HOMOLOGY

Master CRYPTIS
Semester 2

Masters thesis

Anick resolution, Koszul complex, non-commutative Gröbner bases

Adya MUSSON-LEYMARIE

Under the supervision of Cyrille Chenavier

Faculté des Sciences & Techniques

Université de Limoges

Year 2022-2023

Contents

Introduction

This document constitutes my *Masters thesis* for the second-year of master Cryptis, at the University of Limoges. It has been produced during and after my five months long internship at the xlim laboratory in Limoges under the supervision of Cyrille Chenavier. This has been a wonderful opportunity for me to explore the world of pure mathematics. The initial objective of the internship was to get acquainted with the basic tools of homological algebra through the lens of the Anick resolution, the Koszul complex and the use of non-commutative Gröbner bases in that context.

My first step of the journey was to get comfortable manipulating notions related to modules over not necessarily commutative rings and the basic concepts of the theory of associative algebras (augmentations, presentations, free algebras, non-commutative Gröbner bases, *etc*). A particular important part of the process was to get familiar with the use of the tensor product of modules over non-commutative rings, which is central in the subjects of homological algebra I had to address. Then, in order to grasp the most of the generality of homological algebra, one has to study the language coming from category theory; this took me a fair amount of time to understand deeply the inner-workings and motivations. I investigated quite a long time the concept of natural equivalences by trying to understand where the framework of ordinary set theory fails to capture the "essence of naturality". I also dedicated some time to study the notions of universal properties and universal constructions in category theory, which led me to learn more about the Yoneda lemma, the Yoneda embedding and the theory of adjoint functors. However, by lack of time, I was not able to produce a written account on what I have learnt on those topics. After obtaining the basics of category theory, I moved on to learn about the rudiments of homological algebra. As the field was quite abstract for me, I dedicated time to read about the history and the motivations of the discipline. This helped me understand better the subsequent notions I had to absorb. Then, I went on to study in depth the *Anick resolution* for augmented associative algebras. The angle I approached it with was these of the *Gröbner bases*. However, the original material on the subject written by David J. Anick was not given in that kind of language. This led me to write a preprint [ML23] in which I explain the connections between the original setting of the initial article and the subsequent resources treating it through the lens of Gröbner bases. Finally, I studied the (generalised) *Koszul complex* of non-necessarily quadratic homogeneous algebras. I explored it first through its combinatorics point of view but then went on to learn about (generalised) *Koszul duality* which helped me understand the essential ideas behind the topic. The contribution of this thesis is a proof of the equality between the Anick resolution and the Koszul complex for the homogeneous monomial algebras satisfying the so-called *overlap property*.

The outline of this thesis follows a simple requirement to introduce the necessary notions of non-commutative algebra, category theory and homological algebra to understand the proof of the final chapter, being the main new result brought forward by this thesis.

The text is organised in four chapters:

The first chapter can serve as an introduction to the basics of module theory (see in particular the tensor product with Definition 1.1.6.3) and of non-commutative algebra with a special interest for non-commutative Gröbner bases (Definition 1.2.4.4).

The second chapter introduces the basic definitions of the language of the category theory: categories (Definition 2.1.1.1), functors (Definition 2.1.2.1) and natural transformations (Definition 2.1.3.1). It also brings enough material to define the concept of *abelian categories* (Definition 2.2.2.8): those are the categories on which ordinary homological algebra can be applied.

The third chapter addresses the rudiments of homological algebra. In particular, we talk about the Tor and Ext functors (Definitions 3.2.1.4, 3.2.2.1 and 3.2.2.2).

Finally, the fourth chapter is divided in three sections:

- First, we give an overview of the Anick resolution (Theorem 4.1.3.2), prove the equivalence between the different definitions of the so-called *n-chains* (one of the basic but central ingredient in the construction of the resolution) and give a proof for the *minimality* (see Subsection 4.1.5) of the Anick resolution for monomial algebras. We refer to the preprint [ML23] for more details on the matter.

- Second, we introduce the notions of (generalised) Koszul duality and Koszul complex to non-necessarily quadratic homogeneous algebras (Definition 4.2.2.4).

- Finally, we take interest in the special case of *homogeneous monomial algebras* (Definition 1.2.3.5). We show that the Koszul complex is a subcomplex of the Anick resolution in that context (Theorem 4.3.3.2). Then, after defining the overlap property (Definition 4.3.1.1), we prove that the homogeneous monomial algebras satisfying that property have their Anick resolution and their Koszul complex not only isomorphic, but actually equal (and so are their contracting homotopies) (Theorem 4.3.4.4).

The prerequisites to understand this thesis are the basic notions of group theory, linear algebra and ring theory. In particular, we will take for granted the definitions of abelian groups and vector spaces over a field. It is hoped to be accessible to a graduate student in mathematics.

In terms of conventions, we will assume that every ring is unital but not necessarily commutative, every module is unitary, every algebra is associative unitary. Unless specified otherwise, the ideals are taken as two-sided.

Acknowledgements

I would like to thank Cyrille Chenavier for his constant support, kindness, open-mindedness and helpful guidance all along the way as well as being available every time I needed help. I would also like to thank Thomas Cluzeau with whom we had a few meetings and who helped with the proofreading of the preprint.

