f(a, r.b)$, for all $a \in A, b \in B$. Let $\mathrm{Biadd}_{\mathbf{R}}(A, B; C)$ be the abelian group of $\mathbf{R}$-biadditive mappings from $A \times B$ to C and, given A and B, let $\mathfrak{G} : \mathbf{Ab} \to \mathbf{Set}$ be the functor defined by $\mathfrak{G}(C) = \mathrm{Biadd}_{\mathbf{R}}(A, B; C)$ and $\mathfrak{G}(t).h = t \circ h$, where $h \in \mathfrak{G}(C)$ and $t : C \to C'$ is $\mathbb{Z}$-linear ($C' \in \mathbf{Ab}$). The diagram

$$\begin{array}{ccc} A \times B & & \\ h \downarrow & \searrow^{f} & \\ C & \overset{t}{\dashrightarrow} & C' \end{array} \qquad [3.6]$$

leads to the following universal problem for the functor $\mathfrak{G}$ (section 1.2.4): determine an abelian group C and an $\mathbf{R}$-biadditive mapping $h : A \times B \to C$ such that, for any abelian group C' and any $\mathbf{R}$-biadditive mapping $f : A \times B \to C'$, there exists a unique $\mathbb{Z}$-linear mapping $t : C \to C'$ for which the diagram [3.6] commutes.

Let $E = \mathbb{Z}^{(A\times B)}$ (interpreted as the set of formal $\mathbb{Z}$-linear combinations of the pairs $(x, y) \in A \times B$) and let F be the subgroup of E generated by the elements (x, y) corresponding to any one of the three following forms (with the obvious notation):

i) $(x_1 + x_2, y) - (x_1, y) - (x_2, y)$;

ii) $(x, y_1 + y_2) - (x, y_1) - (x, y_2)$;

iii) $(x.\lambda, y) - (x, \lambda.y)$.

Let $A \bigotimes_{\mathbf{R}} B := E/F$ and let $x \otimes y$ be the canonical image of an arbitrary pair $(x, y) \in E$ in E/F. This construction is universal ([MCL 99], section IX.8, Thm. 15):

THEOREM-DEFINITION 3.18.– *$(A \bigotimes_{\mathbf{R}} B, \otimes)$ is a universal object of the functor $\mathfrak{G}$. The $\mathbb{Z}$-module $A \bigotimes_{\mathbf{R}} B$ is called the* tensor product *of A and B; it consists of the* finite *sums $\sum_i x_i \otimes y_i$ $(x_i \in A, y_i \in B)$.*

The tensor product of free modules ${}_{\mathbf{R}}A$, ${}_{\mathbf{R}}B$ is a free $\mathbb{Z}$-module with basis given by the family $(x_i \otimes y_j)_{(i,j)\in I\times J}$, where $(x_i)_{i\in I}$ and $(y_j)_{j\in J}$ are bases of ${}_{\mathbf{R}}A$ and ${}_{\mathbf{R}}B$, respectively ([BKI 12], Chap. II, section 3.7, Cor. 2).

Let $\mathbf{R}, \mathbf{S}, \mathbf{T}$ be three rings, ${}_{\mathbf{R}}A_{\mathbf{S}}$ an $(\mathbf{R}, \mathbf{S})$-bimodule and ${}_{\mathbf{S}}B_{\mathbf{T}}$ an $(\mathbf{S}, \mathbf{T})$-bimodule (section 3.1.1). Then, $A \bigotimes_{\mathbf{S}} B$ has a canonical $(\mathbf{R}, \mathbf{T})$-bimodule structure given by $r\,(x \otimes y)\,t = (rx) \otimes (yt)$ for all $r \in \mathbf{R}, t \in \mathbf{T}, x \in A, y \in B$. Therefore, the following mnemonic device can be useful:

$$\boxed{{}_{\mathbf{R}}\left(({}_{\mathbf{R}}A_{\mathbf{S}}) \bigotimes_{\mathbf{S}} ({}_{\mathbf{S}}B_{\mathbf{T}})\right)_{\mathbf{T}}}.$$

Suppose that the left $\mathbf{R}$-modules E, F are projective (see section 3.3.1) and finitely generated. Then, the abelian group $E^* \otimes_{\mathbf{R}} F$ may be identified with $\mathrm{Hom}_{\mathbf{R}}(E, F)$ by identifying $x^* \otimes y$ with the $\mathbf{K}$-linear mapping $x \mapsto \langle x, x^*\rangle\, y$ ([BKI 12], Chap. II, section 4.2, Cor.).

Let $\mathbf{R}$ be a ring and let $s : E_1 \to E_2$, $t : F_1 \to F_2$ be $\mathbf{R}$-linear mappings, where the E_i are right $\mathbf{R}$-modules and the F_i are left $\mathbf{R}$-modules. We write

$$s \otimes t : E_1 \otimes_{\mathbf{R}} F_1 \to E_2 \otimes_{\mathbf{R}} F_2 : x \otimes y \mapsto (s.x) \otimes (t.y)\,.$$

This $\mathbb{Z}$-linear mapping is uniquely determined.

(II) ADJOINT ISOMORPHISM THEOREM. Let E be a right $\mathbf{R}$-module. Then, $\mathfrak{F}_E = E \otimes_{\mathbf{R}} - : F \mapsto E \otimes_{\mathbf{R}} F$ is a covariant functor of the category ${}_{\mathbf{R}}\mathrm{Mod}$ of left $\mathbf{R}$-modules into $\mathbf{Ab}$ after defining the $\mathbb{Z}$-linear mapping $\mathfrak{F}_E(f) := \mathrm{id}_E \otimes f : \mathfrak{F}_E(F_1) \to \mathfrak{F}_E(F_2)$ for any morphism of left $\mathbf{R}$-modules $f : F_1 \to F_2$. We can also construct the functor $\mathfrak{G}_F = - \otimes_{\mathbf{R}} F$ of the category $\mathrm{Mod}_{\mathbf{R}}$ of right $\mathbf{R}$-modules in $\mathbf{Ab}$, which satisfies $\mathfrak{G}_F(g) = g \otimes \mathrm{id}_F$ for any morphism of right $\mathbf{R}$-modules $g : E_1 \to E_2$. This functor is contravariant.

THEOREM 3.19.– *(*adjoint isomorphism theorem*)*

1) Let ${}_{\mathbf{R}}A_{\mathbf{S}}$ be an $(\mathbf{R}, \mathbf{S})$-bimodule. The following pairs of functors are adjoint:

$$a)\quad \boxed{\left(A \bigotimes_{\mathbf{S}} -, \mathrm{Hom}_{\mathbf{R}}(A, -)\right)}, \quad b)\quad \boxed{\left(- \bigotimes_{\mathbf{R}} A, \mathrm{Hom}_{\mathbf{S}}(A, -)\right)}.$$

2) Therefore, the functors $A \bigotimes_{\mathbf{S}} -$ and $- \bigotimes_{\mathbf{R}} A$ are right-exact (we already know that $\mathrm{Hom}_{\mathbf{R}}(A, -)$ and $\mathrm{Hom}_{\mathbf{S}}(A, -)$ are left-exact: see section 1.2.3).

PROOF.– We will show that the first pair of functors is adjoint (the proof is similar for the second pair). We must show that there exists a functorial isomorphism

$$\mathrm{Hom}_{\mathbb{Z}}\left(A \bigotimes_{\mathbf{S}} -, -\right) \cong \mathrm{Hom}_{\mathbb{Z}}(-, \mathrm{Hom}_{\mathbf{R}}(A, -))\,,$$

which implies that, for any left $\mathbf{S}$-module ${}_{\mathbf{S}}B$ and any abelian group C, there exists an isomorphism of $\mathbb{Z}$-modules

$$\mathrm{Hom}_{\mathbb{Z}}\left(A \bigotimes_{\mathbf{S}} B, C\right) \cong \mathrm{Hom}_{\mathbb{Z}}(B, \mathrm{Hom}_{\mathbf{R}}(A, C))$$

that is natural with respect to B and C. Let $f : A \bigotimes_{\mathbf{S}} B \to C$ be a $\mathbb{Z}$-linear mapping and, for all $b \in B$, consider $f_b : A \to C$ such that

$f_b(a) = f(a \otimes b)$. Then, f_b is $\mathbb{Z}$-linear and $\bar{f} : B \to \mathrm{Hom}_{\mathbb{Z}}(A, C) : b \mapsto f_b$ is $\mathbb{Z}$-linear, and hence, $\bar{f} \in \mathrm{Hom}_{\mathbb{Z}}(B, \mathrm{Hom}_{\mathbf{R}}(A, B))$. Define $\tau_{B,C} : f \mapsto \bar{f}$. To show that $\tau_{B,C}$ is bijective, it is sufficient to show that it has an inverse. Let $g : B \to \mathrm{Hom}_{\mathbf{R}}(A, C)$ be a $\mathbb{Z}$-linear mapping. The mapping $A \times B \ni (a, b) \mapsto g(b)(a)$ is $\mathbb{Z}$-bilinear and (section 3.1.1) for all $s \in \mathbf{S}$ $g(b)(a.s) = (s.g(b))(a) = g(s.b)(a)$, so this mapping is $\mathbf{S}$-biadditive. Therefore, there exists a mapping $\tilde{g} \in \mathrm{Hom}_{\mathbb{Z}}(A \bigotimes_{\mathbf{S}} B, C)$ such that, for all $(a, b) \in A \times B$, $\tilde{g}(a \otimes b) = g(b)(a)$, and $\tau^{-1}_{B,C}$ is the mapping $g \longmapsto \tilde{g}$. ■

If $\mathbf{R}$ is a commutative ring, using the previous notation, $s \otimes t$ is $\mathbf{R}$-linear and $\mathfrak{F}_E$ (resp. $\mathfrak{G}_F$) is a covariant (resp. contravariant) functor from the category of $\mathbf{R}$-modules into itself.

(III) TENSOR PRODUCTS OF ALGEBRAS. Let $\mathbf{K}$ be a commutative ring. The algebras considered in this subsection belong to the category $\mathbf{K}$-Alga of associative and unitary $\mathbf{K}$-algebras (section 2.3.10**(I)**).

Let $\mathbf{A}_1, \mathbf{A}_2$ be two algebras, and let $\mathbf{A} = \mathbf{A}_1 \bigotimes \mathbf{A}_2$ be the tensor product of the $\mathbf{K}$-modules $\mathbf{A}_1$ and $\mathbf{A}_2$. This $\mathbf{K}$-module can be made into an algebra by setting, for all $x_i, y_i \in \mathbf{A}_i$ $(i = 1, 2)$,

$$(x_1 \otimes x_2)(y_1 \otimes y_2) = (x_1 y_1) \otimes (x_2 y_2),$$

in which case the identity element of $\mathbf{A}_1 \bigotimes \mathbf{A}_2$ is $e_1 \otimes e_2$, where e_i is the identity element of each $\mathbf{A}_i$.

Let $(\mathbf{A}_i)_{i \in I}$, $I = \{1, ..., n\}$, be a *finite* family of algebras. We define the tensor product $\bigotimes_{i \in I} \mathbf{A}_i$ inductively by setting $\bigotimes_{i=1}^{k} \mathbf{A}_i = \left(\bigotimes_{i=1}^{k-1} \mathbf{A}_i\right) \bigotimes \mathbf{A}_k$ $(k = 2, ..., n)$. Let $\mathbf{A} = \bigotimes_{i \in I} \mathbf{A}_i$ and $u_i : \mathbf{A}_i \to \mathbf{A} : x_i \mapsto \bigotimes_j x'_j$, where $x'_i = x_i$ and $x'_j = e_i$ for $i \neq j$. It can be shown ([BKI 12], Chap. III, section 4.2, Prop. 5) that the u_i are morphisms of $\mathbf{K}$-Alga (called canonical homomorphisms); that if $i \neq j$, the elements $u_i(x_j)$ and $u_j(x_i)$ are permutable in $\mathbf{A}$ for all $x_i \in \mathbf{A}_i, x_j \in \mathbf{A}_j$, and that $\mathbf{A}$ is generated by the union of the subalgebras $u_i(\mathbf{A}_i)$. The tensor product $\bigotimes_{i \in I} \mathbf{A}_i$ has the universal property (**TENSA**) stated below:

(**TENSA**) Let $\mathbf{B}$ be an algebra and, for all $i \in I$, let $v_j : \mathbf{A}_i \to \mathbf{B}$ be a morphism of $\mathbf{K}$-Alga such that if $i \neq j$, then $v_i(x_j)$ and $v_j(x_i)$ are permutable in $\mathbf{A}$ for all $x_i \in \mathbf{A}_i, x_j \in \mathbf{A}_j$; then, there exists a uniquely determined

morphism $w : \mathbf{A} \to \mathbf{B}$ of $\mathbf{K}$-Alga (called the *canonical homomorphism*) such that $v_i = w \circ u_i$ for all $i \in I$.

Now let $(\mathbf{A}_i)_{i \in I}$ be an *arbitrary* family of algebras. Given any *finite* subset J of I, we define $\mathbf{A}_J = \bigotimes_{i \in J} \mathbf{A}_i$, and write $e_J = \bigotimes_{i \in J} e_i$ for its identity element. Let J, J' be finite subsets of I such that $J \subset J'$, and let $w^J_{J'} : \mathbf{A}_J \to \mathbf{A}_{J'}$ be the canonical homomorphism. Let $\mathfrak{P}_f(I)$ be the increasing filtrant set of finite subsets of I. Then, $\mathfrak{D} = \left\{\mathbf{A}_J, w^J_{J'}; \mathfrak{P}_f(I)\right\}$ is a direct system in $\mathbf{K}$-Alga (section 1.2.8(**I**)) (**exercise**) and we define

$$\bigotimes_{i \in I} \mathbf{A}_i = \varinjlim_{J \in \mathfrak{P}_f(I)} \mathbf{A}_J.$$

The tensor product $\bigotimes_{i \in I} \mathbf{A}_i$ has the universal property (**TENSA**), which we stated above in the case where I is finite, and whose statement is identical when I is arbitrary ([BKI 12], Chap. III, section 4.5, Prop. 8).

For example, let $(X_i)_{i \in I}$ be a family of indeterminates. Let $(J_l)_{l \in L}$ be a partition of I (section 1.1.2). By setting $\mathbf{A}_l = \mathbf{K}\left[(X_i)_{i \in J_l}\right]$, we have that $\bigotimes_{l \in L} \mathbf{A}_l = \mathbf{K}\left[(X_i)_{i \in I}\right]$ (section 2.3.9(**I**)).

(IV) TENSOR PRODUCT OF GRADED ALGEBRAS. Let $(\mathbf{A}_i)_{i \in I}$ be a family of graded algebras $\mathbf{A}_i = (\mathbf{A}_{i,n})_{n \in \mathbb{N}}$ (section 2.3.12). Then, $(\mathbf{A}_n)_{n \in \mathbb{N}}$, where $\mathbf{A}_n = \bigotimes_{i \in I} \mathbf{A}_{i,n}$, is a graded algebra, called the *tensor product* of the family $(\mathbf{A}_i)_{i \in I}$.

A graded algebra $\mathbf{A}$ is said to be *anticommutative* if, for any arbitrary non-zero homogeneous elements x_n, x_m of $\mathbf{A}$ with degrees n and m, respectively, we have that $x_n x_m = (-1)^{nm} x_m x_n$. If also $x_n^2 = 0$ for all $x_n \neq 0$, where n is odd, then $\mathbf{A}$ is said to be *alternating*. If 2 is not a zero-divisor of $\mathbf{A}$, the graded algebra $\mathbf{A}$ is alternating if and only if it is anticommutative. If $\mathbf{A}, \mathbf{B}$ are two anticommutative (resp. alternating) graded algebras, we can equip the tensor product of $\mathbf{K}$-modules $\mathbf{A}, \mathbf{B}$ with the structure of an anticommutative (resp. alternating) algebra by setting

$$(x_n \otimes y_p)(x_m \otimes y_q) = (-1)^{pm} (x_n x_m) \otimes (y_p y_q)$$

(**exercise**). This algebra is called the *skew tensor product* of $\mathbf{A}$ and $\mathbf{B}$, and is written $\mathbf{A} \overset{s}{\otimes} \mathbf{B}$. As above, we can define the skew tensor product ${}^{s}\bigotimes_{i \in I} \mathbf{A}_i$

inductively for a finite family of anticommutative (resp. alternating) graded algebras, then for an arbitrary family of such algebras by taking the inductive limit; the graded algebra thus obtained is anticommutative (resp. alternating). The reader can fill in the details of these claims as an **exercise***, referring to ([BKI 12], Chap. III, section 4.8 & 4.9) if they so wish.

(V) FLAT MODULES AND FAITHFULLY FLAT MODULES.

DEFINITION 3.20.– *1) A right* $\mathbf{R}$*-module* $A_{\mathbf{R}}$ *(resp. a left* $\mathbf{R}$*-module* ${}_{\mathbf{R}}B$*) is said to be* flat *if the functor* $A \bigotimes_{\mathbf{R}} -$ *(resp.* $- \bigotimes_{\mathbf{R}} B$*) is exact. In other words, the right* $\mathbf{R}$*-module* $A_{\mathbf{R}}$ *is flat if and only if, for any exact sequence of left* $\mathbf{R}$*-modules*

$$M' \stackrel{v}{\to} M \stackrel{w}{\to} M'', \qquad [3.7]$$

the sequence of $\mathbb{Z}$*-modules*

$$A \bigotimes_{\mathbf{R}} M' \stackrel{\mathrm{id}_A \otimes v}{\longrightarrow} A \bigotimes_{\mathbf{R}} M \stackrel{\mathrm{id}_A \otimes w}{\longrightarrow} A \bigotimes_{\mathbf{R}} M'' \qquad [3.8]$$

is exact.

2) A right $\mathbf{R}$*-module* $A_{\mathbf{R}}$ *(resp. a left* $\mathbf{R}$*-module* ${}_{\mathbf{R}}B$*) is said to be* faithfully flat *if the functor* $A \bigotimes_{\mathbf{R}} -$ *(resp.* $- \bigotimes_{\mathbf{R}} B$*) is both exact and faithful (section 1.2.1(**III**)). In other words, the right* $\mathbf{R}$*-module* A *is faithfully flat if and only if exactness of the sequence [3.7]* is equivalent *to exactness of the sequence [3.8].*

A right $\mathbf{R}$-module $U_{\mathbf{R}}$ is flat if and only if, for any left ideal $\mathfrak{a}$ in $\mathbf{R}$, the canonical mapping $U \otimes \mathfrak{a} \to U$ is injective, so that $U \otimes \mathfrak{a} \cong U\mathfrak{a}$ ([COH 03b], Thm. 4.6.2). If a right $\mathbf{R}$-module $U_{\mathbf{R}}$ is faithfully flat, it is faithful (section 2.3.2(**III**)), but a flat and faithful $\mathbf{R}$-module can fail to be faithfully flat ([LAM 99], p. 150). If a right $\mathbf{R}$-module $U_{\mathbf{R}}$ is flat, it is faithfully flat if and only if the relation $U \bigotimes_{\mathbf{R}} M = 0$, where $M \in {}_{\mathbf{R}}\mathbf{Mod}$ implies that $M = 0$, or alternatively if for every maximal left ideal $\mathfrak{m}$ we have that $U\mathfrak{m} \neq \mathfrak{m}$ ([BKI 98], Chap. I, section 3.1, Prop. 1).

A direct sum $U = \bigoplus_{i \in I} U_i$ of right $\mathbf{R}$-modules U_i is a flat module if and only if each U_i is a flat module. If so, if one of the U_i is also faithfully flat, then U is faithfully flat (**exercise**). Since the $\mathbf{R}$-module ${}_{\mathbf{R}}\mathbf{R}$ is faithfully flat, every *free* $\mathbf{R}$-module is *faithfully flat*. Hence, if $U \oplus V$ is a free $\mathbf{R}$-module, U is a flat module, or in other words (see section 3.3.1)

COROLLARY 3.21.– *Every* projective $\mathbf{R}$*-module is* flat.

(VI) EXTENSIONS AND RESTRICTIONS OF THE RING OF SCALARS. Let $\mathbf{R}, \mathbf{S}$ be two rings and let $\rho : \mathbf{R} \to \mathbf{S}$ be a ring homomorphism (which can be but is not necessarily inclusion). The ring $\mathbf{S}$ may be equipped with a canonical $(\mathbf{S}, \mathbf{R})$-bimodule structure ${}_{\mathbf{S}}\mathbf{S}_{\mathbf{R}}$ by writing $sr = s\rho(r)$ $(r \in \mathbf{R}, s \in \mathbf{S})$. The functor

$$\rho^* = S \bigotimes_{\mathbf{R}} - : {}_{\mathbf{R}}\mathbf{Mod} \to {}_{\mathbf{S}}\mathbf{Mod}$$

is a right-exact covariant functor, called *extension of the ring of scalars*.

Any left $\mathbf{S}$-module M has a canonical left $\mathbf{R}$-module structure $\rho_*(M)$, where $\rho_* : {}_{\mathbf{S}}\mathbf{Mod} \to {}_{\mathbf{R}}\mathbf{Mod}$ is a forgetful functor (section 1.3.1**(I)**), called *restriction of the ring of scalars*: $\rho_*(M)$ is the abelian group M for which only left-multiplication by the elements $\rho(r), r \in \mathbf{R}$ is allowed. The functor ρ_* is exact and faithful (**exercise**) and the pair of functors (ρ_*, ρ^*) is adjoint (section 1.2.9): see ([BLS 11], Prop. 557).

3.1.6. *Generators and relations*

(I) Let $\mathbf{A}$ be a ring. An $\mathbf{A}$-module M is generated by the family $(\mathbf{w}_j)_{j\in K}$ if and only if every element of M is a linear combination $\sum_{j\in K} \lambda^j.\mathbf{w}_j$, where $(\lambda^j)_{j\in K}$ is a family of elements of $\mathbf{A}$ with finite support. This is equivalent to saying that there exists an $\mathbf{A}$-linear surjection $\varphi : \mathbf{A}^{1\times(K)} \to M$ such that $\varphi(\varepsilon_j) = \mathbf{w}_j$, where $(\varepsilon_j)_{j\in K}$ is the *canonical basis* of $\mathbf{A}^{1\times(K)}$ (ε_j is the family $\left(\delta_j^l\right)_{l\in K}$, where δ_j^l is the Kronecker delta). This gives

LEMMA 3.22.– *Every* $\mathbf{A}$*-module is the quotient of a free module, and more precisely is the quotient of a copower* $\mathbf{A}^{1\times(K)}$ *(section 1.2.6**(II)**) of* ${}_{\mathbf{A}}\mathbf{A}$.

Note that, in general, not every group is the quotient of a free group (section 2.2.1**(IV)**), unless it is abelian. The property stated in lemma 3.22 *is not* the universal property of a free object (section 1.3.4).

(II) If $(\mu_i)_{i\in Q}$ is a generating family of $\ker(\varphi) \subset \mathbf{A}^{1\times(K)}$, then there exists an $\mathbf{A}$-linear surjection $\beta : \mathbf{A}^{1\times(Q)} \to U := \ker(\varphi)$ such that $\beta(\zeta_i) = \mu_i$, where $(\zeta_i)_{i\in Q}$ is the canonical basis of $\mathbf{A}^{1\times(Q)}$. By setting $f = \beta \circ \iota$, where

$\iota : U \to \mathbf{A}^{1\times(K)}$ is inclusion, we obtain the exact sequence (section 3.1.4**(I)**) and the following isomorphism:

$$\mathbf{A}^{1\times(Q)} \xrightarrow{f} \mathbf{A}^{1\times(K)} \xrightarrow{\varphi} M \to 0, \qquad [3.9]$$

$$\boxed{M \cong \operatorname{coker}(f)}.$$

We call $\mathbf{A}^{1\times(K)}$ a *module of generators* and $f\left(\mathbf{A}^{1\times(Q)}\right)$ a *module of relations* of M (these are not uniquely determined by M). The exact sequence [3.9] is called a *presentation* of M. We can identify arbitrary elements $x \in \mathbf{A}^{1\times(Q)}$ and $y \in \mathbf{A}^{1\times(K)}$ with the rows $\mathbf{x}$ and $\mathbf{y}$ that represent them with respect to the *canonical bases* (section 3.1.3**(II)**, and **(I)** above), thus giving an $\mathbf{A}$-linear mapping $f : \mathbf{A}^{1\times(Q)} \to \mathbf{A}^{1\times(K)}$ with representative matrix $R = \operatorname{Mat}(f) \in \mathbf{A}^{Q\times(K)}$ with respect to these bases (definition 3.2). The matrix R is called a *definition matrix* (or *presentation matrix*) of M. This leads to

LEMMA 3.23.– *The mapping*

$$\operatorname{Hom}_{\mathbf{A}}\left(\mathbf{A}^{1\times(Q)}, \mathbf{A}^{1\times(K)}\right) \to \mathbf{A}^{Q\times(K)} : f \mapsto \operatorname{Mat}(f) \qquad [3.10]$$

is a canonical $\mathbb{Z}$*-linear bijection.*

With this notation, $\zeta_i.R$ is the i-th row of R and the mapping f such that $R = \operatorname{Mat}(f)$ is given by $\bullet R : x \mapsto x.R$ (right-multiplication by R). Writing $\mathbf{w}$ for the *column* with j-th element $\mathbf{w}_j = \varphi(\varepsilon_j)$, we obtain $0 = (\varphi \circ f)(x) = \varphi(\zeta_i R) = \varphi\left(\sum_{j\in K} r_i^j.\varepsilon_j\right) = \sum_{j\in K} r_i^j.\mathbf{w}_j$, or in other words $R.\mathbf{w} = 0$. This equality represents the module M (generated by $(\mathbf{w}_j)_{j\in J}$, which we will write as $M = [\mathbf{w}]_{\mathbf{A}}$) with respect to the bases ζ, ε, since

$$\boxed{M = [\mathbf{w}]_{\mathbf{A}} \text{ where } \mathbf{w} \text{ satisfies the single condition } R.\mathbf{w} = 0}. \qquad [3.11]$$

(III) The module M is *finitely generated* if and only if $\operatorname{Card}(K) = k < \infty$, and we say that it is *finitely related* if $\operatorname{Card}(Q) = q < \infty$. The module M is said to be *finitely presented* if $\operatorname{Card}(K) < \infty$ and $\operatorname{Card}(Q) < \infty$. If so, it has a finite definition matrix with dimensions $q \times k$. With these conventions, we can therefore write the exact sequence [3.9] in the form

$$\mathbf{A}^{1\times q} \xrightarrow{\bullet R} \mathbf{A}^{1\times k} \xrightarrow{\text{can}} M \to 0$$

where $\bullet R$ is right-multiplication by R and can is the canonical epimorphism.

(IV) FITTING'S THEOREM. For $i = 1, 2$, let $M_i = \mathbf{A}^{1\times(K_i)}/U_i$ be an $\mathbf{A}$-module, where $U_i \subseteq \mathbf{A}^{1\times(K_i)}$. Consider the following diagram (all arrows of which will be explained):

$$\begin{array}{ccccccc}
0 & \longrightarrow & U_1 & \xrightarrow{\subseteq} & \mathbf{A}^{1\times(K_1)} & \xrightarrow{\text{can}} & M_1 \longrightarrow 0 \\
 & & \downarrow f|_{U_1} & & \downarrow f & & \downarrow \bar{f} \\
0 & \longrightarrow & U_2 & \xrightarrow{\subseteq} & \mathbf{A}^{1\times(K_2)} & \xrightarrow{\text{can}} & M_2 \longrightarrow 0 \\
 & & \downarrow g|_{U_2} & & \downarrow g & & \downarrow \bar{g} \\
0 & \longrightarrow & U_1 & \xrightarrow{\subseteq} & \mathbf{A}^{1\times(K_1)} & \xrightarrow{\text{can}} & M_1 \longrightarrow 0
\end{array}$$

Consider the first two rows. By theorem-definition 2.11, every homomorphism $\bar{f} : M_1 \to M_2$ is induced by some homomorphism $f = (\bullet P) : \mathbf{A}^{1\times(K_1)} \to \mathbf{A}^{1\times(K_2)}$ such that $U_1 P \subseteq U_2$, where $P \in \mathbf{A}^{K_1\times(K_2)}$. We therefore have that $f|_{U_1} : U_1 \to U_2$. The diagram formed by the first two rows therefore commutes, and each row is exact. Furthermore, $\bar{f} = 0$ if and only if $\forall x \in \mathbf{A}^{1\times(K_1)}, f(x) \in U_2$, that is, $\mathbf{A}^{1\times(K_1)} P \subseteq U_2$. Hence, there exists a canonical $\mathbb{Z}$-linear isomorphism from $\mathrm{Hom}_{\mathbf{A}}(M_1, M_2)$ to

$$\left\{P \in \mathbf{A}^{K_1\times(K_2)} : U_1 P \subseteq U_2\right\} / \left\{P \in \mathbf{A}^{K_1\times(K_2)} : \mathbf{A}^{1\times(K_1)} P \subseteq U_2\right\}. \quad [3.12]$$

THEOREM 3.24.– *Let $M_i = \mathbf{A}^{1\times(K_i)}/U_i$ $(i = 1, 2)$ be $\mathbf{A}$-modules. The $\mathbb{Z}$-module $\mathrm{Hom}_{\mathbf{A}}(M_1, M_2)$ is canonically isomorphic to [3.12]. The homomorphism $(\bullet P)_{ind} : \mathbf{A}^{1\times(K_1)}/U_1 \to \mathbf{A}^{1\times(K_2)}/U_2$ induced by $(\bullet P) : \mathbf{A}^{1\times(K_1)} \to \mathbf{A}^{1\times(K_2)}$ is an isomorphism if and only if there exists $(\bullet Q)_{ind} = (\bullet P)_{ind}^{-1} : \mathbf{A}^{1\times(K_2)}/U_2 \to \mathbf{A}^{1\times(K_1)}/U_1$, and this condition is satisfied by $Q \in \mathbf{A}^{K_2\times(K_1)}$ if and only if*

$$U_2 Q \subseteq U_1, \quad \mathbf{A}^{1\times(K_1)}(PQ - I_{K_1}) \subseteq U_1, \quad \mathbf{A}^{1\times(K_2)}(QP - I_{K_2}) \subseteq U_2. \quad [3.13]$$

PROOF.– Consider the final two rows of the diagram. As above, every homomorphism $\bar{g} : M_2 \to M_1$ is induced by some homomorphism

$g = (\bullet Q) : \mathbf{A}^{1\times(K_2)} \to \mathbf{A}^{1\times(K_1)}$, where $Q \in \mathbf{A}^{K_2\times(K_1)}$ and $U_2Q \subseteq U_1$. Thus, the whole diagram commutes, and each row is exact. Furthermore, $\bar{g}$ is a retraction of $\bar{f}$ (section 1.1.1(**III**)) if and only if $\bar{g} \circ \bar{f} = \mathrm{id}_{M_1}$, or in other words if $\forall x \in \mathbf{A}^{1\times(K_1)}, \pi_1(xPQ) = \pi_1(x)$, where $\pi_1 : \mathbf{A}^{1\times(K_1)} \twoheadrightarrow M_1$ is the canonical epimorphism. This condition is equivalent to $\mathbf{A}^{1\times(K_1)}(PQ - I_{K_1}) \subseteq U_1$, where I_{K_1} is the identity matrix of dimensions $\mathrm{Card}(K_1) \times \mathrm{Card}(K_1)$. ■

COROLLARY 3.25.– *(Fitting [FIT 36]) Let* $\mathbf{A}$ *be a weakly finite ring (definition 3.5), and let* $A_i \in \mathbf{A}^{r_i\times k_i}$ $(i = 1, 2)$ *be left-regular matrices (section 2.1.1(**II**)). The following conditions are equivalent:*

i) $\mathrm{coker}(\bullet A_1) \cong \mathrm{coker}(\bullet A_2)$;

ii) There exists a matrix $\begin{bmatrix} A_1 & * \\ * & * \end{bmatrix}$ *with inverse* $\begin{bmatrix} * & * \\ * & A_2 \end{bmatrix}$;

iii) A_1 *and* A_2 *are* stably associated*, which means that (by definition)* $\mathrm{diag}(A_1, I_{m_2})$ *is associated with* $\mathrm{diag}(I_{m_1}, A_2)$ *in* $\mathfrak{M}_{m_1+m_2}(\mathbf{A})$.

PROOF.– (i)⇒(ii): Writing $U_i = \mathbf{A}^{1\times r_i}A_i$, the condition $U_1P \subseteq U_2$, and the three conditions stated in [3.13], are respectively equivalent to $A_1P = BA_2$, $A_2Q = CA_1$, $PQ - I = DA_1$, $QP - I = EA_2$, where B, C, D, E are matrices of suitable dimensions with entries in $\mathbf{A}$. These conditions imply the existence of matrices X_1, X_2, Y_1, Y_2 with entries in A, satisfying

$$\begin{bmatrix} -D & P \\ -C & A_2 \end{bmatrix}\begin{bmatrix} A_1 & -B \\ Q & -E \end{bmatrix} = \begin{bmatrix} I & Y_1 \\ 0 & Y_2 \end{bmatrix}, \begin{bmatrix} A_1 & -B \\ Q & -E \end{bmatrix}\begin{bmatrix} -D & P \\ -C & A_2 \end{bmatrix} = \begin{bmatrix} X_1 & 0 \\ X_2 & I \end{bmatrix}$$

from which we deduce that

$$\begin{bmatrix} -D & P \\ -C & A_2 \end{bmatrix}\begin{bmatrix} A_1 & -B \\ Q & -E \end{bmatrix}\begin{bmatrix} -D & P \\ -C & A_2 \end{bmatrix} = \begin{bmatrix} I & Y_1 \\ 0 & Y_2 \end{bmatrix}\begin{bmatrix} -D & P \\ -C & A_2 \end{bmatrix}$$
$$= \begin{bmatrix} -D & P \\ -C & A_2 \end{bmatrix}\begin{bmatrix} X_1 & 0 \\ X_2 & I \end{bmatrix},$$

hence $Y_2 = I$, $Y_1 = 0$. Since $\mathbf{A}$ is weakly finite, we also have that $X_1 = I$ and $X_2 = 0$. The converse is immediate.

(ii)⇔(iii): **exercise***; see ([COH 85], Sect. 0.6, Thm. 6.2). ■

The isomorphism between $\mathrm{Hom}_{\mathbf{A}}(M_1, M_2)$ and the set of matrices [3.12] is only *canonical* because the modules M_1, M_2 are defined as quotients of *copowers* of ${}_{\mathbf{A}}\mathbf{A}$. If these modules were defined as quotients of free modules, this isomorphism would depend on the choice of bases (see corollary 3.3). Similarly, there exists a $\mathbb{Z}$-linear bijection between the morphisms of free modules and matrices (definition 3.2), but it is not canonical (compare with lemma 3.23). Nevertheless, any quotient of free modules is a quotient of copowers of ${}_{\mathbf{A}}\mathbf{A}$ up to isomorphism, and the converse also holds.

3.1.7. *Modules over Noetherian rings*

A left $\mathbf{A}$-module M is said to be *left Noetherian* if every ascending sequence of submodules is stationary. This is equivalent to saying that every submodule of M is finitely generated (**exercise***: see [BKI 12], Chap. VIII, section 1.1, Prop. 2). The ring $\mathbf{A}$ is left Noetherian (section 2.3.4(**I**)) if and only if the $\mathbf{A}$-module ${}_{\mathbf{A}}\mathbf{A}$ is left Noetherian. Given the short exact sequence of left $\mathbf{A}$-modules

$$0 \to N \to M \to M/N \to 0,$$

M is left Noetherian if and only if N and M/N are both left Noetherian (**exercise***; see [BKI 12], Chap. VIII, section 1.1, Prop. 3). If M is a left $\mathbf{A}$-module and $(N_i)_{i\in I}$ is a *finite* family of submodules, all of which are Noetherian, then $N = \sum_{i\in I} N_i$ is Noetherian.

LEMMA 3.26.– *Let $\mathbf{A}$ be a left Noetherian ring. Then, the $\mathbf{A}$-module M is Noetherian if and only if it is finitely generated.*

PROOF.– This is a necessary condition, by the above. If the ring $\mathbf{A}$ is Noetherian, then for any integer n the free module $\mathbf{A}^{1\times n} = \bigoplus_{i=1}^{n} N_i$, where $N_i = {}_{\mathbf{A}}\mathbf{A}$ for all $i = 1, ..., n$, is Noetherian. Any finitely generated $\mathbf{A}$-module is the quotient of a free module $\mathbf{A}^{1\times n}$ (lemma 3.22), and is therefore Noetherian. ■

THEOREM 3.27.– *If the ring $\mathbf{A}$ is left Noetherian or is a semifir (theorem-definition 3.14), then every finitely generated left $\mathbf{A}$-module is finitely presented.*

PROOF.– Consider the presentation [3.9] of M with $\mathrm{Card}(K) = k < \infty$. Then, $\ker(\varphi) \subset \mathbf{A}^{1\times(K)}$ is finitely generated, so is a quotient of $\mathbf{A}^{1\times(Q)}$, where $\mathrm{Card}(Q) = q < \infty$. ■

THEOREM 3.28.– *i) If M, N are left $\mathbf{A}$-modules, $N \neq 0$, and if there exists a monomorphism $M \oplus N \hookrightarrow M$, then M is not Noetherian.*

ii) Every left Noetherian ring $\mathbf{A}$ is weakly finite. In particular, division rings are weakly finite, and so have the IBN property.

PROOF.– i) If there exists a monomorphism $M \oplus N \hookrightarrow M$, we have that $M_1 \oplus N_1 \subseteq M$ with $M_1 \cong M$ and $N_1 \cong N$. Hence, there exists a monomorphism $M \oplus N \hookrightarrow M_1$, and M_1 contains a submodule $M_2 \oplus N_2$, where $M_2 \cong M$ and $N_2 \cong N$, so $M_2 \oplus N_1 \oplus N_2 \subseteq M$. Continuing this construction, we obtain an infinite direct sum $N_1 \oplus N_2 \oplus ...$ contained in M with $N_i \cong N \neq 0$, so M is not Noetherian. ii) follows from (i) and from lemma 3.26. Division rings are Noetherian rings. ■

COROLLARY 3.29.– *Let $\mathbf{K}$ be a division ring.*

i) Every subspace F of a $\mathbf{K}$-vector space E is a direct factor of E, and we have that

$$\boxed{\dim(F) + \dim(E/F) = \dim(E)}.$$

ii) In particular, Grassmann's formula holds for the vector subspaces of a given space:

$$\boxed{\dim_{\mathbf{K}}(V) + \dim_{\mathbf{K}}(W) = \dim_{\mathbf{K}}(V+W) + \dim_{\mathbf{K}}(V \cap W)}. \quad [3.14]$$

PROOF.– Since E/F is free, i) follows from corollary 3.16 and from [3.2]; ii) follows from (i) and from the exactness of the sequence

$$0 \to V \cap W \to V \oplus W \to V + W \to 0.$$ ■

3.1.8. $\mathfrak{m}$-adic completion

(I) Let $\mathbf{R}$ be a ring and $\mathfrak{m}$ a two-sided ideal in $\mathbf{R}$. Define $\psi_i^j : \mathbf{R}/\mathfrak{m}^j \to \mathbf{R}/\mathfrak{m}^i : x + \mathfrak{m}^j \mapsto x + \mathfrak{m}^i$. This ring homomorphism is well-defined for $j \geq i$, and $\mathfrak{I} = \left\{\mathbf{R}/\mathfrak{m}^i, \psi_i^j; \mathbb{N}\right\}$ is an inverse system (section 1.2.8(**II**)). The projective limit

$$\hat{\mathbf{R}} = \varprojlim \mathbf{R}/\mathfrak{m}^i$$

is called the Hausdorff *completion* of $\mathbf{R}$ with respect to the $\mathfrak{m}$-adic topology.

This terminology can be explained as follows: the countable family $\left(\mathfrak{m}^i\right)_{i\in\mathbb{N}}$ is a filter base in $\mathbf{R}$ ([BKI 71], Chap. I, section 6.3; [P2], section 2.2.1), which defines the so-called $\mathfrak{m}$-adic topology on $\mathbf{R}$, henceforth written as $\mathfrak{T}(\mathfrak{m})$. The countable family $\left(\mathfrak{m}^i\right)_{i\in\mathbb{N}}$ is a fundamental system of neighborhoods of 0 in $\mathfrak{T}(\mathfrak{m})$. The topology $\mathfrak{T}(\mathfrak{m})$ is therefore characterized by the convergence of its sequences, and a sequence (x_n) in $\mathbf{R}$ converges to 0 in $\mathfrak{T}(\mathfrak{m})$ if and only if, for all $i \in \mathbb{N}$, there exists $n \in \mathbb{N}$ such that, $\forall k \geq n$, $x_k \in \mathfrak{m}^i$. If $\mathbf{R}$ is equipped with $\mathfrak{T}(\mathfrak{m})$, the two operations $(x, y) \mapsto x + y$ and $(x, y) \mapsto xy$ from $\mathbf{R} \times \mathbf{R}$ into $\mathbf{R}$, and the operation $x \mapsto -x$ from $\mathbf{R}$ into $\mathbf{R}$, are continuous (**exercise**), so $(\mathbf{R}, \mathfrak{T}(\mathfrak{m}))$ is a topological ring ([BKI 71], Chap. III, section 6.3). The ring $\hat{\mathbf{R}}$ is the Hausdorff completion ([BKI 71], Chap. III, section 6.5; [P2], section 2.4.4) of this ring. The topology $\mathfrak{T}(\mathfrak{m})$ is Hausdorff (section 2.3.3(**III**)) if and only if $\bigcap_{i\geq 1} \mathfrak{m}^i = (0)$, in which case $\mathbf{R}$ may be identified with a subring of its $\mathfrak{m}$-adic completion $\hat{\mathbf{R}}$.

(II) Now let M be an $\mathbf{R}$-module. For $j \geq i$, we have $\mathfrak{m}^j M \subseteq \mathfrak{m}^i M$, so there exists an $\mathbf{R}$-linear mapping $M/\mathfrak{m}^j M \to M/\mathfrak{m}^i M$, which allows us to take the projective limit

$$\hat{M} = \varprojlim M/\mathfrak{m}^i M$$

called the Hausdorff completion of M with respect to the $\mathfrak{m}$-adic topology. This set $\hat{M}$ has a canonical $\left(\hat{\mathbf{R}}, \mathbf{R}\right)$-bimodule structure. We have that $\widehat{\mathfrak{m}^n} = (\widehat{\mathfrak{m}})^n = \mathfrak{m}^n.\hat{\mathbf{R}}$ for every integer $n > 0$, and the topology of $\hat{\mathbf{R}}$ is the $\widehat{\mathfrak{m}}$-adic topology ([BKI 98], Chap. III, section 2.12, Cor. 2). With this notation, the following result can be shown ([ATI 69], Prop. 10.13 & 10.14, & Thm. 10.17):

THEOREM 3.30.– *Let $\mathbf{R}$ be a commutative Noetherian ring.*

1) There is a canonical isomorphism of $\hat{\mathbf{R}}$-modules $\hat{M} \cong \hat{\mathbf{R}} \bigotimes_{\mathbf{R}} M$ and $\hat{\mathbf{R}}$ is a flat $\mathbf{R}$-module.

2) Let M be a finitely generated $\mathbf{R}$-module. We have

$$\ker\left(M \to \hat{M}\right) = \bigcap\nolimits_{n\geq 1} \mathfrak{m}^n M = \{x \in M, \exists \lambda \in 1 + \mathfrak{m} : \lambda x = 0\}$$

(Krull's intersection theorem). In particular, setting $M = {}_{\mathbf{R}}\mathbf{R}$, we see that the $\mathfrak{m}$-adic topology of $\mathbf{R}$ is Hausdorff in both of the following two cases, implying that $\mathbf{R} \subseteq \hat{\mathbf{R}}$:

i) $\mathbf{R}$ is entire and $\mathfrak{m}$ is a proper ideal.

ii) $\mathbf{R}$ *is local and* $\mathfrak{m}$ *is its maximal ideal. In the latter case,* $\hat{\mathbf{R}}$ *is local and* $\hat{\mathfrak{m}}$ *is its maximal ideal.*

The proof of the following result is an **exercise**:

LEMMA 3.31.– *Let* $\mathbf{K}$ *be a commutative ring and define* $\mathfrak{m} = (X_1, ..., X_n)$. *The Hausdorff completion of* $\mathbf{R} = \mathbf{K}[X_1, ..., X_n]$ *with respect to the* $\mathfrak{m}$*-adic topology (section 3.1.8(**I**)) is* $\hat{\mathbf{R}} = \mathbf{K}[[X_1, ..., X_n]]$.

3.1.9. *Ring of fractions*

(I) COMMUTATIVE CASE. Let $\mathbf{A}$ be a commutative ring and let $S \subset \mathbf{A}$ be a *multiplicative set*, that is, a submonoid of $(\mathbf{A}, \times)$ (section 2.1.1**(I)**). We define the set $\mathbf{A}S^{-1}$ of fractions r/s, where $r \in \mathbf{A}$ and $s \in S$. We must also specify when the equality $r/s = r'/s'$ should hold, which is non-trivial when S contains non-regular elements. The relation $\mathcal{R}$ defined on $\mathbf{A} \times S$ by

$$(r, s)\, \mathcal{R}\, (r', s') \Leftrightarrow \exists t \in S : t\,(s'r - sr') = 0$$

is an equivalence relation, and the quotient set (section 1.1.2) $(\mathbf{A} \times S)/\mathcal{R}$ has a canonical ring structure (**exercise**). The ring is written as $\mathbf{A}S^{-1}$, and we have that $SS^{-1} \subset \mathbf{U}\left(\mathbf{A}S^{-1}\right)$. The ring homomorphism $\lambda_S : \mathbf{A} \to \mathbf{A}S^{-1} : r \mapsto r/1$ satisfies

$$\ker(\lambda_S) = \{r \in \mathbf{A}, \exists t \in S : tr = 0\}. \qquad [3.15]$$

Note that SS^{-1} might be a strict subset of $\mathbf{U}\left(\mathbf{A}S^{-1}\right)$. For example, if $\mathbf{A} = \mathbb{Z}$ and $S = {}^2\mathbb{Z}^\times$ is the set of non-zero squares in $\mathbb{Z}$, we have that $2/4 \in \mathbf{A}S^{-1}$ and $(2/4)(2/1) = 4/4 = 1/1$, so $2/4 \in \mathbf{U}\left(\mathbf{A}S^{-1}\right)$ but $2/4 \notin SS^{-1}$. We also have that $0 \in S \Longleftrightarrow \ker(\lambda_S) = \mathbf{A} \Longleftrightarrow \mathbf{A}S^{-1} = 0$.

(II) NON-COMMUTATIVE CASE. When $\mathbf{A}$ is a non-commutative ring, we must take additional precautions ([BLS 11], section 2.5.2). First, we need to distinguish between left fractions $s^{-1}r$ and right fractions rs^{-1}. Consider the case of left fractions. The relation $\mathcal{R}$ stated above is no longer an equivalence relation, and must be replaced with the relation $\mathcal{R}'$ defined by

$$(r, s)\, \mathcal{R}'\, (r', s') \Leftrightarrow \exists q, q' \in \mathbf{A} : qr = q'r' \;\&\; qs = q's' \in S.$$

In order to define the ring of left fractions, we therefore need to assume that the following two conditions are satisfied:

$$(\forall r \in \mathbf{A})\,(\forall s \in S) : Sr \cap \mathbf{A}s = \varnothing, \qquad [3.16]$$

$$(\forall r \in \mathbf{A})\,[(\exists s \in S)\,(rs = 0) \Rightarrow (\exists t \in S)\,(tr = 0)]\,. \qquad [3.17]$$

A multiplicative set satisfying the condition [3.16] is called a *left Ore set*, and a multiplicative set satisfying the conditions [3.16] and [3.17] is called a *left denominator set* (if every element of S is regular, the condition [3.17] is automatically satisfied). Conversely, if S is a left denominator set, the quotient set $(\mathbf{A} \times S)/\mathcal{R}'$ may be canonically equipped with a ring structure whose elements are the left fractions $s^{-1}r$. This ring is written as $S^{-1}\mathbf{A}$, and in the case where $\mathbf{A}$ is commutative, this definition coincides with the one given above (**exercise**).

The kernel of the ring homomorphism $\lambda_S : r \mapsto 1^{-1}r$ is once again given by [3.15]. The elements $s_1, ..., s_n \in S$ have a common left multiple s (section 2.1.1(**II**)) that belongs to S, say $s = q_1 s_1 = ... = q_n s_n$, so the left fractions $s_i^{-1} r_i = s^{-1} q_i r_i$ $(i = 1, ..., n)$ can be reduced to the same denominator. Any two left fractions $s^{-1}r$ and $s'^{-1}r'$ can be multiplied together as follows: since S is a left Ore set, there exist $s'_1 \in S, r'_1 \in \mathbf{A}$ such that $s'_1 r = r'_1 s'$, so

$$\left(s^{-1}r\right)\left(s'^{-1}r'\right) = s^{-1}s_1'^{-1}s'_1 r s'^{-1}r' = \left(s'_1 s\right)^{-1}\left(r'_1 r'\right).$$

Let S be a left denominator set in the ring $\mathbf{A}$. If $\mathfrak{a}$ is a left ideal in $\mathbf{A}$, it immediately follows that $S^{-1}\mathfrak{a} := \left\{s^{-1}a : s \in S, a \in \mathfrak{a}\right\}$ is a left ideal in $S^{-1}\mathbf{A}$. If S is a *denominator set*, every left fraction $s^{-1}r$ can be rewritten in the form of a right fraction $r's'^{-1}$, and $S^{-1}\mathbf{A} = \mathbf{A}S^{-1}$.

THEOREM 3.32.– *Let* $\mathbf{A}$ *be a ring and* $S \subset \mathbf{A}$ *a right denominator set. Then,* $\mathbf{B} = \mathbf{A}S^{-1}$ *is a flat left* $\mathbf{A}$*-module.*

PROOF.– It is sufficient to show that, for every right ideal $\mathfrak{a}$ in $\mathbf{A}$, the mapping $\varphi : \mathfrak{a} \otimes \mathbf{B} \to \mathbf{B}$ is injective (section 3.1.5(**V**)). Each element $z \in \mathfrak{a} \otimes \mathbf{B}$ is of the form $\sum_i a_i \otimes b_i, a_i \in \mathfrak{a}, b_i \in \mathbf{B}$, where the sum has finitely many terms. The b_i are right fractions that can be assumed to be reduced to the same denominator, so $b_i = c_i s^{-1}$ and $z = c \otimes s^{-1}$ with $c \in \mathfrak{a}$. Thus, $\varphi(z) = cs^{-1}$. If $\varphi(z) = 0$, there exists $t \in S$ such that $ct = 0$, which implies that $z = ct \otimes t^{-1}s^{-1} = 0$.■

If $\mathfrak{b} \lhd_r \mathbf{B}$, with $\mathbf{B} = \mathbf{A}S^{-1}$, write $\mathfrak{b} \cap \mathbf{A} := \{r \in \mathbf{A} : r/1 \in \mathfrak{b}\}$. Then, $\mathfrak{b} = (\mathfrak{b} \cap \mathbf{A})\,\mathbf{B}$, and $\mathfrak{b} \cap \mathbf{A} \lhd_r \mathbf{A}$ (**exercise**). Therefore, if $\mathfrak{b} \cap \mathbf{A}$ is a finitely generated (resp. monogenous) right ideal in $\mathbf{A}$, then $\mathfrak{b}$ is a finitely generated (resp. monogenous) right ideal in $\mathbf{B}$, which implies

COROLLARY 3.33.– *If the ring $\mathbf{A}$ is right Noetherian (resp. simple right Artinian, resp. a right Bézout domain, resp. a principal right ideal ring, resp. a principal right ideal domain), then so is $\mathbf{A}S^{-1}$.*

By a similar approach, we can construct the group of fractions of a non-commutative monoid ([COH 85], Sect. 0.8). The classical (commutative) example of this is the construction of $\mathbb{Z}$ from $\mathbb{N}$.

(III) MODULES OVER RINGS OF FRACTIONS. Let $\mathbf{A}$ be a ring, M a left $\mathbf{A}$-module, $S \subset \mathbf{A}$ a left denominator set and $\mathbf{B} = S^{-1}\mathbf{A}$. Since $\mathbf{B}$ is a $(\mathbf{B}, \mathbf{A})$-bimodule (section 3.1.1), we can take the tensor product $M_S := \mathbf{B} \bigotimes_{\mathbf{A}} M$ (section 3.1.5**(I)**), which is a left $\mathbf{B}$-module. The proof of the following result is an **exercise*** in the case where $\mathbf{A}$ is a commutative ring ([ATI 69], Chap. 3; [BKI 98], Chap. II, section 2.5, Prop. 11):

THEOREM 3.34.– *1) Let $\mathfrak{a}, \mathfrak{b}$ be ideals in $\mathbf{A}$. We have that*

$$S^{-1}(\mathfrak{a} + \mathfrak{b}) = S^{-1}\mathfrak{a} + S^{-1}\mathfrak{b}, \quad S^{-1}(\mathfrak{a} \cap \mathfrak{b}) = S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b},$$
$$S^{-1}(\mathfrak{a}\mathfrak{b}) = \left(S^{-1}\mathfrak{a}\right)\left(S^{-1}\mathfrak{b}\right),$$

and the first two equalities also hold when $\mathfrak{a}, \mathfrak{b}$ are submodules of an $\mathbf{A}$-module M.

2) There is a bijection $\left(\mathfrak{p} \mapsto S^{-1}\mathfrak{p}\right)$ between the prime ideals $\mathfrak{p}$ in $\mathbf{A}$ (section 2.3.3), which do not meet S and the prime ideals in $S^{-1}\mathbf{A}$. This correspondence is also a bijection between the ideals in $\mathbf{A}$ maximal among those which do not meet S and the maximal ideals in $S^{-1}\mathbf{A}$. This implies that $\mathfrak{N}\left(S^{-1}\mathbf{A}\right) = S^{-1}\mathfrak{N}(\mathbf{A})$, where $\mathfrak{N}$ is the nilradical (section 2.3.6). In particular, if $\mathbf{A}$ is reduced (definition 2.43), then $S^{-1}\mathbf{A}$ is reduced.

(IV) TORSION. Let $\mathbf{A}$ be a ring and let $S \subset \mathbf{A}$ be a left denominator set. Consider the so-called *canonical* $\mathbf{A}$-linear mapping $\tau_S : M \to \rho_*(M_S)$, where $\rho : \mathbf{A} \to \mathbf{B}$ is inclusion and ρ_* is restriction of the ring of scalars (section 3.1.5**(VI)**). We have that

$$\boxed{\mathcal{T}_S(M) := \ker(\tau_S) = \{x \in M, \exists t \in S : tx = 0\}}$$

(**exercise**). The $\mathbf{A}$-module $\mathcal{T}_S(M)$ is called the *S-torsion submodule* of M. Noether's first isomorphism theorem (theorem 2.12(1)) therefore implies that $M/\mathcal{T}_S(M) \cong \tau_S(M)$. If $\mathcal{T}_S(M) = 0$, the module $M \cong \tau_S(M)$ is said to be *S-torsion-free*. Every free module is S-torsion-free with respect to any left denominator set S. Every submodule or quotient of an S-torsion module is an S-torsion module. The module $\mathbf{B}_\mathbf{A} = S^{-1}\mathbf{A}$ is flat, so the functor $\mathbf{B} \bigotimes_\mathbf{A} - : {}_\mathbf{A}\mathbf{Mod} \to {}_\mathbf{B}\mathbf{Mod}$ is right-exact (**exercise**).

3.1.10. *Division rings of fractions*

(I) Every entire commutative ring has a field of fractions $\mathrm{Q}(\mathbf{A})$. For example, if $\mathbf{K}$ is a field and $(X_i)_{i\in I}$ is a family of indeterminates, the field of fractions of the polynomial ring $\mathbf{K}\left[(X_i)_{i\in I}\right]$ (section 2.3.9**(I)**) is the field of rational fractions $\mathbf{K}\left((X_i)_{i\in I}\right)$. The field of fractions of the ring of formal power series in a single indeterminate $\mathbf{K}[[X]]$ is the field of formal Laurent series $\mathbf{K}((X))$: every element of $\mathbf{K}((X))$ may be uniquely written in the form $a = \sum_i a_i X^i$, where i is allowed to take negative values (compare with [2.23])[3].

(II) In the case of non-commutative rings, an additional condition is required. A ring $\mathbf{A}$ is said to be a *left* Ore domain if it is entire and $\mathbf{A}^\times = \complement_\mathbf{A}\{0\}$ is a left Ore set. In this case, by setting $S = \mathbf{A}^\times$, $\mathrm{Q}(\mathbf{A}) = S^{-1}\mathbf{A}$ is a division ring, called the division ring of left fractions of $\mathbf{A}$; $\mathcal{T}_S(M)$ is called the *torsion submodule* of M and is written as $\mathcal{T}(M)$; the $\mathbf{A}$-module M is said to be *torsion-free* if $\mathcal{T}(M) = 0$. If $\mathbf{A}$ is an Ore domain and the $\mathbf{A}$-module M is flat (section 3.1.5**(V)**), then, for all $a \in \mathbf{A}^\times$, the multiplication $M \to M : m \mapsto am$ is injective (**exercise**), and therefore M is torsion-free. In the case of an $\mathbf{A}$-module, if $\mathbf{A}$ is an Ore domain, we therefore have that

$$\text{free} \Rightarrow \text{projective} \Rightarrow \text{flat} \Rightarrow \text{torsion-free}.$$

THEOREM 3.35.– *Every entire ring is either a left Ore domain, or contains free ideals of infinite rank (lemma-definition 3.7). In particular, every entire left Noetherian ring is a left Ore domain.*

PROOF.– Let $\mathbf{A}$ be an entire ring that is not a left Ore domain, and let $a, b \in \mathbf{A}^\times$ such that $\mathbf{A}a \cap \mathbf{A}b = 0$. Then, $\mathbf{A}a \cap \mathbf{A}ab^i \subseteq \mathbf{A}a \cap \mathbf{A}b = 0$ for all $i \geq 1$,

3 The study of the field of fractions of the ring of power series in several indeterminates is much more difficult [MON 13].

and, for all $n > m$, $\mathbf{A}a \cap \mathbf{A}ab^{n-m} = 0$, so $\mathbf{A}ab^m \cap \mathbf{A}ab^n = 0$. Therefore, the sum $\mathfrak{a}_n = \sum_{0 \leq i \leq n} \mathbf{A}ab^i$ is a direct sum. Furthermore, $\mathbf{A} \to \mathbf{A}ab^i : x \mapsto xab^i$ is an isomorphism, so $\mathfrak{a}_n$ is free of rank n. Since $\mathfrak{a}_n \subsetneq \mathfrak{a}_{n+1}$, $\bigcup_{n \geq 0} \mathfrak{a}_n$ is a free left ideal of infinite rank. ■

By this result and by theorem 3.28(ii), we deduce

COROLLARY 3.36.– *Every left Ore domain is weakly finite.*

LEMMA 3.37.– *Let $M \in {}_{\mathbf{A}}\mathbf{Mod}$. Then, $\dim_{\mathbf{K}}(\mathbf{K} \bigotimes_{\mathbf{A}} M)$ is the cardinal of a maximal free subset of M.*

DEFINITION 3.38.– *Let $\mathbf{A}$ be a left Ore domain and $\mathbf{K} = \mathrm{Q}(\mathbf{A})$.*

i) Let M be an $\mathbf{A}$-module. The cardinal $\dim_{\mathbf{K}}(\mathbf{K} \bigotimes_{\mathbf{A}} M)$ is called the rank *of the $\mathbf{A}$-module M and is written as $\mathrm{rk}_{\mathbf{A}}(M)$.*

ii) Let M, N be two $\mathbf{A}$-modules and let $f : M \to N$ be a homomorphism. Then, the cardinal $\mathrm{rk}_{\mathbf{A}}(\mathrm{im}(f))$ is called the rank *of f and is written as $\mathrm{rk}_{\mathbf{A}}(f)$.*

When $\mathbf{A}$ is implicit, we write rk *instead of* $\mathrm{rk}_{\mathbf{A}}$.

REMARK 3.39.– *Consider an $\mathbf{A}$-module, where $\mathbf{A}$ is a left Ore domain.*

1) The notion of rank given in definition 3.38(i) coincides with the one given in lemma-definition 3.7 when M is a free module. An $\mathbf{A}$-module is a torsion module if and only if it has rank zero.

*2) Let $\mathbf{A}$ be a left Ore domain, let M, N be free $\mathbf{A}$-modules of rank q and k respectively, let $f : M \to N$ be a homomorphism, choose bases of M and N, and let $X \in \mathbf{A}^{q \times k}$ be the representative matrix of f with respect to these bases. By embedding $\mathbf{A}$ into its division ring of left fractions $\mathbf{K}$, we can view X as a subset of $\mathbf{K}^{q \times k}$. Then, $\mathrm{rk}(X)$ (as defined in theorem-definition 2.64) coincides with $\mathrm{rk}_{\mathbf{A}}(f)$ (**exercise**).*

THEOREM 3.40.– *Let $\mathbf{A}$ be a left Ore domain and let M be an $\mathbf{A}$-module.*

1) Suppose that M is finitely generated, and let F be a free submodule of M. Then, M has a free submodule L (not unique in general) such that $L \supseteq F$ and the module M/L is a torsion module.

2) Let $L \subseteq M$ be a free module. The following conditions are equivalent:

i) The module M/L is a torsion module;

ii) $\mathrm{rk}_{\mathbf{A}}(M) = \mathrm{rk}_{\mathbf{A}}(L)$;

iii) L is a maximal free submodule.

PROOF.– 1) Let $B = \{x_1, ..., x_r\}$ $(r \geq 0)$ be a basis of F and let $X \supset B$ be a finite generating set of M. There exists a set $S \supset B$, $S = \{x_1, ..., x_s\}$, with the following property $(\mathbf{L})$:

$(\mathbf{L})$: S is a maximal subset of X such that the $\mathbf{A}$-module $[S]_{\mathbf{A}}$ generated by S is free.

Indeed, if B does not have the property $(\mathbf{L})$, X has an element x_{s+1} such that $[B \cup \{x_{s+1}\}]_{\mathbf{A}}$ is free. If $B \cup \{x_{s+1}\}$ does not have the property $(\mathbf{L})$, there exists an element $x_{s+2} \in X$ such that $[B \cup \{x_{s+1}, x_{s+2}\}]_{\mathbf{A}}$ is free. We thus obtain an ascending sequence (under inclusion) of subsets $S' \supset B$ of X such that $[S']_{\mathbf{A}}$ is free. Since X is finite, the set of the S' has a greatest element, again written as $S = \{x_1, ..., x_s\}$ $(s \geq r)$, which has the property $(\mathbf{L})$. Let $x \in \complement_X S$ and write $L = [S]_{\mathbf{A}} \supseteq F$. The module $[S \cup \{x\}]_{\mathbf{A}} = L + [\{x\}]_{\mathbf{A}}$ is not free, so there exist $a \in \mathbf{A}^{\times}$ and $a_1, ..., a_s \in \mathbf{A}$ such that $ax + \sum_{1 \leq i \leq s} a_i x_i = 0$. Now let $\bar{x}$ be the canonical image of x in M/L. We have that $a\bar{x} = 0$, so $\bar{x}$ is a torsion element, and hence M/L is a torsion module.

2) i)⇒(ii) Let M/L be a torsion module. By exactness of the functor $\mathbf{K} \bigotimes_{\mathbf{A}} -$, the exact sequence $0 \to L \to M \to M/L \to 0$ implies the exact sequence

$$0 \to \mathbf{K} \bigotimes_{\mathbf{A}} L \to \mathbf{K} \bigotimes_{\mathbf{A}} M \to 0 \to 0,$$

so, by corollary 3.29(i), $\mathrm{rk}_{\mathbf{A}}(M) = \mathrm{rk}_{\mathbf{A}}(L)$.

(ii)⇒(iii) Suppose that L is free and $\mathrm{rk}_{\mathbf{A}}(M) = \mathrm{rk}_{\mathbf{A}}(L)$. If $L' \supsetneq L$ is a free submodule of M, we have that $\mathrm{rk}_{\mathbf{A}}(L') > \mathrm{rk}_{\mathbf{A}}(L)$: contradiction.

(iii)⇒(i) Let L be a maximal free submodule of M and let $s = \mathrm{rk}_{\mathbf{A}}(L)$. The proof of (1) with $F = \{0\}$ shows that M/L is a torsion module. ■

Note that, unlike the situation in lemma 3.37, the assumption that M has a finite generating set plays an essential role in part (1) of the above theorem. For example, every $\mathbb{Z}$-module $\frac{1}{n}\mathbb{Z}$ $(n \geq 1)$ is free, and the set of these modules forms a lattice (since $\frac{1}{m}\mathbb{Z} \subseteq \frac{1}{n}\mathbb{Z} \Leftrightarrow m \mid n$) but the $\mathbb{Z}$-module $\mathbb{Q} = \bigcup_{n\geq 1} \frac{1}{n}\mathbb{Z}$ is not free and does not contain any maximal free $\mathbb{Z}$-module. The reader might wish to show the following result as an **exercise*** ([BKI 12], Chap. II, section 7.10):

LEMMA 3.41.– *Let* $\mathbf{A}$ *be a left Ore domain.*

1) For every exact sequence of $\mathbf{A}$*-modules*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'',$$

setting $f_{\mathcal{T}} = f\big|_{\mathcal{T}(M')}$ *and* $g_{\mathcal{T}} = g\big|_{\mathcal{T}(M)}$ *yields the following exact sequence of* $\mathbf{A}$*-modules*

$$0 \to \mathcal{T}\left(M'\right) \xrightarrow{f_{\mathcal{T}}} \mathcal{T}\left(M\right) \xrightarrow{g_{\mathcal{T}}} \mathcal{T}\left(M''\right).$$

2) Let $(M_i)_{i\in I}$ *be a family of* $\mathbf{A}$*-modules. Then,*

$$\mathcal{T}\left(\bigoplus\nolimits_{i\in I} M_i\right) = \bigoplus\nolimits_{i\in I} \mathcal{T}\left(M_i\right).$$

We have the following result ([GEN 60], Prop. 4.1):

LEMMA 3.42.– *(Gentile) Let* $\mathbf{A}$ *be a left Ore domain. The following conditions are equivalent:*

i) Every finitely generated torsion-free $\mathbf{A}$*-module* M *satisfies the following property (**G**):*

*(**G**): There exists a monomorphism* $M \hookrightarrow L$*, where* L *is a finitely generated free* $\mathbf{A}$*-module.*

ii) $\mathbf{A}$ *is a (left* and right*) Ore domain.*

If $\mathbf{A}$ is a left Ore domain and S is a left denominator set (section 3.1.9**(II)**), $S^{-1}\mathbf{A}$ may be identified with a subring of $\mathrm{Q}\left(\mathbf{A}\right)$ containing $\mathbf{A}$.

(III) There exist commutative Bézout domains that are not principal ideal domains (section 2.3.8**(III)**,**(IV)**), for example, the ring $\mathcal{O}\left(\mathbb{C}\right)$ of entire

functions. These rings are not Noetherian (theorem 2.56). Bézout domains may be characterized as follows:

LEMMA 3.43.– *Let* $\mathbf{A}$ *be a ring. The following conditions are equivalent:*

i) $\mathbf{A}$ *is a left Bézout domain;*

ii) $\mathbf{A}$ *is a left Ore domain in which every finitely generated left ideal is free of rank 1;*

iii) $\mathbf{A}$ *is a left Ore domain and a semifir.*

PROOF.– (i)⇒(ii) Let $\mathbf{A}$ be a left Bézout domain and let $\mathfrak{a} \neq 0$ be a finitely generated left ideal. Then $\mathfrak{a}$ is principal, so there exists $y \in \mathfrak{a}$ such that $\mathfrak{a} = \mathbf{A}y$, and hence $x \mapsto xy$ is an isomorphism from $\mathbf{A}$ onto $\mathfrak{a}$. Therefore, $\mathfrak{a}$ is free of rank 1. If $\mathbf{A}$ is not an Ore domain, the ideal $\mathfrak{a}_n$ in the proof of theorem 3.35 is free of rank n: contradiction.

(ii)⇒(iii) this is clear. (iii)⇒(i) Let $\mathbf{A}$ be a semifir. The left ideal $\mathbf{A}x + \mathbf{A}y \subseteq \mathbf{A}$ is free. If $\mathbf{A}$ is also a left Ore domain, then it has the IBN property, and so the left $\mathbf{A}$-modules $\mathbf{A}x + \mathbf{A}y$ and $\mathbf{A}$ are of rank 1, meaning that there exists z such that $\mathbf{A}x + \mathbf{A}y = \mathbf{A}z$, and $\mathbf{A}$ is a left Bézout domain. ■

(IV) VARIATIONS ON EXACT SEQUENCES.

THEOREM 3.44.– *Let* $\mathbf{A}$ *be a ring, and consider the sequence [3.18] below, where* $R_1 \in \mathbf{A}^{s\times q}$, $R_2 \in \mathbf{A}^{q\times k}$, *letting* $M_1 = \operatorname{coker}(\bullet R_1)$*:*

$$0 \longleftarrow \mathbf{A}^{1\times k} \xleftarrow{\bullet R_2} \mathbf{A}^{1\times q} \xleftarrow{\bullet R_1} \mathbf{A}^{1\times s}. \qquad [3.18]$$

i) The sequence [3.18] is exact if and only if R_2 *is left-invertible.*

ii) Suppose that $\mathbf{A}$ *is either left Noetherian or is a semifir*[4]*. Given* $R_2 \in \mathbf{A}^{q\times k}$*, there exists an integer* s *and a matrix* $R_1 \in \mathbf{A}^{s\times q}$ *such that the sequence [3.18] is exact at* $\mathbf{A}^{1\times q}$ *(section 2.2.2).*

iii) Given $R_1 \in \mathbf{A}^{s\times q}$*, there exists a matrix* $R_2 \in \mathbf{A}^{q\times k}$ *such that the sequence [3.18] is exact (resp. is exact at* $\mathbf{A}^{1\times q}$*) if and only if* $M_1 \cong \mathbf{A}^{1\times k}$ *(resp. there exists a monomorphism* $M_1 \hookrightarrow \mathbf{A}^{1\times k}$*; in other words, if and only if the property (***G***) in lemma 3.42 is satisfied).*

4 The notion of *coherent ring* allows us to combine these two cases ([BLS 11], Thm. 514).

PROOF.– i) Let $f_1 := (\bullet R_1)$ and $f_2 := (\bullet R_2)$. If the sequence [3.18] is exact, we have that $\mathbf{A}^{1\times q}/\ker(f_2) \cong \mathbf{A}^{1\times k}$ by Noether's first isomorphism theorem (theorem 2.12(1)), so $\ker(f_2) = \mathrm{im}(f_1)$ is a direct factor of $\mathbf{A}^{1\times q}$; since f_2 is surjective, it has a linear section $s : \mathbf{A}^{1\times k} \hookrightarrow \mathbf{A}^{1\times q}$ (lemma-definition 3.15). Let $S = \mathrm{Mat}(s)$. Since $f_2 \circ s = \mathrm{id}_k$, we have that $SR_2 = I_k$. The converse is obvious.

ii) The $\mathbf{A}$-module $\ker(\bullet R_2)$ is finitely generated. Let R_1 be a matrix whose rows form a finite generating set of $\ker(\bullet R_2)$. Then, the sequence [3.18] is exact at $\mathbf{A}^{1\times q}$.

iii) 1) If the sequence [3.18] is exact at $\mathbf{A}^{1\times q}$, then by theorem-definition 2.11, there exists an induced mapping $(\bullet R_2)_{ind}$ that is injective. 2) Conversely, consider the exact sequence

$$0 \longleftarrow M_1 \xleftarrow{\varphi_1} \mathbf{A}^{1\times q} \xleftarrow{\bullet R_1} \mathbf{A}^{1\times s}.$$

If there exists a monomorphism $\iota_1 : M_1 \hookrightarrow \mathbf{A}^{1\times k}$, let $f_2 = \iota_1 \circ \varphi_1 : \mathbf{A}^{1\times q} \to \mathbf{A}^{1\times k}$ and $R_2 = \mathrm{Mat}(f_2)$. Then, the sequence [3.18] is exact at $\mathbf{A}^{1\times q}$. 3) If $M_1 \cong \mathbf{A}^{1\times k}$, ι_1 is an isomorphism, so f_2 is surjective, and the sequence [3.18] is exact. Conversely, if [3.18] is exact, $(\bullet R_2)_{ind}$ is an isomorphism and $M_1 \cong \mathbf{A}^{1\times k}$. ■

(V) FRACTIONAL IDEALS.

DEFINITION 3.45.– *Let* $\mathbf{A}$ *be a left Ore domain, and let* $\mathbf{K}$ *be its division ring of left fractions. A left* fractional $\mathbf{A}$-ideal $\mathfrak{b}$ *is a submodule of the left* $\mathbf{A}$*-module* $\mathbf{K}$ *such that there exist* $v, v' \in \mathbf{K}^\times$ *satisfying* $\mathfrak{b}v \subseteq \mathbf{A} \subseteq v'\mathfrak{b}$. *We can similarly define right fractional ideals, and two-sided fractional ideals.*

When talking about fractional ideals, it can be helpful to use the term *integral ideal* when referring to the usual meaning of the term ideal, to avoid ambiguity.

DEFINITION 3.46.– *Let* $\mathbf{A}$ *be an Ore domain and let* $\mathfrak{b}$ *be a fractional* $\mathbf{A}$*-ideal. We say that* $\mathfrak{b}$ *is* invertible *if there exists a fractional* $\mathbf{A}$*-ideal* $\mathfrak{c}$ *such that* $\mathfrak{b}\mathfrak{c} = \mathfrak{c}\mathfrak{b} = \mathbf{A}$. *If so, we write that* $\mathfrak{c} = \mathfrak{b}^{-1}$.

3.1.11. *Polynomial rings and skew Laurent polynomials*

(I) The skew polynomials and skew Laurent polynomials studied in this subsection were investigated by H. Poincaré (1884), A. Loevy (1903) and, most importantly, Ø. Ore [ORE 33] (1933). We will introduce this concept with a series of examples:

1) The $\mathbb{C}$-vector space $\mathbb{C}(t)$ of rational functions $t \mapsto f(t)$ with complex values may be equipped with a left $\mathbb{C}[X]$-module structure by writing $X.f := df/dt = \dot{f}$ $(f \in \mathbb{C}(t))$.

2) The $\mathbb{C}$-vector space $\mathbb{C}(t)$ may also be equipped with a left $\mathbb{C}[Y]$-module structure by writing $(Y.f)(t) = f(t+1)$.

1') Let $\mathbf{K} = \mathbb{C}[t]$, $a \in \mathbf{K}$ and $f \in \mathbb{C}(t)$. We have that $(d/dt)(af) = \dot{a}f + a\dot{f}$. With the same conventions as in (1), we can write $X.(af) = aX.f + \dot{a}f = (aX + \dot{a})f$. Let δ be the derivation of $\mathbf{K}$ in the $\mathbf{K}$-module $\mathbf{K}$ (definition 2.68) defined by $\delta(a) = \dot{a}$, which therefore satisfies the Leibniz rule

$$\delta(ab) = a\delta(b) + \delta(a)b. \qquad [3.19]$$

This gives $X.af = (aX + \delta(a))f$, which allows us to equip the abelian group $\mathbf{K}[X] := \bigoplus_{i\geq 0} \mathbf{K}X^i$ with the following rule, called a *commutation rule*

$$Xa = aX + \delta(a). \qquad [3.20]$$

2') Once again choosing $\mathbf{K} = \mathbb{C}[t]$, $a \in \mathbf{K}$, $f \in \mathbb{C}(t)$, with the same conventions as in (2), we can write $Y.(af) = \sigma(a)Y.f$, where $\sigma : \mathbf{K} \to \mathbf{K}$ is the *automorphism* (bijective endomorphism) defined by $\sigma(a)(t) = a(t+1)$, which allows us to equip the abelian group $\mathbf{K}[Y]$ with the commutation rule

$$Ya = \sigma(a)Y. \qquad [3.21]$$

Setting $X = Y - 1$, we thus obtain $Xa = \sigma(a)X + \sigma(a) - a$, and thus

$$\boxed{Xa = \sigma(a)X + \delta(a)} \qquad [3.22]$$

where $\delta(a) := \sigma(a) - a$. For $a, b \in \mathbf{K}$, we therefore have $\delta(ab) = \sigma(ab) - ab = \sigma(a)\sigma(b) - ab = \sigma(a)\sigma(b) - \sigma(a)b + \sigma(a)b - ab$, which implies

that

$$\boxed{\delta(ab) = \sigma(a)\,\delta(b) + \delta(a)\,b}. \qquad [3.23]$$

The relation [3.23] is a generalization of the Leibniz rule [3.19] and [3.22] is a generalization of [3.20]. The endomorphism δ of the additive group $\mathbf{K}$ defined by [3.23] is a derivation (definition 2.68) of the ring $\mathbf{K}$ in the $(\mathbf{K}, \mathbf{K})$-bimodule obtained by equipping the additive group $\mathbf{K}$ with the left action $(a, x) \mapsto \sigma(a)\,x$ and the right action $(a, x) \mapsto xa$.

DEFINITION 3.47.– *Let* $\mathbf{K}$ *be a ring,* σ *an endomorphism of* $\mathbf{K}$ *and* δ *the endomorphism of the additive group* $\mathbf{K}$ *defined by [3.23]. Then,* δ *is called a* σ-derivation *of* $\mathbf{K}$.

We have that $\sigma(1) = 1$ and $\delta(1) = 0$. If the ring $\mathbf{K}$ is commutative, a σ-derivation is said to be *inner* if there exists $m \in \mathbf{K}$ such that $\delta(x) = m(\sigma(x) - 1), \forall x \in \mathbf{K}$, and *outer* if it is not inner. In case (1') above, the derivation is outer, and in case (2'), it is inner. It can be shown ([COH 03b], section 7.3) that there exists a unique ring structure on the abelian ring $\mathbf{K}[X] := \bigoplus_{i \geq 0} \mathbf{K}X^i$ satisfying the relation [3.22], and this ring is denoted by $\mathbf{K}[X; \sigma, \delta]$. Every non-zero element of $\mathbf{K}[X; \sigma, \delta]$ may be uniquely written in the form

$$f = a_0 + a_1 X + ... + a_n X^n, \quad a_n \neq 0 \qquad [3.24]$$

which is called a *left skew polynomial* (since the coefficients are on the left of the indeterminate) and the *degree* of f is defined by $d^\circ(f) = n$ if $f \neq 0$, $d^\circ(0) = -\infty$. This skew polynomial is said to be *unitary* if $a_n = 1$. We have that $d^\circ(f - g) \leq \max\{d^\circ(f), d^\circ(f)\}$. The ring $\mathbf{K}[X; \sigma, \delta]$ is called the *ring of left skew polynomials* with respect to the σ-derivation δ. If $\mathbf{K}$ is entire, we have that $d^\circ(fg) = d^\circ(f) + d^\circ(f)$ and $\mathbf{K}[X; \sigma, \delta]$ is entire. If σ is an *automorphism* of $\mathbf{K}$ (which we will assume throughout the following), with inverse $-\beta$, by setting $\varepsilon = \delta \circ \beta$, the relations [3.23] and [3.22] are, respectively, equivalent to

$$\varepsilon(a'b') = a'\varepsilon(b) + \varepsilon(a')\,\beta(b') \text{ and } a'X = X\beta(a') + \varepsilon(a')$$

where $a' = \sigma(a), b' = \sigma(b)$, so ε is a β-derivation of $\mathbf{K}$ and the element f defined by [3.24] may be uniquely written in the form of a *right* skew polynomial

$$f = a'_0 + Xa'_1 + ... + X^n a'_n, \quad a'_0 = a_0, a'_n \neq 0.$$

THEOREM 3.48.– *Let* $\mathbf{K}$ *be a left (resp. right) Noetherian ring, let* σ *be an* automorphism *of* $\mathbf{K}$ *and let* δ *be a* σ*-derivation of* $\mathbf{K}$*. Then, the ring* $\mathbf{K}[X;\sigma,\delta]$ *is left (resp. right) Noetherian.*

PROOF.– Suppose that $\mathbf{K}$ is right Noetherian and let $\mathbf{A} = \mathbf{K}[X;\sigma,\delta]$. If $\mathbf{A}$ is not right Noetherian, there exists a right ideal $\mathfrak{a}$ in $\mathbf{A}$ that is not finitely generated (section 2.3.4(**I**)). Let $f_1 \in \mathfrak{a}$ be a skew polynomial of minimal degree. If $f_1, ..., f_k \in \mathfrak{a}$, we can choose a skew polynomial f_{k+1} of minimal degree from $\mathfrak{C}_{\mathfrak{a}}\left(\sum_{i=1}^{k} f_i\mathbf{A}\right)$, which allows us to construct an infinite sequence $(f_i)_{i\geq 1}$. Let $n_i = d^\circ(f_i)$ and let a_i be the coefficient of its highest-degree term. We will show that $a_1\mathbf{K} \subsetneq a_1\mathbf{K} + a_2\mathbf{K} \subsetneq ...$ is an infinite chain, which contradicts the fact that $\mathbf{K}$ is right Noetherian. If this chain is finite, there exists k such that $a_{k+1}\mathbf{K} \subseteq a_1\mathbf{K} + ... + a_k\mathbf{K}$ and there exist elements $b_j \in \mathbf{K}$ $(1 \leq j \leq k)$ such that $a_{k+1} = \sum_{1\leq j\leq k} a_j b_j$. Thus,

$$g = f_{k+1} - \sum\nolimits_{j=1}^{k} f_j \sigma^{-n_j}(b_j)\, X^{n_{k+1}-n_j} \in \mathfrak{C}_{\mathfrak{a}}\left(\sum\nolimits_{i=1}^{k} f_i\mathbf{A}\right)$$

with $d^\circ(g) < d^\circ(f_{k+1})$: contradiction. ■

When $\sigma = 1$ (resp. $\delta = 0$, resp. $\sigma = 1$ and $\delta = 0$), the ring $\mathbf{K}[X;\sigma,\delta]$ is written as $\mathbf{K}[X;\delta]$ (resp. $\mathbf{K}[X;\sigma]$, resp. $\mathbf{K}[X]$). In the case where $\sigma = 1$ and $\delta = 0$, we deduce the following result by induction, known as *Hilbert's basis theorem* (or the *Basissatz* in the original German):

COROLLARY 3.49.– *(*Basissatz*) If* $\mathbf{K}$ *is a commutative Noetherian ring, the polynomial ring* $\mathbf{K}[X_1, ..., X_n]$ *is Noetherian.*

COROLLARY 3.50.– *If* $\mathbf{K}$ *is a commutative Noetherian ring, the ring* $\mathbf{R}$ *of formal power series* $\mathbf{K}[[X_1, ..., X_n]]$ *(section 2.3.9(**II**)) is Noetherian and is a flat* $\mathbf{K}$*-module.*

PROOF.– The proof of the fact that the ring $\mathbf{K}[[X_1, ..., X_n]]$ is Noetherian is similar to the proof of theorem 3.48 (**exercise***: see [LAN 99], Chap. IV, Thm. 9.4). By theorem 3.30 and lemma 3.31, $\mathbf{K}[[X_1, ..., X_n]]$ is a flat $\mathbf{R}$-module, where $\mathbf{R} = \mathbf{K}[X_1, ..., X_n]$. The ring $\mathbf{R}$ is a free $\mathbf{K}$-module, and hence is a flat $\mathbf{K}$-module. Since both of the functors $\hat{\mathbf{R}} \bigotimes_{\mathbf{R}} -$ and $\mathbf{R} \bigotimes_{\mathbf{K}} -$ are exact, their composition $\hat{\mathbf{R}} \bigotimes_{\mathbf{K}} -$ is also exact. Hence, $\mathbf{K}[[X_1, ..., X_n]]$ is a flat $\mathbf{K}$-module. ■

(II) Let σ be an automorphism of a ring $\mathbf{K}$. The set $S = \{Y^m : m \geq 1\}$ is a denominator set of $\mathbf{K}[Y;\sigma]$ (**exercise**) and the ring $S^{-1}\mathbf{K} = \mathbf{K}S^{-1}$ is written as $\mathbf{K}\left[Y, Y^{-1};\sigma\right]$. Every non-zero element of $\mathbf{K}\left[Y, Y^{-1};\sigma\right]$ may be written in the form

$$f = (a_0 + a_1X + ... + a_nX^n)\, X^{-m} = X^{-m}\left(a'_0 + Xa'_1 + ... + X^n a'_n\right)$$

where $a_0, a'_0, a_n, a'_n \neq 0$. We call $\mathbf{K}\left[Y, Y^{-1};\sigma\right]$ the ring of *skew Laurent polynomials* with respect to the automorphism σ. If $\mathbf{K}$ is a left Noetherian ring, then $\mathbf{K}\left[Y, Y^{-1};\sigma\right]$ is left Noetherian by theorem 3.48 and corollary 3.33. To avoid complicating the notation, the ring $\mathbf{K}$ is assumed to be commutative in the following (which is only slightly restrictive in practice; the general case is discussed in [MCC 01]).

THEOREM 3.51.– *Let* $\mathbf{K}$ *be a commutative ring.*

1) Let δ *be an outer derivation and suppose that* $\mathbf{A} = \mathbf{K}[X;\delta]$. *The ring* $\mathbf{A}$ *is simple (section 2.3.5**(III)**) if and only if* $\mathbf{K}$ *does not have a proper ideal that is* δ*-stable.*

2) Let σ *be an automorphism of* $\mathbf{K}$ *and* $\mathbf{T} = \mathbf{K}\left[Y, Y^{-1};\sigma\right]$. *The ring* $\mathbf{T}$ *is simple if and only if* $\sigma^N \neq \mathrm{id}_{\mathbf{K}}, \forall N \geq 1$.

PROOF.– (1) If $\mathbf{K}$ has a proper ideal $\mathfrak{a}$ that is δ-stable, then $\mathbf{A}\mathfrak{a} = \mathfrak{a}\mathbf{A}$ is a proper ideal in $\mathbf{A}$ and $\mathbf{A}$ is not simple. Conversely, suppose that $\mathbf{K}$ does not have a proper ideal that is δ-stable and let $\mathfrak{a} \neq 0$ be a two-sided ideal in $\mathbf{A}$. Let $\mathfrak{a}_n$ be the set of coefficients of the highest-degree terms of the skew polynomials belonging to $\mathfrak{a}$ with degree $\leq n$. Then $\mathfrak{a}_n$ is a δ-stable two-sided ideal in $\mathbf{K}$. (2) see ([MCC 01], 1.8.5). ■

Let $\mathbf{K} = \mathbf{k}[t]$ where $\mathbf{k}$ is a field. The ring $\mathbf{K}[X; d/dt]$ may be identified with the 1st Weyl *algebra* $A_1(\mathbf{k})$ (section 2.3.10**(III)**), since $Xt - tX = (d/dt)(t) = 1$. The ring $\mathbf{k}[t]\left[Y, Y^{-1};\sigma\right]$, where σ is the automorphism of $\mathbf{k}[t]$ defined by $(\sigma f)(t) = f(t+1)$, is written as $A'_1(\mathbf{k})$. The ring $\mathbf{k}(t)[X; d/dt]$ (where $\mathbf{k}(t)$ is the field of rational fractions in the indeterminate t) is written as $B_1(\mathbf{k})$. Since the ring $\mathbf{k}$ is Noetherian, $A_1(\mathbf{k})$ and $A'_1(\mathbf{k})$ are Noetherian.

COROLLARY 3.52.– *If the field* $\mathbf{k}$ *has characteristic* 0 *(section 2.3.5**(I)**), the rings* $A_1(\mathbf{k})$ *and* $A'_1(\mathbf{k})$ *are simple.*

PROOF.– 1) $A_1(\mathbf{k})$ is simple: the derivation $\delta = d/dt$ of $\mathbf{k}[t]$ is outer. Suppose that there exists a proper ideal $\mathfrak{a}$ in $\mathbf{k}[t]$ that is δ-stable. Let $f = \sum_{i=0}^{n} f_i t^i \in \mathfrak{a}$ where $f_n \neq 0$. Then, $\delta^n(f) = f_n n! \neq 0$ and $f_n n! \in \mathfrak{a}$. But $f_n n! \in \mathbf{U}(\mathbf{k}[t])$, so $\mathfrak{a} = \mathbf{k}[t]$: contradiction.

2) The proof of the simplicity of $A_1'(\mathbf{k})$ is similar. ■

REMARK 3.53.– *It can also be shown that when* $\mathbf{k}$ *is a field with characteristic* 0, *the* n*-th Weyl algebra* $A_n(\mathbf{k})$ *(section 2.3.10**(III)**) is an entire simple Noetherian ring ([MCC 01], 1.3.5).*

When $\mathbf{k}$ is a field of arbitrary characteristic, the ring $B_1(\mathbf{k})$ is simple. The following result also holds (**exercise**)

THEOREM 3.54.– *Let* $\mathbf{K}$ *be a field, let* σ *be an automorphism of* $\mathbf{K}$ *and let* δ *be a* σ*-derivation of* $\mathbf{K}$. *Then, the degree* $d^\circ : f \mapsto d^\circ(f)$ *is a strictly left and right Euclidean function (section 2.3.8**(V)**) on* $\mathbf{K}[X;\sigma,\delta]$, *which is therefore a Euclidean domain. It follows from corollary 3.33 that the ring* $\mathbf{K}\left[Y, Y^{-1};\sigma\right]$ *is a principal ideal domain.*

3.2. Notions of commutative algebra

3.2.1. *Localization at a prime ideal*

(I) Let $\mathbf{A}$ be a *commutative* ring and let $\mathfrak{p}$ be a prime ideal in $\mathbf{A}$. The set $S = \mathbf{A} - \mathfrak{p} = \complement_{\mathbf{A}}\mathfrak{p}$ is multiplicative. We write $\mathbf{A}_\mathfrak{p} := \left(\complement_{\mathbf{A}}\mathfrak{p}\right)^{-1}\mathbf{A}$.

THEOREM 3.55.– *i) The ring* $\mathbf{A}_\mathfrak{p}$ *is local (section 2.3.7), its Jacobson radical is* $\operatorname{rad}(\mathbf{A}_\mathfrak{p}) = \mathfrak{p}\mathbf{A}_\mathfrak{p}$, *and the residue class field* $\kappa(\mathfrak{p})$ *of* $\mathbf{A}_\mathfrak{p}$ *is canonically isomorphic to the field of fractions of* $\mathbf{A}/\mathfrak{p}$.

ii) There is a bijection $\left(P \mapsto \left(\complement_{\mathbf{A}}\mathfrak{p}\right)^{-1}P\right)$ *between the prime ideals* P *in* $\mathbf{A}$ *that* belong to $\mathfrak{p}$ *and the prime ideals in* $\mathbf{A}_\mathfrak{p}$.

PROOF.– i) The elements of $\mathbf{A}_\mathfrak{p}$ are of the form $r/s, s \notin \mathfrak{p}$. The set of elements such that $r \in \mathfrak{p}$ forms an ideal $\mathfrak{m} = \mathfrak{p}\mathbf{A}_\mathfrak{p}$ of $\mathbf{A}_\mathfrak{p}$. If $r/s \notin \mathfrak{m}$, then $r \notin \mathfrak{p}$, so $r \in S$ and $r/s \in \mathbf{U}(\mathbf{A}_\mathfrak{p})$. Hence, if $\mathfrak{a}$ is an ideal in $\mathbf{A}_\mathfrak{p}$ and $\mathfrak{a} \nsubseteq \mathfrak{m}$, this ideal $\mathfrak{a}$ contains a unit of $\mathbf{A}_\mathfrak{p}$ and so is equal to $\mathbf{A}_\mathfrak{p}$. Hence, $\mathfrak{m}$ is the unique maximal ideal in $\mathbf{A}_\mathfrak{p}$, which is therefore local, and $\operatorname{rad}(\mathbf{A}_\mathfrak{p}) = \mathfrak{p}\mathbf{A}_\mathfrak{p}$ by definition 2.48. Let $\varphi : \mathbf{A} \twoheadrightarrow \mathbf{A}/\mathfrak{p}$ be the canonical epimorphism. Then, $\varphi(S)$ is the set

of elements $\neq 0$ in the entire ring $\mathbf{A}/\mathfrak{p}$, whose field of fractions is therefore $\varphi(S)^{-1}(\mathbf{A}/\mathfrak{p}) \cong \left(S^{-1}\mathbf{A}\right) / \left(S^{-1}\mathfrak{p}\right) = \mathbf{A}_{\mathfrak{p}}/(\mathfrak{p}\mathbf{A}_{\mathfrak{p}})$.

ii) follows from theorem 3.34(2). ■

DEFINITION 3.56.– *The ring $\mathbf{A}_{\mathfrak{p}}$ is called the local ring of $\mathbf{A}$ at $\mathfrak{p}$ (or the local ring of $\mathfrak{p}$).*

(II) The ring $\mathbf{A}_{\mathfrak{p}}$ is an $\mathbf{A}$-algebra. Given an $\mathbf{A}$-module M, we define

$$M_{\mathfrak{p}} = \mathbf{A}_{\mathfrak{p}} \otimes_{\mathbf{A}} M.$$

Every element of $M_{\mathfrak{p}}$ is of the form x/s, $x \in M, s \in \complement_{\mathbf{A}}\mathfrak{p}$. The "localization functor" $\mathbf{A}_{\mathfrak{p}} \otimes_{\mathbf{A}} -$ is exact (theorem 3.32). Applying this functor to $\mathbf{A}$ eliminates every ideal that is not contained in $\mathfrak{p}$. However, it still preserves a number of important properties, "localizing" them as shown by the following:

THEOREM 3.57.– *1) Let M be an $\mathbf{A}$-module.* The following conditions are equivalent*:*

i) $M = 0$;

ii) $M_{\mathfrak{p}} = 0$ *for every prime ideal* $\mathfrak{p}$ *in* $\mathbf{A}$;

iii) $M_{\mathfrak{m}} = 0$ *for every maximal ideal* $\mathfrak{m}$ *in* $\mathbf{A}$.

2) Let $f : M \to N$ be an $\mathbf{A}$-homomorphism. The following conditions are equivalent*:*

i') f is injective (resp. surjective);

ii') $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective (resp. surjective) for each prime ideal $\mathfrak{p}$ in $\mathbf{A}$;

iii') $f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective (resp. surjective) for each maximal ideal $\mathfrak{m}$ in $\mathbf{A}$.

PROOF.– 1). Clearly (i)⇒(ii)⇒(iii). If condition (iii) is satisfied and $M \neq 0$, let $0 \neq x \in M$ and $\mathfrak{a} = \mathrm{Ann}^{\mathbf{A}}(x)$ (section 2.3.2**(III)**). The ideal $\mathfrak{a}$ is a proper ideal, and so is contained in a maximal ideal $\mathfrak{m}$ by Krull's theorem (theorem 2.27). Since $M_{\mathfrak{m}} = 0$, we have that $x/1 = 0$ in $M_{\mathfrak{m}}$, and there exists $\lambda \in \complement_{\mathbf{A}}\mathfrak{m}$ such that $\lambda x = 0$, which is impossible since $\mathrm{Ann}^{\mathbf{A}}(x) \subset \mathfrak{m}$.

2) We have that (i')⇒(ii')⇒(iii') since the functor $\mathbf{A}_{\mathfrak{p}} \otimes_{\mathbf{A}} -$ is exact and every maximal ideal is prime. Suppose that $f_{\mathfrak{m}}$ is injective for each maximal ideal $\mathfrak{m}$. Setting $M' = \ker(f)$, the exact sequence

$$0 \to M' \to M \xrightarrow{f} N \to 0$$

implies the exact sequence

$$0 \to M'_{\mathfrak{m}} \to M_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} N_{\mathfrak{m}} \to 0$$

where $M'_{\mathfrak{m}} = 0$, so by (1) $M' = 0$ and f is injective. In the case where $f_{\mathfrak{m}}$ is surjective, the reasoning is the same with the arrows reversed. ■

We deduce (**exercise***: see [ATI 69], Prop. 3.10):

COROLLARY 3.58.– *Let M be an $\mathbf{A}$-module. The following conditions are equivalent:*

i) M is a flat $\mathbf{A}$-module;

ii) $M_{\mathfrak{p}}$ is a flat $\mathbf{A}_{\mathfrak{p}}$-module for each prime ideal $\mathfrak{p}$ in $\mathbf{A}$;

iii) $M_{\mathfrak{m}}$ is a flat $\mathbf{A}_{\mathfrak{m}}$-module for each maximal ideal $\mathfrak{m}$ in $\mathbf{A}$.

THEOREM 3.59.– *Let $\mathbf{A}$ be a ring and $\Omega = \mathrm{Spm}(\mathbf{A})$ its maximal spectrum (definition 2.26).*

i) Let M be a finitely generated $\mathbf{A}$-module. With the notation introduced in theorem 3.55, if $\kappa(\mathfrak{m}) \otimes_{\mathbf{A}} M = 0, \forall \mathfrak{m} \in \Omega$, then $M = 0$.

ii) Suppose that $\mathbf{A}$ is entire. *If M is a torsion-free $\mathbf{A}$-module,*

$$M = \bigcap\nolimits_{\mathfrak{m} \in \Omega} M_{\mathfrak{m}}, \qquad [3.25]$$

and in particular $\mathbf{A} = \bigcap_{\mathfrak{m} \in \Omega} \mathbf{A}_{\mathfrak{m}}$.

PROOF.– i) We have that $\kappa(\mathfrak{m}) = \mathbf{A}_{\mathfrak{m}}/\mathfrak{m}\mathbf{A}_m$ (definition 2.48), so $\kappa(\mathfrak{m}) \otimes_{\mathbf{A}} M = M_{\mathfrak{m}}/\mathfrak{m}M_{\mathfrak{m}}$. If this module is trivial, $M_{\mathfrak{m}} = \mathfrak{m}M_{\mathfrak{m}}$, so $M_{\mathfrak{m}} = 0$ by Nakayama's lemma (lemma 2.41), and (i) follows from theorem 3.57.

ii) If M is a torsion-free module, it may be identified with an $\mathbf{A}$-submodule of $\mathbf{K} \otimes_{\mathbf{A}} M$. Let $x \in \mathbf{K} \otimes_{\mathbf{A}} M$. The set $\mathfrak{b} = \{a \in \mathbf{A} : ax \in M\}$ is an ideal in $\mathbf{A}$. However, $x \in M_{\mathfrak{m}}$ if and only if $x = y/s$, $y \in M$, $s \notin \mathfrak{m}$, which is equivalent to $\mathfrak{b} \not\subseteq \mathfrak{m}$. Therefore, if $x \in M_{\mathfrak{m}}, \forall \mathfrak{m} \in \Omega$, we have that $\mathfrak{b} = \mathbf{A}$ and $x \in M$. ■

3.2.2. *Notions of algebraic geometry and number theory*

(I) AFFINE ALGEBRAIC GEOMETRY. Localization is a special case of a procedure that is common in algebraic geometry, which we will now present briefly. Let $\mathbf{k}$ be a commutative ring, and consider the system of equations

$$f_j(x) = 0 \quad (j \in J) \qquad [3.26]$$

where $f_j \in \mathbf{P}_I := \mathbf{k}\left[(X_i)_{i\in I}\right]$, $x = (x_i)_{i\in I}$ and the x_i $(i \in I)$ are chosen from an associative and commutative $\mathbf{k}$-algebra $\mathbf{K}$. Let $A = \{f_j : j \in J\}$.

DEFINITION 3.60.– *The set* $\mathcal{Z}_A(\mathbf{K}) = \left\{x \in \mathbf{K}^I : g(x) = 0, \forall g \in A\right\}$ *is called the zero set of* A *in* $\mathbf{K}^I$.

The equalities [3.26] are satisfied if and only if, for every polynomial g belonging to the *ideal* $\mathfrak{a}$ in $\mathbf{k}\left[(X_i)_{i\in I}\right]$ generated by the family $(f_j)_{j\in J}$, we have that $g(x) = 0$ (**exercise**), so $\mathcal{Z}_{\mathfrak{a}}(\mathbf{K}) = \mathcal{Z}_A(\mathbf{K})$. It can be very difficult to characterize this set explicitly. One procedure popularized by A. Grothendieck ([GRO 70], Introd.) determines the set of solutions $\mathcal{Z}_{\mathfrak{a}}(\mathbf{K}')$ of [3.26] in an arbitrary "affine space" $\mathbf{K}'^I$ if doing so is easier, where $\mathbf{K}'$ is an (associative and commutative) $\mathbf{k}$-algebra distinct from $\mathbf{K}$, then asks whether this gives at least a partial solution of the initial problem. Recall that the objects of the category $\mathbf{k}$-Algc of associative, unitary and commutative $\mathbf{k}$-algebras are isomorphic to quotients $\mathbf{P}_I/\mathfrak{a}$, where $\mathfrak{a}$ is an ideal in $\mathbf{P}_I$ (section 2.3.10(**IV**)). We have the covariant functor (section 1.2.1(**I**))

$$\mathbb{E}^I : \mathbf{K}' \mapsto \mathbf{K}'^I, \left(u : \mathbf{K}' \to \mathbf{K}''\right) \mapsto \left(u^I : \mathbf{K}'^I \to \mathbf{K}''^I\right)$$

from $\mathbf{k}$-Algc to $\mathbf{Set}$, called the *standard affine space* of type I over $\mathbf{k}$, where

$$u^I : x = (x_i)_{i\in I} \mapsto u^I(x) = (u(x_i))_{i\in I}.$$

Then, $\mathcal{Z}_{\mathfrak{a}} : \mathbf{K}' \mapsto \mathcal{Z}_{\mathfrak{a}}(\mathbf{K}')$ is a *subfunctor* of $\mathbb{E}^I$ (section 1.2.1(**V**)), since if $g(x) = 0$, where $x \in \mathbf{K}'^I$ and $g \in \mathfrak{a}$, then for any morphism $u : \mathbf{K}' \to \mathbf{K}''$ of $\mathbf{k}$-Algc, we have that $g\left(u^I(x)\right) = 0$.

Moreover, for any $\mathbf{k}$-algebra $\mathbf{K}'$, the mapping

$$\mathbb{F}^I\left(\mathbf{K}'\right) : \mathbf{K}'^I \tilde{\to} \mathrm{Hom}_{\mathbf{k}\text{-Algc}}\left(\mathbf{P}_I, \mathbf{K}'\right) : x \mapsto \left(\tilde{x} : x \mapsto g(x), g \in \mathbf{P}_I\right),$$

called the Gelfand transformation, sends $\mathcal{Z}_{\mathfrak{a}}(\mathbf{K}')$ to the elements of $\mathrm{Hom}_{\mathbf{k}\text{-Algc}}(\mathbf{P}_I, \mathbf{K}')$ that are zero in $\mathfrak{a}$, which are in bijection with the elements of $\mathrm{Hom}_{\mathbf{k}\text{-Algc}}(\mathbf{P}_I/\mathfrak{a}, \mathbf{K}')$ (section 2.3.10(**IV**)). We thus obtain a bijection $\mathcal{Z}_{\mathfrak{a}}(\mathbf{K}') \tilde{\to} \mathfrak{X}_{\mathfrak{a}}(\mathbf{K}') := \mathrm{Hom}_{\mathbf{k}\text{-Algc}}(\mathbf{P}_I/\mathfrak{a}, \mathbf{K}')$, which is a functorial bijection in $\mathbf{K}'$, and so a functorial isomorphism

$$\mathcal{Z}_{\mathfrak{a}} \tilde{\to} \mathfrak{X}_{\mathfrak{a}} := \mathrm{Hom}_{\mathbf{k}\text{-Algc}}(\mathbf{P}_I/\mathfrak{a}, -)$$

where $\mathfrak{X}_{\mathfrak{a}} = \mathbf{j}_{\mathbf{A}}$ is the functor represented by the $\mathbf{k}$-algebra $\mathbf{A} = \mathbf{P}_I/\mathfrak{a}$ (1.2.5(**I**)). The functor $\mathfrak{X}_{\mathfrak{a}}$ is called the *affine space* over $\mathbf{k}$ represented by the $\mathbf{k}$-algebra $\mathbf{A}$. The functors $\mathfrak{X}_{\mathfrak{a}}$ are the objects of a category $\mathbf{k}$-**Aff**, called the category of affine spaces over $\mathbf{k}$, and by Yoneda's lemma (lemma 1.18), we have a functorial isomorphism $\mathbf{j}_{\mathbf{k}\text{-Algc}} : (\mathbf{k}\text{-Algc})^{\mathrm{op}} \tilde{\to} \mathbf{k}$-**Aff**. This justifies Grothendieck's claim that "the original goal of the algebraic geometry over $\mathbf{k}$ is precisely equivalent to the study of arbitrary (associative, unitary and commutative) $\mathbf{k}$-algebras $\mathbf{A}$" ([GRO 70], Introd., section 9).

(II) NUMBER THEORY. The system of equations [3.26] is a system of Diophantine equations when $\mathbf{k} = \mathbf{K} = \mathbb{Z}$ and I is finite: $\mathrm{Card}(I) = m$. Hilbert's basis theorem (corollary 3.49) shows that the ideal $\mathfrak{a}$ is finitely generated, so we may assume that J is finite: $\mathrm{Card}(J) = n$. One initial way of simplifying the problem is to embed $\mathbb{Z}$ in its field of fractions $\mathbb{Q}$ and solve [3.26] in $\mathbb{Q}^m$. Another approach, which much like the first is analogous to the algebraic geometry approach described above, is, given a prime number p, to embed $\mathbb{Z}$ in the ring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$ of elements r/s, where $r, s \in \mathbb{Z}$ and s is not a multiple of p. We can then take the quotient of the equations thus obtained by the ideal $\left(p^k\right)$ in the local ring $\mathbb{Z}_{(p)}$ $(k \geq 1)$. Now,

$$\mathbb{Z}_{(p)}/p^k\mathbb{Z}_{(p)} \cong \mathbb{Z}/p^k\mathbb{Z} \qquad [3.27]$$

(**exercise**), so we have reduced to the problem of solving the congruences

$$f_i(x_1, ..., x_m) \equiv 0 \quad \left(\mathrm{mod}.p^k\right) \quad (i = 1, ..., n \quad ; k \geq 1) \qquad [3.28]$$

or alternatively ([BOR 67], section I.5, Thm. 1), by taking the projective limit, that is, by replacing $\mathbb{Z}_{(p)}$ with its p-adic completion (section 3.1.8(**I**)) $\mathbb{Z}_p := \widehat{\mathbb{Z}_{(p)}}$, to the problem of solving the system of equations

$$f_i(\bar{x}_1, ..., \bar{x}_m) = 0 \quad (i = 1, ..., n) \qquad [3.29]$$

where $\bar{x}_j$ is the canonical image of x_j in $\mathbb{Z}_p$. In fact, as shown by K. Hensel, as a result of the exactness of the "p-adic completion" functor (theorem 3.30), the congruences [3.28] have a solution if and only if the system of equations [3.29] has a solution in $\mathbb{Z}_p^m$. We call $\mathbb{Z}_p$ the ring of p-adic integers. The isomorphism [3.27] implies that the ring $\mathbb{Z}_p$ is also the projective limit (up to isomorphism) of the inverse system

$$\left\{\psi_i^j : \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z} \quad (j \geq i)\right\}.$$

Any element $x \in \mathbb{Z}_p$ may be uniquely written as the sum of a convergent series $\sum_{n=0}^{+\infty} x_n p^n$, where x_n is identified with an element of $\mathbb{N}$ such that $0 \leq x_n \leq p-1$. Conversely, all such series converge in $\mathbb{Z}_p$. The ring $\mathbb{Z}_p$ is entire and its field of fractions $\mathbb{Q}_p$ (section 3.1.10**(I)**), called the field of p-adic numbers, is an extension of $\mathbb{Q}$ (section 2.3.5**(II)**).