Chapter 1

Preliminaries in (non-commutative) algebra

In this chapter, we introduce the notions of module theory and non-commutative algebra required to address the topics of homological algebra we want.

1.1 Module theory

1.1.1 Modules over a ring

We start by giving the basic definitions we will require throughout this thesis.

The main mathematical object manipulated in homological algebra is that of modules over a ring. It can be viewed as a generalisation of vector spaces and abelian groups.

Definition 1.1.1.1 : Left module over a ring

Let $(R, +_R, \times_R, 1_R)$ be a ring with identity.
A *left R-module* is any additive abelian group $(M, +)$ endowed with an external law of composition $R \times M \to M$, usually denoted by adjunction, that verifies the following axioms:

- "Associativity": $\forall r, s \in R, \forall a \in M, (r \times_R s)a = r(sa)$,
- "Left-distributivity": $\forall r, s \in R, \forall a \in M, (r +_R s)a = ra + sa$,
- "Right-distributivity": $\forall r \in R, \forall a, b \in M, r(a + b) = ra + rb$,
- "Identity": $\forall a \in M, 1_R a = a$.

Remark 1.1.1.2 : Axioms versus ring-homomorphism

Alternatively, one can define the structure of module on an additive abelian group $(M, +)$, by providing a unital-ring-homomorphism $\mu : R \to \mathrm{End}(M)$ where $\mathrm{End}(M)$ is the ring of endomorphisms on M (product being the composition of endomorphisms). The multiplication by scalars in R used in the Definition 1.1.1.1 is then defined as $ra := \mu(r)(a)$. It follows from the properties of the unital-ring-homomorphism that the axioms are satisfied.
Conversely, if one is given the structure of a module such as in the definition, one can define the unital-ring-homomorphism: $\mu : r \mapsto (a \mapsto ra)$ that would yield the same multiplication by scalars if one was to define it in the same way as above.

There is no obstacle to define the same kind of structure but considering an external law of composition from the right:

Definition 1.1.1.3 : Right module over a ring

Let $(R, +_R, \times_R, 1_R)$ be a ring with identity.
A *right R-module* is any additive abelian group $(M, +)$ endowed with an external law of composition $M \times R \to M$, usually denoted by adjunction, that verifies the following axioms:

- "Associativity": $\forall r, s \in R, \forall a \in M, a(r \times_R s) = (ar)s$,
- "Left-distributivity": $\forall r, s \in R, \forall a \in M, a(r +_R s) = ar + as$,
- "Right-distributivity": $\forall r \in R, \forall a, b \in M, (a + b)r = ar + br$,
- "Identity": $\forall a \in M, a1_R = a$.

The argument made in Remark 1.1.1.2 can also be applied for the case of right modules *mutatis mutandis* the order of operands.

Remark 1.1.1.4 : Case of a commutative ring

If the base ring R is commutative, then any left R-module can canonically be equipped with a structure of right R-module, and *vice versa*. Indeed, consider M a left R-module where R is commutative. Define the external law of composition on the right $M \times R \to M$ as $(a, r) \mapsto ra$. Then the axioms for right R-modules are verified since we would have for "associativity":

$$a(r \times_R s) = (r \times_R s)a = (s \times_R r)a = s(ra) = (ar)s.$$

Another way to look at it is by noticing that any right R-module is a left R^{opp}-module, where R^{opp} is the opposite ring in which we have $r \times_{R^{\text{opp}}} s := s \times_R r$. Then, since the commutative rings are equal to their opposite rings, any left module is a right module.
It is for this reason that we often simply speak of R-modules when R is commutative since there are no distinction between left and right.
This second way of looking at the relation between left and right modules in terms of opposite ring allows us as well to restrict the definitions to only left modules without losing generality. We will do so in the sequel.

Example 1.1.1.5 : (Abelian groups)

The abelian groups are exactly the $\mathbb{Z}$-modules, where $\mathbb{Z}$ is the ring of integers. The multiplication by scalars is defined as repetitive addition or subtraction. Explicitly, if A is an additive abelian group, define the module structure by:

$$\forall n \in \mathbb{Z}, \forall a \in A, \quad na := \begin{cases} \overbrace{a + a + \cdots + a}^{n \text{ times}} & \text{if } n > 0, \\ 0 & \text{if } n = 0, \\ \underbrace{(-a) + (-a) + \cdots + (-a)}_{-n \text{ times}} & \text{if } n < 0. \end{cases}$$

Example 1.1.1.6 : (Vector spaces)

A vector space over a field $\mathbb{K}$ is just a left $\mathbb{K}$-module. And conversely, every left $\mathbb{K}$-module where $\mathbb{K}$ is a field is a vector space. Since a field is a commutative ring, there are in theory no requirement to mention left. However, the convention for vector spaces is usually to place the scalars on the left of the vectors.

Example 1.1.1.7 : (Rings as modules)

Rings can be viewed as left or right modules over themselves: let R be a unital ring, it is in particular an additive abelian group. Endow this group with the action on the left defined by the ring product on the left and one obtains a left R-module. Similarly, we can view R as a right R-module.