(III) VALUATIONS. Let $\mathbf{K}$ be a field and let Γ be an abelian subgroup of $\mathbb{R}$ equipped with a total order relation. A *valuation with values in* Γ over $\mathbf{K}$ is a surjection $v : \mathbf{K}^\times \to \Gamma$ such that (i) $v(xy) = v(x) + v(y)$ and (ii) $v(x+y) \geq \min\{v(x), v(y)\}$ for all $x, y \in \mathbf{K}^\times$. We also define $v(0) = +\infty$ with the convention that $v < +\infty, \forall v \in \Gamma$, and $\Gamma_\infty = \Gamma \bigcup \{+\infty\}$. We call Γ the *order* of v. Consider a real number $\rho > 1$. The function $|.| : \mathbf{K} \to \mathbb{R}^+$ defined by $|x| = \rho^{-v(x)}$ if $x \neq 0, |0| = 0$, is an *absolute value*, namely $\forall x, y$, $|x| \geq 0$, $|x| = 0 \Leftrightarrow x = 0$, $|xy| = |x|\,|y|$, $|x+y| \leq |x| + |y|$. This absolute value is *ultrametric* in the sense that, in the case considered here, $|x+y| \leq \max\{|x|, |y|\}$. A field $\mathbf{K}$ equipped with an absolute value is called a *valued field*, and an *ultrametric valued field* if this absolute value is ultrametric. In the latter case, the mapping $d : \mathbf{K} \times \mathbf{K} \to \mathbb{R}^+ : (x, y) \mapsto |x - y|$ is an *ultrametric* distance function, where ultrametric means that, $\forall x, y, z$, $d(x, z) \leq \max\{d(x, y), d(y, z)\}$ (**exercise**). The *trivial valuation* (or *improper valuation*) is the valuation such that $\Gamma = \{0\}$.

Let p be a prime number. Every element $x \in \mathbb{Q}^\times$ may be uniquely written in the form $x = up^{v_p(x)}$ where u is coprime to p and $v_p(x) \in \mathbb{Z}$. The mapping $x \mapsto v_p(x)$ is a discrete valuation on $\mathbb{Q}$, which therefore determines an ultrametric distance function d_p. The completion of $\mathbb{Q}$ with respect to this distance function is $\mathbb{Q}_p$. The residue class field of the valuation v_p is $\mathbb{Z}/p\mathbb{Z}$.

Let $\mathbf{K}$ be a field equipped with a valuation v. The set of elements x such that $v(x) \geq 0$ is a $\mathbf{K}$-algebra $\mathbf{A}$ (**exercise**), called the *valuation ring* of v. The valuation ring of $\mathbb{Q}_p$ is $\mathbb{Z}_p$. When $\Gamma \cong \mathbb{Z}$, the valuation v is said to be *discrete*.

DEFINITION 3.61.– *An entire ring* $\mathbf{A}$ *is called a* valuation ring *if there exists a valuation* v *on its field of fractions such that* $\mathbf{A}$ *is the valuation ring of* v. *If* v *is a discrete valuation,* $\mathbf{A}$ *is called a* discrete valuation ring *(*DVR*).*

Let $\mathbf{A}$ be a valuation ring, $\mathbf{K} = \mathrm{Q}(\mathbf{A})$ and v its valuation; each element $x \in \mathbf{K}^\times$ either satisfies $x \in \mathbf{A}$ or $x^{-1} \in \mathbf{A}$, and $x \in \mathbf{U}(\mathbf{A})$ if and only if $v(x) = 0$. Let $\mathfrak{m}_k := \{x \in \mathbf{A} : v(x) > k\}$ $(k \in \mathbb{N})$. The ring $\mathbf{A}$ is local with unique maximal ideal $\mathfrak{m}_0$. The quotient ring $\mathbf{A}/\mathfrak{m}_0$ is called the *residue class field of the valuation* v and is also written $\mathbf{K}/v$. If v is the trivial valuation, $\mathbf{K}/v = \mathbf{K}$. If the valuation v is *discrete*, the only ideals in $\mathbf{A}$ are the $\mathfrak{m}_k$ $(k \in \mathbb{N})$, and there exists $u \in \mathbf{A}$ such that $\mathfrak{m}_k = \mathbf{A}u^k$ and $v(u) = 1$, so $\mathbf{A}$ is a principal ideal domain; conversely, if $\mathbf{A}$ is Noetherian, the valuation v is discrete ([BKI 98], Chap. V, section 3.6, Prop. 9).

Consider a Laurent series $a = \sum_{i \geq p} a_i X^i \in \mathbf{K}((X))$ where the coefficients a_i are in a field $\mathbf{K}$ and $a_p \neq 0$. The order of a is $v(a) = p$ and $v : \mathbf{K}((X)) \to \mathbb{Z}_\infty$ is a discrete valuation. The corresponding DVR is $\mathbf{K}[[X]]$ (section 2.3.9(**II**)).

3.2.3. Supp *and* Ass

(I) In this subsection, $\mathbf{A}$ is always a commutative ring.

DEFINITION 3.62.– *Let* M *be an* $\mathbf{A}$*-module. We define the* support *of* M, *written* Supp(M), *to be the subset of* Spec$(\mathbf{A})$ *(section 2.3.3(**II**)) consisting of the prime ideals* $\mathfrak{p}$ *such that* $M_\mathfrak{p} \neq 0$.

Krull's theorem (theorem 2.27) and theorem 3.57(2) imply that $M = 0 \Leftrightarrow \mathrm{Supp}(M) = \varnothing$. If $\mathfrak{a}$ is an ideal in $\mathbf{A}$, we have that (**exercise**)

$$\mathrm{Supp}(\mathbf{A}/\mathfrak{a}) = \mathrm{V}(\mathfrak{a}). \qquad [3.30]$$

LEMMA 3.63.– *The support of an* $\mathbf{A}$*-module* M *satisfies the following conditions:*

*i) With the notation of section 2.3.3**(III)**,*

$$\text{Supp}\,(M) = \bigcup_{x \in M} \text{V}\left(\text{Ann}^{\mathbf{A}}\,(x)\right).$$

ii) If M is finitely generated, then

$$\text{Supp}\,(M) = \text{V}\left(\text{Ann}^{\mathbf{A}}\,(M)\right)$$

which is a closed set in $\text{Spec}\,(\mathbf{A})$ *(with respect to the Zariski topology (section 2.3.3**(III)**)).*

iii) If $\mathfrak{p} \in \text{Supp}\,(M)$, *then* $\text{V}\,(\mathfrak{p}) \subset \text{Supp}\,(M)$.

PROOF.–

i) We have that $M_{\mathfrak{p}} \neq 0$ if and only if, for all $x \in M$, and every $\lambda \in \mathbf{A}$, $(\lambda x = 0 \Rightarrow \lambda \in \mathfrak{p}) \Leftrightarrow \text{Ann}^{\mathbf{A}}\,(x) \subset \mathfrak{p}$.

ii) Let M be generated by $x_1, ..., x_k$. By (i), $\text{Supp}\,(M) = \bigcup_{1 \leq i \leq k} \text{V}\left(\text{Ann}^{\mathbf{A}}\,(x_k)\right)$ which is therefore a closed set.

iii) If $\mathfrak{p} \in \text{Supp}\,(M)$ and $\mathfrak{p}' \in \text{Spec}\,(\mathbf{A})$ satisfy $\mathfrak{p}' \supset \mathfrak{p}$, then $\mathfrak{p}' \in \text{Supp}\,(M)$ by the proof of (i). ■

DEFINITION 3.64.– *We say that a prime ideal* $\mathfrak{p} \in \text{Spec}\,(\mathbf{A})$ *is* associated *with an* $\mathbf{A}$*-module* M *if there exists an element* $x \in M$ *such that* $\mathfrak{p} = \text{Ann}^{\mathbf{A}}\,(x)$. *The set of prime ideals associated with* M *is written as* $\text{Ass}_{\mathbf{A}}\,(M)$ *(or* $\text{Ass}\,(M)$ *if this is unambiguous).*

From this definition, it follows that, for any prime ideal $\mathfrak{p}$,

$$\mathfrak{p} \in \text{Ass}\,(M) \Leftrightarrow (\exists N \subseteq M : N \cong \mathbf{A}/\mathfrak{p}). \qquad [3.31]$$

LEMMA 3.65.– *Let* $\mathbf{A}$ *be a ring.*

i) If $\mathfrak{p} \in \text{Spec}\,(\mathbf{A})$ *and* $M \subset \mathbf{A}/\mathfrak{p}$, *then* $\text{Ass}\,(M) = \{\mathfrak{p}\}$.

ii) If $M = 0$, *then* $\text{Ass}\,(M) = \varnothing$, *and the converse holds if* $\mathbf{A}$ *is Noetherian.*

iii) If the ring $\mathbf{A}$ *is Noetherian and* M *is an* $\mathbf{A}$*-module, then* $\text{Ann}^{\mathbf{A}}\,(M) = \bigcup_{\mathfrak{p} \in \text{Ass}(M)} \mathfrak{p}$.

iv) If the sequence $0 \to N \to M \to L \to 0$ *is exact, then* $\text{Ass}\,(N) \subset \text{Ass}\,(M) \subset \text{Ass}\,(N) \cup \text{Ass}\,(L)$.

PROOF.– (i) **exercise**. (ii) Everything except the converse is obvious. We can begin by showing (**exercise**) that, when $\mathbf{A}$ is an arbitrary ring, every element that is maximal over $\text{Ann}^{\mathbf{A}}(x), 0 \neq x \in M$, is prime, and so is in $\text{Ass}(M)$. The rest of the argument is straightforward. (iii) Use the result stated above (**exercise**). (iv) is clear. ■

(II) In the following, we study the relationship between Supp and Ass.

LEMMA 3.66.– *Let* $\mathbf{A}$ *be a ring, and let* M *be an* $\mathbf{A}$*-module.*

i) If $\mathfrak{p} \in \text{Spec}(\mathbf{A})$ *contains an element* $\mathfrak{q} \in \text{Ass}(M)$, *then* $\mathfrak{p} \in \text{Supp}(M)$ *(in other words,* $\text{V}(\mathfrak{q}) \subset \text{Supp}(M), \forall \mathfrak{q} \in \text{Ass}(M)$*).*

ii) Conversely, if $\mathbf{A}$ *is* Noetherian, *every ideal* $\mathfrak{p} \in \text{Supp}(M)$ *contains an element* $\mathfrak{q} \in \text{Ass}(M)$. *Hence, any minimal element in* $\text{Supp}(M)$ *belongs to* $\text{Ass}(M)$.

PROOF.– i) If $\mathfrak{p} \supset \mathfrak{q} \in \text{Ass}(M)$, we have that $\mathfrak{q} \cap \left(\complement_{\mathbf{A}}\mathfrak{p}\right) = \varnothing$, so $\mathfrak{q}_{\mathfrak{p}} \in \text{Ass}(M_{\mathfrak{p}})$ (**exercise**), implying that $M_{\mathfrak{p}} \neq 0$ (lemma 3.65(ii)), and hence $\mathfrak{p} \in \text{Supp}(M)$.

ii) If $\mathbf{A}$ is Noetherian, $\mathbf{A}_{\mathfrak{p}}$ is also Noetherian (corollary 3.33). If $M_{\mathfrak{p}} \neq 0$, we therefore have that $\text{Ass}(M_{\mathfrak{p}}) \neq 0$ (lemma 3.65(ii)), so there exists $\mathfrak{q} \in \text{Ass}(M)$ such that $\mathfrak{q} \cap \left(\complement_{\mathbf{A}}\mathfrak{p}\right) = \varnothing$ (**exercise***. For this step, it can be shown using theorem 3.34(2) that the mapping $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ is a bijection from $\text{Ass}_{\mathbf{A}}(M) \cap \Phi$ onto $\text{Ass}_{S^{-1}\mathbf{A}}\left(S^{-1}M\right)$, where $S = \complement_{\mathbf{A}}\mathfrak{p}$ and Φ is the set of prime ideals of $\mathbf{A}$ disjoint from S; see [BKI 98], Chap. IV, section 1.2, Cor.). ■

THEOREM 3.67.– *Let* $\mathbf{A}$ *be a commutative* Noetherian *ring and let* M *be a* finitely generated $\mathbf{A}$*-module.*

*i) There exists a composition series (section 2.2.5**(II)**)*

$$0 = M_0 \subset M_1 \subset ... \subset M_n = M$$

such that $M_i/M_{i-1} \cong \mathbf{A}/\mathfrak{p}_i$ $(i = 1, ..., n;\ \mathfrak{p}_i \in \text{Spec}(\mathbf{A}))$, *and we have that*

$$\text{Ass}(M) \subset \{\mathfrak{p}_1, ..., \mathfrak{p}_n\} \subset \text{Supp}(M); \qquad [3.32]$$

in particular, $\text{Ass}(M)$ *is finite.*

ii) The three sets in [3.32] have the same elements, which are the minimal elements of the set of prime ideals containing $\mathrm{Ann}^{\mathbf{A}}(M)$. *Hence, by theorem 2.45,*

$$\boxed{\sqrt{\mathrm{Ann}^{\mathbf{A}}(M)} = \bigcap_{\mathfrak{p}\in \mathrm{Supp}(M)} \mathfrak{p} = \bigcap_{\mathfrak{p}\in \mathrm{Ass}(M)} \mathfrak{p}}.$$

PROOF.– i) If $M = 0$, there is nothing to show. Otherwise, $\mathrm{Ass}(M) \neq \varnothing$ by lemma 3.65(ii), so by [3.31] there exist $M_1 \subset M$ and $\mathfrak{p}_1 \in \mathrm{Ass}(M)$ such that $M_1 \cong \mathbf{A}/\mathfrak{p}_1$. Similarly, $M/M_1 \neq 0$, so there exist $M' \subset M/M_1$ and $\mathfrak{p}_2 \in \mathrm{Ass}(M/M_1)$ such that $M' \cong \mathbf{A}/\mathfrak{p}_2$. Let $\varphi : M \twoheadrightarrow M/M_1$ be the canonical epimorphism and let $M_2 = \varphi^{-1}(M')$. Then, $M_1 \subset M_2 \subset M$ and $M_2/M_1 \cong \mathbf{A}/\mathfrak{p}_2$. By repeating this construction, we find an ascending series $0 = M_0 \subset M_1 \subset ...$ of submodules of M, which must be stationary since M is Noetherian, so there exists an integer $n \geq 1$ such that $M_n = M$. By lemma 3.65

$$\mathrm{Ass}(M_n) \subset \mathrm{Ass}(M_{n-1}) \cup \mathrm{Ass}(M_n/M_{n-1}) = \mathrm{Ass}(M_{n-1}) \cup \{\mathfrak{p}_n\}$$

and arguing by induction we deduce the first inclusion in [3.32]. Furthermore, $\mathfrak{p}_i \in \mathrm{V}(\mathfrak{p}_i) = \mathrm{Supp}(\mathbf{A}/\mathfrak{p}_i)$ ([3.30]) and $\mathrm{Supp}(\mathbf{A}/\mathfrak{p}_i) = \mathrm{Supp}(M_i/M_{i-1})$, so $\mathfrak{p}_i \in \mathrm{Supp}(M_i) \subset \mathrm{Supp}(M)$ (lemma 3.65(iv)). This completes the proof of [3.32].

ii) The sets $\mathrm{Ass}(M)$ and $\mathrm{Supp}(M)$ have the same minimal elements by lemma 3.66, and by [3.32], these elements are the minimal elements of $\{\mathfrak{p}_1, ..., \mathfrak{p}_n\}$. The minimal elements of $\mathrm{Supp}(M)$ are the minimal elements of $\mathrm{V}\left(\mathrm{Ann}^{\mathbf{A}}(M)\right)$ by lemma 3.63. ■

3.2.4. *Primary decomposition*

(I) In this subsection, all rings are assumed to be commutative. The *primary decomposition* generalizes Gauss's theorem on the decomposition into prime factors in a principal ideal domain (theorem 2.54). Let $\mathbf{A}$ be a ring and let $\mathfrak{q}$ be a proper ideal in $\mathbf{A}$. The proof of the following equivalence is an **exercise**:

LEMMA-DEFINITION 3.68.– *Let* $\mathfrak{q}$ *be a proper ideal in the ring* $\mathbf{A}$.

1) The following conditions are equivalent*:*

i) $\forall r, s \in \mathbf{A} : (rs \in \mathfrak{q}$ *and* $r \notin \mathfrak{q}) \Rightarrow (\exists m \in \mathbb{N}^{\times} : s^m \in \mathfrak{q})$.

ii) Every zero-divisor in $\mathbf{A}/\mathfrak{q}$ *is nilpotent.*

2) The ideal $\mathfrak{q}$ *is said to be* primary *if these equivalent conditions are satisfied.*

Let $\mathfrak{q}$ be a primary ideal, and let $\sqrt{\mathfrak{q}}$ be its radical (definition 2.44). It follows from theorem 2.45 that $\sqrt{\mathfrak{q}}$ is the smallest prime ideal containing $\mathfrak{q}$.

DEFINITION 3.69.– *If* $\mathfrak{q}$ *is a primary ideal and* $\mathfrak{p} = \sqrt{\mathfrak{q}}$*, then* $\mathfrak{q}$ *is said to be* $\mathfrak{p}$-primary.

We have that $\mathrm{Ann}\,(\mathbf{A}/\mathfrak{q}) = \mathfrak{q}$, so if $\mathfrak{q}$ is $\mathfrak{p}$-primary, $\mathfrak{p} = \sqrt{\mathrm{Ann}\,(\mathbf{A}/\mathfrak{q})}$.

If $\mathbf{A}$ is a principal ideal domain (section 2.3.8**(IV)**), the ideal $\mathfrak{q} = (q)$ is primary if and only if $\mathfrak{q} = 0$ or there exist $m \in \mathbb{N}^{\times}$ and a prime element p such that $q = p^m$ (**exercise**). We therefore have that $\mathfrak{q} = (p^m)$ and $\sqrt{\mathfrak{q}} = (p)$, so an ideal is primary if and only if it is a power of a prime ideal (0) or (p). This property does not hold in an arbitrary ring $\mathbf{A}$ ([ATI 69], p. 51, Examples 2 & 3), and we will see later (section 3.3.4**(I)**) that it is a characteristic property of Dedekind domains.

LEMMA 3.70.– *Let* $\mathbf{A}$ *be a ring and let* $\mathfrak{a}$ *be an ideal in* $\mathbf{A}$*. If* $\sqrt{\mathfrak{a}}$ *is maximal (section 2.3.6), then* $\mathfrak{a}$ *is primary. In particular, the powers of a maximal ideal* $\mathfrak{m}$ *are* $\mathfrak{m}$*-primary.*

PROOF.– Let $\sqrt{\mathfrak{a}} = \mathfrak{m}$. The canonical image of $\mathfrak{m}$ in $\mathbf{A}/\mathfrak{a}$ is the nilradical $\mathfrak{N}(\mathbf{A}/\mathfrak{a})$ (definition 2.43). The correspondence theorem (section 2.2.3**(III)**) implies that the ideal $\mathfrak{N}(\mathbf{A}/\mathfrak{a})$ is maximal in $\mathbf{A}/\mathfrak{a}$. Since $\mathfrak{N}(\mathbf{A}/\mathfrak{a})$ is the intersection of all prime ideals in $\mathbf{A}/\mathfrak{a}$ by lemma 2.42, $\mathfrak{N}(\mathbf{A}/\mathfrak{a})$ is the only maximal ideal in $\mathbf{A}/\mathfrak{a}$, and hence $\mathbf{A}/\mathfrak{a}$ is a local ring with Jacobson radical $\mathfrak{N}(\mathbf{A}/\mathfrak{a})$ (section 2.3.5**(IV)**). It thus follows from lemma 2.47 that the elements of $\mathbf{A}/\mathfrak{a}$ are either invertible or nilpotent, and so every zero-divisor in $\mathbf{A}/\mathfrak{a}$ is nilpotent. Now let $r, s \in \mathbf{A}$ be such that $rs \in \mathfrak{a}$ and $r \notin \mathfrak{a}$. The canonical image $\bar{s}$ of s in $\mathbf{A}/\mathfrak{a}$ is a zero-divisor, so there exists $m \in \mathbb{N}^{\times}$ such that $\bar{s}^m = 0$, which implies that $s^m \in \mathfrak{a}$ and $\mathfrak{a}$ is $\mathfrak{m}$-primary. ■

THEOREM 3.71.– *Let* $\mathbf{A}$ *be a* Noetherian *ring. Then, an ideal* $\mathfrak{q}$ *in* $\mathbf{A}$ *is* $\mathfrak{p}$*-primary if and only if*

$$\mathrm{Ass}\left(\mathbf{A}/\mathfrak{q}\right) = \{\mathfrak{p}\}.$$

PROOF.– 1) If $\mathfrak{q}$ is $\mathfrak{p}$-primary and $0 \neq \bar{r} \in \mathbf{A}/\mathfrak{q}$, the last part of the proof of lemma 3.70 shows that $\mathrm{Ann}^{\mathbf{A}}\left(\bar{r}\right) \subset \mathfrak{p}$, so $\sqrt{\mathrm{Ann}^{\mathbf{A}}\left(\bar{r}\right)} = \mathfrak{p}$. Furthermore, $\mathrm{Ass}\left(\mathbf{A}/\mathfrak{q}\right) \neq \varnothing$ (lemma 3.65(ii)), so $\mathrm{Ass}\left(\mathbf{A}/\mathfrak{q}\right) = \{\mathfrak{p}\}$ by definition 3.64.

2) We will show that if $\mathrm{Ass}\left(\mathbf{A}/\mathfrak{q}\right) = \{\mathfrak{p}\}$, then

$$0 \neq M \subset \mathbf{A}/\mathfrak{q} \Rightarrow \sqrt{\mathrm{Ann}^{\mathbf{A}}\left(M\right)} = \mathfrak{p}. \qquad [3.33]$$

By theorem 3.67, $\sqrt{\mathrm{Ann}^{\mathbf{A}}\left(M\right)} = \bigcap_{\mathfrak{p}\in\mathrm{Ass}(M)} \mathfrak{p}$. If $\mathrm{Ass}\left(\mathbf{A}/\mathfrak{q}\right) = \{\mathfrak{p}\}$, we therefore have [3.33] by [3.31].

3) Let $r, s \in \mathbf{A}$ be such that $rs \in \mathfrak{q}$, $r \notin \mathfrak{q}$, and let $\bar{r}$ be the canonical image of x in $\mathbf{A}/\mathfrak{q}$. We have that $s \in \mathrm{Ann}^{\mathbf{A}}\left(\bar{r}\right) \subset \sqrt{\mathrm{Ann}^{\mathbf{A}}\left(\bar{r}\right)}$. If $\mathrm{Ass}\left(\mathbf{A}/\mathfrak{q}\right) = \{\mathfrak{p}\}$, we have that $\sqrt{\mathrm{Ann}^{\mathbf{A}}\left(\bar{r}\right)} = \mathfrak{p}$ by (2), and hence $s \in \mathfrak{p}$. However, $\mathfrak{q} = \mathrm{Ann}\left(\mathbf{A}/\mathfrak{q}\right)$, so by (2) $\sqrt{\mathfrak{q}} = \mathfrak{p}$, which implies that $s \in \sqrt{\mathfrak{q}}$, and there exists an integer $n > 0$ such that $s^n \in \mathfrak{q}$, which shows that $\mathfrak{q}$ is $\mathfrak{p}$-primary. ■

DEFINITION 3.72.– *We say that an ideal* $\mathfrak{a}$ *is* decomposable *if there exist primary ideals* $\mathfrak{q}_1, ..., \mathfrak{q}_k$ *such that*

$$\mathfrak{a} = \bigcap\nolimits_{1\leq i\leq k} \mathfrak{q}_i \qquad [3.34]$$

in which case the right-hand side is called a primary decomposition *of* $\mathfrak{a}$*. This primary decomposition is said to be* reduced *if 1) the prime ideals* $\sqrt{\mathfrak{q}_i}$ *are distinct and 2) for all* $i \in \{1, ..., k\}$, $\mathfrak{q}_i \not\supseteq \bigcap_{j\neq i} \mathfrak{q}_j$.

If the ideal $\mathfrak{a}$ is decomposable, we can reduce to the case where its prime decomposition is reduced by ignoring redundant terms and grouping together the $\mathfrak{q}_i$ with the same radicals, since if $\mathfrak{q}, \mathfrak{q}'$ are two $\mathfrak{p}$-primary ideals, $\mathfrak{q} \cap \mathfrak{q}'$ is a $\mathfrak{p}$-primary ideal.

EXAMPLE 3.73.– *Consider an ideal* $\mathfrak{a}$ *in a principal ring* $\mathbf{A}$. *If* $\mathfrak{a} = (0)$, *then this ideal is prime, and so is primary. If* $\mathfrak{a} \neq 0$, *there exists* $0 \neq a \in \mathbf{A}$ *such that* $\mathfrak{a} = (a)$. *The decomposition [2.19] of* a *into prime factors implies that:*

$$\mathfrak{a} = \prod\nolimits_{p \in P} \left(p^{\alpha_p}\right).$$

*With the notation from section 2.3.3**(III)**,* $\mathrm{V}(\mathfrak{a}) = \{p \in P : \alpha_p \neq 0\}$. *The set* $\mathrm{V}(\mathfrak{a})$ *is finite, and setting* $\mathfrak{q}(\mathfrak{p}) = \left(p^{\alpha_p}\right)$ *for* $p \in \mathrm{V}(\mathfrak{a})$,

$$\mathfrak{a} = \bigcap\nolimits_{\mathfrak{p} \in \mathrm{V}(\mathfrak{a})} \mathfrak{q}(\mathfrak{p}) \qquad [3.35]$$

is a reduced primary decomposition of $\mathfrak{a}$. *This decomposition is unique.*

(II) Uniqueness of reduced primary decompositions (which can always be written in the form [3.35]) is more complex in the general case than in example 3.73.

EXAMPLE 3.74.– *In* $\mathbf{k}[X, Y]$ *(where* $\mathbf{k}$ *is a field),* $(X) \cap (X, Y)^2$ *and* $(X) \cap \left(X^2, Y\right)$ *are two reduced primary decompositions of the same ideal* $\left(X^2, XY\right)$. *However, we still have that* $\sqrt{(X, Y)^2} = \sqrt{(X^2, Y)} = (X, Y)$ ***(exercise)***.

The prime ideals $\sqrt{\mathfrak{q}_i}$ (where the $\mathfrak{q}_i$'s are the primary ideals from equation [3.34]) are said to *belong* to $\mathfrak{a}$. The set $\mathrm{V}(\mathfrak{a})$ of these prime ideals (section 2.3.3(**III**)) is finite. The *first uniqueness theorem* may be stated as follows ([ATI 69], p. 52, Thm. 4.5):

THEOREM 3.75.– *If the primary decomposition [3.34] is reduced, the prime ideals belonging to* $\mathfrak{q}_i$ $(i \in \{1, ..., k\})$ *are uniquely determined up to permutations of the order of the terms.*

To formulate the second uniqueness theorem, we require the following terminology: elements $\mathfrak{p} \in \mathrm{V}(\mathfrak{a})$ that are minimal (with respect to inclusion) are said to be *isolated* (or *minimal*) and the others are said to be *embedded*. In example 3.74, $(X), (X, Y) \in \mathrm{V}(\mathfrak{a})$, and (X) is isolated, whereas (X, Y) is embedded. Let us continue this example:

LEMMA 3.76.– *i) Let* M *be an* $\mathbf{A}$*-module and let* $M[X]$ *be the set of polynomials in* X *with coefficients in* M. *Then,* $M[X]$ *has a canonical* $\mathbf{A}[X]$*-module structure and* $M[X] \cong \mathbf{A}[X] \bigotimes_{\mathbf{A}} M$.

ii) If $\mathfrak{a}$ *is an ideal in* $\mathbf{A}$*, then* $\mathbf{A}[X]/\mathfrak{a}[X] \cong (\mathbf{A}/\mathfrak{a})[X]$;

iii) If $\mathfrak{p} \in \mathrm{Spec}(\mathbf{A})$*, then* $\mathfrak{p}[X] \in \mathrm{Spec}(\mathbf{A}[X])$;

iv) If $\mathfrak{q}$ *is* $\mathfrak{p}$*-primary in* $\mathbf{A}$*, then* $\mathfrak{q}[X]$ *is* $\mathfrak{p}[X]$*-primary in* $\mathbf{A}[X]$;

v) If $\mathfrak{a} = \bigcap_{1 \leq i \leq k} \mathfrak{q}_i$ *is a reduced primary decomposition in* $\mathbf{A}$*, then* $\mathfrak{a}[X] = \bigcap_{1 \leq i \leq k} \mathfrak{q}_i[X]$ *is a reduced primary decomposition in* $\mathbf{A}[X]$;

vi) If $\mathfrak{p}$ *if a minimal prime ideal in* $\mathfrak{a}$*, then* $\mathfrak{p}[X]$ *is a minimal prime ideal in* $\mathfrak{a}[X]$.

PROOF.– i) The canonical structure of $M[X]$ as an $\mathbf{A}[X]$-module is clear. Since $M = \mathbf{A}M$, $M[X]$ coincides with $(\mathbf{A}M)[X]$. The homomorphism

$$\phi : \mathbf{A}[X] \bigotimes\nolimits_{\mathbf{A}} M \to (\mathbf{A}M)[X] : f(X) \bigotimes\nolimits_{\mathbf{A}} m \mapsto f(X)\, m$$

is an isomorphism, hence $M[X] \cong \mathbf{A}[X] \bigotimes_{\mathbf{A}} M$.

ii) Let $\pi : \mathbf{A}[X] \twoheadrightarrow (\mathbf{A}/\mathfrak{a})[X]$ be the canonical epimorphism. Then, $\ker(\pi) = \mathfrak{a}[X]$, which implies that $\mathbf{A}[X]/\mathfrak{a}[X] \cong (\mathbf{A}/\mathfrak{a})[X]$ by Noether's first isomorphism theorem (theorem 2.12(1)).

iii) We have that $\mathfrak{p} \in \mathrm{Spec}(\mathbf{A})$ if and only if $\mathbf{A}/\mathfrak{p}$ is an entire ring. If so, $(\mathbf{A}/\mathfrak{p})[X]$ is an entire ring (section 2.3.9**(I)**), so $\mathfrak{p}[X]$ is a prime ideal in $\mathbf{A}[X]$ by (ii).

iv) If $\mathfrak{q}$ is primary in $\mathbf{A}$, every zero-divisor in $\mathbf{A}/\mathfrak{q}$ is nilpotent (lemma-definition 3.68). Let $f \in \mathbf{A}[X]/\mathfrak{q}[X]$ be a zero-divisor. The coefficients of f are all zero-divisors in $\mathbf{A}/\mathfrak{q}$, so are nilpotent, and consequently f is nilpotent (**exercise**), so $\mathfrak{q}[X]$ is primary in $\mathbf{A}[X]$.

v) and vi) follow from the above. ■

The *second uniqueness theorem* may be stated as follows ([ATI 69], p. 54, Thm. 4.10):

THEOREM 3.77.– *Let* $\mathfrak{a}$ *be a decomposable ideal, and write its primary decomposition in the form [3.35]. Let* $\mathrm{Is}(\mathfrak{a}) \subset \mathrm{V}(\mathfrak{a})$ *be the set of isolated prime ideals in* $\mathfrak{a}$*. Then, the* $\mathfrak{q}(\mathfrak{p})$ $(\mathfrak{p} \in \mathrm{Is}(\mathfrak{a}))$ *are independent of the choice of decomposition.*

This result and its terminology will become more clear once we introduce some basic notions from algebraic geometry in section 3.2.7. The next definition is named after the mathematician E. Lasker:

DEFINITION 3.78.– *A ring* $\mathbf{A}$ *is said to be* Laskerian *if every ideal in* $\mathbf{A}$ *is decomposable.*

Let $\mathbf{A}$ be a ring. An ideal $\mathfrak{a}$ in $\mathbf{A}$ is said to be *irreducible* if it is irreducible in the lattice $\mathbf{L}\left((0), \mathbf{A}\right)$ of all ideals in $\mathbf{A}$ (section 2.1.1**(II)**, 2.3.2**(II)**), i.e.

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \Rightarrow (\mathfrak{a} = \mathfrak{b} \text{ or } \mathfrak{a} = \mathfrak{c}).$$

If $\mathbf{A}$ is a principal ideal domain, the ideal $\mathfrak{a} = (a)$ is irreducible if and only if a is an irreducible element (**exercise**).

LEMMA 3.79.– *In a Noetherian ring, every ideal is a finite intersection of irreducible ideals.*

PROOF.– If not, the set of ideals for which the statement does not hold has a maximal element $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$, where $\mathfrak{b} \supsetneq \mathfrak{a}$ and $\mathfrak{c} \supsetneq \mathfrak{a}$. Then, $\mathfrak{b}$ and $\mathfrak{c}$ are finite intersections of irreducible ideals, and so is $\mathfrak{a}$: contradiction. ■

LEMMA 3.80.– *In a Noetherian ring* $\mathbf{A}$*, every irreducible ideal* $\mathfrak{a}$ *is primary.*

PROOF.– Working in the quotient ring $\mathbf{A}/\mathfrak{a}$ (section 2.3.2**(IV)**), it is sufficient to show that if the ideal (0) is irreducible, then it is primary. Let $xy = 0$ where $y \neq 0$. Consider the ascending sequence of ideals $\text{Ann}^{\mathbf{A}}(x) \subset \text{Ann}^{\mathbf{A}}\left(x^2\right) \subset \ldots$ (section 2.3.2**(III)**). This sequence is stationary (section 2.3.4**(I)**), so there exists an integer $n > 0$ such that $\text{Ann}^{\mathbf{A}}\left(x^{n+j}\right) = \text{Ann}^{\mathbf{A}}\left(x^n\right)$ for all $j \in \mathbb{N}$. Then, $\text{Ann}^{\mathbf{A}}\left(x^n\right) \cap (y) = (0)$. Indeed, since $z \in (y)$, we have that $xz = 0$, and if we also have that $z \in (x^n)$, there exists t such that $z = tx^n$, so $tx^{n+1} = 0$, which implies that $t \in \text{Ann}^{\mathbf{A}}\left(x^{n+1}\right) = \text{Ann}^{\mathbf{A}}\left(x^n\right)$, hence $z = 0$. Since (0) is irreducible and $(y) \neq 0$, we have that $(x^n) = (0)$, so $(0) = (x)^n$ is primary. ■

These two lemmas imply the following result:

THEOREM 3.81.– *(Lasker-Noether) Every Noetherian ring is Laskerian.*

3.2.5. *Elements integral over a ring.* Nullstellensatz

(I) In this subsection, every ring is commutative, and every algebra is associative and unitary. $\mathbf{R}$ denotes a ring and $\mathbf{A}$ denotes an $\mathbf{R}$-algebra. The

$\mathbf{R}$-algebra of polynomials $\mathbf{R}[X_1, ..., X_n]$ in the indeterminates $X_1, ..., X_n$ is finitely generated (section 2.3.10(**II**)); however, it is not finitely generated as an $\mathbf{R}$-module.

DEFINITION 3.82.– *An $\mathbf{R}$-algebra is said to be* finite *(over $\mathbf{R}$) if it is a finitely generated $\mathbf{R}$-module.*

Recall (section 2.3.5(**II**)) that a non-zero polynomial $f \in \mathbf{R}[X]$ is said to be *unitary* if the coefficient of its highest-degree term is equal to 1.

DEFINITION 3.83.– *An element $x \in \mathbf{A}$ is said to be* integral *over $\mathbf{R}$ if x is the root of a* unitary *polynomial $f \in \mathbf{R}[X]$. The relation $f(x) = 0$ is then called the* integral dependence equation *of x over $\mathbf{R}$.*

For example, $x = \sqrt{2}$ is integral over $\mathbb{Z}$ since $x^2 - 2 = 0$. However, $y = \left(1 + \sqrt{3}\right)/2$ is not integral over $\mathbb{Z}$ since $y^2 - y - 1/2 = 0$. The integral complex numbers over $\mathbb{Z}$ are called the *algebraic integers*.

THEOREM 3.84.– *Let $x \in \mathbf{A}$.* The following conditions are equivalent*:*

i) x is integral over $\mathbf{R}$;

ii) The $\mathbf{R}$-algebra $\mathbf{R}[x]$ is a finitely generated $\mathbf{R}$-module (in other words, $\mathbf{R}[x]$ is a finite $\mathbf{R}$-algebra);

iii) There exists a ring $\mathbf{B}$ such that $\mathbf{R} \subset \mathbf{B} \subset \mathbf{A}$, $x \in \mathbf{B}$ and $\mathbf{B}$ is a finitely generated $\mathbf{R}$-module.

PROOF.– (i)⇒(ii) Suppose that $f(x) = 0$, where

$$f = X^n - a_{n-1}X^{n-1} - ... - a_n. \qquad [3.36]$$

Then, $x^n = a_{n-1}x^{n-1} + ... + a_n$ belongs to the $\mathbf{R}$-module M generated by $1, x, ..., x^{n-1}$, and we can show by induction that every power of x belongs to M. Therefore, $\mathbf{R}[x] = M$.

(ii)⇒(iii) is clear, but we still need to show that (iii)⇒(i). Assuming that (iii) holds, let $\{y_1, ..., y_n\}$ be a generating set of the $\mathbf{R}$-module $\mathbf{B}$ (section 2.3.1(**II**)). We therefore have that $xy_i \in \mathbf{B}$ $(i = 1, ..., n)$, so there exist $a_i^j \in \mathbf{R}$ $(i, j = 1, ..., n)$ such that, for all $i \in \{1, ..., n\}$,

$$xy_i = \sum_{j=1}^{n} a_i^j y_j \Leftrightarrow \sum_{j=1}^{n} \left(\delta_i^j x - a_i^j\right) y_j = 0.$$

Cramer's rule [2.31] implies that $dy_i = 0$ $(i = 1, ..., n)$, where $d = \det(C)$, with $c_i^j = \delta_i^j x - a_i^j$. Hence, $db = 0$ for all $b \in \mathbf{B}$, and, in particular, $d.1 = 0$, so $d = 0$. The relation obtained by replacing the indeterminate X with x in [2.32] gives an integral dependence equation for x. ■

By induction, we deduce that if $(x_i)_{1 \leq i \leq n}$ is a finite family of elements of $\mathbf{A}$ such that x_i is integral over $\mathbf{R}[x_1, ..., x_{i-1}]$ for all $i \in \{1, ..., n\}$ (in particular, if each x_i is integral over $\mathbf{R}$), then $\mathbf{R}[x_1, ..., x_n]$ is a finitely generated $\mathbf{R}$-module (**exercise***: see [BKI 98], Chap. V, section 1.1, Prop. 4). In the case $n = 2$, we obtain

COROLLARY 3.85.– *Suppose that the* $\mathbf{R}$*-algebra* $\mathbf{A}$ *is* commutative. *The set* $\mathbf{R}'$ *consisting of the elements of* $\mathbf{A}$ *that are integral over* $\mathbf{R}$ *is a subalgebra of* $\mathbf{A}$.

DEFINITION 3.86.– *i) The* $\mathbf{R}$*-algebra* $\mathbf{A}$ *is said to be* integral *over* $\mathbf{R}$ *if every element of* $\mathbf{A}$ *is integral over* $\mathbf{R}$.

ii) Suppose that $\mathbf{A}$ *is* commutative. *The subalgebra* $\mathbf{R}'$ *of* $\mathbf{A}$ *consisting of the integral elements over* $\mathbf{R}$ *is called the* integral closure *of* $\mathbf{R}$ *in* $\mathbf{A}$. *We say that the* $\mathbf{R}$*-algebra* $\mathbf{A}$ *is* integral *over* $\mathbf{R}$ *if the integral closure of* $\mathbf{R}$ *in* $\mathbf{A}$ *is* $\mathbf{A}$.

iii) Suppose that $\mathbf{R}$ *is entire, and let* $\mathbf{K}$ *be its field of fractions. The integral closure of* $\mathbf{R}$ *in* $\mathbf{K}$ *is called the* integral closure *of* $\mathbf{R}$ *(without qualification). The entire ring* $\mathbf{R}$ *is said to be* integrally closed *if it is equal to its integral closure.*

It follows from theorem 3.84 that every finite $\mathbf{R}$-algebra is integral over $\mathbf{R}$. If $\mathbf{A}$ is commutative, it is finite if and only if it is integral and finitely generated, by [2.26]. Moreover, a field is integrally closed if and only if it is algebraically closed (section 2.3.5(**II**)). Valuation rings are integrally closed (**exercise***: see [BKI 98], Chap. VI, section 1.3, Cor. 1).

The following transitivity relation holds: suppose that the $\mathbf{R}$-algebra $\mathbf{A}$ is commutative and let $\mathbf{B}$ be an $\mathbf{A}$-algebra. If $\mathbf{A}$ is integral over $\mathbf{R}$ and $\mathbf{B}$ is integral over $\mathbf{A}$, then $\mathbf{B}$ is integral over $\mathbf{R}$; conversely, if $\mathbf{B}$ is integral over $\mathbf{R}$, $\mathbf{B}$ is integral over $\mathbf{A}$ (**exercise***: see [BKI 98], Chap. V, section 1.1, Cor 3 of Prop. 2 & Prop. 6).

LEMMA 3.87.– *GCD domains (section 2.3.8(**I**)) are integrally closed.*

PROOF.– If $\mathbf{R}$ is a GCD domain, then by definition (section 2.3.8(**I**)), it is entire. Let $\mathbf{K}$ be its field of fractions and let $x \in \mathbf{K}$ be an integral element over $\mathbf{R}$. There exists an integral equation $f(x) = 0$, where f is of the form [3.36]. We can write $x = b/c$, $b, c \in \mathbf{R}$, $c \neq 0$, where $b \vee c = 1$. We deduce that

$$b^n = c\left(a_{n-1}b^{n-1} + ... + a_1 bc^{n-2} + a_0 c^{n-1}\right),$$

so $c \mid b^n$, and by repeatedly applying the Euclid-Gauss lemma (lemma 2.49(1)), we can show that $c \mid b$, so $c \in \mathbf{U}(\mathbf{R})$ and $x \in \mathbf{R}$. ■

It follows from lemma 3.87 and Gauss's lemma (lemma 2.60) that the ring $\mathbb{Z}\left[(X_i)_{i\in I}\right]$ is integrally closed.

If the algebra $\mathbf{A}$ is commutative, $\mathbf{B}$ is the integral closure of $\mathbf{R}$ in $\mathbf{A}$, and S is a multiplicative set of $\mathbf{R}$, then $S^{-1}\mathbf{B}$ is the integral closure of $S^{-1}\mathbf{R}$ in $S^{-1}\mathbf{A}$ (**exercise***: see [ATI 69], Prop. 5.12). Using theorem 3.57(2), it is straightforward to deduce

THEOREM 3.88.– *Let* $\mathbf{R}$ *be an entire ring.* The following conditions are equivalent*:*

i) $\mathbf{R}$ *is integrally closed;*

ii) $\mathbf{R}_{\mathfrak{p}}$ *is integrally closed for every prime ideal* $\mathfrak{p}$*;*

iii) $\mathbf{R}_{\mathfrak{m}}$ *is integrally closed for every maximal ideal* $\mathfrak{m}$*.*

(II) The following result, known as the *normalization lemma*, was established in 1926:

LEMMA 3.89.– *(E. Noether) Let* $\mathbf{K}$ *be a field and let* $\mathbf{A}$ *be a finitely generated* $\mathbf{K}$*-algebra. There exists an algebraically free family of elements* $y_1, ..., y_r \in \mathbf{A}$ *over* $\mathbf{K}$ *(section 2.3.10(**IV**)) such that* $\mathbf{A}$ *is integral over* $\mathbf{K}[y_1, ..., y_r]$*.*

PROOF.– To simplify the proof, suppose that $\mathbf{K}$ is infinite (even though the result holds for arbitrary $\mathbf{K}$: see [BKI 98], Chap. V, section 3.1, Thm. 1). This assumption is without loss of generality when $\mathbf{K}$ is algebraically closed by lemma 2.34. The $\mathbf{K}$-algebra $\mathbf{A}$ is finitely generated, so let $(x_i)_{1\leq i\leq n}$ be a generating family of the $\mathbf{K}$-module $\mathbf{A}$, where, relabeling the x_i if necessary, we can assume that $(x_i)_{1\leq i\leq r}$ is algebraically free and $x_{r+1}, ..., x_n$ are algebraic over $\mathbf{K}[x_1, ..., x_r]$ (section 2.3.10(**IV**)). We argue by induction on the number n of generators of $\mathbf{A}$.

For $n = r$, there is nothing to show. Suppose that $n > r$ and that the result holds for $n-1$ generators. Since x_n is algebraic over $\mathbf{K}[x_1, ..., x_{n-1}]$, there exists $f \in \mathbf{K}[X_1, ..., X_n]$, $f \neq 0$, such that $f(x_1, ..., x_n) = 0$. Let F be the homogeneous component of f with the highest degree d (section 2.3.12). Since the field $\mathbf{K}$ is infinite, we will show that the following claim (**A**) holds:

(**A**) There exist $\alpha_1, ...\alpha_{n-1} \in \mathbf{K}$ such that $F(\alpha_1, ...\alpha_{n-1}, 1) \neq 0$.

(**A**) can be shown by induction. For $n = 1$, there is nothing to show. For $n > 1$, write $F = \sum_{i=0}^{d} f_i X_1^i$ where the $f_i \in \mathbf{K}[X_2, ..., X_n]$ are homogeneous of degree $d - i$. Since $F \neq 0$, there exists i_0 such that $f_{i_0} \neq 0$. The induction hypothesis implies that we can find $\alpha_2, ..., \alpha_{n-1} \in \mathbf{K}$ such that $f_{i_0}(\alpha_2, ..., \alpha_{n-1}, 1) \neq 0$. Then, $0 \neq F(., \alpha_2, ..., \alpha_{n-1}, 1) \in \mathbf{K}[X_1]$, and since $\mathbf{K}$ is infinite there exists $\alpha_1 \in \mathbf{K}$ such that $F(\alpha_1, \alpha_2, ..., \alpha_{n-1}, 1) \neq 0$ (otherwise $F(., \alpha_2, ..., \alpha_{n-1}, 1)$ would have infinitely many distinct roots, which is impossible).

Now that we have proven the claim (**A**), let $x_i^* := x_i - \alpha_i x_n$ $(i = 1, ..., n-1)$ and

$$\begin{aligned} G(x_1^*, ..., x_{n-1}^*, x_n) &= F(x_1^* - \alpha_1 x_n, ..., x_{n-1}^* - \alpha_{n-1} x_n, x_n) \\ &= F(\alpha_1, ..., \alpha_{n-1}, 1) x_n^d + T \end{aligned}$$

where T is a sum of terms of degree $< d$ in x_n. We have that $G(x_1^*, ..., x_{n-1}^*, x_n) = 0$ and, dividing by $F(\alpha_1, ..., \alpha_{n-1}, 1)$, we find an integral dependence equation for x_n over $\mathbf{A}^* := \mathbf{K}[x_1^*, ..., x_{n-1}^*]$. So $\mathbf{A} = \mathbf{K}[x_1, ..., x_n] = \mathbf{A}^*[x_n]$ is integral over $\mathbf{A}^*$.

Since the induction hypothesis n applies to $\mathbf{A}^* = \mathbf{K}[x_1^*, ..., x_{n-1}^*]$, there exists an algebraically free family $y_1, ..., y_r \in \mathbf{A}^*$ over $\mathbf{K}$ for which $\mathbf{A}^*$ is integral over $\mathbf{B} = \mathbf{K}[y_1, ..., y_r]$. Since $\mathbf{A}^*[x_n]$ is integral over $\mathbf{A}^*$, and $\mathbf{A}^*[x_n] = \mathbf{A}$, $\mathbf{A}$ is integral over $\mathbf{B}$ by transitivity. ■

(III) NULLSTELLENSATZ. Both the weak and strong statements of this theorem (known as the *Nullstellensatz* in German) were shown by Hilbert in 1890.

LEMMA 3.90.– *Let* $\mathbf{k}$ *be a field. (1) Let* $\mathbf{K} \supset \mathbf{k}$ *be a field that is finitely generated as a* $\mathbf{k}$*-algebra. Then,* $\mathbf{K}$ *is a finite-dimensional* $\mathbf{k}$*-vector space,*

and is an algebraic extension of $\mathbf{K}$. *(2) If* $\mathbf{A}$ *is a finitely generated and entire* $\mathbf{k}$*-algebra, it is a field.*

PROOF.– (1): By Noether's normalization lemma (lemma 3.89), there exists an algebraically free family $(y_i)_{1\leq i\leq r}$ of elements of $\mathbf{K}$ over $\mathbf{k}$ such that the $\mathbf{k}$-algebra $\mathbf{K}$ is integral over $\mathbf{A} = \mathbf{k}[y_1, ..., y_r]$. Since $\mathbf{A} \subset \mathbf{K}$, $\mathbf{A}$ is a field, so $r = 0$, $\mathbf{A} = \mathbf{k}$ and the $\mathbf{k}$-algebra $\mathbf{K}$ is integral over $\mathbf{k}$; hence, $\mathbf{K}$ is finite over $\mathbf{k}$ since it is finitely generated, and is an algebraic extension of $\mathbf{k}$ (section 2.3.5(**II**)). (2): Let $a \in \mathbf{A}^\times$; the mapping $x \mapsto ax$ from $\mathbf{A}$ into $\mathbf{A}$ is injective, and so is an automorphism of the finite-dimensional $\mathbf{k}$-vector space $\mathbf{A}$. Thus, there exists $x \in \mathbf{A}$ such that $ax = 1$, so $\mathbf{A}$ is a field. ■

THEOREM 3.91.– *(*Nullstellensatz, weak version*): Let* $\mathbf{k}$ *be a field.*

i) The ideal $\mathfrak{m} = (X_1 - c_1, ..., X_n - c_n)$, $c_i \in \mathbf{k}$ $(i = 1, ..., n)$ *is maximal in* $\mathbf{k}[X_1, ..., X_n]$.

ii) Conversely, if $\mathbf{k}$ *is algebraically closed, every maximal ideal in* $\mathbf{k}[X_1, ..., X_n]$ *is of this form.*

PROOF.– i) The mapping $\mathbf{k}[X_1, ..., X_n] \to \mathbf{k} : f \mapsto f(c_1, ..., c_n)$ is a ring epimorphism with kernel $\mathfrak{m} = (X_1 - c_1, ..., X_n - c_n)$ (we can see this by means of the change of coordinates $Y_i = X_i - c_i$ $(i = 1, ..., n)$), so $\mathbf{k}[X_1, ..., X_n]/\mathfrak{m} \cong \mathbf{k}$ by [2.26], and so the ideal $\mathfrak{m}$ is maximal.

ii) Let $\mathfrak{m}$ be a maximal ideal in $\mathbf{k}[X_1, ..., X_n]$ and $\mathbf{K} = \mathbf{k}[X_1, ..., X_n]/\mathfrak{m}$. Then, $\mathbf{K}$ is an algebraic extension of $\mathbf{k}$ by lemma 3.90(1), and since $\mathbf{k}$ is algebraically closed, $\mathbf{k} = \mathbf{K}$. Let c_i be the canonical image of X_i in $\mathbf{k}$. Since c_i is also its own canonical image, we have $X_i - c_i \in \mathfrak{m}$, and so $\mathfrak{m} \supset (X_1 - c_1, ..., X_n - c_n)$. Hence, $\mathfrak{m} = (X_1 - c_1, ..., X_n - c_n)$ by (i). ■

COROLLARY 3.92.– *Let* $\mathbf{k}$ *be a field and* $\mathfrak{a}$ *an ideal in* $\mathbf{B} := \mathbf{k}[X_1, ..., X_n]$. *Then, either* $\mathfrak{a} = \mathbf{B}$, *or* $\mathfrak{a}$ *has a zero in* Ω^n *(definition 3.60), where* Ω *is an algebraic closure of* $\mathbf{k}$.

PROOF.– If $\mathfrak{a} \neq \mathbf{B}$, $\mathfrak{a}$ is contained in a maximal ideal $\mathfrak{m}$ in $\mathbf{B}$, and $\mathbf{B}/\mathfrak{m}$ is a field, which by lemma 3.90(1) must be algebraic over $\mathbf{k}$. Hence, there exists a monomorphism $\iota : \mathbf{B}/\mathfrak{m} \hookrightarrow \Omega$. Let $\varphi : \mathbf{B} \twoheadrightarrow \mathbf{B}/\mathfrak{m}$ be the canonical surjection. For every $f \in \mathfrak{a}$, $(\iota \circ \varphi)(f) = 0$, so $(\iota \circ \varphi)(\mathfrak{a})$ is a zero of $\mathfrak{a}$ in Ω^n. ■

THEOREM 3.93.– *(*Nullstellensatz, strong version*): Let* $\mathbf{k}$ *be a field,* Ω *an algebraic closure of* $\mathbf{k}$ *and* $\mathfrak{a}$ *an ideal in* $\mathbf{B} := \mathbf{k}[X_1, ..., X_n]$*. Suppose that* $f \in \mathbf{B}$ *satisfies* $f(c) = 0$ *for every zero* c *belonging to the set* $\mathcal{Z}(\mathfrak{a})$ *of zeros of* $\mathfrak{a}$ *in* Ω^n*. Then, there exists an integer* $p > 0$ *such that* $f^p \in \mathfrak{a}$*. Hence,* $\mathcal{Z}\left(\sqrt{\mathfrak{a}}\right) = \mathcal{Z}(\mathfrak{a})$.