Let us introduce a more involved example that will be used a few more times in this thesis to illustrate different notions.

Example 1.1.1.8 : (Module over a group algebra)

Let G be a finite group and $\mathbb{K}$ be a field. Define the group algebra $\mathbb{K}[G]$ to be the set of formal finite linear combination of elements of G with coefficients in $\mathbb{K}$. This is a $\mathbb{K}$-vector space that can be equipped with a structure of associative unitary algebra by defining the product through distributivity. So in particular, $\mathbb{K}[G]$ is a unital ring and can be used as the ground ring for modules.

In *representation theory* [Ser77], $\mathbb{K}[G]$-modules arise naturally when we consider representation of finite groups in the group of invertible matrices with coefficients in $\mathbb{K}$. In more details, let G be a finite group, n a positive integer and $\mathbb{K}$ be field. Then, a *representation* of the group G is a homomorphism of groups $\rho : G \to \mathrm{GL}_n(\mathbb{K})$ (we *represent* the abstract elements of G as invertible matrices with coefficients in our chosen field $\mathbb{K}$). Giving ourselves a representation of G is equivalent to giving ourselves a left $\mathbb{K}[G]$-module. Indeed, consider a vector space V of dimension n. Then: $\mathrm{GL}_n(\mathbb{K}) \cong \mathrm{Aut}(V)$ once a basis of V is fixed. If ρ is a representation of G, then define the following unital-ring-homomorphism:

$$\begin{aligned} \mu_\rho : \quad \mathbb{K}[G] &\to \mathrm{End}(V) \\ \textstyle\sum_g \lambda_g g &\mapsto \textstyle\sum_g \lambda_g \rho(g). \end{aligned}$$

According to Remark 1.1.1.2, this equips V with a structure of $\mathbb{K}[G]$-module.

Conversely, if one is given a unital-ring-homomorphism $\mu : \mathbb{K}[G] \to \mathrm{End}(V)$, then define the group homomorphism $\rho_\mu : G \to \mathrm{End}(V)$ as the restriction of μ to G. In fact, since the elements of G viewed as elements of $\mathbb{K}[G]$ are units of the ring, this group homomorphism ρ_μ takes values in $\mathrm{Aut}(V) \cong \mathrm{GL}_n(\mathbb{K})$. It is therefore a representation of G.

As with most algebraic structures we are now interested in subojects and quotient objects.

Definition 1.1.1.9 : Submodule

Let R be a ring. Let M be a left R-module.

A *submodule* of M is any subgroup N of the additive abelian group M that is closed under scalar multiplication:

$$\forall r \in R, \quad \forall a \in N, \quad ra \in N.$$

It follows directly that any submodule of an R-module is also an R-module.

Definition 1.1.1.10 : Submodule generated by subset

Let R be a ring. Let M be a left R-module. Let $S \subseteq M$ be a subset.
The *submodule generated by* S is the following set:

$$\mathrm{Span}_R(S) := \left\{ \sum_{i=1}^{n} r_i s_i \;\middle|\; n \in \mathbb{N} \;\wedge\; \forall i \in [\![1\,..\,n]\!], \quad r_i \in R \;\wedge\; s_i \in S \right\}.$$

By convention, the empty sum is equal to 0.
For any subset S of M, the set $\mathrm{Span}_R(S)$ is a submodule of M.

Example 1.1.1.11 : (Subgroups)

The submodules of abelian groups seen as $\mathbb{Z}$-modules are exactly the same thing as subgroups of those abelian groups.

Example 1.1.1.12 : (Vector subspaces)

Similarly, the submodules of $\mathbb{K}$-vector spaces viewed as $\mathbb{K}$-modules are exactly the subspaces of those vector spaces.

Example 1.1.1.13 : (Ideals as submodules)

If R is a ring and I is a left-ideal of R, then I can be seen as a submodule of R when we view R as a left module over itself. Indeed, recall that a left-ideal is precisely an additive subgroup of R that is closed under multiplication to the left by elements of R, which is exactly the requirement for being a submodule. In the same manner, any right-ideal is a submodule of R when considering it a right module over itself.

Example 1.1.1.14 : (Trivial submodule)

For any R-module M whose zero element is denoted 0, the set $\{0\}$ is always a submodule, called the *trivial submodule*. We will denote by 0 any trivial module.

Definition 1.1.1.15 : Quotient module

Let R be a ring. Let M be a left R-module. Let N be a submodule of M.
The *quotient module* of M modulo N, denoted ${}^{M}\!/_{N}$, is defined as the quotient group ${}^{M}\!/_{N}$, when considering M and N as additive groups, endowed with the structure of R-module as follows:

$$\forall r \in R, \quad \forall a \in M, \quad r(a+N) := (ra) + N,$$

where $b + N$ is the *coset* of $b \in M$ modulo N.

Once again, we see that this definition generalises perfectly the corresponding notions in group theory and linear algebra.

Example 1.1.1.16 : (Quotient of abelian groups)

The quotient module of an abelian group modulo a subgroup, viewed as $\mathbb{Z}$-modules, is exactly the quotient group of the two.