PROOF.– The following proof is attributed to Rabinowitsch (a pseudonym of G. Rainich). The idea is to introduce a new indeterminate Y and, if $0 \neq f \in \mathbf{k}[X]$ (where $X = (X_i)_{1 \leq i \leq n}$), consider the ideal $\mathfrak{a}'$ generated by $\mathfrak{a}$ and $1 - Yf$ in $\mathbf{k}[X, Y]$. The ideal $\mathfrak{a}'$ has no zeros in Ω^n, so corollary 3.92 implies that $\mathfrak{a}' = \mathbf{k}[X, Y]$. Consequently, there exist an integer $r \geq 0$ and polynomials $g_i \in \mathbf{k}[X, Y]$ and $h_j \in \mathfrak{a}$ $(i = 0, 1, ..., r;\ j = 1, ..., r)$ such that

$$1 = g_0(1 - Yf) + \sum\nolimits_{j=1}^{r} g_j h_j.$$

By substituting f^{-1} for Y and multiplying the above equality by an appropriate power f^p of f to eliminate the denominators, we find $f^p \in \mathfrak{a}$, since the first term on the right cancels. ■

COROLLARY 3.94.– *Let* $\mathbf{k}$ *be a field,* $\mathbf{A}$ *a finitely generated* $\mathbf{k}$*-algebra,* $\mathfrak{a}$ *a proper ideal in* $\mathbf{A}$ *and* $\mathrm{Spm}(\mathbf{A})$ *the maximal spectrum of* $\mathbf{A}$ *(definition 2.26). Then,*

$$\sqrt{\mathfrak{a}} = \bigcap\nolimits_{\mathfrak{m} \in \mathrm{Spm}(\mathbf{A}), \mathfrak{m} \supset \mathfrak{a}} \mathfrak{m};\ \textit{in particular,}\ \mathfrak{N}(\mathbf{A}) = \bigcap\nolimits_{\mathfrak{m} \in \mathrm{Spm}(\mathbf{A})} \mathfrak{m}$$

(compare with lemma 2.42 and theorem 2.45).

PROOF.– By [2.26], we can identify $\mathbf{A}$ with $\mathbf{B}/\mathfrak{b}$, where $\mathbf{B} := \mathbf{k}[X_1, ..., X_n]$ and $\mathfrak{b}$ is an ideal in $\mathbf{B}$. Let $\varphi : \mathbf{B} \to \mathbf{A}$ be the canonical surjection. The mapping $\mathfrak{c} \mapsto \varphi^{-1}(\mathfrak{c})$ is a bijection from the set of ideals of $\mathbf{A}$ onto the set of ideals in $\mathbf{B}$ containing $\mathfrak{b}$ (section 2.2.3**(III)**). Let $\mathfrak{a}' = \varphi^{-1}(\mathfrak{a})$. Writing $\mathcal{Z}(\mathfrak{a}')$ for the set of zeros of $\mathfrak{a}'$ in Ω^n, where Ω is an algebraic closure of $\mathbf{k}$, we have

$$\sqrt{\mathfrak{a}'} = \bigcap_{(c_1, ..., c_n) \in \mathcal{Z}(\mathfrak{a}')} (X - c_1, ..., X - c_n) = \bigcap_{\mathfrak{m}' \in \mathrm{Spm}(\mathbf{B}), \mathfrak{m}' \supset \mathfrak{a}'} \mathfrak{m}'.$$

■

(IV) Corollary 3.94 says that every prime ideal in $\mathbf{A}$ is an intersection of maximal ideals. Any ring with this property is called a Jacobson ring

([BKI 98], Chap. V, section 3.4). The ring $\mathbb{Z}$ is a Jacobson ring (**exercise**). It can be shown that if $\mathbf{A}$ is a Jacobson ring and $\mathbf{B}$ is a finitely generated $\mathbf{A}$-algebra, then $\mathbf{B}$ is a Jacobson ring ([BKI 98], Chap. V, section 3.4, Thm. 3).

3.2.6. *Krull dimension*

(I) KRULL DIMENSION OF A TOPOLOGICAL SPACE. A topological space X is said to be *irreducible* if every finite intersection of non-empty open sets in X is non-empty. A closed subset V of X is therefore irreducible if and only if it cannot be written in the form $V_1 \cup V_2$, where V_1, V_2 are open sets of X strictly contained in V (**exercise**). For a subset $A \subset X$ to be irreducible, it is necessary and sufficient for its closure $\overline{A}$ (the smallest closed set that contains it) to be irreducible (**exercise***: see [BKI 98], Chap. II, section 4.1, Prop. 2). Consider the set $\mathfrak{C}$ of strictly ascending chains of irreducible closed subsets of X. If C is one such chain, and $|C|$ is its length (section 2.1.2**(III)**), we say that $\dim(X) := \sup_{C \in \mathfrak{C}} |C| \in \bar{\mathbb{R}}$ is the Krull *dimension* of X.

(II) KRULL DIMENSION OF A COMMUTATIVE RING. Let $\mathbf{R}$ be a commutative ring and let $\mathrm{Spec}(\mathbf{R})$ be its prime spectrum, equipped with the Zariski topology (section 2.3.3**(III)**).

DEFINITION 3.95.– *The dimension of the topological space* $\mathrm{Spec}(\mathbf{R})$ *is called the dimension of* $\mathbf{R}$ *(written* $\dim(\mathbf{R})$*).*

If $\mathfrak{p} \in \mathrm{Spec}(\mathbf{R})$, then $\mathrm{V}(\mathfrak{p})$ (the set of prime ideals containing $\mathfrak{p}$) is an irreducible closed subset of $\mathrm{Spec}(\mathbf{R})$, and the mapping $\mathfrak{p} \mapsto \mathrm{V}(\mathfrak{p})$ is a bijection from $\mathrm{Spec}(\mathbf{R})$ onto the set of irreducible closed subsets of $\mathrm{Spec}(\mathbf{R})$ (**exercise***: see [BKI 98], Chap. II, section 4.3, Cor. 2 of Prop. 14). Hence, $\dim(\mathbf{R})$ is the upper bound of the set of lengths of the chains of prime ideals in $\mathbf{R}$. It follows from theorem 3.55(ii) that

$$\boxed{\dim(\mathbf{R}) = \sup\{\mathfrak{h}(\mathfrak{p}) : \mathfrak{p} \in \mathrm{Spec}(\mathbf{R})\} = \sup\{\dim(\mathbf{R}_\mathfrak{p}) : \mathfrak{p} \in \mathrm{Spec}(\mathbf{R})\}}.$$

(III) EXAMPLES. For every commutative ring $\mathbf{R} \neq \{0\}$, we have that $\dim(\mathbf{R}) \geq 0$, and $\dim(\mathbf{R}) = 0$ if and only if every prime ideal in $\mathbf{R}$ is maximal, so entire rings of dimension 0 are fields, and a Noetherian ring has dimension 0 if and only if it is Artinian (section 2.3.4**(I)**) (**exercise***: see

[ATI 69], Thm. 8.5). If $\mathbf{K}$ is a field and $\mathbf{A}$ is a non-zero $\mathbf{K}$-algebra integral over $\mathbf{K}$ (definition 3.86(i)), it can be shown that $\dim(\mathbf{A}) = 0$ ([BKI 98], Chap. VIII, section 1.3, Example 6). Since $\dim(\mathbf{K}) = 0$, the notion of dimension considered here is entirely distinct from the one from definition 3.11. Commutative principal ideal domains (like commutative Dedekind domains: see theorem-definition 3.134) have dimension ≤ 1. If $\mathbf{R}$ is a ring, $\mathfrak{a}$ is an ideal in $\mathbf{R}$ and S is a multiplicative subset of $\mathbf{R}$, we have (**exercise**)

$$\sup\left\{\dim(\mathbf{R}/\mathfrak{a}), \dim\left(S^{-1}\mathbf{R}\right)\right\} \leq \dim(\mathbf{R}).$$

(IV) POLYNOMIAL RINGS AND FORMAL POWER SERIES RINGS. We have that $\dim(\mathbf{R}[X]) \geq \dim(\mathbf{R}) + 1$ because if $\mathfrak{p}_0 \subset ... \subset \mathfrak{p}_r$ is a chain of prime ideals in $\mathbf{R}$ with length r, we can construct a chain $\mathfrak{p}'_0 \subset ... \subset \mathfrak{p}'_{r+1}$ of prime ideals in $\mathbf{R}[X]$ with length $r+1$ by setting $\mathfrak{p}'_i = \mathfrak{p}_i\mathbf{R}[X]$ for $0 \leq i \leq n$, and $\mathfrak{p}'_{n+1} = \mathfrak{p}_n\mathbf{R}[X] + X\mathbf{R}[X]$. Using the same reasoning, we can show that $\dim(\mathbf{R}[[X]]) \geq \dim(\mathbf{R}) + 1$, and then by induction that

$$\begin{aligned}&\dim(\mathbf{R}[X_1, ..., X_n]) \geq \dim(\mathbf{R}) + n,\\ &\dim(\mathbf{R}[[X_1, ..., X_n]]) \geq \dim(\mathbf{R}) + n.\end{aligned} \qquad [3.37]$$

THEOREM 3.96.– *If the commutative ring* $\mathbf{R}$ *is Noetherian,*

$$\dim(\mathbf{R}) + n = \dim(\mathbf{R}[X_1, ..., X_n]) = \dim(\mathbf{R}[[X_1, ..., X_n]]). \quad [3.38]$$

PROOF.– We will show the first equality. It is sufficient to show that $\dim(\mathbf{R}[X]) = \dim(\mathbf{R}) + 1$; the general result then follows from Hilbert's basis theorem (corollary 3.49) and an easy argument by induction. Let $\mathfrak{p}$ be a prime ideal with height m in $\mathbf{R}$. There exist $a_1, ..., a_m \in \mathfrak{p}$ such that $\mathfrak{p}$ is a minimal prime ideal in $\mathfrak{a} = (a_1, ..., a_m)$. Then, $\mathfrak{p}[X]$ is a minimal prime ideal in $\mathfrak{a}[X]$ (lemma 3.76(vi)), so $\mathfrak{h}(\mathfrak{p}[X]) \leq m = \mathfrak{h}(\mathfrak{p})$. The reasoning used in the proof of [3.37] now shows that $\dim(\mathbf{R}[X]) = \dim(\mathbf{R}) + 1$.

The second equality follows from lemma 3.31 and the following result ([BKI 98], Chap. VIII, section 3.4, Cor. 2 of Prop. 8): ■

THEOREM 3.97.– *Let* $\mathbf{A}$ *be a commutative Noetherian ring, let* $\mathfrak{a}$ *be an ideal in* $\mathbf{A}$ *and let* $\hat{\mathbf{A}}$ *be the Hausdorff completion of* $\mathbf{A}$ *with respect to the* $\mathfrak{a}$*-adic topology (section 3.1.8(I)). We have that* $\dim\left(\hat{\mathbf{A}}\right) \leq \dim(\mathbf{A})$.

(V) KRULL DIMENSION OF LOCAL RINGS. Let $\mathbf{R}$ be a commutative Noetherian local ring and let $\mathfrak{m} = \text{rad}(R)$, $\kappa_{\mathbf{R}} = \mathbf{R}/\mathfrak{m}$ (section 2.3.7). Let $d(\mathfrak{m})$ be the minimal number of generators of $\mathfrak{m}$.

LEMMA 3.98.– *We have that* $d(\mathfrak{m}) = \dim_{\kappa_{\mathbf{R}}}\left(\mathfrak{m}/\mathfrak{m}^2\right)$.

PROOF.– Let $B = \{x_i : 1 \leq i \leq d\}$ be a minimal generating set of $\mathfrak{m}$, $\bar{x}_i$ the canonical image of x_i in $\mathfrak{m}/\mathfrak{m}^2$, and $\bar{B} = \{\bar{x}_i : 1 \leq i \leq d\}$. We want to show that $\bar{B}$ is a basis of the $\kappa_{\mathbf{R}}$-vector space $\mathfrak{m}/\mathfrak{m}^2$.

If $\bar{B}$ is linearly dependent, there exist $i \in \{1, ..., d\}$ and $r_j \in \kappa_{\mathbf{R}}$, where $j \in \{1, ..., d\}, j \neq i$, such that $\bar{x}_i = \sum_{j \neq i} r_j \bar{x}_j$, and so $x_i \in \sum_{j \neq i} r_j x_j + \mathfrak{m}^2$. Let $C \subseteq \mathfrak{m}$ be the $\mathbf{R}$-module generated by the $x_j, j \in \{1, ..., d\}, j \neq i$. We therefore have

$$C + \mathfrak{m}^2 = \mathfrak{m} \Rightarrow \mathfrak{m}(\mathfrak{m}/C) = \left(C + \mathfrak{m}^2\right)/C = \mathfrak{m}/C.$$

Thus, $\mathfrak{m}/C = 0$ by Nakayama's lemma (lemma 2.41), so $\mathfrak{m} = C$, and B is not minimal: contradiction.

By a similar reasoning, arguing by contradiction, it can be shown that $\bar{B}$ generates the $\kappa_{\mathbf{R}}$-vector space $\mathfrak{m}/\mathfrak{m}^2$ (**exercise**). ■

THEOREM 3.99.– *(Krull) We have that* $\dim(\mathbf{R}) = \mathfrak{h}(\mathfrak{m}) \leq d(\mathfrak{m})$, *so* $\dim(\mathbf{R}) \leq \dim_{\kappa_{\mathbf{R}}}\left(\mathfrak{m}/\mathfrak{m}^2\right)$.

PROOF.– Let $\mathfrak{m} = \left(x_1, ..., x_{d(\mathfrak{m})}\right)$. By the generalized principal ideal theorem (theorem 2.32), $\mathfrak{h}(\mathfrak{m}) \leq d(\mathfrak{m})$. If $\mathfrak{p} \neq \mathfrak{m}$ is a prime ideal, every chain $\mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq ... \supsetneq \mathfrak{p}_h$ of prime ideals with length h gives a chain $\mathfrak{m} \supsetneq \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq ... \supsetneq \mathfrak{p}_h$ with length $h + 1$, so $h < \mathfrak{h}(\mathfrak{m})$. Hence, $\dim(\mathbf{R}) = \mathfrak{h}(\mathfrak{m})$. ■

DEFINITION 3.100.– *A local Noetherian ring* $\mathbf{R}$ *is said to be* regular *if* $\dim(\mathbf{R}) = \dim_{\kappa_{\mathbf{R}}}\left(\mathfrak{m}/\mathfrak{m}^2\right)$. *If so, a* local coordinate system *of* $\mathbf{R}$ *is defined to be any family of* $\mathfrak{m}$ *whose classes* $\left(\text{mod.}\mathfrak{m}^2\right)$ *are a basis of the* $\kappa_{\mathbf{R}}$*-vector space* $\mathfrak{m}/\mathfrak{m}^2$.

THEOREM 3.101.– *If* $\mathbf{R}$ *is a regular local Noetherian ring of dimension* r, *then* $\mathbf{R}[[X_1, ..., X_n]]$ *is a regular local Noetherian ring of dimension* $r + n$.

PROOF.– We know that $\mathbf{R}[[X_1, ..., X_n]]$ is Noetherian (corollary 3.50) and local (lemma 2.62). If $(a_1, ..., a_r)$ is a local coordinate system of $\mathbf{R}$, then $(a_1, ..., a_r, X_1, ..., X_n)$ is a local coordinate system of $\mathbf{R}[[X_1, ..., X_n]]$. ■

If $\mathbf{K}$ is a field, $\mathbf{A} = \mathbf{K}[[X_1, ..., X_n]]$ is a regular local Noetherian ring (theorem 3.101) with residue class field $\kappa_{\mathbf{A}} = \mathbf{K}$ (lemma 2.62), and this ring is complete (lemma 3.31). Conversely ([BKI 98], Chap. VIII, section 5.5, Prop. 6),

THEOREM 3.102.– *Let* $\mathbf{A}$ *be a regular and complete local Noetherian ring whose residue class field* $\kappa_{\mathbf{A}}$ *has characteristic* 0. *Then,* $\mathbf{A} \cong \kappa_{\mathbf{A}}[[X_1, ..., X_n]]$.

The regular local Noetherian rings with dimension 0 are the fields, and those with dimension 1 are the discrete valuation rings (definition 3.61) (**exercise**). It can be shown that a regular local Noetherian ring is not only entire, but is in fact integrally closed ([BKI 98], Chap. VIII, section 5.2, Cor. 1). A local Noetherian ring $\mathbf{A}$ is regular if and only if its completion $\hat{\mathbf{A}}$ is regular ([BKI 98], Chap. VIII, section 5.1, Cor.).

3.2.7. *Algebraic sets*

(I) Now that we have explored the "functorial" approach to algebraic geometry (section 3.2.2**(I)**), we will now discuss the "traditional" approach as conceived at the end of the 19th Century and the beginning of the 20th Century. Let $\mathbf{k}$ be an *algebraically closed field*. We call $\mathbb{A}^n_{\mathbf{k}} := \mathbf{k}^n$ the n-th dimensional *affine space*. Let $A \subset \mathbf{B} := \mathbf{k}[X_1, ..., X_n]$. The set $\mathcal{Z}(A)$ of zeros of A in $\mathbb{A}^n_{\mathbf{k}}$ (definition 3.60) is called the *affine algebraic set* associated with A (in the following, we will omit the adjective *affine*, since *projective* geometry exceeds the scope of this book). Conversely, if $E \subset \mathbb{A}^n_{\mathbf{k}}$, the set $\mathfrak{I}(E) = \{f \in \mathbf{B} : f(x) = 0, \forall x \in E\}$ is an ideal in $\mathbf{B}$ (**exercise**), called the ideal of E in $\mathbf{B}$. If $A \subset A' \subset \mathbf{B}$, then $\mathcal{Z}(A) \supset \mathcal{Z}(A')$ and if $E \subset E' \subset \mathbb{A}^n_{\mathbf{k}}$, then $\mathfrak{I}(E) \supset \mathfrak{I}(E')$, $\mathfrak{I}(E \cup E') = \mathfrak{I}(E) \cap \mathfrak{I}(E')$ (**exercise**), so the two following antitone mappings (with respect to inclusion)

$$\mathfrak{P}(\mathbf{B}) \to \mathfrak{P}(\mathbb{A}^n_{\mathbf{k}}) : A \mapsto A^{\perp} := \mathcal{Z}(A),$$
$$\mathfrak{P}(\mathbb{A}^n_{\mathbf{k}}) \to \mathfrak{P}(\mathbf{B}) : E \mapsto E^{\perp} := \mathfrak{I}(E) \qquad [3.39]$$

form a Galois connection (section 2.1.2**(II)**) that is a lattice morphism from $(\mathfrak{P}(\mathbf{B}), \subset)$ to $(\mathfrak{P}(\mathbb{A}^n_{\mathbf{k}}), \supset)$ (section 2.1.3**(I)**).

(II) The Zariski *topology* of $\mathbb{A}^n_{\mathbf{k}}$ is defined as the topology whose closed sets are the algebraic sets. This indeed satisfies the axioms of a topology, since the

union of two algebraic sets is algebraic, the intersection of a family of algebraic sets is algebraic, and $\varnothing = \mathcal{Z}(\mathbf{B})$ and $\mathbb{A}^n_{\mathbf{k}} = \mathcal{Z}(0)$ are algebraic (**exercise**). An irreducible algebraic set (section 3.2.6**(I)**) is called an *algebraic variety*[5].

For example, in $\mathbf{k}^1$, the closed sets are $\mathbf{k}^1$ and the roots of the polynomials $f \in \mathbf{k}[X]^\times$, i.e. the finite sets; the closed sets of $\mathbf{k}^2$ are $\varnothing$, $\mathbf{k}^2$, curves and points; the closed sets of $\mathbf{k}^3$ are $\varnothing$, $\mathbf{k}^3$, surfaces, curves, points, etc. The Zariski topology is not Hausdorff: the closed sets are "very fine", and so the open sets are "very thick", and in particular the Zariski topology of $\mathbb{C}^n$ is strictly coarser than its usual topology. However, an algebraic set equipped with the Zariski topology is a Kolmogorov space (section 2.3.3) (**exercise**).

The following properties still hold. The first follows from the *Nullstellensatz* (theorem 3.93) and the second follows from the definition: for any ideal $\mathfrak{b} \lhd \mathbf{B}$, $\mathcal{I}(\mathcal{Z}(\mathfrak{b})) = \sqrt{\mathfrak{b}}$, and for any set $E \subset \mathbb{A}^n_{\mathbf{k}}$, $\mathcal{Z}(\mathcal{I}(E)) = \overline{E}$, where $\overline{E}$ is the closure of E in the topological space $\mathbb{A}^n_{\mathbf{k}}$. This implies part (i) of the following result:

THEOREM 3.103.–

i) The Galois connection [3.39] induces a bijection from the set of radical ideals in $\mathbf{B}$ *onto the set of algebraic sets in* $\mathbb{A}^n_{\mathbf{k}}$.

ii) The algebraic set E *is irreducible (section 3.2.6**(I)**) if and only if the ideal* $\mathcal{I}(E)$ *is prime, and so the Galois connection [3.39] induces a bijection between* $\operatorname{Spec}(\mathbf{B})$ *and the set of algebraic varieties in* $\mathbb{A}^n_{\mathbf{k}}$.

PROOF.– (ii) If E is irreducible and $fg \in \mathcal{I}(E)$, then $E \subset \mathcal{Z}(fg) = \mathcal{Z}(f) \cup \mathcal{Z}(g)$, so $E = (E \cap \mathcal{Z}(f)) \cup (E \cap \mathcal{Z}(g))$ where each of the terms in the union is closed. Since E is irreducible, we have either $E = E \cap \mathcal{Z}(f)$ or $E = E \cap \mathcal{Z}(g)$. In the first case, $E \subset \mathcal{Z}(f)$ and $f \in \mathcal{I}(E)$; in the second, $g \in \mathcal{I}(E)$; so, $\mathcal{I}(E)$ is prime. The converse can be shown similarly (**exercise**). ■

A subset of $\mathbb{A}^n_{\mathbf{k}}$ of the form $\Omega_f = \{x \in \mathbb{A}^n_{\mathbf{k}} : f(x) \neq 0\}$, where $f \in \mathbf{k}[X]^\times$ is an irreducible polynomial, is called a *principal open set*. The principal open sets in $\mathbb{A}^n_{\mathbf{k}}$ form a basis for the Zariski topology (see [P2], section 2.1.2); any such set Ω_f is irreducible because $\overline{\Omega_f} = \mathbb{A}^n_{\mathbf{k}}$ is irreducible by theorem 3.103(ii), since the ideal (0) is prime (section 2.3.3**(II)**).

5 For some authors, an algebraic variety is not necessarily irreducible, in which case the terms "algebraic variety" and "algebraic set" are synonymous.

(III) In 3.2.2**(I)**, we saw how the functorial approach to algebraic geometry led us to study the category $\mathbf{k}$-Algc as a whole. Now, let $E = \mathcal{Z}(\mathfrak{b})$ be an algebraic set and let $r_E : \mathbf{B} \to \mathcal{F}(E)$ be the restriction operator $f \mapsto f|_E$, where $\mathcal{F}(E)$ is the ring of polynomial functions over E. Then, r_E is a ring morphism and $\ker(r_E) = \mathfrak{I}(E)$. Hence, (section 2.3.10**(IV)**),

$$\mathcal{F}(E) \cong \Gamma(E) := \mathbf{B}/\mathfrak{I}(E) = \mathbf{B}/\mathfrak{I}(\mathcal{Z}(\mathfrak{b})) = \mathbf{B}/\sqrt{\mathfrak{b}}.$$

This isomorphism reduces the scope of *classical* algebraic geometry to the study of this type of algebras, or, in other words (section 2.3.6), the study of the full subcategory of $\mathbf{k}$-Algc whose objects are *finitely generated reduced* algebras. This limitation is one of the reasons that led A. Grothendieck to reinvent algebraic geometry. A *morphism of algebraic sets* is a mapping $\varphi : E \to F$, that is *regular*, i.e. one that has polynomial components. We write $\mathbf{AlSet}$ for the category of algebraic sets.

THEOREM-DEFINITION 3.104.– *Let $\varphi : E \to F$ be a morphism of algebraic sets. For all $f \in \Gamma(F)$, we define $\varphi^*(f) = f \circ \varphi$. Then, φ^* is a morphism of* $\mathbf{k}$-Algc, *$\varphi^* : \Gamma(F) \to \Gamma(E)$, and $\Gamma : E \to \Gamma(E)$, $\varphi \mapsto \varphi^*$ is a fully faithful contravariant functor $\mathbf{AlSet} \to \mathbf{k}$-Algc **(exercise)**.*

The category $\mathbf{AlSet}$ admits finite products and there is a canonical isomorphism $\Gamma(E \times F) \cong \Gamma(E) \bigotimes_{\mathbf{k}} \Gamma(F)$.

(IV) It follows from theorem 3.103(ii) that an algebraic set E is irreducible if and only if the algebra $\Gamma(E)$ of regular functions on E is an entire ring. Theorem 3.103 and the primary decomposition of ideals (section 3.2.4**(I)**,**(II)**) show that an algebraic set E may be written as the union of a finite number of algebraic varieties $V_1, ..., V_r$, which are uniquely determined if we require that $V_i \not\supseteq V_j$ for $i \neq j$. The V_i $(i = 1, ..., r)$ are called the *irreducible components* of E. Let $E = \mathcal{Z}(\mathfrak{b})$, $\mathfrak{b} = \bigcap_{1 \leq i \leq m} \mathfrak{q}_i$ be a primary decomposition of $\mathfrak{b}$, and let $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$. We have that $E = \bigcup_{1 \leq i \leq m} \mathcal{Z}(\mathfrak{p}_i)$ and the isolated prime ideals are the $\mathfrak{p}_i$ such that $\mathcal{Z}(\mathfrak{p}_i)$ is an irreducible component of E. The other prime ideals $\mathfrak{p}_i$, the embedded prime ideals, are the ideals whose algebraic variety $\mathcal{Z}(\mathfrak{p}_i)$ is embedded in an irreducible variety. For more details, see [EIS 04], [REI 95].

In example 3.74, let $\mathfrak{b} = (X^2, XY)$, $\mathfrak{p}_1 = (X)$, $\mathfrak{p}_2 = (X, Y)$. The algebraic set $\mathcal{Z}(\mathfrak{b})$ is the line $x = 0$ and coincides with $\mathcal{Z}(\mathfrak{p}_1)$, and $\mathcal{Z}(\mathfrak{p}_2)$ is

the origin. The ideal $\mathfrak{b}$ consists of those polynomials $f \in \mathbf{k}[X,Y]$ that vanish at $x = 0$ with multiplicity ≥ 2 at the origin. There are two distinct reduced primary decompositions $\mathfrak{b} = \mathfrak{p}_1 \cap \mathfrak{p}_2^2 = \mathfrak{p}_1 \cap (X^2, Y)$. The prime ideal $\mathfrak{p}_2$ is embedded, which reflects the fact that $\mathcal{Z}(\mathfrak{p}_2) = (0,0) \subsetneq \mathcal{Z}(\mathfrak{p}_1)$; the prime ideal $\mathfrak{p}_1$ is isolated.

(V) Let $E \subset \mathbb{A}^n_{\mathbf{k}}$ be an algebraic variety. Its Krull dimension (section 3.2.6**(I)**) $\dim(E)$ can be clearly and intuitively interpreted: assuming $n \geq 3$, points have dimension 0, curves have dimension 1, surfaces have dimension 2, etc. The bijection established in theorem 3.103(ii) induces a bijection from $\mathrm{Spec}(\Gamma(E))$ onto the set of algebraic subvarieties of E, so

$$\boxed{\dim(\Gamma(E)) = \dim(E)}.$$

3.3. Homological notions

3.3.1. *Projective modules and injective modules*

(I) An $\mathbf{A}$-module P is said to be *projective* if it is a projective object in ${}_{\mathbf{A}}\mathbf{Mod}$ (section 2.2.1), or, in other words, if the functor $\mathbf{j}_P = \mathrm{Hom}_{\mathbf{A}}(P,-) : {}_{\mathbf{A}}\mathbf{Mod} \to \mathbf{Ab}$ is exact, or alternatively if for any exact sequence

$$E_0 \xrightarrow{f} E_1 \xrightarrow{g} E_2$$

in ${}_{\mathbf{A}}\mathbf{Mod}$ the sequence

$$\mathrm{Hom}_{\mathbf{A}}(P,E_0) \xrightarrow{\mathrm{Hom}_{\mathbf{A}}(P,f)} \mathrm{Hom}_{\mathbf{A}}(P,E_1) \xrightarrow{\mathrm{Hom}_{\mathbf{A}}(P,g)} \mathrm{Hom}_{\mathbf{A}}(P,E_2)$$

is exact in $\mathbf{Ab}$ (section 3.1.4**(I)**). Since $\mathbf{j}_P$ is left-exact (section 1.2.9**(I)**), for P to be projective, it is necessary and sufficient for $\mathbf{j}_P$ to be right-exact, i.e. to preserve epimorphisms.

If $P = P' \oplus P''$, then P is projective if and only if P' and P'' are both projective (section 1.2.10**(I)**). Let M, N be two $\mathbf{A}$-modules and let $f : M \twoheadrightarrow N$ be an epimorphism. Let $\beta : {}_{\mathbf{A}}\mathbf{A} \to N$. Then, $\beta(\lambda)$ is of the form $\lambda.y$ $(\lambda \in \mathbf{A}, y \in N)$. There exists $x \in M$ such that $y = f(x)$, so $\beta(\lambda) = \lambda.f(x) = f(\lambda.x)$. Hence, $\beta = f \circ \alpha$ with $\alpha : \lambda \mapsto \lambda.x$. The module ${}_{\mathbf{A}}\mathbf{A}$ is therefore projective, and by [1.8], we have

LEMMA 3.105.– *Every free* $\mathbf{A}$*-module is projective.*

The next result follows from lemmas 3.22 and 3.105:

COROLLARY 3.106.– *Every* $\mathbf{A}$*-module* M *is the quotient of a projective module; in other words, for any* $\mathbf{A}$*-module* M*, there exists a projective* $\mathbf{A}$*-module* P *for which the sequence* $P \to M \to 0$ *is exact. Hence, the category* ${}_{\mathbf{A}}\mathbf{Mod}$ *has* sufficiently many projectives *(section 1.2.10(**I**)).*

THEOREM 3.107.– *The following conditions are equivalent:*

i) P *is projective.*

ii) Every exact sequence

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{\varphi} P \longrightarrow 0 \qquad [3.40]$$

splits (so P *is isomorphic to a direct factor of* M *by lemma-definition 3.15).*

iii) P *is a direct factor of a free module.*

PROOF.– (i)⇒(ii) Consider the diagram

$$\begin{array}{ccccccccc} & & & & & & P & & \\ & & & & & \swarrow^{\varepsilon} & \downarrow{\scriptstyle \nu} & & \\ 0 & \longrightarrow & N & \xrightarrow{f} & M & \xrightarrow{\varphi} & P & \longrightarrow & 0 \end{array}$$

where $\nu = \mathrm{id}_P$. The horizontal row is the exact sequence [3.40], $N = \ker(f)$ and f is inclusion. By (i), there exists $\varepsilon : P \to M$ such that this diagram commutes, and so the exact sequence splits.

(ii)⇒(iii) Let P be a module. By lemma 3.22, there exists a free module M and an epimorphism $\varphi : M \twoheadrightarrow P$, so the sequence [3.40] is exact with $N = \ker(f)$ and where $f : N \to M$ is inclusion. By (ii), this exact sequence splits, so P is a direct factor of a module isomorphic to the free module M.

(iii)⇒(i) If there exists a free module L such that $L = P \oplus P'$, then P and P' are projective, since L is projective. ■

If P is a projective module (resp. a finitely generated projective module), then the canonical homomorphism $c_P : P \to P^{**}$ is injective (resp. bijective) ([BKI 12], Chap. II, section 2.7, Cor. 4). Finitely generated projective $\mathbf{A}$-modules are therefore reflexive (section 3.1.2(**II**)).

(II) An $\mathbf{A}$-module I is *injective* if it is an injective object in ${}_{\mathbf{A}}\mathbf{Mod}$ (section 1.2.10(**II**)), or, in other words, if the (contravariant) functor $\mathbf{h}_I = \mathrm{Hom}_{\mathbf{A}}(-, I) : {}_{\mathbf{A}}\mathbf{Mod}^{\mathrm{op}} \to \mathbf{Ab}$ is exact. Since $\mathbf{h}_I$ is left-exact (section 1.2.9(**I**)), for I to be injective, it is necessary and sufficient for $\mathbf{h}_I$ to be right-exact, i.e. to transform monomorphisms into epimorphisms. By theorem 3.107:

COROLLARY 3.108.– *The $\mathbf{A}$-module I is injective if and only if one of the equivalent conditions (a) or (b) stated below is satisfied:*

a) For every exact sequence $E_0 \xrightarrow{f} E_1 \xrightarrow{g} E_2$ in ${}_{\mathbf{A}}\mathbf{Mod}$, the sequence

$$\mathrm{Hom}_{\mathbf{A}}(E_0, I) \xleftarrow{\mathrm{Hom}_{\mathbf{A}}(f,I)} \mathrm{Hom}_{\mathbf{A}}(E_1, I) \xleftarrow{\mathrm{Hom}_{\mathbf{A}}(g,I)} \mathrm{Hom}_{\mathbf{A}}(E_2, I)$$

is exact in $\mathbf{Ab}$.

b) Every exact sequence $0 \longleftarrow N \xrightarrow{f} M \xleftarrow{\iota} I \longrightarrow 0$ splits.

If $\mathbf{K}$ is a division ring, every vector space over $\mathbf{K}$ is both projective and injective. The following result allows us to characterize injective modules.

THEOREM 3.109.– *(Baer*'s criterion*) The $\mathbf{A}$-module E is injective if and only if every homomorphism $f : \mathfrak{a} \to E$, where $\mathfrak{a}$ is a left ideal in $\mathbf{A}$, can be extended to $\mathbf{A}$, or in other words, is of the form $f(a) = ae$, $e \in E, a \in \mathfrak{a}$.*

PROOF.– Left ideals are submodules of ${}_{\mathbf{A}}\mathbf{A}$, so we need to show that

$$\begin{array}{ccccc} & & E & & \\ & & f\uparrow & & \\ 0 & \longrightarrow & \mathfrak{a} & \xrightarrow{i} & \mathbf{A} \end{array} \quad \Longrightarrow \exists g : \quad \begin{array}{ccccc} & & E & & \\ & & f\uparrow & \nwarrow g & \\ 0 & \longrightarrow & \mathfrak{a} & \xrightarrow{i} & \mathbf{A} \end{array}$$

The necessity of the condition follows from the definition of an injective object (section 1.2.10(**II**)). To show sufficiency, suppose that the following diagram is given (this is the same as the above diagram on the left, with different notations)

$$\begin{array}{ccccc} & & E & & \\ & & f\uparrow & & \\ 0 & \longrightarrow & M & \xrightarrow{i} & N \end{array}$$

where M, N are $\mathbf{A}$-modules and $M \subseteq N$. Let Ω be the set of pairs (M', g'), where $M \subseteq M' \subseteq N$ and $g' : M' \to E$ extends f, and suppose that Ω is

ordered by the relation $(M', g') \leq (M'', g'') \Leftrightarrow M' \subseteq M''$ and g'' extends g'. As in the proof of Zermelo's theorem (theorem 1.5), Ω is inductive and so, by Zorn's lemma (lemma 1.3), has a maximal element $\left(\bar{M}, \bar{g}\right)$. It remains to be shown that $\bar{M} = N$. If not, there exists $b \in \complement_N \bar{M}$, and $\mathfrak{b} = \left\{r \in \mathbf{A} : rb \in \bar{M}\right\}$ is a left ideal $\neq (0)$. Let $h : \mathfrak{b} \to E$ be the homomorphism defined by $h(r) = \bar{g}(rb)$. By the assumptions, there exists a homomorphism $\bar{h} : \mathbf{A} \to E$ extending h. Now, let $\hat{M} = \bar{M} + \mathbf{A}b$ and $\hat{g} : \hat{M} \to E$ be such that

$$\hat{g}(m + rb) = \bar{g}(m) + r\bar{h}(1), \quad \forall m \in \bar{M}, \forall r \in \mathbf{A}.$$

This homomorphism is well-defined and it is easy to check that it extends $\bar{g}$: contradiction. ■

By taking the dual of corollary 3.106 (working in $({}_{\mathbf{A}}\mathbf{Mod})^{\mathrm{op}}$), we deduce

COROLLARY 3.110.– *Every* $\mathbf{A}$*-module* M *is isomorphic to a submodule of some injective* $\mathbf{A}$*-module* I*. Hence, the category* ${}_{\mathbf{A}}\mathbf{Mod}$ *has* sufficiently many injectives *(section 1.2.10(**II**)).*

The product $\prod_{j \in J} I_j$ of $\mathbf{A}$-modules is injective if and only if each I_j is injective (section 1.2.10(**II**)). Furthermore:

THEOREM 3.111.– *If the ring* $\mathbf{A}$ *is left Noetherian, every direct sum of injective* $\mathbf{A}$*-modules is an injective* $\mathbf{A}$*-module.*

PROOF.– Let $(E_k)_{k \in K}$ be a family of injective $\mathbf{A}$-modules, let $\mathfrak{a}$ be a left ideal in $\mathbf{A}$ and let $f : \mathfrak{a} \to E$ be a homomorphism, where $E = \bigoplus_{k \in K} E_k$. By Baer's criterion (theorem 3.109), it is sufficient to show that there exists $\bar{f} : \mathbf{A} \to E$ extending f. Since $\mathbf{A}$ is left Noetherian, $\mathfrak{a}$ is finitely generated, say by $a_1, ..., a_n$. The element $f(a_i) \in E$ may be uniquely written in the form $\sum_{k \in K} f_k(a_i)$, where $f_k(a_i) \in E_k$ and only finitely many of the $f_k(a_i)$ are non-zero. Thus, there exists a finite set of indices S such that $\mathrm{im}(f) \subseteq \bigoplus_{k \in S} E_k$. We have that $\bigoplus_{k \in S} E_k = \prod_{k \in S} E_k$, which is injective. Therefore, there exists a homomorphism $f' : \mathbf{A} \to \mathrm{im}(f)$ that extends f, and $\bar{f} = i \circ f' : \mathbf{A} \to E$ extends f where $i : \bigoplus_{k \in S} E_k \to E$ is inclusion. ■

The notion of a divisible $\mathbf{A}$-module is weaker than that of an injective $\mathbf{A}$-module. Let M be an $\mathbf{A}$-module. An element $m \in M$ is said to be *divisible*

by $a \in \mathbf{A}$ if there exists $m' \in M$ such that $m = am'$, or, in other words, if $m \in aM$.

DEFINITION 3.112.– *Let* $\mathbf{A}$ *be an entire ring*[6]. *The* $\mathbf{A}$*-module* D *is said to be* divisible *if every element* $d \in D$ *is divisible by every element* $a \in \mathbf{A}^{\times}$.

LEMMA 3.113.– *Let* $\mathbf{A}$ *be an entire ring and let* D *be an* $\mathbf{A}$*-module. The following conditions are equivalent:*

i) The $\mathbf{A}$*-module* D *is divisible.*

ii) Given any principal left ideal $\mathfrak{a} = \mathbf{A}a$, *every homomorphism* $f : \mathfrak{a} \to D$ *can be extended to* $\mathbf{A}$.

PROOF.– (i)⇒(ii) Let $f : \mathbf{A}a \to D$, $\lambda \in \mathbf{A}$ and $d = f(a)$. If D is divisible, there exists $d' \in D$ such that $d = ad'$. Let $\bar{f} : {}_{\mathbf{A}}\mathbf{A} \to D$ be the homomorphism defined by $\bar{f}(1) = d'$. We then have $\bar{f}(a) = ad' = d$, so $\bar{f}$ is an extension of f to ${}_{\mathbf{A}}\mathbf{A}$.

(ii)⇒(i) Let $a \in \mathbf{A}^{\times}$, $d \in D$ and $f : \mathbf{A}a \to D$ be such that $f(\lambda a) = \lambda d, \forall \lambda \in \mathbf{A}$. By the assumptions, there exists $\bar{f} : {}_{\mathbf{A}}\mathbf{A} \to D$ extending f. Let $d' = \bar{f}(1)$. Then, $d = \bar{f}(a) = ad'$, so $d \in aD$. ■

COROLLARY 3.114.– *Let* $\mathbf{A}$ *be an entire ring. Every injective* $\mathbf{A}$*-module is divisible.*

REMARK 3.115.– *The converse, which does not hold in general, is obviously true when every left ideal in* $\mathbf{A}$ *is principal, i.e. when* $\mathbf{A}$ *is a principal left ideal domain. See also theorem 3.142. Furthermore, if* $\mathbf{A}$ *is a left Ore domain, then torsion-free* $\mathbf{A}$*-modules are injective if and only if they are divisible ([GEN 60], Prop. 1.1).*

(III) INJECTIVE ENVELOPE.

THEOREM-DEFINITION 3.116.– *Let* M *be an* $\mathbf{A}$*-module. There exists an injective module* I *and a monomorphism* $i : M \hookrightarrow I$ *satisfying the following condition (**E**): (**E**) A submodule* F *of* I *is zero if and only if* $i^{-1}(F)$ *is zero. This module is unique up to isomorphisms that fix the elements of* M. *It is written* $E(M)$ *and is called the* injective envelope *of* M.

6 For the case of a non-entire ring, see ([LAM 99] [3.16], [3.17]).

PROOF.– Suppose that M is a submodule of an injective module E, which we may assume without loss of generality by corollary 3.110. Define $\mathcal{F}$ to be the set of submodules J of E that contain M and satisfy the condition (**E**), ordered by inclusion. This set is inductive, so has a maximal element I_0 by Zorn's lemma. It can be shown that I_0 is a direct factor of E ([BKI 12], Chap. X, section 1.9, Proof of Thm. 2), so $E = I_0 \oplus I_1$, where I_0 and I_1 are both injective (see just before theorem 3.111) and the injective module we are looking for is $I = I_0$. ■

The injective envelope $E(M)$ is therefore a (or, by abuse of language, the) "smallest injective $\mathbf{A}$-module" containing M[7]. We identify M with a submodule of $E(M)$. Below, we will construct the injective envelope of a simple module over a commutative principal ideal domain (section 2.3.8(**IV**)): let $\mathbf{A}$ be one such ring. An $\mathbf{A}$-module S is simple if and only if it is isomorphic to $\mathbf{A}/\mathfrak{p}$, where the ideal $\mathfrak{p}$ is maximal (theorem 2.38), i.e. $\mathfrak{p} = (p)$, where p is prime in $\mathbf{A}$ (theorem 2.57). We write $\mathbf{A}\left(p^i\right) = \mathbf{A}/\left(p^i\right)$ $(i \geq 1)$. The mapping

$$\sigma_j^i : \mathbf{A}\left(p^i\right) \to p^{j-i}\mathbf{A}\left(p^j\right) : x + \left(p^i\right) \mapsto p^{j-i}x + \left(p^j\right), \quad (j \geq i)$$

is an isomorphism that allows us to identify the $\mathbf{A}$-modules $\mathbf{A}\left(p^i\right)$ and $p^{j-i}\mathbf{A}\left(p^j\right) \subseteq \mathbf{A}\left(p^j\right)$. Consider the inclusion $\varphi_j^i : \mathbf{A}\left(p^i\right) \hookrightarrow \mathbf{A}\left(p^j\right)$. Then, $\mathfrak{D} = \left\{\mathbf{A}\left(p^i\right), \varphi_j^i; \mathbb{N}^\times\right\}$ is a direct system (section 1.2.8(**I**)). We now define the inductive limit

$$\mathbf{A}\left(p^\infty\right) := \varinjlim \mathbf{A}\left(p^i\right) = \bigcup\nolimits_{i\geq 1} \mathbf{A}\left(p^i\right).$$

LEMMA 3.117.– *$\mathbf{A}\left(p^\infty\right)$ is the injective envelope of $\mathbf{A}\left(p^i\right)$ for all $i \geq 1$.*

PROOF.– 1) With the identifications described above, we have $\mathbf{A}\left(p^i\right) \subseteq \mathbf{A}\left(p^\infty\right)$.

2) To show that the $\mathbf{A}$-module $\mathbf{A}\left(p^\infty\right)$ is injective, it is sufficient to prove that it is divisible (remark 3.115). Let $0 \neq x \in \mathbf{A}\left(p^\infty\right)$ and $a \in \mathbf{A}^\times$. Let i be the smallest index such that $x \in \mathbf{A}\left(p^i\right)$ and write $a = p^k q$, where $k \in \mathbb{N}$ and q is not divisible by p. We have that $p^k\mathbf{A}\left(p^{i+k}\right) = \mathbf{A}\left(p^i\right)$, so x is of the

7 Even though the injective envelope is "essentially unique", it is not the solution of a universal problem [ADÁ 02].

form $p^k y$, where $y \in \mathbf{A}\left(p^{i+k}\right)$ and so $p^{i+k}y = 0$. Since p^i and q are coprime, there exist $u, v \in \mathbf{A}$ satisfying the Bézout equation $up^i + vq = 1$. Therefore, $up^i x + vqx = x \Rightarrow x = vqx = vp^k qy = avy$, hence $\mathbf{A}\left(p^\infty\right)$ is divisible.

3) Consider an injective $\mathbf{A}$-module containing $\mathbf{A}\left(p^i\right), i \geq 1$. This module therefore contains $p\mathbf{A}\left(p^i\right)$, and so contains $p^{j-i}\mathbf{A}\left(p^i\right)$ for all $j \geq i$. However, $p^{j-i}\mathbf{A}\left(p^i\right)$ may be identified (via the isomorphism σ_j^i) with $\mathbf{A}\left(p^j\right)$. It therefore contains $\mathbf{A}\left(p^\infty\right)$, and hence $\mathbf{A}\left(p^\infty\right) = E\left(\mathbf{A}\left(p^i\right)\right)$. ■

3.3.2. *Malgrange isomorphism*

The ideas in this subsection were proposed by B. Malgrange [MAL 63]. They are similar to the ideas of A. Grothendieck presented in section 3.2.2(**I**) and were greatly inspired by them. Let $\mathbf{A}$ be a ring, W an $\mathbf{A}$-module, $v \in W^Q$ and $R_2 \in \mathbf{A}^{Q\times(K)}$. The problem that we shall study here is whether there exist solutions $w \in W^K$ of the equation

$$R_2.w = v. \qquad [3.41]$$

Let $(r_l)_{l\in S}$ be a generating family of $\ker(\bullet R_2)$, and let $R_1 \in \mathbf{A}^{S\times(Q)}$ be the matrix with l-th row r_l. Then, the sequence

$$\mathbf{A}^{1\times(K)} \xleftarrow{\bullet R_2} \mathbf{A}^{1\times(Q)} \xleftarrow{\bullet R_1} \mathbf{A}^{1\times(S)} \qquad [3.42]$$

is exact (see theorem 3.44). Since $R_1R_2 = 0$, [3.41] implies the *compatibility condition*

$$R_1.v = 0. \qquad [3.43]$$

EXAMPLE 3.118.– *Let* $\mathbf{A}$ *be the ring* $\mathbb{C}[X_1, ..., X_n]$, Ω *a non-empty open set of* $\mathbb{R}^n$ *and let* $W = C^\infty(\Omega)$ *be the* $\mathbb{C}$*-vector space of complex functions that are infinitely differentiable on* Ω. *Since the ring* $\mathbf{A} = \mathbb{C}[X_1, ..., X_n]$ *is Noetherian by Hilbert's basis theorem (corollary 3.49), we can assume that* $K = \{1, ..., k\}$, $Q = \{1, ..., q\}$ *and* $S = \{1, ..., s\}$. *The ring* $\mathbf{A}$ *acts on* W *by* $X_i.f = \partial f/\partial x^i$, *which makes* W *a left* $\mathbf{A}$*-module. Any matrix* $R_2 \in \mathbf{A}^{q\times k}$ *may therefore be interpreted as a matrix of linear operators involving partial derivatives with constant coefficients and [3.41] is a system of linear partial differential equations with right-hand side* $v \in W^q$; *we look for a solution* w *in* W^k.

Let $\mathbf{Cop}_{\mathbf{A}}$ be the category whose objects are the copowers $\mathbf{A}^{1\times(K)}$ of $\mathbf{A}$ (section 1.2.6(**II**)) and whose morphisms are right-multiplication $(\bullet R_2) : \mathbf{A}^{1\times(Q)} \to \mathbf{A}^{1\times(K)}$ by the matrices $R_2 \in \mathbf{A}^{Q\times(K)}$. Let $\mathbf{h}_W\left(\mathbf{A}^{1\times(-)}\right) : \mathbf{Cop}_{\mathbf{A}} \to {}_{\mathbf{A}}\mathbf{Mod}$ be the functor $\mathbf{A}^{1\times(K)} \mapsto \mathbf{h}_W\left(\mathbf{A}^{1\times(K)}\right)$, $(\bullet R_2) \mapsto \mathbf{h}_W(\bullet R_2)$, where $\mathbf{h}_W$ is the functor defined in section 1.2.3. Furthermore, let $\mathbf{Pow}_W$ be the category whose objects are the powers W^K of W and whose morphisms are left-multiplication $(R_2\bullet) : W^K \to W^Q$ by the matrices $R_2 \in \mathbf{A}^{Q\times(K)}$. Let id be the identity functor of $\mathbf{Pow}_W$. The following theorem shows that there exists a functorial isomorphism (section 1.2.2(**I**)) called the *Malgrange isomorphism*.

THEOREM 3.119.– *(Malgrange) There is a functorial isomorphism* $\mathbf{t} : \mathbf{h}_W\left(\mathbf{A}^{1\times(-)}\right) \mapsto \mathrm{id}$ *defined as follows: for every index set* K*, let* $(\varepsilon_k)_{k\in K}$ *be the canonical basis of* $\mathbf{A}^{1\times(K)}$*. Then, for every* $\mathbf{A}$*-homomorphism* $\psi : \mathbf{A}^{1\times(K)} \to W$, $\mathbf{t}_K(\psi) \in W^K$ *is the column whose* k*-th element is* $\psi(\varepsilon_k)$*; for every morphism of copowers* $(\bullet R_2) : \mathbf{A}^{1\times(Q)} \to \mathbf{A}^{1\times(K)}$*, the following diagram commutes:*

$$\begin{array}{ccc} \mathbf{h}_W\left(\mathbf{A}^{1\times(K)}\right) & \overset{\mathbf{h}_W(\bullet R_2)}{\longrightarrow} & \mathbf{h}_W\left(\mathbf{A}^{1\times(Q)}\right) \\ \mathbf{t}_K \downarrow & & \mathbf{t}_Q \downarrow \\ W^K & \overset{R_2\bullet}{\longrightarrow} & W^Q \end{array} \qquad [3.44]$$

PROOF.– It is clear that $\mathbf{t}_K : \mathbf{h}_W\left(\mathbf{A}^{1\times(K)}\right) \to W^K$ is an $\mathbf{A}$-linear isomorphism. Now, let $R_2 \in \mathbf{A}^{Q\times(K)}$ and $\psi : \mathbf{A}^{1\times(K)} \to W$. We have that $(\mathbf{t}_Q \circ \mathbf{h}_W(\bullet R_2))(\psi) = \mathbf{t}_Q(\psi \circ (\bullet R_2))$, so the k-th element of $\mathbf{t}_Q(\psi \circ (\bullet R_2))$ is $R_2.(\psi(\varepsilon_k)) = (R_2\bullet)\psi(\varepsilon_k) = R_2(\mathbf{t}_K(\psi))$. Hence, the diagram [3.44] commutes, which shows that $\mathbf{t}$ is a functorial morphism. ■

Hence, $\mathbf{h}_W\left(\mathbf{A}^{1\times(K)}\right)$ and $\mathbf{h}_W(\bullet R_2)$ may be identified with W^K and $R_2\bullet$, respectively.

COROLLARY 3.120.– *The kernel* $\ker_W(R_2\bullet) := \left\{w \in W^K : R_2.w = 0\right\}$ *may be identified with the abelian group* $\mathbf{h}_W(M)$ *where* $M := \mathrm{coker}_{\mathbf{A}}(\bullet R_2)$.

PROOF.– The contravariant functor $\mathbf{h}_W$ is left-exact, so the exact sequence

$$0 \longleftarrow M \longleftarrow \mathbf{A}^{1\times(K)} \overset{\bullet R_2}{\longleftarrow} \mathbf{A}^{1\times(Q)}$$

implies the exact sequence

$$0 \longrightarrow \mathbf{h}_W(M) \longrightarrow W^K \xrightarrow{R_2\bullet} W^Q. \qquad \blacksquare$$

For every subset $U \subset \mathbf{A}^{1\times(K)}$, define

$$U^{\perp} := \left\{ w \in W^K : r.w = 0, \forall r \in U \right\}.$$

Similarly, for every subset $\mathfrak{S} \subset W^K$, define

$$\mathfrak{S}^{\perp} = \left\{ r \in \mathbf{A}^{1\times(K)} : r.w = 0, \forall w \in \mathfrak{S} \right\}.$$

In particular, we have

$$U^{\perp} = \ker_W(R_2\bullet) \text{ with } U = \mathrm{im}_{\mathbf{A}}(\bullet R_2) := \mathbf{A}^{1\times(Q)} R_2.$$

REMARK 3.121.– *1) It can be useful to make the Malgrange isomorphism* $\ker_W(R\bullet) \cong \mathbf{h}_W(M)$ *more explicit, where* $M := \mathrm{coker}_{\mathbf{A}}(\bullet R) := \mathbf{A}^{1\times(K)}/U$, $U := \mathbf{A}^{1\times(Q)} R$ *and* $\mathbf{h}_W(M) := \mathrm{Hom}_W(M, W)$. *Let* $w \in \ker_W(R\bullet)$ *and* $\phi_w : M \to W : \bar{g} \mapsto gw$ *where* $g \in \mathbf{A}^{1\times(K)}$ *and* $\bar{g} = g + U$.

a) The $\mathbb{Z}$*-linear mapping* $\phi : \ker_W(R\bullet) \to \mathbf{h}_W(M) : w \mapsto \phi_w$ *is well-defined, since*

$$\bar{g}_1 = \bar{g}_2 \Leftrightarrow g_1 - g_2 \in U \Rightarrow ((g_1 - g_2)\, w = 0, \forall w \in \ker_W(R\bullet)).$$

b) ϕ *is injective, since* $\phi_w = 0 \Rightarrow \left(gw = 0, \forall g \in \mathbf{A}^{1\times(K)}\right) \Rightarrow w = 0$.

c) ϕ *is surjective. Indeed, with the above notation, let* $\bar{\sigma} \in \mathbf{h}_W(M)$, $\bar{\sigma} : M \ni \bar{g} \mapsto \bar{\sigma}(\bar{g}) \in W$. *The homomorphism* $\bar{\sigma}$ *is induced by a homomorphism* $\sigma : \mathbf{A}^{1\times(K)} \to W$ *such that* $\sigma(U) = 0$ *(theorem-definition 2.11). After proving theorem 3.119, we identified* σ *with* $\psi(\sigma) = w \in W^K$. *Then,* $\sigma(U) = 0 \Leftrightarrow w \in \ker_W(R\bullet)$, *so* $\bar{\sigma} = \phi_w$ *where* $w \in \ker_W(R\bullet)$.

*2) As we did in section 3.1.6(**II**), it can be useful to write* $\mathbf{w}_i$ $(i \in K)$ *for the canonical image of the* i*-th element of the canonical basis of* $\mathbf{A}^{1\times(K)}$ *in* $M = \mathbf{A}^{1\times(K)}/\mathbf{A}^{1\times(Q)} R$, *and* $\mathbf{w} = (\mathbf{w}_i)_{i\in K}$ *for the column of elements* $\mathbf{w}_i$, *since then* $M = [\mathbf{w}]_{\mathbf{A}}$ *and* $\mathbf{w}$ *satisfies the single condition* $R\mathbf{w} = 0$. *The elements* $\mathbf{w}_i$ *of the* cokernel $M = \mathrm{coker}_{\mathbf{A}}(\bullet R)$ *should not be confused with the components* w_i *of the elements* w *of the* kernel $\ker_W(R\bullet) \subset W^K$, *which also satisfy the condition* $Rw = 0$. *With the notation from (1), it is clear that an element* $w \in \ker_W(R\bullet)$ *is determined by* $\phi_w(\mathbf{w}_i)$ $(i \in K)$.

LEMMA 3.122.– *The two functions* $(\bullet)^{\perp} : U \mapsto U^{\perp}, \mathfrak{S} \mapsto \mathfrak{S}^{\perp}$ *give a Galois connection (section 2.1.2(**II**)) with respect to inclusion. Hence (theorem 2.3),* $U \subset U^{\perp\perp}$, $\mathfrak{S} \subset \mathfrak{S}^{\perp\perp}$.

PROOF.– If $\mathfrak{S} \subset U^{\perp}$ and $r \in U$, $w \in U$, we have that $r.w = 0$, so $r \in \mathfrak{S}^{\perp}$, and the implication $\mathfrak{S} \subset U^{\perp} \Rightarrow U \subset \mathfrak{S}^{\perp}$ therefore holds. By symmetry, this implication is an equivalence. ■

THEOREM 3.123.– *The following conditions are equivalent:*

i) The module ${}_{\mathbf{A}}W$ *is injective.*

ii) For any exact sequence [3.42], the compatibility condition [3.43], where $v \in W^Q$, *implies that equation [3.41] has a solution* $w \in W^K$.

PROOF.– (i)⇒(ii) If W is injective, the functor $\mathbf{h}_W = \mathrm{Hom}_{\mathbf{A}}(-, W)$ is exact, so the exactness of the sequence [3.42] implies that the first row of the diagram

$$\begin{array}{ccccc} \mathbf{h}_W\left(\mathbf{A}^{1\times(K)}\right) & \xrightarrow{\mathbf{h}_W(\bullet R_2)} & \mathbf{h}_W\left(\mathbf{A}^{1\times(Q)}\right) & \xrightarrow{\mathbf{h}_W(\bullet R_1)} & \mathbf{h}_W\left(\mathbf{A}^{1\times(N)}\right) \\ \mathbf{t}_K \downarrow & & \mathbf{t}_Q \downarrow & & \mathbf{t}_N \downarrow \\ W^K & \xrightarrow{R_2\bullet} & W^Q & \xrightarrow{R_1\bullet} & W^N \end{array} \qquad [3.45]$$

is exact. This diagram commutes by theorem 3.119, so the second row of the diagram is exact.

(ii)⇒(i) Let $\mathfrak{a}$ be a left ideal in $\mathbf{A}$, let $(a_j)_{j\in Q}$ be a generating family of $\mathfrak{a}$ and let $R_2 \in \mathbf{A}^{Q\times 1}$ be the column with j-th element a_j. Let $(r_l)_{l\in N}$ be a generating family of $\ker_{\mathbf{A}}(\bullet R_2)$ and let $R_1 \in \mathbf{A}^{N\times(Q)}$ be the matrix with l-th row r_l. Then, the sequence [3.42] is exact, and since $\mathrm{im}_{\mathbf{A}}(\bullet R_2) = \mathfrak{a}$, the sequence

$$0 \longleftarrow \mathfrak{a} \xleftarrow{(\bullet R_2)_{ind}} \mathbf{A}^{1\times(Q)} \xleftarrow{\bullet R_1} \mathbf{A}^{1\times(N)},$$

is exact, where $(\bullet R_2)_{ind} : \mathbf{A}^{1\times(Q)} \to \mathfrak{a}$ is the homomorphism induced by $\bullet R_2$ (theorem-definition 2.11), so $\mathfrak{a} = \mathrm{coker}_{\mathbf{A}}(\bullet R_1)$. By corollary 3.120, $\mathrm{Hom}_{\mathbf{A}}(\mathfrak{a}, W) = \ker_W(R_1\bullet)$. Now, (ii) implies that $\ker_W(R_1\bullet) = \mathrm{im}_W(R_2\bullet)$, so $(R_2\bullet)_{ind} : W = \mathrm{Hom}_{\mathbf{A}}({}_{\mathbf{A}}\mathbf{A}, W) \to \mathrm{Hom}_{\mathbf{A}}(\mathfrak{a}, W)$ is an epimorphism, and hence, for any $\mathbf{A}$-homomorphism $f : \mathfrak{a} \to W$, there exists an $\mathbf{A}$-homomorphism $f' : {}_{\mathbf{A}}\mathbf{A} \to W$ such that $f = (R_2\bullet)_{ind}(f')$. Therefore, for all $a \in \mathfrak{a}$, $f(a) = (R_2\bullet)_{ind}(f')(a) = (R_2\bullet)_{ind}(f')(1).a = w.a$ with $w = (R_2\bullet)_{ind}(f')(1)$. By Baer's criterion (theorem 3.109), W is injective. ■

If the ring $\mathbf{A}$ is left Noetherian (as in example 3.118, by Hilbert's basis theorem: see section 3.1.7), the statement of the theorem also holds when the index sets N, Q, P are finite.

3.3.3. *Injective cogenerators*

(I) Suppose that the ring $\mathbf{A}$ is the one from example 3.118 and suppose that, as in this example, [3.41] is identified with a system of differential equations. For simplicity, we shall consider the case where $n = 1$ (ordinary differential equations). Let W be an $\mathbf{A}$-module with the action $(\mathbf{A}, W) \to W$ uniquely determined by the relation $X.f = df/dt$. Consider first the case with right-hand side $v = 0$. Given R_2, i.e. the equations of the differential system, we can find $\ker_W (R_2 \bullet)$, as we will see in detail in section 3.4.2. Here, we are interested in the opposite approach: which conditions are required, and to what extent do the solutions of [3.41] in W^k allow the equations to be determined? Clearly, if $W = \{0\}$, this is impossible. The differential equation $df/dt - af = 0$ must have non-zero solutions for every $a \in \mathbb{C}$, so W must contain every exponential $t \mapsto e^{at}$ (which we will simply write e^{at}). The set of all solutions of the equation $(d/dt - a)^n f = 0$ is the $\mathbb{C}$-vector space generated by the exponential polynomials $e^{at}, te^{at}, ..., t^{n-1}e^{at}$, so any $\mathbf{A}$-module satisfying the desired properties must contain the $\mathbf{A}$-module $W_0 = \bigoplus_{a \in \mathbb{C}} \mathbb{C}[t]\, e^{at}$, called the vector space *of exponential polynomials* (over $\mathbb{C}$).

(II) Let $\mathbf{A}$ be a ring. We say that an $\mathbf{A}$-module W is a cogenerator if it is a cogenerator in the category ${}_{\mathbf{A}}\mathbf{Mod}$ (section 1.2.11), i.e. if the functor $\mathbf{h}_W : {}_{\mathbf{A}}\mathbf{Mod}^{\mathrm{op}} \to \mathbf{Ab}$ is faithful.

LEMMA 3.124.– *Let W be an $\mathbf{A}$-module. The following conditions are equivalent:*

i) W is a cogenerator;

ii) For every homomorphism $0 \neq f : M_1 \to M_2$, there exists $g : M_2 \to W$ such that $g \circ f \neq 0$;

iii) For every element $x \neq 0$ in an $\mathbf{A}$-module M, there exists $g : M \to W$ such that $g(x) \neq 0$.

iv) For every $\mathbf{A}$-module M, there exists an index set I and a monomorphism $M \hookrightarrow W^I$.

PROOF.– We have that (i)⇔(ii) by the definition of a cogenerating object, and (i)⇔(iv) by proposition 1.25(2). (ii)⇒(iii) Let $f : \mathbf{A} \to M$ be the homomorphism uniquely determined by the relation $f(1) = x$. Let $g : M \to W$ be such that $g \circ f \neq 0$. We have that $g(x) \neq 0$. (iii)⇒(iv) If $M = 0$, there is nothing to show. If $M \neq 0$, for all $0 \neq x \in M$, let $\pi_x : M \to W$ be such that $\pi_x(x) \neq 0$. Then, $\pi = (\pi_x)_{x \in I}$ is a monomorphism $M \hookrightarrow W^I$ with $I = \{x \in M : x \neq 0\}$. ■

Hence, if W, W' are $\mathbf{A}$-modules such that $W' \supseteq W$, and W is a cogenerator, then W' is a cogenerator. The following result, established in ([OBE 90], p. 35, Thm. 61) and ([BLS 09], p. 2056, Thm. 2.13), answers the question from **(I)**:

THEOREM 3.125.– *The following conditions are equivalent:*

i) The $\mathbf{A}$*-module* W *is a cogenerator;*

ii) $\mathbf{Sol}_W := \mathbf{h}_W({}_{\mathbf{A}}\mathbf{Mod})$ *is a subcategory of* $\mathbf{Ab}$ *and the functor* $\mathfrak{S}_W : {}_{\mathbf{A}}\mathbf{Mod} \to \mathbf{Sol}_W$ *induced by* $\mathbf{h}_W$ *is faithful;*

iii) For any submodule $U \subseteq \mathbf{A}^{1\times(K)}$, $U = U^{\perp\perp}$, *or, in other words, the Galois connection from lemma 3.122, is bijective;*

iv) Given two matrices $R \in \mathbf{A}^{Q\times(K)}, R' \in \mathbf{A}^{Q'\times(K)}$ *(whose rows have the same cardinal* $\mathrm{Card}(K)$*), we have that* $\ker_W(R'\bullet) \subseteq \ker_W(R\bullet)$ *if and only if there exists a matrix* $X \in \mathbf{A}^{Q\times(Q')}$ *such that* $R = XR'$.

PROOF.– (i)⇔(ii) by the definition of a cogenerating module and lemma 3.17. (i)⇒(iii): If $r \in \mathfrak{C}_{\mathbf{A}^{1\times(K)}}U$ and $\bar{r} = r + U$, we have that $\bar{r} \neq 0$. Therefore, by lemma 3.124, there exists $\bar{\eta} : \mathbf{A}^{1\times(K)}/U \to W$ such that $\bar{\eta} \neq 0$, and by theorem-definition 2.11, the homomorphism $\bar{\eta}$ is induced by $\eta : \mathbf{A}^{1\times(K)} \to W$ such that $\eta(U) = 0 \Leftrightarrow \eta \in U^{\perp}$. Since $\eta(r) \neq 0$, we have that $r \notin U^{\perp\perp}$. (iii)⇒(i): If $U = U^{\perp\perp}$ for all $U \subseteq \mathbf{A}^{1\times(K)}$, the mapping $M := \mathbf{A}^{1\times(K)}/U \mapsto U^{\perp}$ is injective, because

$$U_1^{\perp} = U_2^{\perp} \Rightarrow U_1^{\perp\perp} = U_2^{\perp\perp} \Rightarrow \mathbf{A}^{1\times(K)}/U_1 = \mathbf{A}^{1\times(K)}/U_2.$$

Therefore, the mapping $\phi_M := (w)_{w \in U^{\perp}} : M \to W^{U^{\perp}}$ is injective, which proves (i) by proposition 1.25(2). (iii)⇒(iv) if $R = XR'$, it is clear that $\ker_W(R'\bullet) \subseteq \ker_W(R\bullet)$. Conversely, if this inclusion holds, let $U = \mathrm{im}_{\mathbf{A}}(\bullet R), U' = \mathrm{im}_{\mathbf{A}}(\bullet R')$. We have $U'^{\perp} \subseteq U^{\perp}$, so $U'^{\perp\perp} \supseteq U^{\perp\perp}$ and

by (i) $U' \supseteq U$, which implies that $\mathrm{im}_{\mathbf{A}}(\bullet R') \supseteq \mathrm{im}_{\mathbf{A}}(\bullet R)$. The homomorphism $(\bullet R') : \mathbf{A}^{1\times(Q')} \to \mathrm{im}_{\mathbf{A}}(\bullet R')$ is an epimorphism and the free module $\mathbf{A}^{1\times(Q)}$ is projective (lemma 3.105). Therefore (section 1.2.10**(I)**), there exists a homomorphism $(\bullet X) : \mathbf{A}^{1\times(Q)} \to \mathbf{A}^{1\times(Q')}$ such that $R = XR'$, like in the following commutative diagram:

$$\begin{array}{ccc} & & \mathbf{A}^{1\times(Q)} \\ & {\scriptstyle(\bullet X)}\swarrow & \downarrow{\scriptstyle(\bullet R)} \\ \mathbf{A}^{1\times(Q')} & \xrightarrow{(\bullet R')} & \mathrm{im}_{\mathbf{A}}(\bullet R') \end{array}$$

(iv)⇒(iii): Let $U \subseteq \mathbf{A}^{1\times(K)}$. This module is the quotient of a free module $\mathbf{A}^{1\times(Q)}$ (lemma 3.22), and so, there exists an epimorphism $\varphi : \mathbf{A}^{1\times(Q)} \twoheadrightarrow U$. Let $f : \mathbf{A}^{1\times(Q)} \to \mathbf{A}^{1\times(K)} : x \mapsto \varphi(x)$. The homomorphism f is represented by a matrix R with respect to the canonical bases, or in other words, $f = (\bullet R)$ and $U = \mathbf{A}^{1\times(Q)}R$. Similarly, $U^{\perp\perp} \subseteq \mathbf{A}^{1\times(K)}$ is of the form $U^{\perp\perp} = \mathbf{A}^{1\times(Q')}R'$. We have that $U^{\perp\perp\perp} = U^{\perp}$ (theorem 2.3), so $\ker_W(R'\bullet) = \ker_W(R\bullet)$, hence (by (iv)) there exists $X' \in \mathbf{A}^{Q'\times(Q)}$ such that $R' = X'R$, and therefore, $U^{\perp\perp} = \mathbf{A}^{1\times(Q')}X'R \subseteq U$. Consequently, $U^{\perp\perp} = U$. ■

(III) An $\mathbf{A}$-module is an injective cogenerator if and only if $\mathbf{h}_W$ is exact and faithful (section 3.3.1**(II)**), or, in other words, if $\mathfrak{S}_W : {}_{\mathbf{A}}\mathbf{Mod} \to \mathbf{Sol}_W$ is an *exact anti-isomorphism* (lemma 3.17 & section 1.2.2**(I)**). This implies

THEOREM 3.126.– *The following conditions are equivalent:*

i) W is an injective cogenerator;

ii) Given three $\mathbf{A}$-modules M_1, M_2, M_3, the sequence $M_1 \xleftarrow{f} M_2 \xleftarrow{g} M_3$ is exact in ${}_{\mathbf{A}}\mathbf{Mod}$ if and only if the sequence

$$\mathbf{h}_W(M_1) \xrightarrow{\mathbf{h}_W(f)} \mathbf{h}_W(M_2) \xrightarrow{\mathbf{h}_W(g)} \mathbf{h}_W(M_3)$$

is exact in $\mathbf{Ab}$.

COROLLARY 3.127.– *Let W be an injective $\mathbf{A}$-module. The following conditions are equivalent:*

i) W is a cogenerator;

ii) For every simple $\mathbf{A}$-module S, $\mathrm{Hom}_{\mathbf{A}}(S, W) \neq 0$;

iii) For every simple $\mathbf{A}$*-module* S*, there exists an index set* I *and a monomorphism* $S \hookrightarrow W^I$.

PROOF.– The implication (i)⇒(ii) is obvious and (ii)⇒(iii) follows from the proof of lemma 3.124.

(iii)⇒(ii): Let $f : S \hookrightarrow W^I : x \mapsto (f_i(x))_{i\in I}$. If $0 \neq x \in S$, there exists $i \in I$ such that $f_i(x) \neq 0$, so $\mathrm{Hom}_{\mathbf{A}}(S, W) \neq 0$.

(ii)⇒(i): Let $M \neq 0$ be an $\mathbf{A}$-module and $0 \neq x \in M$; the submodule $\mathbf{A}x$ of M has a simple quotient S by corollary 2.35. If $\mathrm{Hom}_{\mathbf{A}}(S, W) \neq 0$, we have that $\mathrm{Hom}_{\mathbf{A}}(\mathbf{A}x, W) \neq 0$ and there exists a non-zero homomorphism $f : \mathbf{A}x \to W$. Since W is injective, Baer's criterion (theorem 3.109) implies that there exists a non-zero homomorphism $g : M \to W$ such that $g|_{\mathbf{A}x} = f$, so $g(x) \neq 0$ and W is a cogenerator by lemma 3.124. ■

In particular, if $\mathbf{K}$ is a division ring, every left $\mathbf{K}$-vector space is an injective cogenerator (**exercise**).

DEFINITION 3.128.– *Let* $\mathbf{A}$ *be a ring and let* $(S_i)_{i\in I}$ *be a family of simple* $\mathbf{A}$*-modules. We say that this family is a* representative system *of simple* $\mathbf{A}$*-modules if, for every simple* $\mathbf{A}$*-module* S*, there exists exactly one index* $i \in I$ *such that* $S \cong S_i$.

COROLLARY-DEFINITION 3.129.– *Let* $\mathbf{A}$ *be a ring,* $(S_i)_{i\in I}$ *a representative system of simple* $\mathbf{A}$*-modules, and* $E(S_i)$ *the injective envelope of* S_i *(theorem-definition 3.116).*

i) The $\mathbf{A}$*-module* $W_0 := \bigoplus_{i\in I} E(S_i)$ *is a cogenerator, and is injective if* $\mathbf{A}$ *is left Noetherian. The* $\mathbf{A}$*-module* $E(W_0)$ *is an injective cogenerator.*

ii) An $\mathbf{A}$*-module* W *is a cogenerator if and only if there is a monomorphism* $W_0 \hookrightarrow W$.

The $\mathbf{A}$*-module* W_0 *(which is unique up to isomorphism) is called the* canonical $\mathbf{A}$-cogenerator.

PROOF.– i) immediately follows from corollary 3.127 and theorem 3.111.

ii): If there exists a monomorphism $W_0 \hookrightarrow W$, then W is a cogenerator by lemma 3.124. Conversely, let W be a cogenerator. For every simple $\mathbf{A}$-module

S, by lemma 3.124 there exists a homomorphism $0 \neq g : S \to W$ that may be extended to a homomorphism $\bar{g} : E(S) \to W$ (section 1.2.10**(I)**) such that $\bar{g}|_S \neq 0$. Then, $\ker(\bar{g}) \cap S \subsetneq S$, and since S is simple, $\ker(\bar{g}) \cap S = 0$. Therefore, $\bar{g}$ is a monomorphism $E(S) \hookrightarrow W$. For all $i \in I$, we thus have $E(S_i) \hookrightarrow W$, so $W_0 \hookrightarrow W$. ■

(IV) Let $\mathbf{A}$ be a principal ideal domain. With the notation from lemma 3.117, the $\mathbf{A}$-module

$$W_0 = \bigoplus\nolimits_{p \in P} \mathbf{A}\left(p^{\infty}\right)$$

is therefore a canonical cogenerator, where P is a representative system of prime elements of $\mathbf{A}$ (definition 2.53). Since $\mathbf{A}$ is Noetherian, W_0 is injective.

EXAMPLE. Let us return to the example considered in the introduction of this subsection: we have that $\mathbf{A} = \mathbb{C}[X]$, which is a principal ideal domain (section 2.3.9**(I)**). The prime elements of $\mathbf{A}$ are the $X - a, a \in \mathbb{C}$. For $n \geq 1$, let $C_{n,a}$ be the $\mathbb{C}$-vector space generated by the n exponential polynomials $e^{at}, te^{at}, ..., t^{n-1}e^{at}$. Let

$$\psi : \mathbf{A} \twoheadrightarrow C_{n,a} : p \mapsto p\left(d/dt\right) t^{n-1} e^{at}.$$

We have that $\ker \psi = \left(p_a^n\right)$, where $p_a(X) := X - a$. Hence, by Noether's first isomorphism theorem (theorem 2.12(1)), we have the isomorphism of $\mathbf{A}$-modules $C_{n,a} \cong \mathbf{A}\left(p_a^n\right) := \mathbf{A}/\left(p_a^n\right)$, which implies that

$$W_0 \cong \sum_{n \geq 1, a \in \mathbb{C}} C_{n,a} = \bigoplus\nolimits_{a \in \mathbb{C}} \mathbb{C}[t]\, e^{at},$$

which is consistent with the heuristic analysis performed at the beginning of this subsection. Let $W = C^{\infty}(\mathbb{R})$ be the space of infinitely differentiable functions on the real line. We have that $W \supseteq W_0$, so W is a cogenerating $\mathbf{A}$-module. Moreover, the elementary theory of linear differential equations with constant coefficients shows that W is divisible. It is therefore an injective cogenerator.

(V) Recall that a subspace A of a real or complex vector space is convex if whenever two arbitrary points x, y belong to A, the interval $[x, y] = \{\lambda x + (1 - \lambda) y : \lambda \in [0, 1] \subset \mathbb{R}\}$ is included in A. In the more

general case in example 3.118, we have the following result. Part (i) (which is difficult to prove[8]) was established by L. Ehrenpreis, V. Palamodov and B. Malgrange (see, for example, [PAL 70], Chap. VII, Cor. 4, p. 309); part (ii) was shown in [OBE 90], [OBE 95]:

THEOREM 3.130.– *Suppose that the open set* $\Omega \subset \mathbb{R}^n$ *is convex.*

i) The $\mathbb{C}[X_1, ..., X_n]$*-module* $C^\infty(\Omega)$ *is injective.*

ii) The canonical $\mathbb{C}[X_1, ..., X_n]$*-cogenerator is the space of exponential polynomials*

$$W_0 = \bigoplus\nolimits_{a \in \mathbb{C}^n} \mathbb{C}[x]\, e^{\langle a, x\rangle}$$

where $\langle -, - \rangle$ *is the usual Hermitian product in* $\mathbb{C}^n$*, i.e.* $\langle a, x\rangle = \sum_{k=1}^n \bar{a}_k x_k$*. Hence,* $C^\infty(\Omega) \supset W_0$ *is an injective cogenerator.*

(VI) We will now consider one important example of an injective cogenerating module, which begins by constructing an injective module:

LEMMA 3.131.– *Let* $\mathbf{B}$ *be a ring,* ${}_{\mathbf{B}}F$ *a* $\mathbf{B}$*-module and* ${}_{\mathbf{B}}P_{\mathbf{A}}$ *a* $(\mathbf{B}, \mathbf{A})$*-bimodule. If* F *is an injective* $\mathbf{B}$*-module and* P *is a flat right* $\mathbf{A}$*-module, then the* $\mathbf{A}$*-module* $\mathrm{Hom}_{\mathbf{B}}(P, F)$ *is injective.*

PROOF.– If $I = \mathrm{Hom}_{\mathbf{B}}(P, F)$, we need to show that the functor $\mathbf{h}_I(-, I)$ transforms monomorphisms into epimorphisms. Let $u : M \hookrightarrow M'$ be a monomorphism of $\mathbf{A}$-modules. The adjoint isomorphism theorem (theorem 3.19) implies that the following diagram commutes

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbf{A}}(M, \mathrm{Hom}_{\mathbf{B}}(P, F)) & \xrightarrow{\mathrm{Hom}_{\mathbf{A}}(u, \mathbf{1})} & \mathrm{Hom}_{\mathbf{A}}(M', \mathrm{Hom}_{\mathbf{B}}(P, F)) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathbf{B}}(P \bigotimes_{\mathbf{A}} M, F) & \xrightarrow{\mathrm{Hom}(\mathrm{id}_P \otimes u, \mathrm{id}_F)} & \mathrm{Hom}_{\mathbf{B}}(P \bigotimes_{\mathbf{A}} M', F) \end{array}$$

where the vertical arrows are the canonical isomorphisms and where $\mathbf{1} = \mathrm{id} : \mathrm{Hom}_{\mathbf{B}}(P, F) \to \mathrm{Hom}_{\mathbf{B}}(P, F)$. Since the $\mathbf{A}$-module P is flat, the functor $P \bigotimes_{\mathbf{A}} -$ is exact, $\mathrm{id}_P \otimes u$ is a monomorphism of $\mathbf{B}$-modules, and since the $\mathbf{B}$-module F is injective, $\mathrm{Hom}(\mathrm{id}_P \otimes u, \mathrm{id}_F)$ is an epimorphism, implying that $\mathrm{Hom}_{\mathbf{A}}(u, \mathbf{1})$ is an epimorphism. ■

8 A proof is given in French in the Wikipedia article *"Principe fondamental d'Ehrenpreis"*.

THEOREM 3.132.– *Let* $\mathbf{B}$ *be a ring,* ${}_{\mathbf{B}}F$ *an injective cogenerating* $\mathbf{B}$*-module and* ${}_{\mathbf{B}}P_{\mathbf{A}}$ *a* $(\mathbf{B}, \mathbf{A})$*-bimodule. If* P *is a faithfully flat right* $\mathbf{A}$*-module (definition 3.20), the* $\mathbf{A}$*-module* $\mathrm{Hom}_{\mathbf{B}}(P, F)$ *is an injective cogenerator.*

PROOF.– The $\mathbf{A}$-module $\mathrm{Hom}_{\mathbf{B}}(P, F)$ is injective (lemma 3.131). If S is a simple $\mathbf{A}$-module, by the adjoint isomorphism theorem (theorem 3.19), there is a canonical isomorphism of abelian groups

$$\mathrm{Hom}_{\mathbf{A}}(S, \mathrm{Hom}_{\mathbf{B}}(P, F)) \cong \mathrm{Hom}_{B}\left(P \bigotimes_{\mathbf{A}} S, F\right).$$

Since P is faithfully flat, the functor $P \bigotimes_{\mathbf{A}} -$ is faithful, and hence injective (lemma 3.17), hence $P \bigotimes_{\mathbf{A}} S \neq 0$, so $\mathrm{Hom}_{B}(P \bigotimes_{\mathbf{A}} S, F) \neq 0$, since F is a cogenerator (theorem 3.125), and so the $\mathbf{A}$-module $\mathrm{Hom}_{\mathbf{B}}(P, F)$ is a cogenerator (corollary 3.127). ■

COROLLARY 3.133.– *Let* $\mathbf{A}$ *be a ring that is a* $\mathbf{K}$*-algebra, where* $\mathbf{K}$ *is a field. The* $\mathbf{A}$*-module* $\mathbf{A}^* := \mathrm{Hom}_{\mathbf{K}}(\mathbf{A}, \mathbf{K})$ *is a left and right injective cogenerator.*

PROOF.– Simply apply theorem 3.132 with $\mathbf{B} = \mathbf{K}$ and $P = {}_{\mathbf{K}}\mathbf{K}$. ■

3.3.4. *Dedekind domains*

The results in this subsection and the next subsection are given without proof, with a few exceptions.

(I) COMMUTATIVE CASE. There are several equivalent ways of defining *commutative* Dedekind domains. Each definition is useful in its own right.

THEOREM-DEFINITION 3.134.– *Let* $\mathbf{A}$ *be an entire commutative ring. The following conditions are equivalent:*

1) $\mathbf{A}$ *has dimension* ≤ 1 *(in other words, every proper prime ideal in* $\mathbf{A}$ *is maximal) and is Noetherian, and one of the following conditions is satisfied:*

i) $\mathbf{A}$ *is integrally closed;*

ii) Every primary ideal $\mathfrak{q}$ *in* $\mathbf{A}$ *(section 3.2.4(**I**)) is of the form* $\mathfrak{p}^n$*, where the ideal* $\mathfrak{p}$ *is prime;*

iii) For every prime ideal $\mathfrak{p} \neq (0)$*, the local ring* $\mathbf{A}_{\mathfrak{p}}$ *(section 3.2.1(**I**)) is a discrete valuation ring (definition 3.61).*

2) Every non-zero ideal in $\mathbf{A}$ *is a product of prime ideals.*

3) Every non-zero ideal in $\mathbf{A}$ *is invertible (definition 3.46).*

4) $\mathbf{A}$ *is a* hereditary *ring, i.e. every ideal in* $\mathbf{A}$ *is projective.*

$\mathbf{A}$ *is called a Dedekind domain if one of the equivalent conditions listed above is satisfied.*

(1)⇔(2)⇔(3) see ([ZAR 58/60], section V.6, Thm. 12, 13), ([ATI 69], Thm. 9.3). (3)⇔(4) see ([COH 03a], Prop. 10.5.1). The notion of hereditary ring was introduced by Cartan and Eilenberg [CAR 56].

Consider an entire Noetherian ring. This ring is called a Krull ring if it is integrally closed ([BKI 98], Chap. VII, section 1.4, Cor.). Thus, a ring is a Dedekind domain if and only if it is a Krull ring of dimension ≤ 1.

THEOREM 3.135.– *Let* $\mathbf{A}$ *be a commutative entire ring. The following conditions are equivalent:*

a) $\mathbf{A}$ *is a Dedekind domain;*

b) Every non-zero ideal in $\mathbf{A}$ *is a product of maximal ideals;*

c) The monoid of non-zero fractional ideals (definition 3.45) is a group under multiplication;

d) Every finitely generated torsion-free $\mathbf{A}$*-module is projective;*

e) Every submodule of a projective $\mathbf{A}$*-module is projective;*

f) Every quotient of an injective $\mathbf{A}$*-module is injective;*

g) Every divisible $\mathbf{A}$*-module is injective.*

It is immediate that (a)⇔(b) and (c)⇒(a) is clear. (a)⇒(c) see ([ZAR 58/60], section V.6, Thm. 11). (a)⇔(d)⇔(e)⇔(f)⇔(g) see ([COH 03a], Prop. 10.6.6; [CAR 56], Chap. I, Thm. 5.4, Chap. VII, Prop. 5.1).

Condition (c) implies that every ideal $\mathfrak{a} \neq (0)$ may be uniquely written in the form

$$\mathfrak{a} = \prod_{\mathfrak{p} \in \mathrm{Spec}(\mathbf{A})} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{a})},$$

where the prime ideals $\mathfrak{p}$ are distinct and all but finitely many of the $n_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}$ are zero, and where $\mathfrak{a}$ is an integral ideal if and only if the $n_{\mathfrak{p}}(\mathfrak{a})$ are all ≥ 0.

This property is a generalization of Gauss's theorem (theorem 2.54). The next result is one of the reasons that a Dedekind domain is important ([ZAR 58/60], section V.8, Thm. 19):

THEOREM 3.136.– *Let* $\mathbf{A}$ *be a Dedekind domain,* $\mathbf{K}$ *its field of fractions and let* $\mathbf{L}$ *be a finite algebraic extension of* $\mathbf{K}$ *(section 2.3.5(**II**)). Then, the integral closure* $\mathbf{A}'$ *of* $\mathbf{A}$ *in* $\mathbf{L}$ *(definition 3.86(ii)) is a Dedekind domain.*

For example, $\mathbb{Z}$ is a Dedekind domain since it is Euclidean, and therefore, a principal ideal domain. The same is true for the ring $\mathbb{Z}\left[\sqrt{-1}\right] = \mathbb{Z} \oplus \sqrt{-1}\mathbb{Z}$. However, the ring $\mathbb{Z}\left[\sqrt{-5}\right]$ is not a UFD, and so is not a principal ideal domain, since

$$2.3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$$

gives two distinct decompositions of 6 into prime factors (**exercise**). A *number field* $\mathbf{K}$ is a finite algebraic extension of $\mathbb{Q}$, and such a field is called a *quadratic field* if the extension $\mathbf{K}/\mathbb{Q}$ is of degree 2 (section 2.3.5(**II**)). As a consequence of theorem 3.136, the ring $\mathfrak{O}_{\mathbf{K}} := \mathbf{K} \cap \mathfrak{A}$ of integers of $\mathbf{K}$, where $\mathfrak{A}$ is the ring of algebraic integers (section 3.2.5(**I**)), is a Dedekind domain ([ATI 69], Thm. 9.5). Now, we have ([SAM 67], section II.5, Thm. 1):

THEOREM 3.137.– *Let* $\mathbf{K} = \mathbb{Q}\left(\sqrt{d}\right)$ *be a quadratic field with* $d \in \mathbb{Z}$ *square-free (therefore* $\sim\equiv 0 \pmod 4$*).*

a) If $d \equiv 2$ *or* $d \equiv 3 \pmod 4$, *the ring* $\mathfrak{O}_{\mathbf{K}}$ *consists of all elements of the form* $a + b\sqrt{d}$ *with* $a, b \in \mathbb{Z}$.

b) If $d \equiv 1 \pmod 4$, *the ring* $\mathfrak{O}_{\mathbf{K}}$ *consists of all elements of the form* $\frac{1}{2}\left(u + v\sqrt{d}\right)$ *with* $u, v \in \mathbb{Z}$ *of the same parity.*

In particular, with $\mathbf{K} = \mathbb{Q}\left(\sqrt{-5}\right)$, we have that $\mathfrak{O}_{\mathbf{K}} = \mathbb{Z}\left[\sqrt{-5}\right]$, since $-5 \equiv 3 \pmod 4$. Consequently, $\mathbb{Z}\left[\sqrt{-5}\right]$ is a Dedekind domain, and the principal ideal (6) may be uniquely written as the product of (non-principal) prime ideals in this ring (see [STE 02], section 5.5, Exerc. 2).

THEOREM 3.138.– *For a Dedekind domain to be a principal ideal domain, it is necessary and sufficient for it to be a UFD.*

PROOF.– This condition is necessary by theorem 2.56. Conversely, let $\mathbf{A}$ be a UFD, $\mathfrak{p} \neq (0)$ a prime ideal in $\mathbf{A}$ and $0 \neq a \in \mathfrak{p}$ an element of the form [2.19].

By lemma 2.30, there exists $p \in P$ such that $n_p(a) > 0$ and $(p) \subseteq \mathfrak{p}$. The principal ideal (p) is prime by lemma 2.31. If $\mathbf{A}$ is also a Dedekind domain, (p) is maximal by theorem-definition 3.134, so $(p) = \mathfrak{p}$. Every ideal in $\mathbf{A}$ is therefore a product of principal ideals by theorem-definition 3.134, so is a principal ideal. ■

(II) NON-COMMUTATIVE CASE. We have the following result ([CAR 56], Chap. VII, Prop. 3.2; [GEN 60], Prop. 3.1):

LEMMA 3.139.– *Let* $\mathbf{A}$ *be a left Ore domain,* $\mathbf{K} = \mathrm{Q}(A)$ *its division ring of left fractions and* $\mathfrak{a} \neq 0$ *a left ideal in* $\mathbf{A}$*. The following conditions are equivalent:*

1) There exist elements $q_1, ..., q_n \in \mathbf{K}$ *and* $a_1, ..., a_n \in \mathfrak{a}$ *such that* $\mathfrak{a}.q_i \subseteq \mathbf{A}$ $(i = 1, ..., n)$ *and* $\sum_{1 \leq i \leq n} q_i a_i = 1$.

2) $\mathfrak{a}$ *is projective.*

Note that if $\mathbf{A}$ is commutative, condition (1) says that $\mathfrak{q}\mathfrak{a} = \mathbf{A}$, where $\mathfrak{q}$ is the fractional ideal generated by $q_1, ..., q_n$, or, in other words, that the ideal $\mathfrak{a}$ is invertible (definition 3.46). A left ideal $\mathfrak{a}$ satisfying the condition (1) (in the non-commutative case) is therefore said to be *invertible* ([GEN 60], section 3). (The definition of an invertible ideal given in ([MCC 01], 4.2.5) is not the same.)

DEFINITION 3.140.– *Let* $\mathbf{A}$ *be an entire ring. This ring is called a left Dedekind domain if it is left hereditary, i.e. if every left ideal in* $\mathbf{A}$ *is projective.*

This definition extends the characterization of a Dedekind domain given by theorem-definition 3.134(4) to the non-commutative case. It can be shown that every left ideal in a left Dedekind domain is finitely generated ([GEN 60], Cor. 3.1), so any such ring is left Noetherian. Furthermore, in a Dedekind domain, every (left or right) ideal is generated by 2 elements ([MCC 01], 5.7.7). The non-principal (left or right) ideals are said to be *essential*.

The importance of non-commutative Dedekind domains lies in the following result ([MCC 01], 7.11.2):

THEOREM 3.141.– *Let* $\mathbf{K}$ *be a commutative Dedekind domain and suppose that either* $\mathbf{A} = \mathbf{K}[X; \delta]$ *or* $\mathbf{A} = \mathbf{K}\left[Y, Y^{-1}; \sigma\right]$*, with the notation of theorem 3.51. The following conditions are equivalent:*

1) $\mathbf{A}$ *is simple;*

2) $\mathbf{A}$ *is a non-commutative Dedekind domain.*

In particular, it follows from corollary 3.52 that if $\mathbf{k}$ is a field of characteristic 0, then the $\mathbf{k}$-algebras $A_1(\mathbf{k})$ and $A_1'(\mathbf{k})$ are non-commutative Dedekind domains (but unlike $B_1(\mathbf{k})$ are not principal ideal domains). The equivalences (a)⇔(g) in theorem 3.135 can be extended to the non-commutative case ([GEN 60], Cor. 3.3; [LAM 99], [3.23]):

THEOREM 3.142.– *Let* $\mathbf{A}$ *be an entire ring.* The following conditions are equivalent*:*

1) $\mathbf{A}$ *is a left Dedekind domain;*

2) Every divisible left $\mathbf{A}$*-module is injective.*

3.3.5. *Global dimension*

(I) RESOLUTIONS. Let M be an $\mathbf{A}$-module and consider the exact sequences

$$\longrightarrow \ldots \longrightarrow E_n \xrightarrow{d_n} E_{n-1} \longrightarrow \ldots \longrightarrow E_1 \xrightarrow{d_1} E_0 \xrightarrow{\varphi} M \longrightarrow 0, \qquad [3.46]$$

$$\longleftarrow \ldots \longleftarrow E^n \xleftarrow{d^n} E^{n-1} \longleftarrow \ldots \longleftarrow E^1 \xleftarrow{d^1} E^0 \xleftarrow{\iota} M \longleftarrow 0. \qquad [3.47]$$

The exact sequence [3.46] (resp. [3.47]) is called a *left* (resp. *right*) resolution of M. The module $\ker d_i$ (resp. $\ker d^i$), where $i \geq 1$, is called the i-th *syzygy*[9] (resp. *cosyzygy*) of the resolution. If $E_n \neq 0$ and $E_i = 0$ for all $i \geq n$, the left resolution [3.46] is said to have *length* n. Similarly, if $E^n \neq 0$ and $E^i = 0$ for $i \geq n$, the right resolution [3.47] is said to have length n.

If each E_i in the left resolution [3.46] is free (resp. projective, resp. flat), this resolution is said to be *free* (resp. *projective*, resp. *flat*). It is said to be *finite free* if it has finite length and each E_i is finite free. If each E^i in the right resolution [3.47] is *injective*, this resolution is said to be *injective*.

9 The term comes from the Greek word for *connection*, and is commonly used in astronomy to describe the situation where three or more celestial bodies are aligned or opposed.

THEOREM 3.143.– *Let M be an $\mathbf{A}$-module.*

i) This module has free, projective, flat and injective resolutions;

ii) If $\mathbf{A}$ is left Noetherian or a semifir and M is finitely generated, M has a resolution [3.46], where each E_i is finite free.

PROOF.– i) 1) We know that M is the quotient of a free module E_0 (lemma 3.22), which gives the exact sequence $E_0 \longrightarrow M \longrightarrow 0$. There exists a presentation of M, i.e. an exact sequence [3.9] that can be written in the form $E_1 \longrightarrow E_0 \longrightarrow M \longrightarrow 0$, where E_1 is free. We can continue this reasoning until we find a free resolution of M. This resolution is projective and flat by corollary 3.21 and lemma 3.105.

2) A projective resolution [3.46] in the category $\mathbf{Mod}_{\mathbf{A}^{\mathrm{OP}}}$ is an injective resolution in the category ${}_{\mathbf{A}}\mathbf{Mod}$ (section 1.2.10**(II)** & 2.3.1**(II)**).

ii) follows from the proof of theorem 3.27. ■

(II) GLOBAL DIMENSION. Let $\mathbf{A}$ be a ring and M an $\mathbf{A}$-module.

DEFINITION 3.144.– *The projective (resp. flat, resp. injective) dimension of M, written as* pd (M) *(resp.* fd (M), *resp.* id (M)*) is the smallest length of a projective (resp. flat, resp. injective) resolution of M, and is defined as $+\infty$ if no such resolution exists.*

Hence, pd $(M) = 0$ (resp. fd $(M) = 0$, resp. id $(M) = 0$) if and only if M is projective (resp. flat, resp. injective). If M has a free finite resolution of length $\leq n$, then pd $(M) \leq n$ by lemma 3.105.

In the rest of this subsection, we will assume that $\mathbf{A}$ is Noetherian. We then have

$$\begin{aligned}\sup\{\mathrm{pd}\,(M) : M \in {}_{\mathbf{A}}\mathbf{Mod}\} &= \sup\{\mathrm{id}\,(M) : M \in {}_{\mathbf{A}}\mathbf{Mod}\} \\ &= \sup\{\mathrm{fd}\,(M) : M \in {}_{\mathbf{A}}\mathbf{Mod}\}\end{aligned}$$

and this quantity does not change if we replace ${}_{\mathbf{A}}\mathbf{Mod}$ by $\mathbf{Mod}_{\mathbf{A}}$ (this is not correct if $\mathbf{A}$ is not assumed to be Noetherian: see ([ROT 09], section 8.1) and ([MCC 01], Chap. 7)).

DEFINITION 3.145.– *The above quantity is called the* global dimension *(or* homological dimension*) of $\mathbf{A}$, and is written as* gld$\mathbf{A}$.

We therefore have:

i) $\text{gld}\mathbf{A} = 0$ if and only if $\mathbf{A}$ is semi-simple (by theorem 2.37), and, in particular, if $\mathbf{A}$ is a division ring.

ii) $\text{gld}\mathbf{A} \leq 1$ if and only if $\mathbf{A}$ is hereditary.

Moreover, let $\mathbf{K}$ be a Noetherian ring, σ an automorphism of $\mathbf{K}$ and δ a σ-derivation of $\mathbf{K}$. Then ([MCC 01], Chap. 7),

iii) $\text{gld}\mathbf{K} \leq \text{gld}\mathbf{K}[X;\sigma,\delta] \leq \text{gld}\mathbf{K} + 1$ if $\text{gld}\mathbf{K} < +\infty$,

iv) $\text{gld}\mathbf{K}[Y;\sigma] = \text{gld}\mathbf{K} + 1$.

If $\mathbf{K}$ is a commutative ring, then ([ROT 09], Thm. 8.7)

v) $\text{gld}\mathbf{K}[X_1, ..., X_n] = \text{gld}\mathbf{K} + n$ (*Hilbert's syzygy theorem,* 1st version).

If $\mathbf{k}$ is a field of characteristic 0, and $A_n(\mathbf{k})$ is the n-th Weyl algebra over $\mathbf{k}$ (section 2.3.10**(III)**),

vi) $\text{gld}A_n(\mathbf{k}) = n$.

Let $S \subset \mathbf{A}$ be a denominator set (section 3.1.9**(II)**). Then,

vii) $\text{gld}S^{-1}\mathbf{A} \leq \text{gld}\mathbf{A}$.

The following result was established by J.P. Serre, M. Auslander and D. Buchsbaum ([LAM 99], (5.94)):

THEOREM-DEFINITION 3.146.– *Let* $\mathbf{A}$ *be a commutative Noetherian ring.*

1) If $\mathbf{A}$ *is local, this ring is regular (definition 3.100) if and only if, for all* $\mathfrak{p} \in \text{Spec}(\mathbf{A})$, *the local ring* $\mathbf{A}_\mathfrak{p}$ *is regular.*

2) The following conditions are equivalent:

a) The local ring $\mathbf{A}_\mathfrak{p}$ *is regular for all* $\mathfrak{p} \in \text{Spec}(\mathbf{A})$.

b) The local ring $\mathbf{A}_\mathfrak{m}$ *is regular for all* $\mathfrak{m} \in \text{Spm}(\mathbf{A})$.

3) Whenever one of the equivalent conditions listed in (2) is satisfied, the ring $\mathbf{R}$ *is said to be* regular.

4) If $\mathbf{A}$ *is regular, then* $\text{gld}\mathbf{A} = \dim(\mathbf{A})$. *If* $\mathbf{A}$ *is such that* $\text{gld}\mathbf{A} < \infty$, *then* $\mathbf{A}$ *is regular. Conversely, if* $\mathbf{A}$ *is* local *and regular, then* $\text{gld}\mathbf{A} < \infty$.

Finally, the following result was established by R. Swan ([LAM 06], Chap. II, (5.7)):

THEOREM 3.147.– *If* $\mathbf{A}$ *is a commutative regular Noetherian ring, then the Noetherian ring* $\mathbf{A}[X]$ *is regular.*

COROLLARY 3.148.– *Let* $\mathbf{K}$ *be a field. Then,* $\text{gld}\mathbf{K}[X_1, ..., X_n] = n$ *and* $\text{gld}\mathbf{K}[[X_1, ..., X_n]] = n$.

PROOF.– The first equality follows from property (v), since $\text{gld}\mathbf{K} = 0$. It can also be shown as follows: the ring $\mathbf{K}[X_1, ..., X_n]$ is Noetherian by Hilbert's basis theorem (corollary 3.49) and is regular by theorem 3.147 (since $\mathbf{K}$ is regular), so $\text{gld}\mathbf{K}[X_1, ..., X_n] = \dim(\mathbf{K}[X_1, ..., X_n])$, and the last quantity is equal to $\dim(\mathbf{K}) + n = 0 + n = n$ by theorem 3.96. The second equality follows from theorem 3.101 and theorem-definition 3.146(4). ■

Let $\mathbf{K}$ be a field and M a finitely generated $\mathbf{K}[X_1, ..., X_n]$-module. The first equality in corollary 3.148 implies that the smallest length of a projective resolution of M is $\leq n$. We can show a more precise version using the Quillen-Suslin theorem, which gave a positive answer to Serre's conjecture ([LAM 06], Chap. V, Thm. 2.9):

THEOREM-DEFINITION 3.149.– *(Quillen-Suslin) Let* $\mathbf{K}$ *be a field (or, more generally, a commutative principal ideal domain) and define* $\mathbf{A} = \mathbf{K}[X_1, ..., X_n]$. *Then,* $\mathbf{A}$ *is* projective-free*, i.e. every finitely generated projective* $\mathbf{A}$*-module is free.*

Other examples of projective-free rings are given in [LAM 06]; there is no non-commutative version of the Quillen-Suslin theorem, but we do have the following result:

THEOREM 3.150.– *Every (not necessarily commutative) local ring* $\mathbf{A}$ *is projective-free.*

PROOF.– 1) Let P be a projective $\mathbf{A}$-module and $\{\bar{x}_1, ..., \bar{x}_n\}$ a minimal generating set of P. There exists a free module F with basis $\{x_1, ..., x_n\}$, where $\varphi : F \twoheadrightarrow P : x_i \mapsto \bar{x}_i$ is the canonical epimorphism (lemma 3.22). Let $K = \ker(\varphi)$ and $\mathfrak{m} = \text{rad}(\mathbf{A})$ (section 2.3.7). We have that $K \subseteq \mathfrak{m}F$.

Indeed, if not, there exists $y = \sum_{1\leq i\leq n} a_i x_i \in K$ $(a_i \in \mathbf{A})$ such that $y \notin \mathfrak{m}F$. One of the a_i, say a_1, therefore does not belong to $\mathfrak{m}$. Thus, $a_1 \in \mathbf{U}(\mathbf{A})$ (lemma 2.47). Let $u = a_1^{-1}$. We have that $\sum_{1\leq i\leq n} a_i \bar{x}_i = 0$, so $\bar{x}_1 = -u \sum_{2\leq i\leq n} a_i \bar{x}_i$, which contradicts the minimality of $\{\bar{x}_1, ..., \bar{x}_n\}$.

2) The exact sequence $0 \to K \to F \to P \to 0$ splits, so $F = K \oplus P'$ where $P' \cong P$. Thus, $\mathfrak{m}F = \mathfrak{m}K \oplus \mathfrak{m}P'$, and since $\mathfrak{m}K \subseteq K \subseteq \mathfrak{m}F$,

$$K = K \cap \mathfrak{m}F = K \cap \left(\mathfrak{m}K \oplus \mathfrak{m}P'\right) = \mathfrak{m}K \oplus \left(K \cap \mathfrak{m}P'\right) = \mathfrak{m}K.$$

However, K is finitely generated, so by Nakayama's lemma (lemma 2.41), $K = 0$, and $P \cong F$. ■

(III) Corollary 3.148 and theorem-definition 3.149 imply a second version of *Hilbert's syzygy theorem* (compare with statement (v) of **(II)** shown previously). This result was proved by Hilbert in 1890 (who therefore used a very different approach!). We require another notion in order to state this result in the general context of graded modules:

DEFINITION 3.151.– *The resolution [3.46] is said to be* graded free *if* $\mathbf{A}$ *is graded, the* E_i *are free graded modules, and the mappings* d_i *are graded of type* 0 *(section 2.3.12). This resolution is said to be* finite graded free *if the* E_i *are also finitely generated.*

THEOREM 3.152.– *(*Hilbert's syzygy theorem, *2nd version): If* $\mathbf{K}$ *is a field and* M *is a graded* $\mathbf{K}[X_1, ..., X_n]$*-module, the* n*-th syzygy of its graded free resolution [3.46] is a free module, and hence* M *has a graded free resolution of length* n*. If* M *is finitely generated, this graded free resolution is finite.*

3.3.6. *Bézout equations*

In this subsection, $\mathbf{A}$ is a weakly finite ring (definition 3.5).

DEFINITION 3.153.– *An* $\mathbf{A}$*-module* P *is said to be* stably free *of rank* $r \geq 0$ *if there exists an integer* $q \geq 0$ *such that* $P \oplus \mathbf{A}^{1\times q} \cong \mathbf{A}^{1\times(q+r)}$.

It is clear that any free $\mathbf{A}$-module of rank r is stably free of rank r.

THEOREM 3.154.– *Let* P *be an* $\mathbf{A}$*-module.* The following conditions are equivalent*:*

i) P is stably free of rank $k-q \geq 0$;

ii) $P \cong \operatorname{coker}(f)$ where the monomorphism $f : \mathbf{A}^{1\times q} \hookrightarrow \mathbf{A}^{1\times k}$ splits (definition 3.15);

*iii) With $R = \operatorname{Mat}(f)$ (section 3.1.6(**II**)), the matrix Bézout equation $RX = I_q$ has a solution; in other words, R is right-invertible ;*

iv) P is projective and has a finite free resolution of length ≤ 1.

PROOF.– (i)⇒(ii): Let $F = P \oplus \mathbf{A}^{1\times q}$ be a free module of rank k and let $\psi : F \xrightarrow{\sim} \mathbf{A}^{1\times k}$ be an isomorphism. Define $\iota : \mathbf{A}^{1\times q} \hookrightarrow F$ to be inclusion and $\pi : P \oplus \mathbf{A}^{1\times q} \twoheadrightarrow P$ to be projection, and consider the following commutative diagram, the top row of which is exact, and where $\varphi := \pi \circ \psi^{-1}$:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbf{A}^{1\times q} & \xrightarrow{\iota} & F & \xrightarrow{\pi} & P \longrightarrow 0 \\ & & & f \searrow & \downarrow \psi & \nearrow \varphi & \\ & & & & \mathbf{A}^{1\times k} & & \end{array}$$

Since $f = \psi \circ \iota$ and ι splits, f splits and we obtain the split exact sequence:

$$0 \longrightarrow \mathbf{A}^{1\times q} \xrightarrow{f} \mathbf{A}^{1\times k} \xrightarrow{\varphi} P \longrightarrow 0. \qquad [3.48]$$

(ii)⇒(i): If the exact sequence [3.48] splits, we have that $\mathbf{A}^{1\times k} \cong f\left(\mathbf{A}^{1\times q}\right) \oplus P$ and $\mathbf{A}^{1\times q} \cong f\left(\mathbf{A}^{1\times q}\right)$, from which we deduce (i).

(ii)⇔(iii) The homomorphism $f : \mathbf{A}^{1\times q} \to \mathbf{A}^{1\times k}$ is a split monomorphism if and only if f is left-invertible (lemma-definition 3.15), which is equivalent to saying that R is right-invertible. (ii)⇔(iv) obvious. ■

If $R = \begin{bmatrix} a & b \end{bmatrix}$, $X = \begin{bmatrix} x \\ y \end{bmatrix}$, we have that $RX = 1$ if and only if $ax+by = 1$, which is the classical Bézout equation (section 2.3.8(**III**)).