Example 1.1.1.17 : (Quotient of vector spaces)

The quotient module of a $\mathbb{K}$-vector space modulo a subspace, when seen as $\mathbb{K}$-modules, is precisely the quotient space of the two.

Definition 1.1.1.18 : Bimodule

Let R and S be rings.
A (R, S)-*bimodule* is any set M that can be viewed simultaneously as a left R-module and a right S-module, whose underlying additive groups are the same, and that satisfy the following additional "associativity" property:

$$\forall r \in R, \quad \forall a \in M, \quad \forall s \in S, \quad (ra)s = r(as).$$

Remark 1.1.1.19 : Bimodule as a left-module

Giving a (R, S)-bimodule is equivalent to giving a left $(R \otimes_{\mathbb{Z}} S)$-module where $\otimes_{\mathbb{Z}}$ is the tensor product defined in Definition 1.1.6.3.

Example 1.1.1.20 : (Subring of center)

If R is a ring, denote by $Z(R)$ its center, *i.e.* the set of elements in R that commute multiplicatively with every other elements in R. This is a subring of R. Indeed, $1 \in Z(R)$ by the axioms of unital rings. Then, one can see that $Z(R)$ is an additive subgroup:

$$\forall a, b \in Z(R), \quad \forall r \in R, \quad (a - b)r = ar - br = ra - rb = r(a - b).$$

And finally that $Z(R)$ is closed under multiplication:

$$\forall a, b \in Z(R), \quad \forall r \in R, \quad r(ab) = (ra)b = (ar)b = a(rb) = a(br) = (ab)r.$$

It follows that we can use the center of any ring as a base ring for modules.
In particular, if M is a left R-module, then it can be viewed as an $(R, Z(R))$-bimodule defining the right $Z(R)$-module as $as := sa$ for all $a \in M$ and $s \in Z(R)$ viewed as an element of R. The "associativity" condition is then satisfied since:

$$(ra)s := s(ra) = (sr)a = (rs)a = r(sa) =: r(as).$$

More generally, if S is any subring of $Z(R)$, then any left R-module can be seen as a (R, S)-bimodule.

1.1.2 Homomorphisms of modules

Now that we have defined the basic algebraic objects we are working with, it comes up naturally to interest ourselves in the relations they hold towards each other and how to transform one into another.

Definition 1.1.2.1 : Linear maps between modules

Let R be a ring. Let M and N be left R-modules.
An *homomorphism of R-modules*, or *R-linear map*, from M to N is any additive group homomorphism $f : M \to N$ that satisfies the following property:

$$\forall r \in R, \quad \forall a \in M, \quad f(ra) = rf(a).$$

Proposition 1.1.2.2 : Composition preserves linearity

Let R be a ring. Let $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ be two R-linear maps between left R-modules.
The composite map $g \circ f$ is also R-linear.

Proof. Let $a, b \in M_1$ and $r \in R$:

$$(g \circ f)(a + rb) = g(f(a + rb)) = g(f(a) + rf(b)) = g(f(a) + rgf(b) = (g \circ f)(a) + r(g \circ f)(b).$$

□

Just as for group theory, we have the notion of *kernel* and *cokernel* as well as the *image*.

Definition 1.1.2.3 : Image, kernel, cokernel

Let R be a ring. Let M and N be left R-modules. Let $f : M \to N$ be an R-linear map.
The *kernel* of f is the set:

$$\ker(f) := \{a \in M \mid f(a) = 0\}.$$

It is a submodule of M.
The *image* of f is the set:

$$\mathrm{im}(f) := \{f(a) \in N \mid a \in M\}.$$

It is a submodule of N.
The *cokernel* of f is the quotient module:

$$\mathrm{coker}(f) := {}^{N}/_{\mathrm{im}(f)}.$$

The well-known properties of injectivity and surjectivity in group theory translate as well here with modules:

Proposition 1.1.2.4

Let R be a ring. Let M and N be left R-modules. Let $f : M \to N$ be an R-linear map.
Then:

$$f \text{ is injective} \quad \Leftrightarrow \quad \ker(f) = 0.$$

$$f \text{ is surjective} \quad \Leftrightarrow \quad \mathrm{im}(f) = N \quad \Leftrightarrow \quad \mathrm{coker}(f) = 0.$$

Proof. By definition, f is injective if and only if for all $a, b \in M$, $f(a) = f(b)$ implies $a = b$. But $f(a) = f(b)$ is equivalent to $f(a-b) = 0$ which is equivalent to $a-b \in \ker(f)$. Thus, if $\ker(f) = 0$, then injectivity follows. Conversely, if f is injective and $a \in \ker(f)$, then $f(a) = 0 = f(0)$, hence we have $a = 0$.

Surjectivity being equivalent to the equality image = codomain follows directly from the definition of surjective maps and the tautology $\mathrm{im}(f) \subseteq \mathrm{codom}(f)$. The other equivalence follows directly from the definition of the cokernel. $\square$

Example 1.1.2.5 : (Zero map)

Given any two left R-modules M and N over a ring R, the map $0 : M \to N$ that sends every element of M to the zero element of N is called the *zero map*. Whenever M or N is the trivial module, then there exists no map from M to N other than the zero map.