DEFINITION 3.155.– *A matrix $R \in \mathbf{A}^{q\times k}$ $(k \geq q)$ is said to be* completable *if there exists a matrix $R' \in \mathbf{A}^{(k-q)\times k}$ such that $\begin{bmatrix} R \\ R' \end{bmatrix}$ is invertible.*

THEOREM 3.156.– *Let $P \cong \operatorname{coker}(\bullet R)$ be an $\mathbf{A}$-module where $R \in \mathbf{A}^{q\times k}$ $(k \geq q)$ is right-invertible. The module P is free if and only if R is completable.*

PROOF.– 1) If R is completable, there exists a matrix $\begin{bmatrix} X & X' \end{bmatrix} \in \mathrm{GL}_k(\mathbf{A})$ such that

$$\begin{bmatrix} R \\ R' \end{bmatrix} \begin{bmatrix} X & X' \end{bmatrix} = \begin{bmatrix} I_q & 0 \\ 0 & I_{k-q} \end{bmatrix}. \qquad [3.49]$$

With the notation from [3.11], we have that $P \cong [\mathbf{v}]_{\mathbf{A}}$ where $\mathbf{v} = \begin{bmatrix} X & X' \end{bmatrix} \mathbf{w}$ and $[\mathbf{v}]_{\mathbf{A}} \cong \mathrm{coker}\left(\bullet \begin{bmatrix} I_q & 0 \end{bmatrix}\right) \cong \mathbf{A}^{k-q}$. 2) Conversely, let $P \cong \mathbf{A}^{k-q}$, R be a definition matrix of P, and suppose that X satisfies $RX = I_q$. We have the split exact sequence [3.48], where $R = \mathrm{Mat}(f)$ and where φ has a linear section s. Choosing a basis in P, and writing X' and R' for the matrices representing φ and s, respectively, we have that

$$\begin{bmatrix} R \\ R' \end{bmatrix} \begin{bmatrix} X & X' \end{bmatrix} = \begin{bmatrix} I_q & 0 \\ * & I_{k-q} \end{bmatrix}.$$

Since $\mathbf{A}$ is weakly finite, $\begin{bmatrix} R \\ R' \end{bmatrix}$ is invertible. ■

DEFINITION 3.157.– *A weakly finite ring* $\mathbf{A}$ *is called an Hermite ring if every stably free* $\mathbf{A}$*-module is free.*

Thus, over an Hermite ring, a matrix is completable if and only if it is right-invertible. It follows from the definitions that every projective-free ring (theorem-definition 3.149) is an Hermite ring.

3.3.7. *Preabelian caregories and abelian categories*

(I) PREADDITIVE CATEGORIES. A category $\mathcal{C}$ is *preadditive* if every set $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ is an abelian group and if the composition of morphisms is $\mathbb{Z}$-bilinear. In most cases, we assume that there exists an object 0 (section 1.1.1(**IV**)). Let $\mathcal{C}$ be a preadditive category with 0 and let $f : X \to Y$ be a morphism. Consider the preordered sets P_X and Q^Y consisting of all morphisms with codomain X and domain Y, respectively (section 1.1.1(**III**)). The equalizer $\mathrm{eq}(f, 0)$ of $(f, 0)$ is called the *kernel* of f and is written $\ker(f)$; this is a pair (κ, K), where $\kappa : K \hookrightarrow X$ is a monomorphism such that $f \circ \kappa = 0$ and any morphism $\alpha \in P_X$ such that $f \circ \alpha = 0$ factors through κ, i.e. there exists a unique morphism α' such that $\alpha = \kappa \circ \alpha'$. Dually, the

coequalizer $\mathrm{coeq}(f,0)$ is called the *cokernel* of f and is written $\mathrm{coker}(f)$; this is a pair (γ, C) where $\gamma : Y \twoheadrightarrow C$ is an epimorphism such that $\gamma \circ f = 0$ and every morphism $\beta \in Q^Y$ such that $\beta \circ f = 0$ factors through γ, i.e. there exists a unique morphism β' such that $\beta = \beta' \circ \gamma$. If $\ker(f)$ and $\mathrm{coker}(f)$ exist, we define the *image* $\mathrm{im}(f)$ and the *coimage* $\mathrm{coim}(f)$ of f by the relations

$$\mathrm{im}(f) = \ker(\mathrm{coker}(f)), \quad \mathrm{coim}(f) = \mathrm{coker}(\ker(f)).$$

With this definition, the kernel and the cokernel, and hence the image and the coimage, are viewed as morphisms. In other situations, it can be more useful to view them as pairs (f, A), where A is an object of $\mathcal{C}$ and f is the associated $\mathcal{C}$-morphism (which can sometimes be implied as in **(V)** below).

If $\mathcal{C}$ and $\mathcal{D}$ are two preadditive categories, a functor $\mathfrak{F} : \mathcal{C} \to \mathcal{D}$ is said to be *additive* if $\mathfrak{F}_{\mathrm{Mor}}$ is $\mathbb{Z}$-linear (see section 3.1.4**(II)**). If so, if $\mathcal{C}$ and $\mathcal{D}$ both have a 0 object and $\mathfrak{F}$ is faithful, then $\mathfrak{F}$ is injective and $\mathfrak{F}(\mathcal{C})$ is a subcategory of $\mathcal{D}$ (lemma 3.17).

(II) ADDITIVE CATEGORIES.

LEMMA-DEFINITION 3.158.– *Let $\mathcal{C}$ be a preadditive category with 0, $(X_i)_{1\leq i\leq n}$ a finite family of objects of $\mathcal{C}$ and X an object of $\mathcal{C}$, and define $2n$ morphisms $\mathrm{pr}_i : X \to X_i$, $\mathrm{inj}_i : X_i \to X$, such that $\mathrm{pr}_i \mathrm{inj}_j = \delta_i^j \mathrm{id}_{X_j}$.*

1) The following conditions are equivalent*:*

i) $\sum_{1\leq i\leq n} \mathrm{inj}_i \mathrm{pr}_i = \mathrm{id}_X$*;*

ii) $X = \coprod_{1\leq i\leq n} X_i$ *with the canonical injections* $\mathrm{inj}_i : X_i \to X$*;*

iii) $X = \prod_{1\leq i\leq n} X_i$ *with the canonical projections* $\mathrm{pr}_i : X \to X_i$*.*

2) Whenever the equivalent conditions listed in (1) are satisfied, $(X, \mathrm{pr}_i, \mathrm{inj}_i)_{1\leq j\leq n}$ is called a biproduct *of the X_i and is written as $X = \bigoplus_{1\leq i\leq n} X_i$.*

An *additive category* is a preadditive category with 0 together with a biproduct $\bigoplus$ for each pair of objects. In an additive category, let f be a morphism with a kernel and a cokernel, and consider the following diagram,

where $\pi : X \twoheadrightarrow \operatorname{coim} f$ is the canonical epimorphism and $\iota : \operatorname{im}(f) \hookrightarrow Y$ is inclusion:

$$\begin{array}{ccccccc} \ker(f) & \xrightarrow{\kappa} & X & \xrightarrow{f} & Y & \xrightarrow{\gamma} & \operatorname{coker}(f) \\ & & \pi \downarrow & & \uparrow \iota & & \\ & & \operatorname{coim}(f) & \xrightarrow{\breve{f}} & \operatorname{im}(f) & & \end{array}$$

LEMMA-DEFINITION 3.159.– *1) There exists a unique morphism* $\breve{f} : \operatorname{coim}(f) \to \operatorname{im}(f)$ *that makes this diagram commute, called the* induced morphism.

2) If $\breve{f}$ *is an isomorphism, the morphism* f *is said to be* strict.

PROOF.– Since $f \circ \kappa = 0$ and $\pi = \operatorname{coim}(f) = \operatorname{coker}(\kappa)$, there exists a unique morphism $\varphi : \operatorname{coim}(f) \to Y$ such that $f = \varphi \circ \pi$. Then, $\gamma \circ f = \gamma \circ \varphi \circ \pi = 0$, and since π is an epimorphism, this implies that $\gamma \circ \varphi = 0$. Thus, there exists a unique morphism $\breve{f} : \operatorname{coim}(f) \to \operatorname{im}(f)$ such that $\varphi = \iota \circ \breve{f}$. ■

(III) PREABELIAN CATEGORIES. An additive category in which every morphism has a kernel and a cokernel (and therefore also an image and a coimage) is said to be *preabelian*. In any such category, a *monomorphism* (resp. an *epimorphism*) is a morphism $f : X \to Y$ such that $\ker(f) = 0$ (resp. $\operatorname{coker}(f) = 0$). We then write $f : X \hookrightarrow Y$ (resp. $f : X \twoheadrightarrow Y$). The following result is a consequence of the definitions:

LEMMA 3.160.– *Let* $\mathcal{C}$ *be a preabelian category,* X *an object of* $\mathcal{C}$*, and the preordered sets* P_X *and* Q^X *(section 1.1.1**(III)**).*

1) Let $v \in P_X$, $u \in Q^X$, *and the composition* $\xrightarrow{v} X \xrightarrow{u}$ *. We have that*

$$v \preceq \ker(u) \Leftrightarrow u \circ v = 0 \Leftrightarrow \operatorname{coker}(v) \succeq u,$$

thus, the mappings

$$\ker : Q^X \to P_X, \quad \operatorname{coker} : P_X \to Q^X$$

*form a Galois connection (section 2.1.2**(II)**), so that*

$$\ker(u) = \ker(\operatorname{coker}(\ker(u))) = \ker(\operatorname{coim}(u)) = \operatorname{im}(\ker(u)),$$
$$\operatorname{coker}(v) = \operatorname{coker}(\ker(\operatorname{coker}(v))) = \operatorname{coker}(\operatorname{im}(v)) = \operatorname{coim}(\operatorname{coker}(v)).$$

2) In particular, v is a kernel if and only if $v = \text{im}(v)$, u is a cokernel if and only if $u = \text{coim}(u)$, and if $u = \text{im}(v)$, then $\text{coker}(u) = \text{coker}(v)$ *and* $\text{im}(u) = \text{im}(v) = u$.

LEMMA 3.161.– *In a preabelian category $\mathcal{C}$, let $f : X \to Y$ be a morphism. The canonical monomorphism $\kappa : \ker(f) \hookrightarrow X$ and the canonical epimorphism $\gamma : Y \twoheadrightarrow coker(f)$ are strict.*

PROOF.– Since κ is a monomorphism, we have that $\text{coim}(\kappa) \cong \kappa = \ker(f)$, and $\ker(f) = \text{im}(\kappa)$ by lemma 3.160(2). For γ the rationale is similar. ■

LEMMA-DEFINITION 3.162.– *In a preabelian category $\mathcal{C}$, consider the sequence*

$$E_0 \xrightarrow{f_1} E_1 \xrightarrow{f_2} E_2 \qquad [3.50]$$

where $f_2 \circ f_1 = 0$.

1) There exists a canonical morphism $\psi : \text{im}(f_1) \to \ker(f_2)$.

2) The sequence [3.50] is said to be strictly exact *(resp.* coexact*) if the canonical morphism ψ is an isomorphism and f_1 (resp. f_2) is a strict morphism ([SCH 99], Def. 1.1.9)*[10].

PROOF.– Since $f_2 \circ f_1 = 0$, there exists a unique morphism $c : \text{coker}(f_1) \to E_2$ such that $c \circ \gamma_1 = f_2 \circ f_1$, where $\gamma_1 : E_1 \twoheadrightarrow \text{coker}(f_1)$. Let $\iota_1 : \text{im}(f_1) \hookrightarrow E_1$. Then, $f_2 \circ \iota_1 = c \circ \gamma_1 \circ \iota_1$. Let $\kappa_2 : \ker(f_2) \hookrightarrow E_1$. By definition of κ_2, there exists a unique morphism $\psi : \text{im}(f_1) \to \ker(f_2)$ such that $\iota_1 = \kappa_2 \circ \psi$.■

In $\mathcal{C}$, we can similarly define strictly exact (resp. strictly coexact) sequences of more than two morphisms, such as [3.3].

THEOREM 3.163.– *Let $\mathcal{C}$ be a preabelian category.*

In $\mathcal{C}$, a sequence

$$E_0 \xleftarrow{f_1} E_1 \xleftarrow{f_2} E_2 \longleftarrow 0 \qquad [3.51]$$

is strictly exact if and only if f_2 is a kernel of f_1.

10 In [PAL 70] (Chap. I, section 1, Def. 8), the sequence [3.50] is said to be *exact* if and only if it is both strictly exact and strictly coexact in the above terminology.

Dually, in $\mathcal{C}$ a sequence

$$E_0 \xrightarrow{f_1} E_1 \xrightarrow{f_2} E_2 \longrightarrow 0 \qquad [3.52]$$

is strictly coexact if and only if f_2 is a cokernel of f_1.

PROOF.– Assume that [3.51] is strictly exact. We have that $f_2 \cong \text{coim}\,(f_2) \cong \text{im}\,(f_2) = \ker(f_1)$. Conversely, if $f_2 = \ker(f_1)$, we have that $f_2 = \text{im}\,(f_2)$, hence $\text{im}\,(f_2) = \ker(f_1)$ and f_2 is a strict monomorphism by lemma 3.161. The other statement follows by duality. ■

The characterization of left-exact and right-exact additive functors using strictly exact sequences in preabelian categories is similar to the characterization in the category of modules (see section 3.1.4(**II**))[11]:

COROLLARY 3.164.– *Let $\mathfrak{F} : \mathcal{C} \to \mathcal{D}$ be an additive functor, where $\mathcal{C}$ and $\mathcal{D}$ are two abelian categories.*

i) If $\mathfrak{F}$ is covariant, it is left-exact *if and only if strict exactness of [3.51] implies strict exactness of*

$$\mathfrak{F}(E_0) \xleftarrow{\mathfrak{F}(f_1)} \mathfrak{F}(E_1) \xleftarrow{\mathfrak{F}(f_2)} \mathfrak{F}(E_2) \longleftarrow 0. \qquad [3.53]$$

ii) The covariant functor $\mathfrak{F}$ is right-exact *if and only if strict coexactness of [3.52] implies strict coexactness of*

$$\mathfrak{F}(E_0) \xrightarrow{\mathfrak{F}(f_1)} \mathfrak{F}(E_1) \xrightarrow{\mathfrak{F}(f_2)} \mathfrak{F}(E_2) \longrightarrow 0. \qquad [3.54]$$

iii) Dually, if $\mathfrak{F}$ is contravariant, it is left-exact (resp. right-exact) if and only if strict coexactness of [3.52] (resp. strict exactness of [3.51]) implies strict exactness of [3.53] (resp. strict coexactness of [3.54]).

PROOF.– (i): $\mathfrak{F}$ is left-exact if and only if it preserves kernels by corollary 1.23. (ii) and (iii) are deduced from (i) by reversing the arrows. ■

(IV) ABELIAN CATEGORIES. A category $\mathcal{C}$ is said to be *abelian* if it is preabelian and every morphism is strict. The category ${}_{\mathbf{A}}\mathbf{Mod}$ (where $\mathbf{A}$ is an

11 In [SCH 99], left-exact and right-exact functors are called strongly left-exact and strongly right-exact respectively.

arbitrary ring) is abelian. Consider the preordered set $(P_X, \preceq)$ of all morphisms with codomain X (section 1.1.1**(III)**). By taking the quotient, this relation $\preceq$ induces an order relation $\leq$ on the set $\mathfrak{P}(X)$ of subobjects of X, and we have the following result ([FRE 64], Chap. II):

THEOREM-DEFINITION 3.165.– *Let $\mathcal{C}$ be an abelian category and let X be an object of $\mathcal{C}$. Then, $(\mathfrak{P}(X), \leq)$ is a lattice (section 2.1.3**(I)**).*

We call the infimum of two objects of X their intersection*, and the supremum of these two objects their* union *(see example 2.4(1)).*

The theorem ([MIT 65], Chap. VI, Thm. 7.2) below shows that any diagram-chasing proof in ${}_{\mathbf{A}}\mathbf{Mod}$ is also valid in $\mathcal{C}$ by considering the full subcategory of $\mathcal{C}$ whose objects are the sources and targets of the various morphisms of the diagram:

THEOREM 3.166.– *(Freyd-Mitchell) Given any small abelian category $\mathcal{C}$ (section 1.1.2), there exists a ring A and a fully faithful exact covariant functor $\mathcal{C} \to {}_{\mathbf{A}}\mathbf{Mod}$.*

In an abelian category $\mathcal{C}$, strictly exact or coexact sequences are simply said to be *exact*, as in ${}_{\mathbf{A}}\mathbf{Mod}$ (section 3.1.4**(I)**). Noether's isomorphisms (theorem 2.12) hold in an abelian category written additively with the notions of intersection and union from theorem-definition 3.165. The same is true for the product isomorphism [2.13] (resp. the coproduct isomorphism [2.14], by replacing $\bigoplus$ with $\coprod$), provided that the products (resp. coproducts) exist in $\mathcal{C}$. Theorem 3.166, for example, makes the following result easier to prove, generalizing Noether's isomorphisms:

LEMMA 3.167.– *(*nine or 3×3 lemma*) In an abelian category, consider the following commutative diagram:*

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \dashrightarrow & A_1 & \dashrightarrow & B_1 & \dashrightarrow & C_1 & \dashrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A_2 & \longrightarrow & B_2 & \longrightarrow & C_2 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \dashrightarrow & A_3 & \dashrightarrow & B_3 & \dashrightarrow & C_3 & \dashrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

and suppose that the middle row and column are exact. Then, the first row is exact if and only if the third row is exact.

PROOF.– Write α_i for the arrow $A_i \rightarrow B_i$, β_i for the arrow $B_i \rightarrow C_i$ $(i = 1, 2, 3)$ and d for each vertical arrow. We simply need to show that exactness of the bottom row implies exactness of the top row, as this implies the converse in the opposite category. The argument, which we can perform in ${}_{\mathbf{A}}\mathbf{Mod}$ by the Freyd-Mitchell theorem, is a typical example of "diagram chasing". The reader can follow the argument by retracing each relation step by step on the diagram (the process becomes almost automatic).

1) α_1 is injective because $d \circ \alpha_1 = \alpha_2 \circ d$ and α_2, d are injective.

2) We will show that β_1 is surjective. Let $c_1 \in C_1$. We need to show that there exists $b_1 \in B_1$ such that $c_1 = \beta_1 b_1$, or equivalently, since d is injective, that $dc_1 = d\beta_1 b_1$. There exists $b_2 \in B_2$ such that $dc_1 = \beta_2 b_2$. Then, $\beta_3 db_2 = 0$ and since $\mathrm{im}\,(\alpha_3) = \ker(\beta_3)$, there exists $a_3 \in A_3$ such that $db_2 = \alpha_3 a_3$. There also exists $a_2 \in A_2$ such that $da_2 = a_3$, so $db_2 = \alpha_3 da_2 = d\alpha_2 a_2$, which implies that $d(b_2 - \alpha_2 a_2) = 0$, which again implies that $b_2 - \alpha_2 a_2 = 0$. Take $b_1 \in \ker(d) \subseteq B_1$. Then, $db_1 = b_2 - \alpha_2 a_2$, hence $d\beta_1 b_1 = \beta_2 db_1 = \beta_2(b_2 - \alpha_2 a_2) = \beta_2 b_2 = dc_1$.

3) We will show that $\ker(\beta_1) \subseteq \mathrm{im}\,(\alpha_1)$. Let $b_1 \in B_1$ be such that $\beta_1 b_1 = 0$. We need to show that there exists $a_1 \in A_1$ such that $b_1 = \alpha_1 a_1$. Now, $0 = d\beta_1 b_1 = \beta_2 db_1$, and since $\mathrm{im}\,(\alpha_2) = \ker(\beta_2)$, there exists $a_2 \in A_2$ such that $db_1 = \alpha_2 a_2$, so $\alpha_3 da_2 = d\alpha_2 a_2 = d^2 b_1 = 0$, and since α_3 is injective, $a_2 \in \ker(d : A_2 \rightarrow A_3)$, so there exists $a_1 \in A_1$ such that $a_2 = da_1$. Hence, $d\alpha_1 a_1 = \alpha_2 da_1 = \alpha_2 a_2 = db_1$, and so $d(\alpha_1 a_1 - b_1) = 0$, which implies that $b_1 = \alpha_1 a_1$.

4) We will show that $\mathrm{im}\,(\alpha_1) \subseteq \ker(\beta_1)$, or equivalently that $\beta_1 \circ \alpha_1 = 0$. We have that $d \circ \beta_1 \circ \alpha_1 = \beta_2 \circ \alpha_2 \circ d = 0$, so $\beta_1 \circ \alpha_1 = 0$ because $d : C_1 \rightarrow C_2$ is injective. ■

We immediately deduce ([POM 01], p. 728)

COROLLARY 3.168.– *Let* $\mathbf{A}$ *be an Ore domain,* M *an* $\mathbf{A}$*-module,* U *a submodule of* M *and* $\mathcal{T}(.)$ *the torsion submodule of the module in*

parentheses. The following diagram commutes and is exact:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{T}(U) & \longrightarrow & U & \longrightarrow & \frac{\mathcal{T}(M)+U}{\mathcal{T}(M)} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{T}(M) & \longrightarrow & M & \longrightarrow & \frac{M}{\mathcal{T}(M)} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \frac{\mathcal{T}(M)}{\mathcal{T}(U)} & \longrightarrow & \frac{M}{U} & \longrightarrow & \frac{M}{\mathcal{T}(M)+U} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

PROOF.– Exactness of the first row follows from Noether's second isomorphism (theorem 2.12); exactness of the second row and the first two columns is obvious, and exactness of the third column follows from Noether's third isomorphism. Finally, the exactness of the third row follows from the nine lemma. ■

By "chasing", analogously to the proof of lemma 3.167, we obtain the *snake lemma* in an abelian category (for modules, see [BKI 12], Chap. X, section 1.2, Prop. 2):

LEMMA 3.169.– *(*snake*) Given the exact commutative diagram*

$$\begin{array}{ccccccc}
 & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow 0 \\
 & & \alpha\downarrow & & \beta\downarrow & & \gamma\downarrow & \\
0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' &
\end{array}$$

there exists an exact sequence (Figure 3.1)

$$\ker\alpha \to \ker\gamma \to \ker\gamma \to \operatorname{coker}(\alpha) \to \operatorname{coker}(\beta) \to \operatorname{coker}(\gamma)$$

and $\ker\gamma \to \operatorname{coker}(\alpha)$ *is called the* connecting morphism *(see below, definition 3.171(1)).*

(V) PROJECTIVE LIMITS AND INJECTIVE LIMITS. By proposition 1.22, the projective limits $\varprojlim_{i\in I} Y_i$ exist in an abelian category $\mathcal{C}$ if and only if the

products $\prod_{i\in I} Y_i$ exist in $\mathcal{C}$. The canonical morphism $\beta_i : \varprojlim_{i\in I} Y_i \to Y_i$ is defined as the composition

$$\beta_i : Y := \bigcap_{i\preceq j} \ker\left(\mathrm{pr}_i - \psi_i^j \circ \mathrm{pr}_j\right) \subset \prod_{i\in I} Y_i \overset{\mathrm{pr}_i}{\to} Y_i.$$

where $\mathrm{pr}_i : \prod_{i\in I} Y_i \to Y_i$ is canonical projection. Similarly, the injective limits $\varinjlim_{i\in I} X_i$ exist in $\mathcal{C}$ if and only if the coproducts $\coprod_{i\in I} X_i$ exist in $\mathcal{C}$. The canonical morphism $\alpha_i : X_i \to \varinjlim_{i\in I} X_i$ is given by the composition

$$\alpha_i : X_i \to \left(\coprod_{i\in I} X_i\right) \longrightarrow \left(\coprod_{i\in I} X_i\right) / \left(\sum_{i\preceq j} \mathrm{im}\left(\mathrm{inj}_i - \mathrm{inj}_j \circ \varphi_j^i\right)\right)$$

where $\mathrm{inj}_i : X_i \to \coprod_{i\in I} X_i$ is canonical injection.

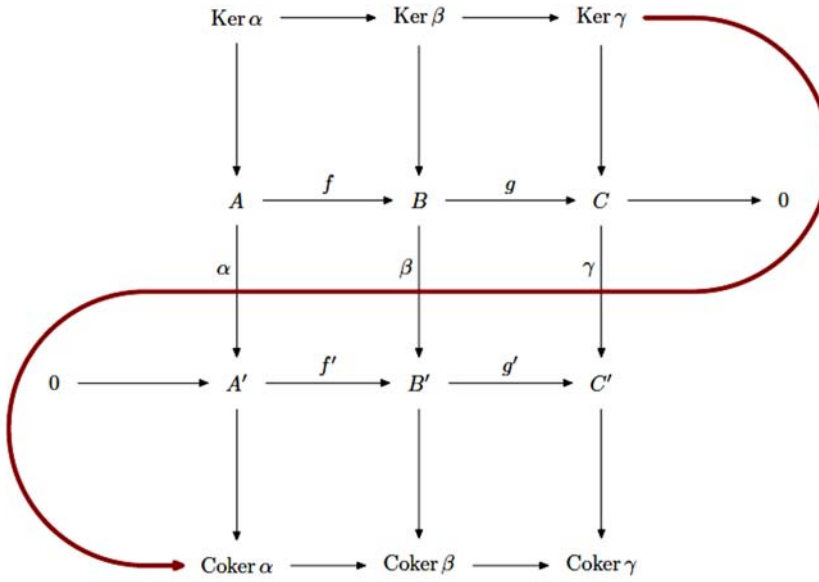


Figure 3.1. *Snake lemma*

3.3.8. *Complexes. Notions of algebraic topology*

(I) COMPLEXES. Let $\mathbf{R}$ be a ring equipped with the trivial gradation (section 2.3.12) and let $C_\bullet = \bigoplus_{p\in\mathbb{Z}} C_p$, $C^\bullet = \bigoplus_{p\in\mathbb{Z}} C^p$ be graded $\mathbf{R}$-modules.

Instead of [3.46] and [3.47], consider the following sequences of $\mathbf{R}$-modules and $\mathbf{R}$-linear mappings:

$$... \longrightarrow C_{p+1} \xrightarrow{d_{p+1}} C_p \xrightarrow{d_p} C_{p-1} \longrightarrow ... \quad [3.55]$$

$$... \longleftarrow C^{p+1} \xleftarrow{d^p} C^p \xleftarrow{d^{p-1}} C^{p-1} \longleftarrow ... \quad [3.56]$$

The sequences [3.55], [3.56] are called $\mathbf{R}$-*complexes* if, for all $p \in \mathbb{Z}$, $d_p \circ d_{p+1} = 0$ (for the first) and $d^p \circ d^{p-1} = 0$ (for the second).

(II) HOMOLOGY. The complex [3.55] is called a *chain complex* $C_\bullet = (C_p)_{p\in\mathbb{Z}}$. The mapping $d_\bullet = (d_p) : C_\bullet \to C_\bullet$ is a graded endomorphism of degree -1 (section 2.3.12), called a *codifferential* (or sometimes simply a *differential*, if this does not create ambiguity). $C_\bullet$ is called a *codifferential graded* $\mathbf{R}$-*module* ([DIE 82], t. 9, Ann. 30.7). The graded modules $\mathbf{Z}(C_\bullet) = \ker(d_\bullet)$ and $\mathbf{B}(C_\bullet) = \operatorname{im}(d_\bullet)$ are, respectively, known as the *cycle* and the *boundary* of $C_\bullet$.

The relation $d_\bullet \circ d_\bullet = 0$ implies that $\mathbf{B}(C_\bullet) \subseteq \mathbf{Z}(C_\bullet)$, and $\mathbf{H}(C_\bullet) = \mathbf{Z}(C_\bullet)/\mathbf{B}(C_\bullet)$ is called the *homology module* of $C_\bullet$. By explicitly considering the components of $C_\bullet$, we obtain

$$\mathbf{Z}_p(C_\bullet) = \ker(d_p), \mathbf{B}_p(C_\bullet) = \operatorname{im}(d_{p+1}), \mathbf{H}_p(C_\bullet) = \mathbf{Z}_p(C_\bullet)/\mathbf{B}_p(C_\bullet).$$

We call $\mathbf{H}_p(C_\bullet)$ the p-th homology module of $C_\bullet$. We have the following exact sequences, which are said to be canonical:

$$0 \to \mathbf{Z}_p(C_\bullet) \to C_p \xrightarrow{\delta_p} \mathbf{B}_{p-1}(C_\bullet) \to 0, \quad [3.57]$$

$$0 \to \mathbf{B}_p(C_\bullet) \to \mathbf{Z}_p(C_\bullet) \to \mathbf{H}_p(C_\bullet) \to 0, \quad [3.58]$$

$$0 \to \mathbf{B}_p(C_\bullet) \to C_p \to C_p/\mathbf{B}_p(C_\bullet) \to 0, \quad [3.59]$$

$$0 \to \mathbf{H}_p(C_\bullet) \to C_p/\mathbf{B}_p(C_\bullet) \xrightarrow{\bar{\delta}_p} \mathbf{B}_{p-1}(C_\bullet) \to 0 \quad [3.60]$$

where [3.57] follows from Noether's first isomorphism, [3.58] follows from the definition of $\mathbf{H}_p(C_\bullet)$, [3.59] is obvious, and [3.60] is a consequence of

[3.57] and Noether's third isomorphism. We have that $\mathbf{H}_p(C_\bullet) = 0$ if and only if $\ker(d_p) = \text{im}(d_{p+1})$. From [3.60] and [3.58] replacing p by $p-1$, we deduce the fifth canonical exact sequence

$$0 \to \mathbf{H}_p(C_\bullet) \to C_p/\mathbf{B}_p(C_\bullet) \longrightarrow \mathbf{Z}_{p-1}(C_\bullet) \to \mathbf{H}_{p-1}(C_\bullet) \to 0. \quad [3.61]$$

A morphism of $\mathbf{R}$-complexes $u : C_\bullet \to C'_\bullet$ (also called a *morphism of chains*) is a graded homomorphism of degree 0 (section 2.3.12) such that $d' \circ u = u \circ d$, which therefore makes the following diagram commute

$$\begin{array}{ccccccc} \ldots \longrightarrow & C_{p+1} & \xrightarrow{d_{p+1}} & C_p & \xrightarrow{d_p} & C_{p-1} & \longrightarrow \ldots \\ & u_{p+1}\downarrow & & u_p\downarrow & & u_{p-1}\downarrow & \\ & C'_{p+1} & \xrightarrow{d'_{p+1}} & C'_p & \xrightarrow{d'_p} & C'_{p-1} & \longrightarrow \ldots \end{array} \quad [3.62]$$

This defines the category $\mathbf{R}$-$\mathbf{Comp}$ of $\mathbf{R}$-complexes, which is abelian (section 3.3.7(**IV**)) ([ROT 09], Prop. 5.100). For example, $\ker(u)$ is the complex with homogeneous components $(\ker(u_p))$. The canonical exact sequences imply the following short exact sequences in $\mathbf{R}$-$\mathbf{Comp}$

$$0 \to \mathbf{Z}_\bullet(C_\bullet) \to C_\bullet \xrightarrow{\delta} \mathbf{B}_\bullet(C_\bullet)(-1) \to 0, \quad [3.63]$$

$$0 \to \mathbf{B}_\bullet(C_\bullet) \to \mathbf{Z}_\bullet(C_\bullet) \to \mathbf{H}_\bullet(C_\bullet) \to 0, \quad [3.64]$$

$$0 \to \mathbf{B}_\bullet(C_\bullet) \to C_\bullet \to C_\bullet/\mathbf{B}_\bullet(C_\bullet) \to 0, \quad [3.65]$$

$$0 \to \mathbf{H}_\bullet(C_\bullet) \to C_\bullet/\mathbf{B}_\bullet(C_\bullet) \xrightarrow{\bar{\delta}} \mathbf{B}_\bullet(C_\bullet)(-1) \to 0. \quad [3.66]$$

where, for example, $\mathbf{B}_\bullet(C_\bullet)(-1)$ is the translated complex $\mathbf{B}_p(C_\bullet)(-1) = \mathbf{B}_{p-1}(C_\bullet)$. The complex $\mathbf{H}_\bullet(C_\bullet)$ measures the "non-exactness" of the sequence of the d_p. The relation $d'_p \circ u_p = u_{p-1} \circ d_p, \forall p \in \mathbb{Z}$, implies that $u_p(\mathbf{Z}_p(C_\bullet)) \subseteq \mathbf{Z}_p(C'_\bullet)$ and $u_p(\mathbf{B}_p(C_\bullet)) \subseteq \mathbf{B}_p(C'_\bullet)$ (**exercise**), and so there exists a homomorphism $\mathbf{H}_p(u) : \mathbf{H}_p(C_\bullet) \to \mathbf{H}_p(C'_\bullet)$ induced by u_p (theorem-definition 2.11). Hence, $u : C_\bullet \to C'_\bullet$ induces a morphism of chains $\mathbf{H}_\bullet(u)$ in $\mathbf{R}$-$\mathbf{Comp}$, from which it follows that

$$\mathbf{H}_\bullet : C_\bullet \mapsto \mathbf{H}(C_\bullet), \quad \left(u : C_\bullet \to C'_\bullet\right) \mapsto \left(\mathbf{H}_\bullet(u) : \mathbf{H}_\bullet(C_\bullet) \to \mathbf{H}\left(C'_\bullet\right)\right)$$

is an additive functor (section 3.3.7(**III**)) from $\mathbf{R}$-**Comp** to $\mathbf{R}$-**Comp**, called the "homological functor". Consider a short exact sequence of $\mathbf{R}$-complexes (to lighten the notation, the symbol for the index is omitted)

$$0 \to C' \overset{u}{\to} C \overset{v}{\to} C'' \to 0. \qquad [3.67]$$

The morphism $u : C' \to C$ induces morphisms $\mathbf{Z}_\bullet(u) : \mathbf{Z}_\bullet(C') \to \mathbf{Z}_\bullet(C)$ and $\bar{u} : C'/\mathbf{B}_\bullet(C') \to C/\mathbf{B}_\bullet(C)$; by writing the canonical exact sequences as columns, we obtain the exact commutative diagram (**exercise**)

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & \mathbf{H}_p(C') & \overset{\mathbf{H}_p(u)}{\longrightarrow} & \mathbf{H}_p(C) & \overset{\mathbf{H}_p(v)}{\longrightarrow} & \mathbf{H}_p(C'') \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & C'_p/\mathbf{B}_p(C') & \overset{\bar{u}_p}{\longrightarrow} & C_p/\mathbf{B}_p(C) & \overset{\bar{v}_p}{\longrightarrow} & C''_p/\mathbf{B}_p(C'') \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 \longrightarrow & \mathbf{Z}_{p-1}(C') & \overset{\mathbf{Z}_{p-1}(u)}{\longrightarrow} & \mathbf{Z}_{p-1}(C) & \overset{\mathbf{Z}_{p-1}(v)}{\longrightarrow} & \mathbf{Z}_{p-1}(C'') & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & \mathbf{H}_{p-1}(C') & \overset{\mathbf{H}_{p-1}(u)}{\longrightarrow} & \mathbf{H}_{p-1}(C) & \overset{\mathbf{H}_{p-1}(v)}{\longrightarrow} & \mathbf{H}_{p-1}(C'') & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & 0 & & 0 & & 0 &
\end{array}$$

and the snake lemma (lemma 3.169) implies

THEOREM 3.170.– *For any p, there exists a homomorphism $\partial_p(u,v) : \mathbf{H}_p(C'') \to \mathbf{H}_{p-1}(C')$ that determines a homomorphism of graded modules $\partial_\bullet(u,v)$ of degree -1. We have the following long exact sequence of $\mathbf{R}$-modules:*

$$\begin{array}{l}
\ldots \to \mathbf{H}_{p+1}(C'') \overset{\partial_{p+1}(u,v)}{\to} \mathbf{H}_p(C') \overset{\mathbf{H}_p(u)}{\longrightarrow} \mathbf{H}_p(C) \overset{\mathbf{H}_p(v)}{\longrightarrow} \mathbf{H}_p(C'') \\
\qquad \overset{\partial_p(u,v)}{\to} \mathbf{H}_{p-1}(C') \overset{\mathbf{H}_{p-1}(u)}{\longrightarrow} \mathbf{H}_{p-1}(C) \overset{\mathbf{H}_{p-1}(v)}{\longrightarrow} \mathbf{H}_{p-1}(C'') \to \ldots
\end{array}$$

DEFINITION 3.171.– *1) The long exact sequence stated above is called the* exact sequence of homology modules *associated with the short exact sequence [3.67] and $\partial_\bullet(u,v)$ is called the* connecting morphism. *The long exact sequence of homology modules may be written more concisely as the exact triangle*

$$\begin{array}{ccc}
 & \mathbf{H}(C) & \\
\mathbf{H}(u) \nearrow & & \searrow \mathbf{H}(v) \\
\mathbf{H}(C') & \longleftarrow & \mathbf{H}(C'') \\
 & \partial(u,v) &
\end{array} \qquad [3.68]$$

where, to lighten the notation, $\mathbf{H} = \mathbf{H}_\bullet$ *and* $\partial\,(u, v) = \partial_\bullet\,(u, v)$.

2) Given two complexes C, C', *a* homologism *from* C *to* C' *is a morphism* u *such that* $\mathbf{H}\,(u)$ *is bijective.*

3) A complex C *is called* null-homologous *if* $\mathbf{H}\,(C) = 0$.

From the above, we deduce (**exercise**)

COROLLARY 3.172.– *i) Consider the exact sequence of complexes [3.67]. If two of the complexes* C', C, C'' *are null-homologous, the third is too. For* u *(resp.* v*) to be a homologism, it is necessary and sufficient for* C'' *(resp.* C'*) to be null-homologous. For* $\partial\,(u, v)$ *to be bijective, it is necessary and sufficient for* C *to be null-homologous.*

ii) If $\ker\,(u)$ *and* coker (u) *are null-homologous, then* u *is a homologism.*

We have that $\mathbf{H}_\bullet\,(u) = 0$ if and only if $u\,(\ker d_\bullet) \subseteq \mathrm{im}\,(d'_\bullet)$ (by theorem-definition 2.11(2)), which implies

COROLLARY-DEFINITION 3.173.– *To have* $\mathbf{H}_\bullet\,(u) = 0$ *(in which case we say that* u *is* homologous *to* 0*), it is sufficient for the following condition (*$\boldsymbol{H}_0$*) to be satisfied:*

($\boldsymbol{H}_0$*): There exists a graded homomorphism* $s : C_\bullet \to C'_\bullet$ *of degree* $+1$, $s = \left(s_p : C_p \to C'_{p+1}\right)$, *such that* $u = d' \circ s + s \circ d$, *or in other words (see [3.62]),*

$$\forall p \in \mathbb{Z},\ u_p = d'_{p+1} \circ s_p + s_{p-1} \circ d_p. \qquad [3.69]$$

The graded homomorphism s *is called a* homotopy, *and the condition (*$\boldsymbol{H}_0$*) is described by saying that* u *is* homotopic *to* 0. *We say that two morphisms of* $\mathbf{R}$*-complexes* $u, v : C_\bullet \to C'_\bullet$ *are* homologous *(resp.* homotopic*) if* $u - v$ *is homologous (resp. homotopic) to* 0, *and so two morphisms of* $\mathbf{R}$*-complexes are homologous if they are homotopic (the converse is false). A complex* $C_\bullet$ *is said to be homotopic to* 0 *if* $\mathrm{id}_{C_\bullet}$ *is homotopic to the zero mapping.*

REMARK 3.174.– *The above still holds,* mutatis mutandis, *if we work in an arbitrary abelian category* $\mathcal{C}$ *instead of the category* ${}_{\mathbf{R}}\mathbf{Mod}$ *([ROT 09], section 5.5, section 6.1). We can similarly define the objects cycle, boundary and homology of index* p, $\mathbf{Z}\,(C_p)$, $\mathbf{B}_p\,(C_\bullet)$ *and* $\mathbf{H}_p\,(C_\bullet)$, *respectively, partly by applying Noether's isomorphisms (section 3.3.7(**IV**)). However, to recreate*

each step of the process in this more general context, we would require notions such as graded categories *that we cannot explore here. We write* $\mathcal{C}$**-comp** *for the abelian category of* $\mathcal{C}$*-complexes containing the sequences of objects and sequences of morphisms in* $\mathcal{C}$.

(III) COHOMOLOGY. Dually, the complex [3.56] in ${}_{\mathbf{R}}\mathbf{Mod}$ is called a *cochain complex* $C^\bullet = (C^p)_{p\in\mathbb{Z}}$. The mapping $d^\bullet = (d^p) : C^\bullet \to C^\bullet$ is a graded morphism of degree $+1$ such that $d^\bullet \circ d^\bullet = 0$ and so is called a *differential*. The complex $C^\bullet$ is a *differential graded* $\mathbf{R}$*-module* (*[DIE 82],* t. 9, Ann. 30.2). To go from $C_\bullet$ to $C^\bullet$, we need to change p to $-p$. The complexes

$$\mathbf{Z}\left(C^\bullet\right) = \ker\left(d^\bullet\right), \mathbf{B}\left(C^\bullet\right) = \operatorname{im}\left(d^\bullet\right), \mathbf{H}\left(C^\bullet\right) = \mathbf{Z}\left(C^\bullet\right)/\mathbf{B}\left(C^\bullet\right)$$

are, respectively, called the *cocycle*, the *coboundary* and the *cohomology* of the complex $C^\bullet$. Their components are

$$\mathbf{Z}^p\left(C^\bullet\right) = \ker\left(d^p\right), \mathbf{B}^p\left(C^\bullet\right) = \operatorname{im}\left(d^{p-1}\right), \mathbf{H}^p\left(C^\bullet\right) = \mathbf{Z}^p\left(C^\bullet\right)/\mathbf{B}^p\left(C^\bullet\right).$$

Repeating what we said earlier after changing p to $-p$, we can define the abelian category $\mathbf{R}$**-Comp** of cochain complexes, as well as the additive "cohomological functor" $\mathbf{H}^\bullet$. The canonical exact sequences [3.63], [3.64], [3.65], [3.66], [3.61] remain the same except for changes in the notation; for example, [3.66] becomes

$$0 \to \mathbf{H}^\bullet\left(C^\bullet\right) \to C^\bullet/\mathbf{B}^\bullet\left(C^\bullet\right) \overset{\bar{\delta}}{\to} \mathbf{B}^\bullet\left(C^\bullet\right)(-1) \to 0$$

where the homogeneous components of the complex $B^\bullet\left(C^\bullet\right)$ are $B^{p+1}\left(C^\bullet\right)$.

The statement of theorem 3.170 remains valid after changing p to $-p$, giving the *long exact sequence of cohomology module*s

$$\ldots \to \mathbf{H}^{p-1}\left(C''\right) \overset{\partial^{p-1}(u,v)}{\to} \mathbf{H}^p\left(C'\right) \overset{\mathbf{H}^p(u)}{\longrightarrow} \mathbf{H}^p\left(C\right) \overset{\mathbf{H}^p(v)}{\longrightarrow} \mathbf{H}^p\left(C''\right) \overset{\partial^p(u,v)}{\to} \mathbf{H}^{p+1}\left(C'\right) \overset{\mathbf{H}^{p+1}(u)}{\longrightarrow} \mathbf{H}^{p+1}\left(C\right) \overset{\mathbf{H}^{p+1}(v)}{\longrightarrow} \mathbf{H}^{p+1}\left(C''\right) \to \ldots$$

which again implies the exact triangle [3.68], where the connecting morphism $\partial\left(u,v\right) = \partial^\bullet\left(u,v\right)$ is now graded of degree $+1$ and $\mathbf{H} = \mathbf{H}^\bullet$. In the context of cochains, a *homotopy* is a graded homomorphism $s : C^\bullet \to C'^\bullet$ of degree -1, $s = \left(s^p : C^p \to C'^{p-1}\right)$, and a morphism of cochains u is homotopic to

0 if and only if there exists a homotopy s such that $u = d' \circ s + s \circ d$, or in other words (see [3.62]),

$$\forall p \in \mathbb{Z},\ u^p = d'^{p-1} \circ s^p + s^{p+1} \circ d^p;$$

remark 3.174 still holds.

In ${}_{\mathbf{R}}\mathrm{Mod}$, let $\left(B^i\right)_{i \geq -1}$ be a complex of cochains, and $\left(A_j^\bullet\right)_{j \geq -2}$ a sequence of complexes of cochains, with $B^{-1} = 0$ and $\left(A_{-2}^\bullet\right) = 0$. Consider the following commutative diagram:

$$\begin{array}{ccccc}
 & & & & 0 \\
 & & & & \downarrow \\
 & & 0 & \longrightarrow & A_{-1}^\bullet \\
 & & \downarrow & & \downarrow \\
0 & \longrightarrow & B^0 & \longrightarrow & A_0^\bullet \\
 & & \downarrow & & \downarrow \\
0 & \longrightarrow & B^1 & \longrightarrow & A_1^\bullet \\
 & & \downarrow & & \downarrow \\
0 & \longrightarrow & B^2 & \longrightarrow & A_2^\bullet \\
 & & \downarrow & & \downarrow \\
 & & \vdots & & \vdots
\end{array}$$

We can show the following ([PAL 70], Chap. I, section 2):

THEOREM 3.175.– *If the row* $0 \longrightarrow A_{-1}^*$ *is a complex and the rows* $0 \longrightarrow B^i \longrightarrow A_i^\bullet$ $(i \geq 0)$ *are all exact sequences of* $\mathbf{R}$*-modules, then there exist canonical isomorphisms*

$$\mathbf{H}^p\left(A_{-1}^\bullet\right) \cong \mathbf{H}^p\left(B^\bullet\right), \quad p \geq 0.$$

(IV) HOMOTOPY IN ALGEBRAIC TOPOLOGY. All the terminology introduced above relates to elementary questions in algebraic topology. Homotopy in the sense of corollary-definition 3.173, introduced by S. Lefschetz in 1930 ([LEF 30], Chap. II, section 2), reflects the original meaning of definition 3.176 below ([ROT 88], Chap. 1), given by M. Dehn and P. Heegaard (1907) (for more details, see [LEF 49], Chap. V, section 1.2).

DEFINITION 3.176.– *Given two topological spaces* X, Y*, two continuous mappings* $f, g : X \to Y$ *are* homotopic *(written* $f \simeq g$*) if there exists a*

continuous mapping $F : X \times [0,1] \to Y$ *such that* $F(x,0) = f(x)$ *and* $F(x,1) = g(x), \forall x \in X$. *We say that these spaces* X, Y *are* homotopically equivalent *(or* of the same homotopy type*) if there exist continuous mappings* $h : X \to Y$ *and* $k : Y \to X$ *such that* $k \circ h \simeq \mathrm{id}_X$ *and* $h \circ k \simeq \mathrm{id}_Y$ *(this is obviously an equivalence relation, as is the property of being homotopic for two continuous mappings).*

(V) SIMPLICIAL HOMOLOGY. Let $\{v_1, ..., v_n\}$ be the canonical basis of $\mathbb{R}^n$ (with the canonical orientation) and let $v_0 = 0$. For all $n \geq 0$, let

$$\Delta^n = \left\{ \sum_{i=0}^{n} t_i v_i : t_i \geq 0, \sum_{0 \leq i \leq n} t_i = 1 \right\}$$

be the closed convex envelope of $\{v_0, v_1, ..., v_n\}$, written $[v_0, v_1, ..., v_n]$. Write $(t_0, t_1, ..., t_n)$ for the point $\sum_{i=0}^{n} t_i v_i \in \Delta^n$.

DEFINITION 3.177.– Δ^n *is called a* standard n-simplex. *The* i*-th* face *of* Δ^n *is defined as the set* $[v_0, ..., \hat{v}_i, ..., v_n]$ *(the notation* $\hat{v}_i$ *means that* v_i *is omitted). The (oriented)* boundary *of* Δ_n *is*

$$\partial \Delta_n = \bigcup_{i=0}^{n} (-1)^i [v_0, ..., \hat{v}_i, ..., v_n]$$

where the factor of -1 *indicates that the orientation is reversed.*

EXAMPLE 3.178.– *Consider the triangle* $\Delta^2 = [v_0, v_1, v_2]$ *in a plane. The canonical orientation of the plane is the usual trigonometric orientation. The oriented boundary of* Δ^2 *is*

$$\begin{aligned} \partial \Delta^2 &= [v_0, v_1] \cup [v_1, v_2] \cup [v_2, v_0] \\ &= [v_0, v_1, \hat{v}_2] \cup [\hat{v}_0, v_1, v_2] \cup (-[v_0, \hat{v}_1, v_2]) \end{aligned}$$

*(**exercise**: draw a diagram!). The face with index* 0 *is* $[v_1, v_2]$ *(opposite to* v_0*), the face with index* 1 *is* $[v_0, v_2]$ *(opposite to* v_1*), etc.*

We can take (finite) linear combinations of simplexes with integer coefficients. In the plane, consider the tile bounded by the square $ABCD$ where $A = (0,0)$, $B = (1,0)$, $C = (1,1)$, $D = (0,1)$, with the same orientation (**exercise**: draw a diagram!). This tile is the "sum" of the two simplexes bounded by the triangles ABD and BCD. Its boundary is the

square $ABCD$, the sum of the oriented boundaries of these two triangles, where the shared edge DB cancels. This tile can be "triangulated" another way, by saying that it is the "sum" of the two simplexes bounded by the triangles ABC and ACD.

(VI) SINGULAR HOMOLOGY.

DEFINITION 3.179.– *Let X be a topological space.*

1) A p-simplex *in X is a continuous mapping $\sigma : \Delta^p \to X$.*

2) The i-th face operator is $\epsilon_i^p : \Delta^{p-1} \to \Delta^p$ defined by

$$\epsilon_i^p : (t_0, ...t_{p-1}) \mapsto \begin{cases} (0, t_0, ..., t_{p-1}) \text{ if } i = 0 \\ (t_0, ...t_{i-1}, 0, t_i, ..., t_{p-1}) \text{ if } i > 0. \end{cases}$$

3) Let $\sigma : \Delta^p \to X$ be a p-simplex. If $p = 0$, we set $\partial_0(\sigma) = 0$, and if $p \geq 1$, $\partial_p(\sigma)$ is the $(p-1)$-simplex

$$\partial_p(\sigma) = \sum\nolimits_{i=0}^{p} (-1)^i \sigma \circ \epsilon^i. \qquad [3.70]$$

where ∂_p is the boundary operator.

By taking linear combinations of simplexes with integer coefficients, we obtain chains:

DEFINITION 3.180.– *Let X be a topological space. We define $S_{-p}(X) = \{0\}$ for all $p < 0$ and, for all $p \in \{0, ..., n\}$, we write $S_p(X)$ for the free abelian group (section 3.1.3**(II)**), whose basis is given by the p-simplexes of X. The elements of $S_p(X)$ are called* p-chains *of X. A p-chain is therefore a formal linear combination of p-simplexes with integer coefficients, and its* boundary *is calculated by applying the* same linear combination *to the boundaries of these p-simplexes.*

It is possible to show the following result **(exercise***: see [ROT 09], Prop. 1.22):

THEOREM 3.181.– *The diagram*

$$... \longrightarrow S_{p+1}(X) \xrightarrow{d_{p+1}} S_p(X) \xrightarrow{d_p} S_{p-1}(X) \longrightarrow ...$$

is a chain complex $S_p(X)$.

We therefore write $\mathbf{Z}_p(X) = \ker(d_p)$, $\mathbf{B}_p(X) = \text{im}(d_{p+1})$, $\mathbf{H}_p(X) = \mathbf{Z}_p(X)/\mathbf{B}_p(X)$. If two topological spaces X, Y are homotopically equivalent, then $\mathbf{H}_p(X) \cong \mathbf{H}_p(Y), \forall p \geq 0$ ([ROT 09], Cor. 1.26). If $f : X \to Y$ is a continuous mapping (where X, Y are topological spaces), $f \circ \sigma : \Delta^p \to Y$ is a p-simplex (definition 3.179(1)), so f determines a morphism of complexes $S_\bullet(f)$ from $S_\bullet(X)$ to $S_\bullet(Y)$, which gives the homology complex $\mathbf{H}_\bullet(f)$. Consequently, for all $p \geq 0$, $\mathbf{H}_p : \mathbf{Top} \to \mathbf{Ab}$:

$$X \mapsto \mathbf{H}_p(X), \quad [f : X \to Y] \mapsto [\mathbf{H}_p(f) : \mathbf{H}_p(X) \to \mathbf{H}_p(Y)]$$

is a functor. If two continuous mappings $f, g : X \to Y$ are homotopic, then $\mathbf{H}_p(f) = \mathbf{H}_p(g), \forall p \geq 0$ ([ROT 09], Thm. 6.14).

In many applications, it is necessary to replace the above complex $S_\bullet(X)$ by $S_\bullet(X; G) := S_\bullet(X) \bigotimes_{\mathbb{Z}} G$, where G is an abelian group (often $\mathbb{R}$). We therefore obtain the homology groups $\mathbf{H}_p(X; G)$, which take values in G, where $\mathbf{H}_p(X; G) := \mathbf{Z}_p(X; G)/\mathbf{B}_p(X; G)$ with $\mathbf{Z}_p(X; G) := \ker(d_p \otimes \text{id}_G)$, $\mathbf{B}_p(X; G) := \text{im}(d_{p+1} \otimes \text{id}_G)$. In general, $\mathbf{H}_p(X; G) \ncong \mathbf{H}_p(X) \bigotimes_{\mathbb{Z}} G$ and the relation between $\mathbf{H}_p(X; G)$ and $\mathbf{H}_p(X) \bigotimes_{\mathbb{Z}} G$ is established using the *universal coefficient theorem* (see theorem 3.187). This theorem implies that $\mathbf{H}_p(X; G) \cong \mathbf{H}_p(X) \bigotimes_{\mathbb{Z}} G$, whenever $\mathbf{H}_p(X)$ and $\mathbf{H}_{p-1}(X)$ are free $\mathbb{Z}$-modules or G is a torsion-free abelian group (for example, $\mathbb{R}$).

Let $X = \{a\}$. The only p-chain in X is the constant mapping σ_p with value a. We have that $\sigma_p \circ \epsilon^i = \sigma_{p-1}$, so by [3.70], $\partial_p(\sigma_p) = 0$ if p is even, $\partial_p(\sigma_p) = \sigma_{p-1}$ if p is odd. Hence, $\mathbf{Z}_p(X) = \mathbb{Z}\sigma_p$ if p is even, $\mathbf{Z}_p(X) = 0$ if p is odd, $\mathbf{B}_p(X) = 0$ if p is odd or $p = 0$, $\mathbf{B}_p(X) = \mathbb{Z}\sigma_p$ if p is even and > 0. This implies that $\mathbf{H}_0(X) \cong \mathbb{Z}$ and $\mathbf{H}_p(X) = \{0\}$ if $p \neq 0$.

A topological space X is said to be *contractible* to a $(a \in X)$ if id_X is homotopic to the constant mapping $X \to X : x \mapsto a$ ([BKI 16], Chap. III, section 1.3, Example 3); this is equivalent to saying that X is homotopically equivalent to $\{a\}$ ([ROT 88], Thm. 1.12), or, in other words, that it can be reduced to $\{a\}$ by means of a continuous deformation. We therefore have

THEOREM 3.182.– *If the topological space X is contractible to a point, we have that $\mathbf{H}_0(X) \cong \mathbb{Z}$ and $\mathbf{H}_p(X) = \{0\}$ if $p \neq 0$.*

Consider, for example, a subset U of $\mathbb{R}^n$ that is *star-shaped* around a point $x_0 \in U$, i.e. which satisfies the property that if $x_1 \in U$ then the closed interval

$[x_0, x_1] := \{tx_0 + (1-t)\, x_1 : t \in [0,1]\}$ is included in U. Any such space U is contractible to x_0. However, the space between two concentric spheres with different radii in $\mathbb{R}^3$ is not contractible to any point.

If $(X_\alpha)_{\alpha \in A}$ is a partition of X, where the X_α are open sets, and if G is an arbitrary abelian group, we have that $\mathbf{H}_p(X;G) \cong \bigoplus_{\alpha \in A} \mathbf{H}_p(X_\alpha;G)$ (**exercise***; see [DIE 82], vol. 9, (24.22.5)). We can show that if S_n is the unit sphere around 0 in $\mathbb{R}^n$, we have that $\mathbf{H}_0(S_n) \cong \mathbf{H}_n(S_n) \cong \mathbb{Z}$ and $\mathbf{H}_p(S_n) = 0$ if $p \neq 0, n$ ([DIE 82], vol. 9, (24.22.9)).

(VII) DE RHAM COHOMOLOGY.

ANTISYMMETRIC TENSORS. Let $\mathbf{K}$ be a commutative ring containing $\mathbb{Q}$ and let $E = \mathbf{K}^n$. Consider the tensor product $\mathbf{T}^p(E) = \bigotimes^p E$ defined inductively by $\bigotimes^0 E = \mathbf{K}$, $\bigotimes^{i+1} E = \left(\bigotimes^i E\right) \bigotimes E$ (section 3.1.5(**I**)). Given a permutation σ of $\{1, ..., p\}$ and $x_1 \otimes x_2 \otimes ... \otimes x_p \in \mathbf{T}^p(E)$, set $\sigma.(x_1 \otimes x_2 \otimes ... \otimes x_p) = x_{\sigma^{-1}(1)} \otimes x_{\sigma^{-1}(2)} \otimes ... \otimes x_{\sigma^{-1}(p)}$. Since every element of $\bigotimes^p E$ is a sum of elements of the form $x_1 \otimes x_2 \otimes ... \otimes x_p$, this determines a $\mathbf{K}$-linear mapping $\sigma : \mathbf{T}^p(E) \to \mathbf{T}^p(E)$. For all $z \in \mathbf{T}^p(E)$, set $\boldsymbol{a}.z = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma)(\sigma.z)$. An element of $z \in \mathbf{T}^p(E)$ is called a *contravariant tensor* of order n over E, $\boldsymbol{a}.z$ is its *antisymmetrization*, and $\bigwedge^p E := \boldsymbol{a}.\mathbf{T}^p(E)$ is the space of *antisymmetric contravariant tensors* of order n over E. If $z_p \in \bigwedge^p E$, we have that $\boldsymbol{a}.z_p = p!z_p$ (**exercise**). Given two antisymmetric tensors $z_p \in \bigwedge^p E$, $z_q \in \bigwedge^q E$, we write

$$z_p \wedge z_q = \frac{1}{p!q!}\boldsymbol{a}(z_p \otimes z_q)$$

so that

$$\left(\bigwedge^p E\right) \wedge \left(\bigwedge^q E\right) = \bigwedge^{p+q} E.$$

Let $(e_i)_{1 \leq i \leq n}$ be the canonical basis of E and let $x_i = \sum \xi_i^j e_j$ be the representation of a vector $x_i \in E$ with respect to this basis. Then,

$$x_1 \wedge x_2 \wedge ... \wedge x_m = \sum_H \det\left(X^H\right) e_H$$

where H ranges over the set of subsets of $\{1, 2, ..., n\}$ with m elements $j_1 < j_2 < ... < j_m$ and X^H is the square matrix (η_{hk}) of order n satisfying $\eta_{hk} = \xi_{h,j_k}$, $1 \leq h, k \leq n$.

ALTERNATING p-LINEAR FORMS. We can repeat the above after replacing E with its dual E^*. This yields the space $\bigwedge^p E^*$ of *alternating p-linear forms* (or *p-forms*, or *p-covectors*) on E. The space $\bigwedge^p E^*$ may be identified with $\left(\bigwedge^p E\right)^*$ and

$$\left\langle x_1 \wedge x_2 \wedge ... \wedge x_p, x_1^* \wedge x_2^* \wedge ... \wedge x_p^* \right\rangle = \det\left(\left\langle x_i, x_j^* \right\rangle\right).$$

We write $\bigwedge E^* = \bigoplus_{p\geq 0} \bigwedge^p E^*$ (with $\bigwedge^0 E^* := \mathbf{K}$) and the canonical $\mathbf{K}$-bilinear mapping $\wedge : \left(\bigwedge^p E^*\right) \times \left(\bigwedge^q E^*\right) \to \bigwedge^{p+q} E^*$ is called the *exterior product* (which induces an endomorphism of $\bigwedge E^*$). Then, $\bigwedge E^*$ is an alternating graded algebra (section 3.1.5**(IV)**), since if $u_p \in \bigwedge^p E^*, v_q \in \bigwedge^q E^*$, then

$$\boxed{u_p \wedge v_q = (-1)^{pq}\, v_q \wedge u_p}.$$

DIFFERENTIAL p-FORMS. Suppose now that $\mathbf{K} = \mathbb{R}$. Let U be a non-empty connected subset[12] of $\mathbb{R}^n$. We write $\Omega^p(U)$ for the space of C^∞ functions from U to $\bigwedge^p E^*$. Each element of $\Omega^p(U)$, called a *differential p-form* on U (or a field of p-forms of class C^∞ on U), can be uniquely written in the form

$$\omega = \sum_{i_1,...,i_p} \alpha_{i_1,...,i_p} dx^1 \wedge ... \wedge dx^p,$$

where $\alpha_{i_1,...,i_p} \in \Omega^0(U)$ and $dx^i \in \Omega^1(U)$ is the differential of the i-th coordinate function. Then, $\Omega^\bullet(U) = \bigoplus_{p\geq 0} \Omega^p(U)$ is an $\mathbb{R}$-complex of cochains and $(\Omega^\bullet(U), \wedge)$ is an alternating graded algebra. We define the $\mathbb{R}$-linear mapping $d : \Omega^p(U) \to \Omega^{p+1}(U)$ as

$$d\omega = \sum_{i_1,...,i_p} \left(\sum_{1\leq j\leq n} \frac{\partial^j \alpha_{i_1,...,i_p}}{\partial x^j} dx^j \right) \wedge dx^1 \wedge ... \wedge dx^p;$$

this operator d is called the *exterior differential*. This choice of terminology is justified by theorem 3.183. Let $\omega = \sum_{1\leq i\leq n} \alpha_i dx^i \in \Omega^1(U)$. We have that $d\omega = \sum_{0\leq i<j\leq n} \left(\partial\alpha_j/\partial x^i - \partial\alpha_i/\partial x^j\right) dx^i \wedge dx^j \in \Omega^2(U)$. If

12 An open subset of $\mathbb{R}^n$ is connected if and only if it is path-connected, i.e. "in a single piece" (the notion of path-connectedness is formally defined below).

there exists $f \in \Omega^0(U)$ such that $\omega = df := \sum_{1\leq i\leq n} \left(\partial f/\partial x^i\right) dx^i$ (i.e. if ω is an "exact differential", or coboundary), then $d\omega = \sum_{0\leq i<j\leq n} \left(\partial^2 f/\partial x^i \partial x^j - \partial^2 f/\partial x^j \partial x^i\right) dx^i \wedge dx^j = 0$ by Schwarz's theorem. A differential 1-form ω such that $d\omega = 0$ is said to be *closed*, or alternatively a *cocycle*. Writing $d^p : \Omega^p(U) \to \Omega^{p+1}(U)$ for d (which makes the exterior differential more explicit), we obtain the following result (**exercise**):

THEOREM 3.183.– *The graded homomorphism* $d^{\bullet}: \Omega^{\bullet}(U) \to \Omega^{\bullet}(U)$ *has degree* $+1$ *and satisfies* $d^{\bullet 2} = 0$, *so is a* differential. *Therefore, every coboundary is a cocycle.*

A cocycle is not always a coboundary, which motivates the definition of the p-th de Rham cohomology space

$$\boxed{\mathbf{H}^p(U;\mathbb{R}) = \ker\left(d^p\right)/\mathrm{im}\left(d^{p-1}\right)}.$$

We set $d^{-1} = 0$, so $\mathbf{H}^0(U;\mathbb{R}) = \mathbb{R}$ (**exercise**). The $\mathbf{H}^p(U;\mathbb{R}), p \geq 1$, characterize the "non-exactness" of the d^p.

NOTIONS OF ALGEBRAIC TOPOLOGY. A *path* in a topological space X is a continuous mapping $\gamma : [0,1] \to X$. This path is said to have *origin* $a \in X$ if $\gamma(0) = a$, and *end* b if $\gamma(1) = b$; it is said to be *closed* if its two endpoints are equal, i.e. $\gamma(0) = \gamma(1)$. If γ and δ are two paths, the first with endpoints a and b, and the second with endpoints b and c, they can be composed to give a single path with endpoints a and c, written $\gamma * \delta$, since, by choosing a suitable affine change of variables, γ and δ can be reformulated as continuous mappings from $[0,1/2]$ to X and from $[1/2,1]$ to X such that $\gamma(1/2) = \delta(1/2) = b$ (**exercise**). Let G be the set of paths in X and define $G_{a,b}$ to be the set of paths with endpoints a and b. *Juxtaposition* $*$ sends $G_{a,b} \times G_{b,c}$ to $G_{a,c}$. This binary operation is therefore *associative* when the juxtapositions are possible, $G_{a,b}$ has two *neutral elements* with respect to $*$, namely the constant paths $e_a : t \mapsto a$ and $e_b : t \mapsto b$ (the first on the left, the second on the right, since whenever $\gamma \in G_{a,b}, \gamma = e_a * \gamma = \gamma * e_b$) and every path $\lambda \in G_{a,b}$ has an *inverse* with respect to $*$, namely the path $\gamma^{-1} : t \mapsto \lambda(1-t)$, which is in $G_{b,a}$ and satisfies $\gamma * \gamma^{-1} = e_a$ and $\gamma^{-1} * \gamma = e_b$. Therefore, $(G, *)$ has an algebraic structure analogous to a group structure, except that the juxtaposition $(\gamma, \delta) \mapsto \gamma * \delta$ is not always defined. We say that the set of paths in X equipped

with the binary operation $*$ is a *groupoid*. If $\gamma, \gamma' : [0,1] \to X$ are two paths with the same endpoints, we write $\gamma \sim \gamma'$ if they are homotopic, and $[\gamma]$ for the homotopy class of γ. It is easy to see (**exercise**) that if γ and δ are juxtaposable, $[\gamma * \delta]$ only depends on $[\gamma]$ and $[\delta]$ and so can be written $[\gamma] * [\delta]$. Now, the set of homotopy classes $\varpi(X)$ of the paths in X, equipped with the binary operation $*$, has a groupoid structure: it is known as the Poincaré groupoid. The subset $\pi_1(X, a)$ of $\varpi(X)$ with elements $[\gamma]$ such that γ is a closed path with origin a is a group (**exercise**), called the *Poincaré group*, or *fundamental group*, of X at point a.

A topological space X is said to be *path-connected* if, for every two points $x, y \in X$, there exists a path with endpoints x and y. If X, Y are two topological spaces, X is path-connected and $f : X \to Y$ is continuous, then its image $f(X)$ is path-connected (**exercise**). In the following, we write $\mathbf{Toppc}$ for the category of path-connected spaces and continuous mappings (this is a full subcategory of $\mathbf{Top}$). It can be shown that if $X \in \mathbf{Toppc}$, then $\pi_1(X, x) \cong \pi_1(X, y), \forall x, y \in X$ ([ROT 88], Thm. 3.6), so $\pi_1(X, a)$ can be more simply written as $\pi_1(X)$, and

$$\pi_1 : X \mapsto \pi_1(X),$$
$$[h : X \to Y] \mapsto [\pi_1(h) : \pi_1(X) \to \pi_1(Y) : [\gamma] \mapsto [h \circ \gamma]]$$

is a (covariant) functor from $\mathbf{Toppc}$ to $\mathbf{Grp}$. (For another approach that does not require topological spaces to be path-connected, using the idea of "pointed spaces" instead, see [ROT 88].)

A space $X \in \mathbf{Toppc}$ is said to be *simply connected*[13] if $\pi_1(X) = \{1\}$, or alternatively if every closed path in X is homotopic to a constant path $[0,1] \to X : t \mapsto a$. Intuitively, this means that X "doesn't have any holes": a disc is simply connected but a disc with a point removed is not. The space between two concentric spheres with distinct radii in $\mathbb{R}^3$ is simply connected, although it is not contractible to any point.

THEOREM 3.184.– *(Poincaré's lemma) Let U be an open non-empty subset of $\mathbb{R}^n$. (i) For $\mathbf{H}^1(U; \mathbb{R})$ to be trivial, it is sufficient for U to be simply connected. (ii) For all the de Rham cohomology spaces $\mathbf{H}^p(U; \mathbb{R}), p \geq 1$, to be trivial, it is sufficient for U to be contractible to a point.*

13 Some authors do not require simply connected spaces to be connected.

PROOF.– We will only show (i) in the case where $U \subset \mathbb{R}^n$ is star-shaped around a point a that we can assume is the origin 0 by translating the coordinate system; for the general case, see ([MAD 97], Cor. 6.10). Let $\omega = \sum_i \alpha_i dx^i \in \Omega^1(U)$ be a closed differential form on U and define

$$f : U \to \mathbb{R} : x \mapsto \int_0^1 \omega(tx)\, x dt.$$

This function is well defined because the hypotheses state that, for all $t \in [0,1]$ and for all $x \in U$, we have $tx \in U$. Writing (e_i) for the canonical basis, we therefore have

$$\begin{aligned}\frac{\partial f}{\partial x^i} &= \int_0^1 \omega(tx)\, e_i dt + \int_0^1 t \sum\nolimits_k \frac{\partial \omega}{\partial x^i}(tx)\, x_k e_k dt \\ &= \int_0^1 \alpha_i(tx)\, dt + \int_0^1 t \sum\nolimits_k \frac{\partial \alpha_k}{\partial x^i}(tx)\, x_k e_k dt.\end{aligned}$$

Write the first integral on the right-hand side as I_1 and the second as I_2. Since ω is closed, $\partial\alpha_k/\partial x^i = \partial\alpha_i/\partial x^k$ and it follows that

$$I_2 = \int_0^1 t \sum\nolimits_k \frac{\partial \alpha_i}{\partial x^k}(tx)\, x_k e_k dt.$$

Now define

$$h : [0,1] \to \mathbb{R} : t \mapsto \alpha_i(tx) \Rightarrow h'(t) = \sum\nolimits_k \frac{\partial \alpha_i}{\partial x^k}(tx)\, x_k.$$

Integrating I_2 by parts gives

$$I_2 = [t\alpha_i(tx)]_0^1 - \int_0^1 \alpha_i(tx)\, dt.$$

Therefore, $I_1 + I_2 = \alpha_i(x)$. Hence, $df = \sum_i \left(\partial f/\partial x^i\right) dx^i = \sum_i \alpha_i dx^i = \omega$, and $\mathbf{H}^p(U;\mathbb{R}) = 0$. ■

If U, V are two homotopically equivalent non-empty connected open subsets of $\mathbb{R}^n$, then they have the same de Rham cohomology spaces ([MAD 97], Thm. 6.8). If U, V are two disjoint open sets of $\mathbb{R}^n$, we have that $\mathbf{H}^p(U \cup V;\mathbb{R}) \cong \mathbf{H}^p(U;\mathbb{R}) \oplus \mathbf{H}^p(V;\mathbb{R})$ (**exercise***; this is a special case of the Mayer-Vietoris theorem: see [MAD 97], Thm. 13.3).

3.3.9. *Derived functors*

(I) LEFT DERIVED FUNCTORS. Let M be an $\mathbf{R}$-module. This module is determined up to isomorphism by the projective left resolution [3.46] (theorem 3.143). This also holds if M is an object in an abelian category $\mathcal{A}$ with sufficiently many projectives (section 1.2.10**(I)**). No information is lost if we replace M by 0 in this resolution, since $M \cong \operatorname{coker}(d_1)$. If M' is another object in $\mathcal{A}$, by doing the same, we obtain the two rows in the following diagram, which are both chain complexes:

$$\begin{array}{rcccccccccc}
\mathbf{E}_M = \ldots \to & E_n & \overset{d_n}{\to} & E_{n-1} & \to \ldots \to & E_1 & \overset{d_1}{\to} & E_0 & \to 0 \\
& \downarrow \bar{f}_n & & \downarrow \bar{f}_{n-1} & & \downarrow \bar{f}_1 & & \downarrow \bar{f}_0 & \\
\mathbf{E}_{M'} = \ldots \to & E'_n & \overset{d'_n}{\to} & E'_{n-1} & \to \ldots \to & E'_1 & \overset{d'_1}{\to} & E'_0 & \to 0
\end{array}$$

Let $f : M \to M'$ be a morphism. This morphism induces a morphism of chains $\bar{f} = \left(\bar{f}_n\right)$ such that $\varphi' \circ \bar{f}_0 = f \circ \varphi$ where $\varphi : E_0 \twoheadrightarrow M$ and $\varphi' : E'_0 \twoheadrightarrow M'$ are the canonical epimorphisms; the morphism $\bar{f}$ is said to lie *over* f, and makes the above diagram commute. It is not unique, but if $\bar{f}, \bar{g}$ are two morphisms of chains over f, then it can be shown by induction that they are homotopic ("comparison theorem": see [ROT 09], Thm. 6.16).

Let $\mathcal{B}$ be an abelian category. By applying a *covariant* additive functor $\mathfrak{F} : \mathcal{A} \to \mathcal{B}$ to the above diagram, in $\mathcal{B}$, we obtain the commutative diagram

$$\begin{array}{rcccccccccc}
\mathfrak{F}(\mathbf{E}_M) = \ldots \to & \mathfrak{F}(E_n) & \overset{\mathfrak{F}(d_n)}{\to} & \mathfrak{F}(E_{n-1}) & \to \ldots & \overset{\mathfrak{F}(d_1)}{\to} & \mathfrak{F}(E_0) & \to 0 \\
& \downarrow \mathfrak{F}\left(\bar{f}_n\right) & & \downarrow \mathfrak{F}\left(\bar{f}_{n-1}\right) & & & \downarrow \mathfrak{F}\left(\bar{f}_0\right) & \\
\mathfrak{F}(\mathbf{E}_{M'}) = \ldots \to & \mathfrak{F}(E'_n) & \overset{\mathfrak{F}(d'_n)}{\to} & \mathfrak{F}\left(E'_{n-1}\right) & \to \ldots & \overset{\mathfrak{F}\left(d'_1\right)}{\to} & \mathfrak{F}(E'_0) & \to 0
\end{array}$$

of chain complexes (section 3.3.8**(II)**). The morphism of chains $\mathfrak{F}\left(\bar{f}\right) = \left(\mathfrak{F}\left(\bar{f}_n\right)\right)$ is over $\mathfrak{F}(f)$, so if $\mathbf{H}_\bullet$ is the homological functor (section 3.3.8**(II)**), $\mathbf{H}_\bullet\left(\mathfrak{F}\left(\bar{f}\right)\right)$ only depends on f by corollary-definition 3.173, which implies

COROLLARY-DEFINITION 3.185.– *Let $\mathcal{A}$ be an abelian category with sufficiently many projectives and let $\mathfrak{F} : \mathcal{A} \to \mathcal{B}$ be a covariant additive functor. For all $n \in \mathbb{Z}$, $L_n(\mathfrak{F}) : \mathcal{A} \to \mathcal{A} : M \mapsto \mathbf{H}_n(\mathfrak{F}(\mathbf{E}_M))$,*

$$\left[f : M \to M'\right] \mapsto \left[\mathbf{H}_n\left(\mathfrak{F}\left(\bar{f}\right)\right) : \mathbf{H}_n(\mathfrak{F}(\mathbf{E}_M)) \to \mathbf{H}_n(\mathfrak{F}(\mathbf{E}_{M'}))\right]$$

is a covariant additive functor, called the n-th left derived functor *of $\mathfrak{F}$.*

We define $L_n(\mathfrak{F})(M) = 0$ for $n < 0$. By theorem 3.170, we obtain the following result ([ROT 09], Thm. 6.27, 6.29(i)):

THEOREM 3.186.– *1) Let*

$$0 \to M' \overset{u}{\to} M \overset{v}{\to} M'' \to 0 \qquad [3.71]$$

be a short exact sequence in an abelian category $\mathcal{A}$ with sufficiently many projectives, $\mathcal{B}$ an abelian category and $\mathfrak{F} : \mathcal{A} \to \mathcal{B}$ an additive covariant functor. We then have the following long exact sequence in $\mathcal{B}$:

$$\begin{aligned}
&\ldots \to L_n(\mathfrak{F})(M') \overset{L_n(\mathfrak{F})(u)}{\to} L_n(\mathfrak{F})(M) \overset{L_n(\mathfrak{F})(v)}{\to} L_n(\mathfrak{F})(M'') \overset{\partial_n}{\to} \\
&\quad \to L_{n-1}(\mathfrak{F})(M') \overset{L_{n-1}(\mathfrak{F})(u)}{\to} L_{n-1}(\mathfrak{F})(M) \overset{L_{n-1}(\mathfrak{F})(v)}{\to} L_{n-1}(\mathfrak{F})(M'') \overset{\partial_{n-1}}{\to} \\
&\qquad \ldots \\
&\quad \to L_0(\mathfrak{F})(M') \overset{L_0(\mathfrak{F})(u)}{\to} L_0(\mathfrak{F})(M) \overset{L_0(\mathfrak{F})(v)}{\to} L_0(\mathfrak{F})(M'') \to 0, \qquad [3.72]
\end{aligned}$$

where the ∂_i are the connecting morphisms.

*2) If $\mathfrak{F}$ is right-exact, there exists a functorial isomorphism $L_0(\mathfrak{F}) \tilde{\to} \mathfrak{F}$ (section 1.2.2**(I)**) that allows these two functors to be identified.*

(II) Tor. Let $A \in \mathbf{Mod_R}$ and $B \in {}_{\mathbf{R}}\mathbf{Mod}$. Consider the right-exact covariant functors (theorem 3.19(3)) $- \bigotimes_{\mathbf{R}} B$ and $A \bigotimes_{\mathbf{R}} -$. We write

$$\mathrm{Tor}_n^{\mathbf{R}}(-, B) = L_n\left(- \bigotimes_{\mathbf{R}} B\right), \quad \mathrm{tor}_n^{\mathbf{R}}(A, -) = L_n\left(A \bigotimes_{\mathbf{R}} -\right).$$

Therefore, if [3.71] is an exact sequence of right $\mathbf{R}$-modules and B is a left $\mathbf{R}$-module, we obtain the long exact sequence

$$\begin{aligned}
&\ldots \to \mathrm{Tor}_n^{\mathbf{R}}(M', B) \to \mathrm{Tor}_n^{\mathbf{R}}(M, B) \to \mathrm{Tor}_n^{\mathbf{R}}(M'', B) \overset{\partial_n}{\to} \\
&\quad \to \mathrm{Tor}_{n-1}^{\mathbf{R}}(M', B) \to \mathrm{Tor}_{n-1}^{\mathbf{R}}(M, B) \to \mathrm{Tor}_{n-1}^{\mathbf{R}}(M'', B) \overset{\partial_{n-1}}{\to} \\
&\qquad \ldots \\
&\quad \to M' \bigotimes_{\mathbf{R}} B \overset{u \otimes \mathrm{id}_B}{\to} M \bigotimes_{\mathbf{R}} B \overset{v \otimes \mathrm{id}_B}{\to} M'' \bigotimes_{\mathbf{R}} B \to 0.
\end{aligned}$$

It can be shown that, for all $A \in \mathbf{Mod_R}$ and $B \in {}_{\mathbf{R}}\mathbf{Mod}$, $\mathrm{tor}_n^{\mathbf{R}}(A, B) \cong \mathrm{Tor}_n^{\mathbf{R}}(A, B)$, so we can identify the two bifunctors

(section 1.2.3) $\mathrm{Tor}_n^{\mathbf{R}}(-,-)$ and $\mathrm{tor}_n^{\mathbf{R}}(-,-)$, and set

$$\boxed{\mathrm{Tor}_n^{\mathbf{R}} = L_n\left(-\bigotimes_{\mathbf{R}}-\right):\ {}_{\mathbf{R}}\mathbf{Mod}\times\mathbf{Mod}_{\mathbf{R}}\to\mathbf{Ab}}.$$

By definition 3.20, the module $A_{\mathbf{R}}$ is flat if and only if $\mathrm{Tor}_n^{\mathbf{R}}(A,-)=0,\forall n\geq 1$, and the module ${}_{\mathbf{R}}B$ is flat if and only if $\mathrm{Tor}_n^{\mathbf{R}}(-,B)=0,\forall n\geq 1$.

(III) RIGHT DERIVED FUNCTORS. Everything that we said about the left derived functors of additive covariant functors can be adapted to apply to the right derived functors $R_n(\mathfrak{F})$ of covariant additive functors $\mathfrak{F}:\mathcal{A}\to\mathcal{B}$ by replacing the projective left resolutions $\mathbf{E}_M$ with injective right resolutions $\mathbf{E}^M$, and the homological functor $\mathbf{H}_\bullet$ with the cohomological functor $\mathbf{H}^\bullet$. If $\mathcal{A}$ has sufficiently many injectives, we therefore define, for any $n\in\mathbb{Z}$, the n-th right derived functor of $\mathfrak{F}:R_n(\mathfrak{F}):\mathcal{A}\to\mathcal{B}$ (which is covariant)

$$M\mapsto\mathbf{H}^n\left(\mathfrak{F}\left(\mathbf{E}^M\right)\right),\quad\left[f:M\to M'\right]\mapsto\mathbf{H}^n\left(\mathfrak{F}\left(\bar{f}\right)\right)$$

where $\bar{f}:\mathbf{E}^M\to\mathbf{E}^{M'}$ is a morphism of *cochains* over f (dual notion of a morphism of chains over f). The details of this adaptation are left to the reader as an **exercise** (see [LAN 99], Chap. XX, section 5 & section 6); however, note that when adapting theorem 3.186(1), the short exact sequence [3.71] gives the long exact sequence [3.72], where $L_\bullet$ is replaced by $R_\bullet$ *and the arrows are reversed*. The adapted version of theorem 3.186(2) shows that if $\mathfrak{F}$ is left-exact, then there exists a functorial isomorphism $R_0(\mathfrak{F})\tilde{\to}\mathfrak{F}$ that allows these two functors to be identified.

A *contravariant* additive functor $\mathfrak{G}:\mathcal{A}\to\mathcal{B}$, where $\mathcal{A}$ and $\mathcal{B}$ are abelian categories, is a *covariant* additive functor $\mathcal{A}^{\mathrm{op}}\to\mathcal{B}$. An injective right resolution $\mathbf{E}^M$ in $\mathcal{A}$ corresponds to a projective left resolution $\mathbf{E}_M$ in $\mathcal{A}^{\mathrm{op}}$. Therefore, if $\mathcal{A}$ has sufficiently many projectives, we define the n-th right derived functor of $\mathfrak{G}:R^n(\mathfrak{G}):\mathcal{A}\to\mathcal{B}$ (which is contravariant):

$$M\mapsto\mathbf{H}^n\left(\mathfrak{F}\left(\mathbf{E}_M\right)\right),\quad\left[f:M\to M'\right]\mapsto\mathbf{H}^n\left(\mathfrak{G}\left(\bar{f}\right)\right).$$

(IV) EXT. Let $\mathcal{A}$ be an abelian category. The functors $\mathrm{Hom}_{\mathcal{A}}(X,-):\mathcal{A}\to\mathbf{Ab}$ and $\mathrm{Hom}_{\mathcal{A}}(-,Y):\mathcal{A}\to\mathbf{Ab}$ are both right-exact for any two objects X and Y; the first is covariant and the second is contravariant (section 1.2.3 & 1.2.9**(I)**). If $\mathcal{A}$ has sufficiently many injectives

(resp. projectives) (section 1.2.10), we define $\mathrm{Ext}^n_{\mathcal{A}}(X,-) = R_n(\mathrm{Hom}_{\mathcal{A}}(X,-))$ (resp. $\mathrm{ext}^n_{\mathcal{A}}(-,Y) = R^n(\mathrm{Hom}_{\mathcal{A}}(-,Y))$). If $\mathcal{A}$ has sufficiently many projectives and injectives, the abelian groups $\mathrm{Ext}^n_{\mathcal{A}}(X,Y)$ and $\mathrm{ext}^n_{\mathcal{A}}(X,Y)$ are isomorphic for any two objects X, Y; they can therefore be identified, which allows us to define the bifunctor $\mathrm{Ext}^n_{\mathcal{A}} : \mathcal{A} \times \mathcal{A}^{\mathrm{op}} \to \mathbf{Ab}$:

$$\boxed{\mathrm{Ext}^n_{\mathcal{A}}(X,-) = R_n(\mathrm{Hom}_{\mathcal{A}}(X,-)), \quad \mathrm{Ext}^n_{\mathcal{A}}(-,Y) = R^n(\mathrm{Hom}_{\mathcal{A}}(-,Y))}$$

for all $X, Y \in \mathrm{Ob}(\mathcal{A})$. By identification, we have $\mathrm{Ext}^0_{\mathcal{A}}(-,-) = \mathrm{Hom}_{\mathcal{A}}(-,-)$. By definition, an object X is projective (resp. injective) if and only if $\mathrm{Ext}^n_{\mathcal{A}}(X,-) = 0, \forall n \geq 1$ (resp. $\mathrm{Ext}^n_{\mathcal{A}}(-,Y) = 0, \forall n \geq 1$).

Consider the short exact sequence [3.71] in $\mathcal{A}$ and let N be an object of $\mathcal{A}$. We obtain the following two long exact sequences (where $1 = \mathrm{id}_N$):

$$\begin{array}{c} 0 \to \mathrm{Hom}_{\mathcal{A}}(N,M') \overset{\mathrm{Hom}_{\mathcal{A}}(1,u)}{\to} \mathrm{Hom}_{\mathcal{A}}(N,M) \overset{\mathrm{Hom}_{\mathcal{A}}(1,v)}{\to} \mathrm{Hom}_{\mathcal{A}}(N,M'') \overset{\partial^1}{\to} \\ \mathrm{Ext}^1_{\mathcal{A}}(N,M') \overset{\mathrm{Ext}^1_{\mathcal{A}}(1,u)}{\to} \mathrm{Ext}^1_{\mathcal{A}}(N,M) \overset{\mathrm{Ext}^1_{\mathcal{A}}(1,v)}{\to} \mathrm{Ext}^1_{\mathcal{A}}(N,M'') \overset{\partial^2}{\to} \\ \cdots \\ \overset{\partial^n}{\to} \mathrm{Ext}^n_{\mathcal{A}}(N,M') \overset{\mathrm{Ext}^n_{\mathcal{A}}(1,u)}{\to} \mathrm{Ext}^n_{\mathcal{A}}(N,M) \overset{\mathrm{Ext}^n_{\mathcal{A}}(1,v)}{\to} \mathrm{Ext}^n_{\mathcal{A}}(N,M'') \to \ \ldots, \end{array}$$

$$\begin{array}{c} \overset{\partial^1}{\leftarrow} \mathrm{Hom}_{\mathcal{A}}(M',N) \overset{\mathrm{Hom}_{\mathcal{A}}(u,1)}{\leftarrow} \mathrm{Hom}_{\mathcal{A}}(M,N) \overset{\mathrm{Hom}_{\mathcal{A}}(v,1)}{\leftarrow} \mathrm{Hom}_{\mathcal{A}}(M'',N) \leftarrow 0 \\ \overset{\partial^2}{\leftarrow} \mathrm{Ext}^1_{\mathcal{A}}(M',N) \overset{\mathrm{Ext}^1_{\mathcal{A}}(u,1)}{\leftarrow} \mathrm{Ext}^1_{\mathcal{A}}(M,N) \overset{\mathrm{Ext}^1_{\mathcal{A}}(v,1)}{\leftarrow} \mathrm{Ext}^1_{\mathcal{A}}(M'',N) \\ \cdots \\ \ldots \leftarrow \mathrm{Ext}^n_{\mathcal{A}}(M',N) \overset{\mathrm{Ext}^n_{\mathcal{A}}(u,1)}{\leftarrow} \mathrm{Ext}^n_{\mathcal{A}}(M,N) \overset{\mathrm{Ext}^n_{\mathcal{A}}(1,v)}{\leftarrow} \mathrm{Ext}^n_{\mathcal{A}}(M'',N) \overset{\partial^n}{\leftarrow} \end{array}$$

Thanks to the functors $\mathrm{Tor}^{\mathbf{R}}_n$ and $\mathrm{Ext}^n_{\mathcal{A}}$, we can state the following theorem ([ROT 09], Cor. 7.57 & 7.60):

THEOREM 3.187.– *(*universal coefficient theorem*) Let X be a topological space and G an abelian group. Then, for all $p \geq 0$,*

$$\mathbf{H}_p(X;G) \cong \left(\mathbf{H}_p(X) \bigotimes\nolimits_{\mathbb{Z}} G\right) \oplus \mathrm{Tor}^{\mathbb{Z}}_1(\mathbf{H}_{p-1}(X;G)),$$

$$\mathbf{H}^p(X;G) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbf{H}_p(X), G) \oplus \mathrm{Ext}^1_{\mathbb{Z}}(\mathbf{H}_{p-1}(X), G).$$

3.4. Modules over principal ideal domains and related notions

3.4.1. *Modules over Bézout domains*

(I) SECONDARY OPERATIONS. Let $\mathbf{A}$ be a ring. In section 2.3.11**(II)**, we defined the *elementary operations* on the rows and columns of a matrix $R \in \mathbf{A}^{q\times k}$. For the following, we also need to define the *secondary operations*. A secondary operation on the rows (resp. columns) of R consists of left-multiplying (resp. right-multiplying) two rows (resp. two columns) of R by an invertible 2×2 matrix over $\mathbf{A}$, which corresponds to left-multiplying (resp. right-multiplying) R by a matrix known as a *secondary* matrix.

(II) MATRICES OVER BÉZOUT DOMAINS.

LEMMA 3.188.– *Let $\mathbf{A}$ be a right Ore domain. An arbitrary row $\begin{bmatrix} a & b \end{bmatrix} \in \mathbf{A}^{1\times 2}$ is right-equivalent (definition 3.4) to a diagonal form $\begin{bmatrix} d & 0 \end{bmatrix}$ if and only if $\mathbf{A}$ is a right Bézout domain (section 2.3.8**(III)**). If so, d is a gcld of a and b.*

PROOF.– i) Let $\mathbf{A}$ be a right Bézout domain, $\begin{bmatrix} a & b \end{bmatrix}$ a non-zero row and d a gcld of a, b. We have $a = da'$, $b = db'$ where a', b' do not have any common right divisors other than units, so $a'\mathbf{A}+b'\mathbf{A} = \mathbf{A}$. The row $\begin{bmatrix} a' & b' \end{bmatrix}$ is therefore right-invertible, and hence $P = \text{coker}\left(\bullet \begin{bmatrix} a' & b' \end{bmatrix}\right)$ is stably free (theorem 3.154), so torsion-free (section 3.1.10**(II)**). Hence, there exists a free module L such that $P \subseteq L$ (lemma 3.42). Since $\mathbf{A}$ is a semifir, P is free (theorem-definition 3.14), so $\begin{bmatrix} a' & b' \end{bmatrix}$ is completable (theorem 3.156). Let $Q^{-1} \in \text{GL}_2(\mathbf{A})$ be a matrix with first row $\begin{bmatrix} a' & b' \end{bmatrix}$. We have that

$$\begin{bmatrix} a & b \end{bmatrix} Q = \begin{bmatrix} d & 0 \end{bmatrix}. \qquad [3.73]$$

ii) Conversely, suppose that for any non-zero row $\begin{bmatrix} a & b \end{bmatrix}$ there exists a matrix Q for which [3.73] holds. Then, $d \in a\mathbf{A} + b\mathbf{A}$ and $\begin{bmatrix} a & b \end{bmatrix} = \begin{bmatrix} d & 0 \end{bmatrix} Q^{-1}$, so $a, b \in d\mathbf{A}$ and $a\mathbf{A} + b\mathbf{A} = d\mathbf{A}$. Therefore, every finitely generated right ideal is principal and $\mathbf{A}$ is a right Bézout domain. ■

Adapting this result to the case where $\mathbf{A}$ is a left Bézout domain is left to the reader (consider 2×1 columns instead of 1×2 rows; d is a gcrd of a and b).

COROLLARY-DEFINITION 3.189.– *Let $\mathbf{A}$ be a left Bézout domain and let $A \in \mathbf{A}^{q\times k}$ be a matrix of rank r.*

1) The matrix A is left-equivalent to an upper triangular matrix T, known as a left Hermite form of A.

2) There exists a permutation matrix $P \in \mathrm{GL}_k(\mathbf{A})$ such that the left Hermite form of AP is $\begin{bmatrix} A_1 \\ 0 \end{bmatrix}$, where A_1 has r non-zero rows.

PROOF.– 1) If the i-th column of $A = (a_{i,j})$ is non-zero, we can move an element $a_{j,i} \neq 0$ to position (i,i) using type (iii) elementary row operations. Next, using secondary row operations, we can successfully replace $a_{i,i}$ by a gcrd of $(a_{i,i}, a_{i+1,i})$ and $a_{i+1,i}$ by 0, then the new $a_{i,i}$ by a gcrd of $(a_{i,i}, a_{i+2,i})$ and $a_{i+2,i}$ by 0, etc. By continuing this process for each non-zero column, we obtain an upper triangular matrix.

2) It is sufficient to choose P such that the first r columns AP form a submatrix of rank r. ■

THEOREM 3.190.– *Let $\mathbf{A}$ be a Bézout domain and let $A \in \mathbf{A}^{q\times k}$ be a matrix of rank r. This matrix is equivalent to a matrix of the form $\begin{bmatrix} T & 0 \\ 0 & 0 \end{bmatrix}$, where $T \in \mathfrak{M}_r(\mathbf{A})$ has rank r*[14].

PROOF.– With the notation from corollary-definition 3.189, there exists a permutation matrix $P_1 \in \mathrm{GL}_r(\mathbf{A})$ such that the right Hermite form of $P_1 A_1$ is $\begin{bmatrix} T & 0 \end{bmatrix}$. ■

LEMMA-DEFINITION 3.191.– *Let $\mathbf{A}$ be a Bézout domain and let $A \in \mathbf{A}^{q\times k}$ be a matrix of rank r.*

i) There exists a matrix $L \in \mathfrak{M}_q(\mathbf{A})$ that is a left divisor of A (i.e. there exists $A' \in \mathbf{A}^{q\times k}$ such that $A = LA'$) and such that every left divisor L' of A is a left divisor of L.

ii) Any such matrix L is called a greatest left divisor (gld) *of A.*

iii) If $r = q$, then every gld of A is right-equivalent (definition 3.4) to L.

14 It was claimed in [BLS 11] (Corol. & Def. 651) that T is triangular, which does not hold in general (this false claim is not used throughout the rest of the cited reference).

PROOF.– (i) By theorem 3.190, there exist matrices $P \in \mathrm{GL}_q(\mathbf{A})$, $Q \in \mathrm{GL}_k(\mathbf{A})$ and a matrix $T' \in \mathbf{A}^{q\times r}$, of rank r, such that

$$QAP = \begin{bmatrix} T' & 0 \end{bmatrix} \Rightarrow A = \begin{bmatrix} L & 0 \end{bmatrix} P \text{ with } L = Q^{-1}T'.$$

iii) Let L, L' be two gld's of A. Then, L' is a left divisor of L and there exists $C \in \mathfrak{M}_q(\mathbf{A})$ such that $L = L'C$. Similarly, there exists a matrix $C' \in \mathfrak{M}_q(\mathbf{A})$ such that $L' = LC'$. Therefore, $L(I_q - CC') = 0$ and, since $\mathrm{rk}(L) = q$, L is invertible over $\mathrm{Q}(\mathbf{A})$, which implies that $CC' = I_q$. Since $\mathbf{A}$ is weakly finite (lemma 3.43 and corollary 3.36), C and C' are invertible.■

(III) MODULES OVER BÉZOUT DOMAINS. In the rest of this subsection, $\mathbf{A}$ is a left Bézout domain.

THEOREM 3.192.– *1) Let M be a finitely generated left $\mathbf{A}$-module. Let $\mathcal{T}(M)$ be the torsion submodule of M (section 3.1.10(**II**)). Then, there exists a free $\mathbf{A}$-module F such that*

$$\boxed{M = \mathcal{T}(M) \oplus F}$$

and $\mathrm{rk}(F) = \mathrm{rk}(M)$ *(definition 3.38); this module F is maximal among the free submodules of M.*

2) In particular, if M is torsion-free, it is free.

PROOF.– Since $\mathbf{A}$ is a semifir, M is finitely presented (theorem 3.27). Hence, there exist integers $q, k \geq 0$ and a matrix $R \in \mathbf{A}^{q\times k}$ such that $M \cong \mathrm{coker}(\bullet R)$. By theorem 3.190, there exists $T \in \mathfrak{M}_r(\mathbf{A})$ of rank r such that

$$\mathrm{coker}(\bullet R) \cong \mathrm{coker}\left(\bullet \begin{bmatrix} T & 0 \\ 0 & 0 \end{bmatrix}\right) \cong \mathrm{coker}\left(\bullet [\underbrace{T}_{r} \vdots \underbrace{0}_{k-r}]\right)$$
$$\cong \mathrm{coker}(\bullet T) \oplus F$$

where $\mathrm{coker}(\bullet T) \cong \mathcal{T}(M)$ and $\mathrm{rk}(F) = k - r = \mathrm{rk}(M)$. Since $M/F \cong \mathcal{T}(M)$, F is maximal among the free submodules of M by theorem 3.40. ■

In particular, let $R \in \mathbf{A}^{q\times k}$. Then, $\mathrm{coker}(\bullet R)$ is free of rank $k - r$ if and only if there exist a matrix $U \in \mathrm{GL}_q(\mathbf{A})$ and a permutation matrix

$P \in \mathrm{GL}_k(\mathbf{A})$ for which $URP = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$. This equality can be interpreted as a generalized form of a Bézout equation.

3.4.2. *Modules over principal ideal domains*

(I) NORMAL FORM OF A MATRIX. In the previous subsection, we saw that over a left (resp. right) Bézout domain, any matrix is equivalent to an upper (resp. lower) triangular matrix. We now ask which additional assumptions are required over an Ore domain $\mathbf{A}$ for an arbitrary matrix A to be equivalent to a diagonal form $\Sigma = \mathrm{diag}(e_1, ..., e_r, 0, ..., 0)$ where $e_r \neq 0$ and $e_i \parallel e_{i+1}$ for $1 \leq i \leq r-1$; recall that $e_i \parallel e_{i+1}$ means that e_i is a *total divisor* of e_{i+1} (section 2.1.1**(II)**). We then have $r = \mathrm{rk}(A)$ (theorem-definition 2.64 and remark 3.39).

DEFINITION 3.193.– *A diagonal matrix Σ with the above assumption is called a* normal form *of A. A normal form is called a* Smith form *in the case where $\mathbf{A}$ is commutative, and a* Jacobson-Teichmüller form *in the non-commutative case.*

THEOREM 3.194.– *(Kaplansky) Let $\mathbf{A}$ be an Ore domain. An arbitrary matrix $A \in \mathbf{A}^{q \times k}$ is equivalent to a normal form if and only if (i) $\mathbf{A}$ is a Bézout domain and (ii) the 2×2 matrices over $\mathbf{A}$ are all equivalent to a normal form.*

PROOF.– This condition is necessary by lemma 3.188. We will show that it is sufficient. Let $A \in \mathbf{A}^{q \times k}$, $3 \leq q$ and $k \leq m$ (without loss of generality). The induction hypothesis states that normal form reduction is possible for smaller q and for smaller k given the same q. Let $A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}$, where A_1 is the first row of A. We can find invertible matrices (products of elementary and secondary matrices) P_1, Q_1 such that $P_1 A_2 Q_1 = \mathrm{diag}(x, ...) = B$ (normal form). We obtain

$$C = \begin{bmatrix} 1 & 0 \\ 0 & P_1 \end{bmatrix} \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} Q_1 = \begin{bmatrix} A_1 Q_1 \\ B \end{bmatrix}.$$

Write $C = \begin{bmatrix} D \\ E \end{bmatrix}$, where D consists of the first two rows. By the induction hypothesis, we can find invertible matrices (products of elementary and

secondary matrices) P_2, Q_2 such that $F = P_2 D Q_2 = \text{diag}\,(y, ...)$ (normal form), hence

$$H = \begin{bmatrix} P_2 & 0 \\ 0 & I_{q-2} \end{bmatrix} \begin{bmatrix} D \\ E \end{bmatrix} Q_2 = \begin{bmatrix} F \\ G \end{bmatrix}.$$

Then, y is a total divisor of all the elements of F; since $D \sim F$, y is a total divisor of all the elements of D, so of the elements of C, of the elements of B and finally of x. We have that $E \sim_r G$, so x (and *a fortiori* y) is a total divisor of all the elements of G. Therefore, y is a total divisor of all the elements of H. Hence,

$$H \sim \begin{bmatrix} y & 0 \\ * & * \end{bmatrix} \sim \begin{bmatrix} y & 0 \\ 0 & K \end{bmatrix}$$

where the second equivalence is obtained using elementary row operations, and y is a total divisor of all the elements of K. By the assumptions, K has a normal form, so $A \sim H$ does too. ■

COROLLARY 3.195.– *If* $\mathbf{A}$ *is a commutative GCD domain (section 2.3.8(**I**)) and* $A \in \mathbf{A}^{q \times k}$ *has a normal form* $\Sigma = \text{diag}\,(e_1, ..., e_r, 0, ..., 0)$, *then the* e_i *are unique up to multiplication by units of* $\mathbf{A}$.

PROOF.– If $A = (a_{ij}) \neq 0$, we have that $e_1 \sim \gcd(a_{ij})$, and $e_1 e_2 ... e_n$ is a gcd of the n-th order minors, for all $n \leq r$. ■

The following concept was introduced by I. Kaplansky [KAP 49] (the reference considers a slightly more general setting, since the rings are allowed to have zero-divisors).

DEFINITION 3.196.– *An* elementary divisor ring *is an Ore domain* $\mathbf{A}$, *over which every finite matrix has a normal form.*

COROLLARY 3.197.– *Let* $\mathbf{A}$ *be an elementary divisor ring. Then, the elementary and secondary matrices in* $\mathfrak{M}_n(\mathbf{A})$ *generate* $\text{GL}_n(\mathbf{A})$.

PROOF.– Let $A \in \text{GL}_n(\mathbf{A})$. The normal form of A is I_n, so by the proof of theorem 3.194, there exist matrices $U, V \in \text{GL}_n(\mathbf{A})$ that are products of elementary and secondary matrices and which satisfy $U^{-1} A V = I_n$. Hence, $A = U V^{-1}$. ■

REMARK 3.198.– *Let $A \in \mathbf{A}^{q\times k}$, where $\mathbf{A}$ is an elementary divisor ring. The most effective way of reducing A to a normal form Σ is to perform a sequence of appropriate row and column operations. This gives $U^{-1}AV = \Sigma$, but the invertible matrices U, V are implicit, unless we "track" each operation. To do this, we can simply write*

$$\begin{bmatrix} U^{-1} & 0_{q\times k} \\ 0_{k\times q} & I_k \end{bmatrix} \underbrace{\begin{bmatrix} A & I_q \\ I_k & 0_{k\times q} \end{bmatrix}}_{A'} \begin{bmatrix} V & 0_{k\times q} \\ 0_{q\times k} & I_q \end{bmatrix} = \begin{bmatrix} \Sigma & U^{-1} \\ V & 0_{k\times q} \end{bmatrix},$$

and continue performing these operations on A' until A is transformed into Σ, which explicitly gives U^{-1} and V in the matrix on the right.

THEOREM 3.199.– *(Kaplansky) Let $\mathbf{A}$ be a commutative entire ring. This ring is an elementary divisor ring if and only if (i) it is a Bézout domain and (ii) for all elements $a, b, c \in \mathbf{A}$ such that $(a, b, c) = (1)$, there exist $p, q \in \mathbf{A}$ such that $(pa, pb + qc) = (1)$ (where $(.)$ is the ideal generated by the element(s) in parentheses).*

PROOF.– 1) Condition (i) is necessary by lemma 3.188. To show that (ii) is necessary, consider the matrix

$$A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \qquad [3.74]$$

where $(a, b, c) = (1)$, and suppose that there exist two invertible matrices P, Q such that PAQ is in normal form. Then, by the proof of corollary 3.195, $PAQ = \text{diag}\,(u, e)$, where u is a unit in $\mathbf{A}$. Writing $P = \begin{bmatrix} p & * \\ q & * \end{bmatrix}$, $Q = \begin{bmatrix} x & y \\ * & * \end{bmatrix}$, we obtain $(pax + pby + qcy) = (1)$, i.e. $((pa)\,x + (pb + qc)\,y) = (1)$, and thus, $(pa, pb + qc) = (1)$.

2) We will show that ((i), (ii)) is a sufficient condition. By (i) and lemma 3.188, we can suppose that A is of the form [3.74], where $(a, b, c) = (1)$. If $(pa, pb + qc) = (1)$, we have that $(p, q) = (1)$, so, as in the proof of lemma 3.188, the matrix $\begin{bmatrix} p & q \end{bmatrix}$ is completable, and there exists an invertible matrix $P = \begin{bmatrix} p & q \\ * & * \end{bmatrix}$, which gives $PA = \begin{bmatrix} pa & pb + qc \\ * & * \end{bmatrix}$. By performing elementary

column operations, we obtain $A \sim \begin{bmatrix} 1 & * \\ * & * \end{bmatrix}$, and by means of two further elementary operations, we find $A \sim \begin{bmatrix} 1 & 0 \\ 0 & * \end{bmatrix}$. ■

Let $\mathbf{A}$ be a commutative UFD and let $a, c \in \mathbf{A}$, $a \neq 0$. The decomposition of a and c into prime factors (theorem 2.54) allows us to write a in the form rs, where s is the product of all prime factors shared by a and c. We therefore have that $(r, c) = (1)$ and every divisor $d \in \complement_{\mathbf{A}}\mathbf{U}(\mathbf{A})$ of s satisfies $(d, c) \neq (1)$. This remark leads to the notion of an *adequate ring*, introduced by O. Helmer:

DEFINITION 3.200.– *A commutative Bézout domain* $\mathbf{A}$ *is* adequate *if, for all* $a, c \in \mathbf{A}$, $a \neq 0$, *there exist* $r, s \in \mathbf{A}$ *such that* $a = rs$, $(r, c) = (1)$, *and every divisor* $d \in \complement_{\mathbf{A}}\mathbf{U}(\mathbf{A})$ *of* s *satisfies* $(d, c) \neq (1)$.

THEOREM 3.201.– *(Helmer) Every adequate ring* $\mathbf{A}$ *is an elementary divisor ring.*

PROOF.– Let $\mathbf{A}$ be an adequate ring and suppose that $a, b, c \in \mathbf{A}$ satisfy $(a, b, c) = (1)$. If $a = 0$, we have that $(b, c) = (1)$, so condition (ii) of the statement of theorem 3.199 is satisfied. Suppose now that $a \neq 0$. We will show that there exists q such that $(a, b + qc) = (1)$, which is sufficient to prove that condition (ii) once again holds. Write $a = rs$ where r, s satisfy the condition stated in definition 3.200. Since $(r, c) = (1)$, the Bézout equation $cq + rx = 1 - ba$ has a solution (q, x); therefore, $cq + brs = 1 - rx$, so the congruence $cq + b \equiv 1 \pmod{r}$ can be solved to find q. After choosing an element q, let $(d) = (a, qc + b)$. There exist y, z such that $dy = cq + b = 1 - rz$, so $(d, r) = (1)$ (by Bézout), and since $a = rs$, $d \mid s$. If $d \notin \mathbf{U}(\mathbf{A})$, by the hypotheses $(d, c) \neq (1)$, but $d \mid a$ and $d \mid (qc + b)$, so $(a, b, c) \neq (1)$: contradiction. ■

It can easily be shown that the ring of entire functions (example 2.55) is adequate (**exercise**: use the Weierstrass factorization theorem, see Example 2.55). Since it is a Bézout domain, it is an elementary divisor ring. We currently do not know (as of 2017) of any examples of Bézout domains that are not elementary divisor rings.