Example 1.1.2.6 : (Identity)

If M is a left R-module over a ring R, then the identify function $\mathrm{id}_M : M \to M$ given by $\mathrm{id}_M(a) = a$, for all $a \in M$, is R-linear. It is both surjective and injective.

Example 1.1.2.7 : (Canonical injection)

Let R be a ring, M be a left R-module and N a submodule of M. Then, the map $i_N : N \to M$ defined as the restriction of the identity map id_M to N is R-linear. Moreover, since id_M is injective, all of its restriction are too, in such a way that i_N is injective. It is called the *canonical injection* of N in M.

Example 1.1.2.8 : (Canonical projection)

Let R be a ring, M be a left R-module and N a submodule of M. The map $\pi_N : M \to {}^{M}/_{N}$ that associates to each $a \in M$ its coset $a + N$ is R-linear. Furthermore, this map is surjective and is called the *canonical projection* of M modulo N.

Definition 1.1.2.9 : Isomorphism

Let R be a ring. Let M and N be left R-modules.
An *isomorphism of R-modules* between M and N is any R-linear map $f : M \to N$ that is bijective, *i.e.* both injective and surjective.
If there exists an isomorphism between M and N, we write $M \cong N$.

Proposition 1.1.2.10

Let R be a ring. Let M and N be left R-modules. Let $f : M \to N$ be an R-linear map.
Then, f is an isomorphism of R-modules if, and only if, there exists a two-sided inverse of f that is R-linear.

Proof. If f is an isomorphism then it is bijective and thus admits an inverse map $f^{-1} : N \to M$ defined for all $a \in N$ by $f^{-1}(a) = a_f$ where a_f is the unique antecedent of a by f. Notice that, since $f(ra) = rf(a)$, then $(ra)_f = ra_f$. Therefore, we have:

$$f^{-1}(a + rb) = f^{-1}(f(a_f) + f((rb)_f)) = f^{-1}(f(a_f + rb_f)) = a_f + rb_f = f^{-1}(a) + rf^{-1}(b).$$

Hence, f^{-1} is R-linear.

Conversely, assuming f has a two-sided inverse of f that is R-linear, then f is bijective by the properties of two-sided inverse of any map. Hence, it is an isomorphism of R-modules. $\square$

Theorem 1.1.2.11 : (First isomorphism theorem)

Let R be a ring. Let M and N be left R-modules. Let $f : M \to N$ be an R-linear map. Then:

$$M/\ker(f) \cong \operatorname{im}(f)$$

Proof. Consider the mapping $\varphi : M/\ker(f) \to \operatorname{im}(f)$, $a + \ker(f) \mapsto f(a)$. It is well-defined since if $a + \ker(f) = b + \ker(f)$, then $a - b \in \ker(f)$ and thus $f(a) = f(b)$. The R-linearity of φ follows directly from the R-linearity of f. Let $b = f(a) \in \operatorname{im}(f)$. Then $\varphi(a + \ker(f)) = b$, making φ surjective. Let $a + \ker(f) \in \ker(\varphi)$, then $0 = \varphi(a + \ker(f)) = f(a)$ so $a \in \ker(f)$ hence $a + \ker(f) = 0 + \ker(f)$ which is the zero element in $M/\ker(f)$. Therefore, φ is indeed injective and thus an isomorphism of R-modules. □

Proposition 1.1.2.12 : Addition of linear maps

Let R be a ring. Let M and N be left R-modules. Let $f, g : M \to N$ be R-linear maps. Then the following map is R-linear:

$$\begin{aligned} f + g : M &\to N \\ a &\mapsto (f+g)(a) := f(a) + g(a). \end{aligned}$$

Proof. Let $a, b \in M$ and $r \in R$:

$$\begin{aligned} (f+g)(a+rb) &= f(a+rb) + g(a+rb) && \text{by definition of } f+g \\ &= f(a) + rf(b) + g(a) + rg(b) && \text{by } R\text{-linearity of } f \text{ and } g \\ &= (f(a)+g(a)) + r(f(b)+g(b)) && \text{since } N \text{ is a } R\text{-module} \\ (f+g)(a+rb) &= (f+g)(a) + r(f+g)(b) && \text{by definition of } f+g \end{aligned}$$

□

Proposition 1.1.2.13 : Multiplication by scalar of linear map

Let R and S be rings. Let M and N be left R-modules. Let $f : M \to N$ be a R-linear map. If M is (R, S)-bimodule, then for all $s \in S$ the following map is R-linear:

$$\begin{aligned} sf : M &\to N \\ a &\mapsto (sf)(a) := f(as). \end{aligned}$$

If N is (R, S)-bimodule, then for all $s \in S$ the following map is R-linear:

$$\begin{aligned} fs : M &\to N \\ a &\mapsto (fs)(a) := f(a)s. \end{aligned}$$

Proof. Suppose M is a (R, S)-bimodule. Let $a, b \in M$, $r \in R$ and $s \in S$:

$$\begin{aligned} (sf)(a+rb) &= f((a+rb)s) && \text{by definition of } sf \\ &= f(as + rbs) && \text{since } M \text{ is a } (R,S)\text{-bimodule} \\ &= f(as) + rf(bs) && \text{by } R\text{-linearity of } f \\ &= (sf)(a) + r(sf)(b) && \text{by definition of } sf \end{aligned}$$

Suppose now N is (R,S)-bimodule. Let $a,b \in M$, $r \in R$ and $s \in S$:

$$\begin{aligned}
(fs)(a+rb) &= f(a+rb)s && \text{by definition of } fs \\
&= (f(a)+rf(b))s && \text{by } R\text{-linearity of } f \\
&= f(a)s + r(f(b)s) && \text{since } N \text{ is a } (R,S)\text{-bimodule} \\
&= (fs)(a) + r(fs)(b) && \text{by definition of } fs
\end{aligned}$$

□

Proposition 1.1.2.14 : Structure on linear maps

Let R be a ring. Let M and N be left R-modules.
The set $\operatorname{Hom}_R(M,N)$ consisting of all R-linear maps from M to N can be endowed with a structure of left or right $Z(R)$-module.
In particular, it is an abelian group.
In the case of R being commutative, then $\operatorname{Hom}_R(M,N)$ is a R-module.

Proof. The additive operation is given by Proposition 1.1.2.12. It follows directly from the definition and the fact that the codomain is a module that $\operatorname{Hom}_R(M,N)$ is an abelian group for that operation whose zero element is the zero map (Example 1.1.2.5).

The scalar multiplication to the left (resp. to the right) is given by the first map (resp. the second) defined in Proposition 1.1.2.13. Indeed, we have seen in Example 1.1.1.20 that any left R-module can be seen as a $(R, Z(R))$-bimodule.

Only remains to check for the axioms of $Z(R)$-module. We consider the left version.

Let $f,g \in \operatorname{Hom}_R(M,N)$, $r,s \in Z(R)$ and $a \in M$:

$$\begin{aligned}
(r(f+g))(a) &= (f+g)(ar) = f(ar)+g(ar) = (rf)(a)+(rg)(a), \\
((r+s)f)(a) &= f(a(r+s)) = f(ar+as) = f(ar)+f(as) = (rf)(a)+(sf)(a), \\
((rs)f)(a) &= f(ars) = (sf)(ar) = (r(sf))(a), \\
(1f)(a) &= f(a1) = f(a).
\end{aligned}$$

□

1.1.3 Exact sequences of modules

Definition 1.1.3.1 : Exact sequences of modules

Let R be a ring.
An *exact sequence of left R-modules* consists of a family $(M_n)_{n\in\mathbb{Z}}$ of left R-modules together with a family of R-linear maps $\left(f_n : M_n \to M_{n-1}\right)_{n\in\mathbb{Z}}$:

$$\dots \xrightarrow{f_{n+2}} M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \xrightarrow{f_{n-1}} \dots$$

such that for all $n \in \mathbb{Z}$, we have $\operatorname{im}(f_{n+1}) = \ker(f_n)$.

Note that there is no need to label arrows that go from or to the trivial module 0 since, as we noticed in Example 1.1.2.5, there is only one such map: the zero map.

In this definition, we assume that the sequence go on forever on both sides. However, it is often the case that the sequences are finite for at least one of the two directions. We trust the reader in being able to adapt the definition for such sequences.

Proposition 1.1.3.2

Let R be a ring. Let A and B be left R-modules. Let $f : A \to B$ be a R-linear map. Then:

- The sequence $0 \to A \xrightarrow{f} B$ is exact if and only if f is injective.
- The sequence $A \xrightarrow{f} B \to 0$ is exact if and only if f is surjective.
- The sequence $0 \to A \xrightarrow{f} B \to 0$ exact if and only if f is an isomorphism.

Proof. The first two assertions follow directly from Proposition 1.1.2.4. The last statement follows from the fact that bijective is equivalent to surjective and injective. □

Definition 1.1.3.3 : Short exact sequence of modules

Let R be a ring. A *short exact sequence of R-modules* is any exact sequence of the form:

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

where A, B and C are left R-modules and f and g are R-linear maps.

Example 1.1.3.4 : (Extension)

When we have short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$, then we say that B is an *extension* of C by A. The reason behind that name is the following. Since f is injective, we can identify A with the submodule $\mathrm{im}(f)$ of B. However, by exactness, $\mathrm{im}(f) = \ker(g)$ and g is surjective. It follows from the first isomorphism theorem (Theorem 1.1.2.11) that $C \cong {}^{B}/_{\mathrm{im}(f)}$ where $\mathrm{im}(f)$ can be identified with A.
In summary, a short exact sequence enables to express that an object A can be seen as a subobject of an object B while an object C is the quotient of that object B by that object A. The terminology is justified by the fact that it means we *extend* A into B with respect to C.

Example 1.1.3.5 : (Short exact sequence from first isomorphism theorem)

If R is a ring, M and N left R-modules and $f : M \to N$ an R-linear map, then the first isomorphism theorem (Theorem 1.1.2.11) can be expressed as saying that the following short sequence is exact:

$$0 \to \ker(f) \xrightarrow{i} M \xrightarrow{\overline{f}} \mathrm{im}(f) \to 0$$

where i is the canonical injection of $\ker(f)$ into M and $\overline{f}$ is the corestriction of f to $\mathrm{im}(f)$.