(II) MODULES OVER ELEMENTARY DIVISOR RINGS. Let M be a finitely generated $\mathbf{A}$-module, where $\mathbf{A}$ is a (not necessarily commutative) elementary divisor ring. By theorem 3.194, $\mathbf{A}$ is a Bézout domain, so (theorem-definition

3.14) is a semifir; it follows by theorem 3.27 that M is finitely presented, i.e. $M \cong \text{coker}\,(\bullet A)$, where $A \in \mathbf{A}^{q\times k}$ and

$$A \sim \text{diag}\,(e_1, ..., e_r, 0, ..., 0)\,,\ e_r \neq 0,\ e_i \parallel e_{i+1}\ \ (1 \leq i \leq r-1)\,. \quad [3.75]$$

We therefore obtain $M = \mathcal{T}(M) \oplus F$, where $F \cong M/\mathcal{T}(M)$ is a free module and $\mathcal{T}(M) \cong \bigoplus_{i=1}^{r} \text{coker}\,(e_i)$, which implies that

$$\boxed{\mathcal{T}(M) \cong \bigoplus_{i=1}^{r} \mathbf{A}/\mathbf{A}e_i}\,. \quad [3.76]$$

If the ring $\mathbf{A}$ is commutative, the principal ideals $\mathfrak{a}_i = \mathbf{A}e_i$ are uniquely determined by M (corollary 3.195).

DEFINITION 3.202.– *Let $\mathbf{A}$ be an elementary divisor ring and let M be a finitely generated $\mathbf{A}$-module. With the above notation, suppose that the proper principal ideals $\mathfrak{a}_i$ (i.e. those for which e_i is not a unit) are uniquely determined by M up to similarity (section 2.3.8**(III)**). Then, these principal ideals $\mathfrak{a}_i \neq \mathbf{A}$ $(i = 1, ..., r'; r' \leq r)$ are called the non-zero* invariant factors *of M. We also say that M has s zero* invariant factors*, where $s = \text{rk}\,(M/\mathcal{T}(M))$.*

In the situation described above, the $\mathbf{A}$-module M is therefore the sum of monogenous submodules:

$$M = \bigoplus_{i=1}^{m} C_i, \quad [3.77]$$

$$C_i \cong \mathbf{A}/\mathfrak{b}_i, \quad \mathfrak{b}_1 \subseteq \mathfrak{b}_2 \subseteq ... \subseteq \mathfrak{b}_m \subsetneq \mathbf{A} \quad [3.78]$$

where $m = r' + s$ and the principal left ideals $\mathfrak{b}_1 = ... = \mathfrak{b}_s = 0$ and $\mathfrak{b}_{s+i} = \mathfrak{a}_{r'-i+1}$ $(1 \leq i \leq r')$ are the *invariant factors* of M. The generators of the $\mathfrak{b}_i$'s are often also called the invariant factors of M, by abuse of language.

(III) CASE OF PRINCIPAL IDEAL DOMAINS. In the rest of this subsection, except where otherwise stated, $\mathbf{A}$ is a (not necessarily commutative) principal ideal domain.

THEOREM 3.203.– *(Jacobson-Teichmüller-Nakayama) The ring $\mathbf{A}$ is an elementary divisor ring, and in the decomposition [3.77], [3.78] of a finitely generated $\mathbf{A}$-module M, the principal ideals $\mathfrak{b}_i$ are uniquely determined by M up to similarity, thus are the invariant factors of M.*

PROOF.– 1) By theorem 3.194, to show that $\mathbf{A}$ is an elementary divisor ring, it suffices to show that every matrix $A \in \mathfrak{M}_2(\mathbf{A})$ is equivalent to a normal form.

a) If $A = 0$, there is nothing to show. Otherwise, using elementary operations, we can move a non-zero element to position $(1,1)$. Since $\mathbf{A}$ is atomic, the length $\mathfrak{d}(a_{11}) = |a_{11}|$ is finite (section 2.1.2**(III)** & 2.3.8). By lemma 3.188, using a secondary column operation, A can be transformed into a form with first row $\begin{bmatrix} a_{11} & 0 \end{bmatrix}$ with a new a_{11} with length less than or equal to the previous length. The same method can be applied to the first column, making the element in position $(2,1)$ zero. This can potentially cause the element in position $(1,2)$ to become non-zero, but if so $|a_{11}|$ is reduced. After finitely many operations, we obtain a diagonal form $\operatorname{diag}(a_1, a_2)$.

b) For all $x, y \in \mathbf{A}$,

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix} \begin{bmatrix} y & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} a_1' & a_1 \\ a_2 & 0 \end{bmatrix}$$

where $a_1' = a_1 y + x a_2 \in a_1\mathbf{A} + \mathbf{A}a_2$. However, $a_1\mathbf{A} + \mathbf{A}a_2 \supsetneq a_1\mathbf{A}$ unless $\mathbf{A}a_2 \subseteq a_1\mathbf{A}$, i.e. $\mathbf{A}a_2\mathbf{A} \subseteq a_1\mathbf{A}$, and this last condition is satisfied if and only if $a_1 \mid c \mid a_2$, where c is an invariant generator of $\mathbf{A}a_2\mathbf{A}$ (lemma 2.21(ii)), i.e. $a_1 \parallel a_2$. In the other case, we can choose x, y such that $a_1 = a_1' q$, where $q \in \complement_{\mathbf{A}}\mathbf{U}(\mathbf{A})$, and $|a_1'| < |a_1|$.

c) By iterating the whole of this process, we reduce $|a_1|$ until $a_1 \parallel a_2$, i.e. until we obtain a normal form.

2) The uniqueness of the principal ideals $\mathfrak{b}_i$ up to similarity was shown by Nakayama in 1938 using the Krull-Remak-Schmidt theorem (theorem 2.9(3)) (see [COH 85], Chap. 8, Thm. 2.4), which allows us to derive the following result ([COH 85], Chap. 8, Cor. 2.5): ■

COROLLARY 3.204.– *Let M, N, N' be finitely generated $\mathbf{A}$-modules such that $M \oplus N \cong M \oplus N'$. Then, $N \cong N'$.*

REMARK 3.205.– *The matrices corresponding to the elementary and secondary operations generate* $\mathrm{GL}_n(\mathbf{A})$. *If the ring $\mathbf{A}$ is Euclidean, the reduction of the length $|a_{11}|$ can be replaced by the reduction of $\theta(a_{11})$ using the Euclidean division algorithm [2.20], and hence,* $\mathrm{GL}_n(\mathbf{A}) = \mathrm{E}_n(\mathbf{A})\,\mathrm{D}_n(\mathbf{A}) = \mathrm{D}_n(\mathbf{A})\,\mathrm{E}_n(\mathbf{A})$ *(see relation (a) in theorem*

2.65). P.M. Cohn showed in 1966 that there exist commutative principal ideal domains that are not Euclidean, for example, $\mathbb{Q}\sqrt{-19}$. *Secondary operations are required to reduce matrices to normal form over these rings.*

DEFINITION 3.206.– *Let* $\mathbf{A}$ *be an Ore domain. A monogenous* $\mathbf{A}$*-module* $T \cong \mathbf{A}/\mathfrak{u}$, *where* $\mathfrak{u}$ *is a non-zero left ideal (i.e. such that* T *is a torsion module), is said to be* cyclic.

COROLLARY 3.207.– *Suppose that the principal ideal domain* $\mathbf{A}$ *is simple (section 2.3.5**(III)**). Let* T *be a finitely generated torsion* $\mathbf{A}$*-module. Then,* T *is cyclic and unbounded (section 2.3.2**(III)**).*

PROOF.– Suppose that T is not cyclic. Then, we have $T \cong \bigoplus_{i=1}^{r} \mathbf{A}/\mathbf{A}e_i$, $r > 1$, $e_i \parallel e_{i+1}$ $(1 \leq i \leq r-1)$. Therefore, $e_1 \parallel e_2$ and there exists an invariant element c such that $e_1 \mid c \mid e_2$, and $\mathbf{A}c = c\mathbf{A} \neq (0)$ is a proper ideal of $\mathbf{A}$, so $\mathbf{A}$ is not simple. If $T \cong \mathbf{A}/\mathbf{A}u$ is bounded, there exists $a \neq 0$ such that $aT = 0$, so $a\mathbf{A} = \mathbf{A}u$ is a two-sided ideal $\neq 0$ and $\mathbf{A}$ is not simple. ■

(IV) THEORY OF ELEMENTARY DIVISORS.

DEFINITION 3.208.– *Let* $\mathbf{A}$ *be a ring and* M *an* $\mathbf{A}$*-module. The module* M *is said to be* indecomposable *if* $M = N \oplus N'$ *implies that* $N = 0$ *or* $N' = 0$.

Let $\mathbf{A}$ be a commutative principal ideal domain[15]. Let $C \cong \mathbf{A}/\mathbf{A}a$ $(a \neq 0)$ be a cyclic $\mathbf{A}$-module. The reduced primary decomposition [3.35] of $\mathbf{A}a$ allows us to write

$$\mathbf{A}a = \bigcap_{i=1}^{k} \mathbf{A}q_i$$

where the q_i are powers of prime elements and are pairwise coprime; by the Chinese remainder theorem (theorem 2.25),

$$\mathbf{A}/\mathbf{A}a \cong \bigoplus_{i=1}^{k} \mathbf{A}/\mathbf{A}q_i,$$

where the modules $\mathbf{A}/\mathbf{A}q_i$ are indecomposable. Furthermore, by the Krull-Remak-Schmidt theorem (theorem 2.9(3)) and lemma 2.51, the principal ideals $\mathbf{A}q_i$ are uniquely determined up to permutation of indices.

15 For the non-commutative case, see [COH 85] (section 8.2, Prop. 2.6).

DEFINITION 3.209.– *The principal ideals* $\mathbf{A}q_i$ *are the* elementary divisors *of the cyclic module* $\mathbf{A}/\mathbf{A}a$. *Given the torsion* $\mathbf{A}$*-module* $T = \mathcal{T}(M)$ *from [3.76], the elementary divisors of the cyclic submodules* $\mathbf{A}/\mathbf{A}e_i$ *are called the* elementary divisors *of* T. *The multiplicity of these elementary divisors is defined as the number of times that they occur. We also say that* $s = \text{rk}\,(M/\mathcal{T}(M))$ *is the multiplicity of the elementary divisor* 0 *of* M.

Let $\mathbf{A}\pi_i$ $(i = 1, ..., n)$ be the elementary divisors of M (taking into account multiplicities). This module M can therefore be decomposed as a direct sum of indecomposable submodules

$$\boxed{M \cong \bigoplus_{i=1}^{n} (\mathbf{A}/\mathbf{A}\pi_i)}. \qquad [3.79]$$

The elementary divisors can be easily calculated from the invariant factors. For example, let $A \in \mathbb{C}[X]^{3\times 3}$ be a matrix whose invariant factors are $e_1 = (X-1)^2(X-2)$, $e_2 = (X-1)^2(X-2)^2$, $e_3 = (X-1)^2(X-2)^2(X-3)$. The elementary divisors π_i and their multiplicities μ_i are the following:

$\pi_1 = (X-1)^2$	$\mu_1 = 3$
$\pi_2 = (X-2)^2$	$\mu_2 = 2$
$\pi_3 = X-2$	$\mu_3 = 1$
$\pi_4 = X-3$	$\mu_4 = 1$

Conversely, we can find the invariant factors e_j from the elementary divisors π_l by writing out the table whose i-th row is the elementary divisors that are multiples of the same prime element, arranged by decreasing length and accounting for multiplicities (filling the row with 1's if necessary). The product of the columns gives the e_j in decreasing order. Returning to the above example:

$\pi_1 = (X-1)^2$	$\pi_1 = (X-1)^2$	$\pi_1 = (X-1)^2$
$\pi_2 = (X-2)^2$	$\pi_2 = (X-2)^2$	$\pi_3 = X-2$
$\pi_4 = X-3$	1	1
$e_3 = \pi_1\pi_2\pi_4$	$e_2 = \pi_1\pi_2$	$e_1 = \pi_1\pi_3$

(V) LENGTH OF MODULES OVER PRINCIPAL IDEAL DOMAINS. Let $\mathbf{A}$ be a ring and let M be an $\mathbf{A}$-module. The length $|M|$ of M (if it is finite) is the

length of any Jordan-Hölder series of M. If $N \subseteq M$, then $|M| = |N| + |M/N|$ (section 2.2.5(**II**)) and if $M = N \oplus N'$, we can easily show (**exercise**) that $|M| = |N| \oplus |N'|$.

Let $\mathbf{A}$ be a principal ideal domain and let M be an $\mathbf{A}$-module. For $|M|$ to be finite, M must clearly be finitely generated. The module ${}_{\mathbf{A}}\mathbf{A}$ has finite length if and only if $\mathbf{A}$ is Artinian (section 2.3.4(**I**)), so if $\mathbf{A}$ is Artinian and M is finitely generated, this module has finite length by [3.77], [3.78].

LEMMA 3.210.– *Let $\mathbf{A}$ be a non-Artinian principal ideal domain. An $\mathbf{A}$-module M has finite length if and only if M is a finitely generated torsion module.*

PROOF.– We just saw that this condition is necessary. We will show that it is sufficient in the commutative case (although it is also true in the non-commutative case: see section 3.4.5). It suffices to consider the decomposition [3.79], which implies that $|M| \cong \sum_{i=1}^{n} |\mathbf{A}/(\pi_i)|$. Consider an arbitrary elementary divisor $\mathbf{A}\pi$. We can write $\pi = \prod_{j=1}^{k} p_j$, where the p_j are prime. In the composition series

$$0 = \frac{\left(\prod_{j=1}^{k} p_j\right)}{\left(\prod_{j=1}^{k} p_j\right)} \subsetneq \frac{\left(\prod_{j=2}^{k} p_j\right)}{\left(\prod_{j=1}^{k} p_j\right)} \subsetneq \ldots \subsetneq \frac{(p_k)}{\left(\prod_{j=1}^{k} p_j\right)} \subsetneq \frac{(1)}{\left(\prod_{j=1}^{k} p_j\right)} = \frac{\mathbf{A}}{(\pi)}$$

the quotients

$$\frac{\left(\prod_{j=l}^{k} p_j\right) / \left(\prod_{j=1}^{k} p_j\right)}{\left(\prod_{j=l+1}^{k} p_j\right) / \left(\prod_{j=1}^{k} p_j\right)} \cong \frac{\left(\prod_{j=l}^{k} p_j\right)}{\left(\prod_{j=l+1}^{k} p_j\right)} \cong \frac{\mathbf{A}}{(p_l)}$$

(by applying Noether's third isomorphism theorem (theorem 2.12(3)) and the isomorphism $\mathbf{A}/(p_l) \xrightarrow{\sim} \left(\prod_{j=l}^{k} p_j\right) / \left(\prod_{j=l+1}^{k} p_j\right)$ (multiplication by $\prod_{j=l+1}^{k} p_j$)) are simple (section 2.3.5(**III**)), so the above composition series is a Jordan-Hölder series of length k and $|\mathbf{A}/(\pi)| = k$. ■

3.4.3. *Pseudo-linear transformations*

(I) In this subsection, $\mathbf{K}$ is a field, σ is an automorphism of $\mathbf{K}$ and δ is a σ-derivation of $\mathbf{K}$. The ring of skew polynomials $\mathbf{A} = \mathbf{K}[X; \sigma, \delta]$ is therefore a

Euclidean domain (theorem 3.54), and thus, a principal ideal domain (theorem 2.59). Let M be an $\mathbf{A}$-module. The indeterminate X acts on the elements of $\mathbf{K}$ and M by [3.22], meaning that $(X\bullet) : M \to M : v \mapsto X.v$ is a $\mathbb{Z}$-linear mapping such that, for all $v \in M, \lambda \in \mathbf{K}$,

$$X.(\lambda v) = \sigma(\lambda) X.v + \delta(\lambda) v.$$

The interpretation of the ring $\mathbf{A}$ as a ring of differential or difference operators was explained in 3.1.11(**I**). When $\sigma = \mathrm{id}_{\mathbf{K}}$ and $\delta = 0$, we simply have $\mathbf{A} = \mathbf{K}[X]$ and the mapping $(X\bullet) : M \to M$ is $\mathbf{K}$-linear.

Let $\rho_* : {}_{\mathbf{A}}\mathbf{Mod} \to {}_{\mathbf{K}}\mathbf{Vect}$ be the restriction of the ring of scalars (section 3.1.5(**VI**)), write $M_{[\mathbf{K}]} = \rho_*(M)$ and $\theta := \rho_*(X\bullet) : M_{[\mathbf{K}]} \to M_{[\mathbf{K}]}$. This mapping is additive and, for all $v \in M_{[\mathbf{K}]}, \lambda \in \mathbf{K}$, satisfies

$$\theta(\lambda v) = \sigma(\lambda)\theta(v) + \delta(\lambda) v. \qquad [3.80]$$

Any such mapping θ is called a *pseudo-linear transformation* (with respect to the σ-derivation δ). It is $\mathbf{K}$-linear (so it is an *endomorphism* of the $\mathbf{K}$-vector space $M_{[\mathbf{K}]}$) if and only if $\sigma = \mathrm{id}_{\mathbf{K}}$ and $\delta = 0$. Generalizing the usual notions for endomorphisms of $\mathbf{K}$-vector spaces, we say that $\lambda \in \mathbf{K}$ is an *eigenvalue* of the pseudo-linear transformation θ if there exists $v \in M^{\times}_{[\mathbf{K}]}$ such that $\theta(v) = \lambda v$, and, if so, that v is an *eigenvector* associated with the eigenvalue λ.

Clearly, the $\mathbf{K}$-vector space $M_{[\mathbf{K}]}$ can only be finite-dimensional if the $\mathbf{A}$-module M is finitely generated. We also have the following result:

LEMMA 3.211.– *Let M be a finitely generated $\mathbf{A}$-module. Then M is a torsion module if and only if the $\mathbf{K}$-vector space $M_{[\mathbf{K}]}$ is finite-dimensional. If so, consider the decomposition [3.76] of M as a direct sum of cyclic submodules. We have that* $\dim_{\mathbf{K}}\left(M_{[\mathbf{K}]}\right) = \sum_{i=1}^{r} d^{\circ}(e_i)$.

PROOF.– 1) If M is not a torsion module, there exists a free element $m \in M$. For every $f \in \mathbf{A}^{\times}$, we therefore have $f(X).m \neq 0$, so $\left(X^i.m\right)_{i\geq 0}$ is an infinite sequence of $\mathbf{K}$-linearly independent elements, which shows that $\dim_{\mathbf{K}}\left(M_{[\mathbf{K}]}\right) \geq \aleph_0$. 2) Conversely, if M is a torsion module, by [3.76] and exactness of the functor ρ_*, we have

$$M_{[\mathbf{K}]} \cong \bigoplus\nolimits_{i=1}^{r} (\mathbf{A}/\mathbf{A}e_i)_{[\mathbf{K}]}. \qquad [3.81]$$

For an arbitrary index i, let $N = \mathbf{A}/\mathbf{A}e_i$, $f = e_i$, $n = d^\circ(f)$,

$$f = X^n + f_1 X^{n-1} + ... + f_n. \qquad [3.82]$$

Then, $N = [\mathbf{x}]_{\mathbf{A}}$, where the generator $\mathbf{x}$ satisfies the equality $f(X).\mathbf{x} = 0$ (remark 3.121(2)). Let $\eta_i = X^{n-i}.\mathbf{x}$ $(1 \leq i \leq n)$ and let $\overrightarrow{\eta}$ be the column with i-th element η_i. We have that

$$X.\overrightarrow{\eta} = C_f \overrightarrow{\eta} \text{ where } C_f = \begin{bmatrix} -f_1 & -f_2 & \cdots & \cdots & -f_n \\ 1 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{bmatrix}, \qquad [3.83]$$

so the components of $X.\overrightarrow{\eta}$ belong to $[\overrightarrow{\eta}]_{\mathbf{K}}$; hence, the components of $X^j.\overrightarrow{\eta}$ belong to $[\eta]_{\mathbf{K}}$ for all $j \geq 0$ and $N_{[\mathbf{K}]} = [\overrightarrow{\eta}]_{\mathbf{K}}$ is finite-dimensional. In fact, $\{\eta_i : 0 \leq i \leq n-1\}$ is a basis of $N_{[\mathbf{K}]}$, which therefore has dimension n. The remaining claims are obvious. ■

A torsion $\mathbf{A}$-module M is cyclic if and only if it is of the form $\mathbf{A}/\mathbf{A}f$, $f \in \mathbf{A}^\times$ (definition 3.206). In this case, assuming without loss of generality that the skew polynomial f is given by [3.82], $V = M_{[\mathbf{K}]}$ has basis $\left\{\theta^{n-1}(\mathbf{x}), ..., \theta(\mathbf{x}), \mathbf{x}\right\}$, where $\mathbf{x}$ is a generator of M, $\theta(V) \subseteq V$ and $\theta|_V : V \to V$ is represented by C_f with respect to this basis; C_f is called the *companion matrix* of the skew polynomial f.

DEFINITION 3.212.– *The above* $\mathbf{K}$*-vector space* V *is said to be* θ-cyclic *(or simply* cyclic *if the meaning is clear) and the pseudo-linear transformation* $\theta|_V : V \to V$ *(or any matrix representing* θ *with respect to some basis of* V*) is said to be* cyclic.

(II) MATRIX REPRESENTATION. Let M be a finitely generated torsion $\mathbf{A}$-module and let $\mathcal{B} = \{x_i : 1 \leq i \leq n\}$ be a basis of $M_{[\mathbf{K}]}$. There exist elements a_i^j $(1 \leq i, j \leq n)$ such that

$$\theta(x_i) = \sum\nolimits_{1 \leq j \leq n} a_i^j x_j.$$

Let $\overrightarrow{x}$ and $\overrightarrow{y}$ be the columns with elements x_j and $\theta(x_i)$, respectively, and let A be the matrix $\left(a_i^j\right)$. We therefore have

$$\boxed{\overrightarrow{y} = A\overrightarrow{x}}.$$

DEFINITION 3.213.– *The matrix $A \in \mathfrak{M}_n(K)$ is called the representative matrix of the pseudo-linear transformation θ with respect to the basis $\mathcal{B}$.*

In particular, the companion matrix C_f given by [3.83] is the representative matrix of the restriction of θ to $[\mathbf{A}/\mathbf{A}f]_{[\mathbf{K}]}$ with respect to the basis $\{\eta_i : 1 \leq i \leq n\}$, where η_n is a generator of $\mathbf{A}/\mathbf{A}f$ and $\eta_i = \theta^{n-i}(\eta_n)$.

Let $\mathbf{v} \in M_{[\mathbf{K}]}$, let v_i $(1 \leq i \leq n)$ be its components with respect to the above basis $\mathcal{B}$ and let $\overleftarrow{v}$ be the row containing the v_i, so that $\mathbf{v} = \overleftarrow{v}\,.\,\overrightarrow{x}$. Set $\mathbf{w} = \theta(\mathbf{v})$. By [3.80],

$$\begin{aligned}\mathbf{w} &= \theta\left(\sum_{1\leq i\leq n} v_i x_i\right) = \sum_{1\leq i\leq n} \theta(v_i x_i) = \sum_{1\leq i\leq n} (\sigma(v_i)\,\theta(x_i) + \delta(v_i)\,x_i) \\ &= \left[\sigma(v_1)\cdots\sigma(v_n)\right] A\overrightarrow{x} + \left[\delta(v_1)\cdots\delta(v_n)\right]\overrightarrow{x},\end{aligned}$$

from which we deduce the following result:

LEMMA 3.214.– *With respect to the basis $\mathcal{B} = (\overrightarrow{x})$, θ is the mapping $\overleftarrow{v} \mapsto \sigma(\overleftarrow{v})\,A + \delta(\overleftarrow{v})$.*

(III) CHANGE OF BASIS. Let $\mathcal{B}' = \left(\overrightarrow{x'}\right)$ be another basis of $M_{[\mathbf{K}]}$ (possibly distinct from $\mathcal{B}$), where $\overrightarrow{x'}$ is the column with elements x'_i $(1 \leq i \leq n)$. Let $P \in \mathrm{GL}_n(\mathbf{K})$ be the change-of-basis matrix, i.e. the matrix that represents the mapping $\mathrm{id}_{M_{[\mathbf{K}]}} : \left(M_{[\mathbf{K}]}, \left(\overrightarrow{x'}\right)\right) \to \left(M_{[\mathbf{K}]}, (\overrightarrow{x})\right)$ satisfying

$$\overrightarrow{x'} = P\overrightarrow{x}.$$

Let A' be the representative matrix of the pseudo-linear transformation θ with respect to the basis $\left(\overrightarrow{x'}\right)$. Let $\overleftarrow{v}_x$ and $\overleftarrow{v}_{x'}$ be the rows representing

$\mathbf{v}$ with respect to the bases $(\overrightarrow{x})$ and $\left(\overrightarrow{x'}\right)$, respectively. We have that $\mathbf{v} = \overleftarrow{v}_x.\overrightarrow{x} = \overleftarrow{v}_{x'}.\overrightarrow{x'} = \overleftarrow{v}_{x'}.P\overrightarrow{x}$, so

$$\overleftarrow{v}_x = \overleftarrow{v}_{x'}.P.$$

In the following, the mappings σ and δ are extended in the natural way to the $\mathbf{K}$-vector space $\mathbf{K}^{1\times n}$ and the $\mathbf{K}$-algebra $\mathfrak{M}_n(\mathbf{K})$. Choosing the same notation as above for $\mathbf{w} = \theta(\mathbf{v})$, by lemma 3.214, we find

$$\overleftarrow{w}_x = \sigma\left(\overleftarrow{v}_x\right)A + \delta\left(\overleftarrow{v}_x\right), \quad \overleftarrow{w}_{x'} = \sigma\left(\overleftarrow{v}_{x'}\right)A' + \delta\left(\overleftarrow{v}_{x'}\right), \quad \overleftarrow{w}_x = \overleftarrow{w}_{x'}.P, \tag{3.84}$$

and by using [3.23],

$$\begin{aligned}\overleftarrow{w}_{x'}.P &= \sigma\left(\overleftarrow{v}_{x'}.P\right)A + \delta\left(\overleftarrow{v}_{x'}.P\right)\\ &= \sigma\left(\overleftarrow{v}_{x'}\right)\left(\sigma(P)A + \delta(P)\right) + \delta\left(\overleftarrow{v}_{x'}\right)P\\ &\Rightarrow \overleftarrow{w}_{x'} = \sigma\left(\overleftarrow{v}_{x'}\right)\left(\sigma(P)A + \delta(P)\right)P^{-1} + \delta\left(\overleftarrow{v}_{x'}\right)\end{aligned}$$

and, finally, by the second equality in [3.84],

$$\boxed{A' = \left(\sigma(P)A + \delta(P)\right)P^{-1}}. \tag{3.85}$$

In general, the sum or the composition of two pseudo-linear transformations is not a pseudo-linear transformation. If $\sigma = \mathrm{id}$ and $\delta = 0$, or, in other words, if θ is an endomorphism of the $\mathbf{K}$-vector space $M_{[\mathbf{K}]}$, [3.85] is the usual *similarity relation* $A' = PAP^{-1}$ (and we say that the matrices A and A' are *similar*).

DEFINITION 3.215.– *Two matrices $A, A' \in \mathfrak{M}_n(\mathbf{K})$ are said to be (σ,δ)-conjugate if there exists a matrix $P \in \mathrm{GL}_n(\mathbf{K})$ for which the relation [3.85] is satisfied. In other words, two matrices $A, A' \in \mathfrak{M}_n(\mathbf{K})$ are (σ,δ)-conjugate if (and only if) they represent the same pseudo-linear transformation (possibly with respect to different bases).*

Let V, V' be two $\mathbf{K}$-vector spaces of same dimension, $\varphi : V \tilde{\to} V'$ an isomorphism and $\theta : V \to V$ a pseudo-linear transformation. It immediately holds that $\theta' = \varphi \circ \theta \circ \varphi^{-1} : V' \to V'$ is a pseudo-linear transformation, which motivates

DEFINITION 3.216.– *Two pseudo-linear transformations $\theta : V \to V$ and $\theta' : V' \to V'$ are* similar *if there exists an isomorphism $\varphi : V \tilde{\to} V'$ such that $\theta' = \varphi \circ \theta \circ \varphi^{-1}$.*

Similarity of pseudo-linear transformations is an equivalence relation.

THEOREM 3.217.– *Two pseudo-linear transformations $\theta : V \to V$ and $\theta' : V' \to V'$ are similar if and only if they are represented by (σ, δ)-conjugate matrices with respect to (arbitrary or given) bases of V and V'.*

PROOF.– We can identify V with V', as well as φ^{-1} with $\mathrm{id}_V : \left(V, \left(\overrightarrow{x'}\right)\right) \to (V, (\overrightarrow{x}))$, where $x'_i = \varphi(x_i)$ $(i = 1, ..., n)$. The theorem then follows from definition 3.215. ■

Recall that, by definition, two skew polynomials $f, f' \in \mathbf{A}$ are similar if (and only if) $\mathbf{A}/\mathbf{A}f \cong_{\mathbf{A}} \mathbf{A}/\mathbf{A}f'$ (section 2.3.8).

COROLLARY 3.218.– *Two skew polynomials $f, f' \in \mathbf{A}$ are similar if and only if their companion matrices $C_f, C_{f'}$ (see [3.83]) are (σ, δ)-conjugate. A matrix is cyclic if and only if it is (σ, δ)-conjugate to a companion matrix.*

PROOF.– The isomorphism φ is induced by $\mathrm{id}_{\mathbf{A}}$, so we have $\varphi : X^{i-1} + \mathbf{A}f \mapsto X^{i-1} + \mathbf{A}f'$ $(i = 1, ..., n)$. However, C_f is the matrix of the pseudo-linear transformation $(X\bullet) : (\mathbf{A}/\mathbf{A}f)_{[\mathbf{K}]} \to (\mathbf{A}/\mathbf{A}f)_{[\mathbf{K}]}$ with respect to the basis $\left\{X^{n-1} + \mathbf{A}f, ..., X + \mathbf{A}f, 1 + \mathbf{A}f\right\}$, and a similar property holds for $C_{f'}$. The corollary therefore follows from theorem 3.217. ■

Let $\theta : V \to V$ be a pseudo-linear transformation, where V is a finite-dimensional $\mathbf{K}$-vector space. The direct sum decompositions [3.81] of V and [3.75], [3.83] lead to

THEOREM-DEFINITION 3.219.– (Rational canonical form)

1) There exist an integer $r \geq 1$ and subspaces $V_i \subseteq V$ $(1 \leq i \leq n)$ for which the following conditions are satisfied:

i) $V = \bigoplus_{1 \leq i \leq r} V_i$;

ii) For all $i \in \{1, ..., r\}$, $\theta(V_i) \subseteq V_i$ *and* $\theta|_{V_i}$ *is cyclic;*

iii) With respect to an arbitrary basis of V_i, *the matrix of* $\theta|_{V_i}$ *is* (σ, δ)*-conjugate to a companion matrix* C_{e_i}, *where the skew polynomial* e_i *is unitary (section 3.1.11(**I**)) and* $e_i \parallel e_{i+1}$ $(1 \leq i \leq r-1)$;

iv) The integer r *is uniquely determined, as are the skew polynomials* e_i *up to similarity.*

2) The block-diagonal matrix $\operatorname{diag}(C_{e_1}, ..., C_{e_r})$ *is called the* rational canonical form *of the pseudo-linear transformation* θ *and the unitary skew polynomials* e_i *are called the* similarity invariants *of* θ.

(IV) JORDAN NORMAL FORM. In the rest of this subsection, we will assume that $\sigma = \mathrm{id}_{\mathbf{K}}$ and $\delta = 0$, so that θ is an endomorphism of a finite-dimensional $\mathbf{K}$-vector space V. We therefore have $V = M_{[\mathbf{K}]}$, where M is a finitely generated torsion module that decomposes into [3.79], where the ideal (π_i) (or, by abuse of language, their unitary generators π_i) are the elementary divisors of M. We therefore have that

$$V \cong \bigoplus_{i=1}^{n} W_i, \quad W_i = (\mathbf{A}/\mathbf{A}\pi_i)_{[\mathbf{K}]}$$

where the $\pi_i \in \mathbf{K}[X]$ are powers of irreducible polynomials. Suppose that $\mathbf{K}$ contains all the roots of the π_i (which is necessarily true if $\mathbf{K}$ is algebraically closed). Then, π_i is of the form $(X - \lambda_i)^{\mu(\pi_i)}$, where λ_i is the root of π_i and $1 \leq \mu(\pi_i) = \dim_{\mathbf{K}}(V_i)$ is its multiplicity. Let $\mathbf{x}$ be a generator of the cyclic $\mathbf{A}$-module $\mathbf{A}/\mathbf{A}\pi_i$, which implies that $(X - \lambda_i)^{\mu(\pi_i)}.\mathbf{x} = 0$. Let $\eta_{i,j} = (\theta_i - \lambda_i \mathrm{id}_{V_i})^{j-1}(\mathbf{x})$ and $\overrightarrow{\eta}_i$ be the column of these $\eta_{i,j}$ $(1 \leq j \leq \mu(\pi_i))$, where $\theta_i = \theta|_{V_i}$. Then, $\eta_{i,1} = \mathbf{x}$ and

$$\begin{cases} \eta_{i,2} = (\theta_i - \lambda_i \mathrm{id}_{V_i})\,\eta_{i,1}, \\ \eta_{i,3} = (\theta_i - \lambda_i \mathrm{id}_{V_i})\,\eta_{i,2}, \\ \vdots \\ 0 = (\theta_i - \lambda_i \mathrm{id}_{V_i})\,\eta_{i,\mu(\pi_i)} \end{cases} \Leftrightarrow \begin{cases} \theta_i(\eta_{i,1}) = \lambda_i \eta_{i,1} + \eta_{i,2}, \\ \theta_i(\eta_{i,2}) = \lambda_i \eta_{i,2} + \eta_{i,3}, \\ \vdots \\ \theta_i\left(\eta_{i,\mu(\pi_i)}\right) = \lambda_i \eta_{i,\mu(\pi_i)} \end{cases}$$

so, with respect to the basis $\{\overrightarrow{\eta}_i\}$, θ_i is represented by the Jordan block $J_{\mu(\pi_i)}(\lambda_i) \in \mathfrak{M}_{\mu(\pi_i)}(\mathbf{K})$ defined by

$$J_{\mu(\pi_i)}(\lambda_i) = \underbrace{\begin{bmatrix} \lambda_i & 1 & 0 & \cdots & \cdots & 0 \\ 0 & \lambda_i & 1 & \ddots & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \ddots & \\ \vdots & & \ddots & \ddots & 1 & 0 \\ \vdots & & & 0 & \lambda_i & 1 \\ 0 & 0 & \cdots & \cdots & 0 & \lambda_i \end{bmatrix}}_{\mu(\pi_i)}$$

Therefore, the endomorphism θ is represented by its Jordan form $\text{diag}\left[J_{\mu(\pi_1)}(\lambda_1), ..., J_{\mu(\pi_n)}(\lambda_n)\right]$ with respect to a suitable basis. The *minimal polynomial* of θ_i is π_i and the minimal polynomial of θ is $\pi = \prod_{i=1}^{n} \pi_i$: this is defined as the smallest-degree polynomial such that $\pi(\theta) = 0$. The Cayley-Hamilton theorem [2.33] shows that $\pi(X)$ divides the characteristic polynomial $\det(X.I_k - \theta)$. The endomorphism θ is diagonalizable if and only if the elementary divisors π_i all have degree one.

Note that, given a matrix $A \in \mathfrak{M}_k(\mathbf{K})$, to determine its Jordan normal form, it suffices to determine the Smith form Σ of $R = X.I_k - A$. This is because the invariant factors of R are the *similarity invariants* e_j of A $(1 \leq j \leq r)$ (theorem-definition 3.219(2)). From these elements, we immediately obtain the elementary divisors π_i, then (assuming that their roots λ_i are in $\mathbf{K}$) the Jordan blocks $J_{\mu(\pi_i)}(\lambda_i)$ $(1 \leq i \leq n)$. There exists a (non-unique) change-of-basis matrix P such that PAP^{-1} is a diagonal array of Jordan blocks, called the *Jordan normal form* of A:

$$\boxed{PAP^{-1} = \text{diag}\left[J_{\mu(\pi_1)}(\lambda_1), ..., J_{\mu(\pi_n)}(\lambda_n)\right]}.$$

3.4.4. *Systems of linear differential equations with constant coefficients*

The introductory example in section 3.3.3 suggests a general method for solving linear differential equations with constant coefficients; this application, although elementary and well known ([BKI 76], Chap. IV, section 2), deserves

to be presented explicitly. The principal ideal domain $\mathbf{A} = \mathbb{C}[X]$ acts on $W = C^\infty(\mathbb{R})$ by $X.f = df/dt$. Let $R_2 \in \mathbf{A}^{q\times k}$ and consider the system of differential equations [3.41], where $v \in C^\infty(\mathbb{R})^q$ is given and the unknown w is sought in $C^\infty(\mathbb{R})^k$. By replacing X with the differential operator $\partial := d/dt$ for purposes of clarity, [3.41] may be rewritten as

$$R_2(\partial)\, w = v. \qquad [3.86]$$

Continuing as in remark 3.198, we obtain matrices $U \in \mathrm{GL}_q(\mathbf{A})$ and $V \in \mathrm{GL}_k(\mathbf{A})$ such that $U^{-1}R_2V = \mathrm{diag}(e_1, ..., e_r, 0, ..., 0)$, where the e_i $(i = 1, ..., r)$ are non-zero unitary polynomials uniquely determined by the condition $e_i \mid e_{i+1}$ $(i = 1, ..., r-1)$. By setting $w' = V^{-1}w$ and $v' = U^{-1}v$, [3.86] is equivalent to

$$e_i(\partial)\, w'_i = v'_i \qquad (i = 1, ..., r), \qquad [3.87]$$

$$0 = v'_i \qquad (i = r+1, ..., q). \qquad [3.88]$$

The system [3.86] therefore only has solutions if condition [3.88] is satisfied; this coincides with the compatibility condition [3.41] (**exercise**). Theorems 3.130 and 3.123 (taking $n = 1$ in the first) show that this necessary condition is also sufficient, which we will confirm in the calculations given below. To solve [3.87], it can be useful to choose one of the equations and delete the index i, which gives

$$e(\partial)\, w' = v'. \qquad [3.89]$$

Since the case where $e(\partial) = 1$ is trivial, suppose that $d^\circ(e) = n \geq 1$. Now set

$$\eta = \begin{bmatrix} \partial^{n-1}w' \\ \vdots \\ \partial w' \\ w' \end{bmatrix}, \quad \upsilon = \begin{bmatrix} v' \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Equation [3.89] may be written as $\partial\eta = C_e\eta + \upsilon$, where C_e is the companion matrix of the polynomial e. We deduce the classical formula (see,

for example, [BLS 10], section 12.5.2)

$$\eta(t) = e^{C_e t}\eta_0 + \int_0^t e^{C_e(t-\tau)}\upsilon(\tau)\,d\tau.$$

where $\eta_0 \in \mathbb{C}^n$. To calculate $\exp(C_e t)$, it suffices to determine the Jordan normal form $J = \text{diag}\left[J_{\mu(\pi_1)}(\lambda_1), ..., J_{\mu(\pi_m)}(\lambda_m)\right]$ of C_e. Indeed, since $PC_eP^{-1} = J$, we have that $\exp(C_e t) = P^{-1}\exp(Jt)P$, where

$$\exp(Jt) = \text{diag}\left[\exp\left(J_{\mu(\pi_1)}(\lambda_1)t\right), ..., \exp\left(J_{\mu(\pi_m)}(\lambda_m)t\right)\right], \text{ and}$$

$$\exp\left(J_\mu(\lambda)t\right) = e^{\lambda t}\begin{bmatrix} 1 & t & \frac{t^2}{2} & \cdots & \frac{t^{\mu-1}}{(\mu-1)!} \\ 0 & 1 & & \ddots & \vdots \\ \vdots & \ddots & \ddots & & \frac{t^2}{2} \\ \vdots & & & 1 & t \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}.$$

3.4.5. *Modules over Dedekind domains*

In this subsection, $\mathbf{A}$ is a Dedekind domain (section 3.3.4(**II**)) and M is a finitely generated $\mathbf{A}$-module.

THEOREM 3.220.– *There exists a projective $\mathbf{A}$-module P such that*

$$\boxed{M = \mathcal{T}(M) \oplus P}.$$

In particular, if M is torsion-free, it is projective.

PROOF.– Let $N = M/\mathcal{T}(M) \cong P$. Since N is finitely generated and torsion-free, we can assume that $N \subseteq \mathbf{Q}(\mathbf{A})^{1\times n}$ (lemma 3.42(i)) where $\mathbf{Q}(\mathbf{A})$ is the division ring of left fractions. The module N has finitely many generators. Let c be a common denominator of these generators. Then, $N \cong cN \subseteq \mathbf{A}^{1\times n}$, so N is projective (theorem 3.135(e)). The exact sequence

$$0 \to \mathcal{T}(M) \to M \to P \to 0$$

therefore splits. ■

To conclude, we will simply list a few brief claims. Proofs can be found in ([MCC 01], 5.7.4, 5.7.8; [BKI 98], Chap. VII, section 4.10, Prop. 23).

THEOREM 3.221.– *i) If $M = P$ is torsion-free, there exist an integer $n \geq 0$ and a left ideal $\mathfrak{a}$ such that*

$$\boxed{P \cong \mathbf{A}^{1\times n} \oplus \mathfrak{a}}$$

(generalization of theorem 3.192(2)).

ii) There exist cyclic $\mathbf{A}$-modules (definition 3.206) $C_i \cong \mathbf{A}/\mathfrak{b}_i$ $(1 \leq i \leq r)$ such that

$$\boxed{\mathcal{T}(M) \cong \bigoplus_{i=1}^{r} C_i}$$

(where the $\mathfrak{b}_i$ are non-zero left ideals), and $\mathcal{T}(M)$ has finite length (generalization of [3.77] and lemma 3.210).

iii) If $\mathbf{A}$ is commutative, there exist a finite index set I, a family of maximal ideals $(\mathfrak{m}_i)_{i\in I}$ and a family of integers $(\mu_i)_{i\in I}$, $\mu_i \geq 1$ such that

$$\boxed{\mathcal{T}(M) \cong \bigoplus_{i\in I} (\mathbf{A}/\mathfrak{m}_i^{\mu_i})},$$

and these families are unique up to permutations of the set I (generalization of [3.79]).

Bibliography

[ADÁ 02] ADÁMEK J., HERRLICH H., THOLEN W., "Injective hulls are not natural", *Algebra Universalis*, vol. 48, no. 4, pp. 379–388, 2002.

[ADÁ 04] ADÁMEK J., HERRLICH H., STRECKER G.E., *Abstract and Concrete Categories*, 2nd ed., John Wiley, 2004.

[AND 00] ANDERSON D.D., "GCD domains, Gauss' lemma, and contents of polynomials", in CHAPMAN S.T., GLAZ S. (eds.), *Non-Noetherian Commutative Ring Theory*, Kluwer Academic Publishers, 2000.

[ATI 69] ATIYAH M.F., MACDONALD I.G., *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[BJÖ 79] BJÖRK J.-E., *Rings of Differential Operators*, North-Holland, 1979.

[BOR 67] BOREVITCH Z.I., CHAFAREVITCH I.R., *Théorie des nombres*, Gauthier-Villars, 1967.

[BKI 70] BOURBAKI N., *Théorie des ensembles*, Hermann, 1970.

[BKI 71] BOURBAKI N., *Topologie générale*, Hermann, 1971.

[BKI 76] BOURBAKI N., *Fonctions d'une variable réelle*, Hermann, 1976.

[BKI 98] BOURBAKI N., *Algèbre commutative*, Masson, 1998.

[BKI 12] BOURBAKI N., *Algèbre*, Hermann, 2012.

[BKI 16] BOURBAKI N., *Topologie algébrique*, Springer, 2016.

[BLS 09] BOURLÈS H., OBERST U., "Duality for differential-difference systems over Lie groups", *SIAM Journal on Control and Optimization*, vol. 48, pp. 2051–2084, 2009.

[BLS 10] BOURLÈS H., *Linear Systems*, ISTE Ltd, London and John Wiley & Sons, New York, 2010.

[BLS 11] BOURLÈS H., MARINESCU B., *Linear Time-Varying Systems*, Springer, 2011.

[CAR 56] CARTAN H., EILENBERG S., *Homological Algebra*, Princeton University Press, 1956.

[COH 63] COHN P.M., "Noncommutative unique factorization domains", *Transactions of the American Mathematical Society*, vol. 109, pp. 313–331, 1963.

[COH 81] COHN P.M., *Universal Algebra*, D. Reidel Publishing Company, 1981.

[COH 85] COHN P.M., *Free Rings and Their Relations*, 2nd ed., Academic Press, 1985.

[COH 95] COHN P.M., *Skew Fields*, Cambridge University Press, 1995.

[COH 03a] COHN P.M., *Basic Algebra*, Springer, 2003.

[COH 03b] COHN P.M., *Further Algebra and Applications*, Springer, 2003.

[COU 95] COUTINHO S.C., *A Primer of Algebraic $\mathcal{D}$-modules*, London Mathematical Society, 1995.

[DIE 43] DIEUDONNÉ J., "Les déterminants sur un corps non commutatif", *Bulletin de la S.M.F.*, vol. 71, no. 2, pp. 27–45, 1943.

[DIE 82] DIEUDONNÉ J., *Éléments d'analyse*, vol. 1–9, Gauthier-Villars, 1982.

[DOU 05] DOUADI R., DOUADY A., *Algèbre et théories galoisinennes*, Cassini, 2005.

[EHR 70] EHRENPREIS L., *Fourier Analysis in Several Complex Variables*, Wiley, 1970.

[EIL 45] EILENBERG S., MACLANE S., "General theory of natural equivalences", *Transactions of the American Mathematical Society*, vol. 58, no. 2, pp. 231–294, 1945.

[EIL 52] EILENBERG S., STEENROD N., *Foundations of Algebraic Topology*, Princeton University Press, 1952.

[EIS 04] EISENBUD D., *Commutative Algebra with a View Toward Algebraic Geometry*, Springer, 2004.

[FEL 71] FELGNER U., "Comparison of the axioms of local and universal choice", *Fundamenta Mathematicae*, vol. 71, no. 1, pp. 43–62, 1971.

[FIT 36] FITTING H., "Uber den Zusammenhang zwischen dem Begriff der Gleichartigkeit zweier Ideale und dem Äquivalenzbegriff der Elementarteilertheorie", *Mathematische Annalen*, vol. 112, pp. 572–582, 1936.

[FRE 64] FREYD P., *Categories – An Introduction to the Theory of Functors*, Harper & Row, 1964.

[FRO 83] FROIDEVAUX C., "La fonction logique ε de Hilbert à travers les 'Grundlagen der Mathematik"', *Mathématiques et sciences humaines*, vol. 84, pp. 65–82, 1983.

[GEL 03] GELFAND S.I., MANIN Y.I., *Methods of Homological Algebra*, 2nd ed., Springer, 2003.

[GEN 60] GENTILE E.R., "On rings with one-sided field of quotients", *Proceedings of the American Mathematical Society*, vol. 11, no. 13, pp. 380–384, 1960.

[GOD 64] GODEMENT R., *Cours d'algèbre*, Hermann, 1964.

[GRO 57] GROTHENDIECK A., "Sur quelques points d'algèbre homologique", *Tohoku Mathematical Journal*, vol. 9, pp. 119–221, 1957.

[GRO 70] GROTHENDIECK A., DIEUDONNÉ J., *Éléments de Géométrie Algébrique I*, 2nd ed., Springer-Verlag, 1970.

[GRO 72] GROTHENDIECK A., VERDIER J.L., "Préfaisceaux", in ARTIN M., GROTHENDIECK A., VERDIER J.L. (eds), *SGA 4: Théorie des topos et cohomologie des schémas*, Springer-Verlag, 1972.

[HIL 39] HILBERT D., BERNAYS P., *Grundlagen der Mathematik II*, Springer-Verlag, 1939.

[JAC 37] JACOBSON N., "Pseudo-linear transformations", *Annals of Mathematics*, vol. 38, no. 2, pp. 484–507, 1937.

[KAP 49] KAPLANSKY I., "Elementary divisors and modules", *Transactions of the American Mathematical Society*, vol. 66, no. 2, pp. 464–491, 1949.

[KAS 95] KASIHWARA M., "Algebraic study of systems of partial differential equations", *Mémoires de la Société Mathématique de France*, vol. 63, pp. I–XIV + 1–72, 1995 (translation of the original Japonese text published in 1970).

[KAS 06] KASHIWARA M., SCHAPIRA P., *Categories and Sheaves*, Springer, 2006.

[KRI 98] KRIVINE J.L., *Théorie des ensembles*, Cassini, 1998.

[LAM 99] LAM T.Y., *Lectures on Modules and Rings*, Springer, 1999.

[LAM 01] LAM T.Y., *A First Course in Noncommutative Rings*, Springer, 2001.

[LAM 06] LAM T.Y., *Serre's Problem on Projective Modules*, Springer, 2006.

[LAN 99] LANG S., *Algebra*, 3rd ed., Addison-Wesley, 1999.

[LEF 30] LEFSCHETZ S., *Topology*, American Mathematical Society, 1930.

[LEF 49] LEFSCHETZ S., *Introduction to Topology*, Princeton University Press, 1949.

[LER 95] LEROY A., "Pseudo linear transformations and evaluation in Ore extensions", *Bulletin of the Belgian Mathematical Society – Simon Stevin*, vol. 2, pp. 321–347, 1995.

[MAC 14] MACKEVICIUS V., *Integral and Measure*, ISTE Ltd, London and John Wiley & Sons, New York, 2014.

[MAD 97] MADSEN I., TORNEHAVE J., *From Calculus to Cohomology*, Cambridge University Press, 1997.

[MAI 93] MAISONOBE P., SABBAH C. (eds), *$\mathcal{D}$-modules cohérents et holonomes*, Hermann, 1993.

[MAL 63] MALGRANGE B., "Systèmes différentiels à coefficients constants", *Séminaire Bourbaki*, vol. 8, no. 246, pp. 79–89, 1962–1963.

[MAT 92] MATHIAS A.R.D., "The ignorance of Bourbaki", *The Mathematical Intelligencer*, vol. 14, no. 3, pp. 4–13, 1992.

[MCC 01] MCCONNELL J.C., ROBSON J.C., *Noncommutative Noetherian Rings*, American Mathematical Society, 2001.

[MCL 98] MACLANE S., *Categories for the Working Mathematician*, 2nd ed., Springer, 1998.

[MCL 99] MACLANE S., BIRKHOFF G., *Algebra*, 3rd ed., Macmillan, 1999.

[MON 13] MONFORTE A.A., KAUERS M., "Formal Laurent series in several variables", *Expositiones Mathematicae*, vol. 31, pp. 350–367, 2013.

[MIT 65] MITCHELL B., *Theory of Categories*, Academic Press, New York, 1965.

[OBE 90] OBERST U., "Multidimensional constant linear systems", *Acta Applicandae Mathematicae*, vol. 20, pp. 1–175, 1990.

[OBE 95] OBERST U., "Variations on the fundamental principle for linear systems of partial differential and difference equations with constant coefficients", *Applicable Algebra in Engineering, Communication and Computing*, vol. 6, nos. 4/5, pp. 211–243, 1995.

[ORE 33] ORE O., "Theory of non-commutative polynomials", *Annals of Mathematics*, vol. 34, pp. 480–508, 1933.

[PAL 70] PALAMODOV V.P., *Linear Differential Operators with Constant Coefficients*, Springer-Verlag, 1970.

[POM 01] POMMARET J.F., *Partial Differential Control Theory*, vol. II, Kluwer Academic Publishers, 2001.

[REI 95] REID M., *Undergraduate Commutative Algebra*, Cambridge University Press, 1995.

[REM 98] REMMERT R., *Classical Topics in Complex Function Theory*, Springer, 1998.

[ROT 88] ROTMAN J.J., *An Introduction to Algebraic Topology*, Springer, 1988.

[ROT 02] ROTMAN J.J., *Advanced Modern Algebra*, Prentice-Hall, 2002.

[ROT 09] ROTMAN J.J., *An Introduction to Homological Algebra*, 2nd ed., Springer, 2009.

[RUD 87] RUDIN W., *Real and Complex Analysis*, 3rd ed., McGraw Hill, 1987.

[SAM 67] SAMUEL P., *Théorie algébrique des nombres*, Hermann, Paris, 1967.

[SCH 99] SCHNEIDERS J.-P., "Quasi-abelian categories and sheaves", *Mémoires de la Société Mathématique de France*, vol. 76, pp. 1–140, 1999.

[STE 02] STEWART I., TALL D., *Algebraic Number Theory and Fermat's Last Theorem*, 3rd ed., A.K. Peters Ltd., 2002.

[VAN 31] VAN DER WAERDEN B.L., *Moderne Algebra*, Springer-Verlag, 1931 (English translation: *Algebra*, 7th edition, Springer-Verlag, 1991; references are always given with respect to this edition).

[ZAR 58/60] ZARISKI O., SAMUEL P., *Commutative Algebra*, D. van Nostrand, 1958–1960.

Cited Authors

Index

A, B

C, D

E, F

G, H

I, J, K

L, M

N, O, P

Q, R

S, T

U, V, W, Y, Z

The three volumes of this series of books, of which this is the first, put forward the mathematical elements that make up the foundations of a number of contemporary scientific methods: modern theory on systems, physics and engineering.

This first volume focuses primarily on algebraic questions: categories and functors, groups, rings, modules and algebra. Notions are introduced in a general framework and then studied in the context of commutative and homological algebra; their application in algebraic topology and geometry is therefore developed. These notions play an essential role in algebraic analysis (analytico-algebraic systems theory of ordinary or partial linear differential equations).

The book concludes with a study of modules over the main types of rings, the rational canonical form of matrices, the (commutative) theory of elemental divisors and their application in systems of linear differential equations with constant coefficients.

Henri Bourlès is Full Professor and Chair at the Conservatoire National des Arts et Métiers, Paris, France.

ELSEVIER
iSTE PRESS
www.iste.co.uk
9 781785 481734