Here is a categorical generalisation of the rank-nullity theorem of linear algebra for modules:

Theorem 1.1.3.6 : (Splitting lemma)

Let R be a ring. Consider the following short exact sequence of left R-modules:

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0.$$

The following conditions are equivalent:

(i) There exists a R-linear map $r : B \to A$ such that $r \circ f = \mathrm{id}_A$.

(ii) There exists a R-linear map $s : C \to B$ such that $g \circ s = \mathrm{id}_C$.

(iii) There exists an isomorphism $h : B \to A \oplus C$ such that hf is the natural injection of A into $A \oplus C$ and gh^{-1} is the natural projection of $A \oplus C$ onto C.

Proof. An open-access proof is available on the Wikipedia page of the splitting lemma. □

Definition 1.1.3.7 : Split short exact sequence of modules

A *split short exact sequence of modules* is any short exact sequence that satisfy one of the equivalent conditions of the splitting lemma (Theorem 1.1.3.6).

1.1.4 Operations on submodules

Proposition 1.1.4.1 : Closure of submodules under arbitrary intersection

Let R be a ring. Let M be a left R-module. Let $(M_i)_{i\in I}$ be an arbitrary non-empty family of submodules of M.
Then: $\bigcap_{i\in I} M_i$ is a submodule of M.

Proof. Denote by $N := \bigcap_{i\in I} M_i$. Let $a, b \in N$ and $r \in R$. Then $a, b \in M_i$ for all $i \in I$.
Thus, $a + rb \in M_i$ for all $i \in I$, which exactly means that $a + rb \in N$. Finally, since all submodules contains 0, we have $0 \in N$. So N is a submodule of M. □

Proposition 1.1.4.2 : Characterisation of submodule generated by subset

Let R be a ring. Let M be a left R-module. Let S be a subset of M.
Then, the submodule generated by S is the smallest submodule of M that contains N. In symbols:

$$\langle S \rangle = \bigcap_{\substack{N \text{ submodule } M \\ S \subseteq N}} N$$

Proof. Recall the definition of $\langle S \rangle$ from Definition 1.1.1.10. Write M_S the right-hand side of the equality. Let $a \in \langle S \rangle$. Then, there exists $n \in \mathbb{N}$, $(r_1, \cdots, r_n) \in R^n$ and $(s_1, \cdots, s_n) \in S_n$ such that $a = \sum_{i=1}^n r_i s_i$. Since $S \subseteq M_S$ and M_S is a submodule, it follows that $a \in M_S$, hence $\langle S \rangle \subseteq M_S$.
Conversely, we have already noticed that $\langle S \rangle$ is a submodule of M. Moreover, it contains S. Then, since M_S is the smallest submodule of M that contains N, then $M_S \subset \langle S \rangle$. □

Definition 1.1.4.3 : Sum of submodules

Let R be a ring. Let M be a left R-module. Let $(M_i)_{i\in I}$ be a family of submodules of M. The *sum* of the family $(M_i)_{i\in I}$ of submodules is defined as:

$$\sum_{i\in I} M_i := \left\langle \bigcup_{i\in I} M_i \right\rangle = \left\{ \sum_{j=1}^{n} a_j \;\middle|\; n\in\mathbb{N} \;\wedge\; \forall j\in [\![1\,..\,n]\!],\quad \exists i_j\in I,\quad a_j\in M_{i_j} \right\}$$

1.1.5 Direct sums of modules

Definition 1.1.5.1 : Direct product of modules

Let R be a ring. Let $(M_i)_{i\in I}$ be a non-empty family of left R-modules.
The *direct product* of the family is the left R-module whose underlying set is the cartesian product $\prod_{i\in I} M_i$ and whose operations are defined component-wise:

$$\forall\, (a_i)_{i\in I}, (b_i)_{i\in I} \in \prod_{i\in I} M_i,\quad (a_i)_{i\in I} + (b_i)_{i\in I} := (a_i+b_i)_{i\in I}\,,$$

$$\forall\, (a_i)_{i\in I} \in \prod_{i\in I} M_i,\quad \forall r\in R,\quad r\,(a_i)_{i\in I} := (ra_i)_{i\in I}\,.$$

Definition 1.1.5.2 : Direct sum of submodules

Let R be a ring. Let M be a left R-module. Let $(M_i)_{i\in I}$ be a non-empty family of submodules of M.
The module M is said to be the *direct sum* of the family $(M_i)_{i\in I}$ of submodules if it verifies:

$$\forall a\in M,\quad \exists! J\subseteq I,\quad \mathrm{card}(J)<\infty \;\wedge\; \exists!\,(a_j)_{j\in J}\in \prod_{j\in J}(M_j\setminus\{0\}),\quad a=\sum_{j\in J} a_j.$$

In which case, we write $M=\bigoplus_{i\in I} M_i$.

Proposition 1.1.5.3 : Characterisation direct sum

Let R be a ring. Let M be a left R-module. Let $(M_i)_{i\in I}$ be a non-empty family of submodules of M.
Then:

$$M=\bigoplus_{i\in I} M_i \;\Leftrightarrow\; M\subseteq \sum_{i\in I} M_I \;\wedge\; \forall i_0\in I,\quad M_{i_0}\cap \sum_{\substack{i\in I\\ i\neq i_0}} M_i \subseteq \{0\}\,.$$

Proof. Recall the notion of sum of submodules from Definition 1.1.4.3.

Suppose M is the direct sum. Then, it follows from the definition that every element of M is written has a finite sum of elements of the family. By contradiction, suppose there exists $i_0\in I$ such that $M_{i_0}\cap\sum_{\substack{i\in I\\ i\neq i_0}} M_i$ contains element $a_{i_0}\neq 0$. Then, this element $a_{i_0}\in M$ admits two different decomposition in finite sums of elements in the submodules. Which contradicts the direct sum assumption.

Conversely, assuming $M\subseteq\sum_{i\in I} M_i$ means that every element of M admits at least one decomposition in a sum of elements of the submodules. Remains to show that this decomposition is unique when we suppose additionally the second condition in the conjunction. By contradiction, suppose they are two different decomposition $0\neq a=\sum_{j\in J} a_j=\sum_{g\in G} b_g$ as the one defined in

Definition 1.1.5.2. Since they are different and $a \neq 0$, there exists $j_0 \in J$ such that $0 \neq a_{j_0} \neq b_g$ for all $g \in G$. Then, $0 \neq a_{j_0} = \sum_{g \in G} b_g - \sum_{\substack{j \in J \\ j \neq j_0}} a_j$. It follows that $0 \neq a_{j_0} \in M_{j_0} \cap \sum_{\substack{i \in I \\ i \neq j_0}} M_i$. □

Proposition 1.1.5.4 : Direct sum and direct product coincide for finite families

Let R be a ring, M be a left R-module, $n \in \mathbb{N}^*$ and $M_1, \cdots, M_n$ be n submodules of M. Then:

$$M = \bigoplus_{i=1}^{n} M_i \quad \Rightarrow \quad M \cong \prod_{i=1}^{n} M_i.$$

Proof. Suppose that $M = \bigoplus_{i=1}^n M_i$. Consider the map:

$$\begin{aligned} f : M &\to \textstyle\prod_{i=1}^n M_i \\ a &\mapsto (a_1, \cdots, a_n) \end{aligned}$$

where a_i is either zero or the non-zero value in M_i appearing in the decomposition from Definition 1.1.5.2. It is an R-linear map because $a + rb = \sum_{i=1}^n a_i + r \sum_{i=1}^n b_i = \sum_{i=1}^n a_i + rb_i$.

Let $(a_1, \cdots, a_n) \in \prod_{i=1}^n M_i$. Then $a := \sum_{i=1}^n a_i$ is such that $a \in M$ and $f(a) = (a_1, \cdots, a_n)$. Hence, f is surjective.

Let $a \in \ker(f)$, that is, $f(a) = (0, \cdots, 0)$. This means that the subset J of indices in the definition of the direct sum is empty. But the only element of M with such an empty decomposition is 0. Hence, $\ker(f) = \{0\}$ and thus f injective. □

Definition 1.1.5.5 : Direct summand of module

Let R be a ring. Let M a left R-module.
A *direct summand* of M is any submodule A of M such that there exists a submodule B of M satisfying $M = A \oplus B$.
In that case, B is called a *complementary submodule* of A in M.

Proposition 1.1.5.6

Let R be a ring. Let M a left R-module. Let A be a submodule of M.
Then, A is a direct summand of M if, and only if, there exists an R-linear map $r : M \to A$ such that for all $a \in A$, $r(a) = a$.
In such a case, we say that A is a *retract* of M.

Proof. A proof of that statement can be found in [Rot09, Corollary 2.23]. □

1.1.6 Tensor products of modules

Definition 1.1.6.1 : Biadditive map

Let R be a ring. Let A be a right R-module and B a left R-module. Let G be an additive abelian group.
A map $f : A \times B \to G$ is said to be R-*biadditive* if it satisfies the following identities:

- $\forall a, a' \in A, \quad \forall b \in B, \quad f(a + a', b) = f(a, b) + f(a', b),$
- $\forall a \in A, \quad \forall b, b' \in B, \quad f(a, b + b') = f(a, b) + f(a, b'),$
- $\forall a \in A, \quad \forall b \in B, \quad \forall r \in R, \quad f(ar, b) = f(a, rb).$

Definition 1.1.6.2 : Bilinear map

Let R be a *commutative* ring. Let A, B and M be R-modules.
A map $f : A \times B \to M$ is said to be R-*bilinear* if it is R-biadditive and verifies:

$$\forall a \in A, \quad \forall b \in B, \quad \forall r \in R, \quad f(ar, b) = f(a, rb) = rf(a, b).$$

Definition 1.1.6.3 : Tensor product of modules

Let R be a ring. Let A be a right R-module and B a left R-module.
The *tensor product* of A and B consists of an abelian group $A \otimes_R B$ and an R-biadditive map $h : A \times B \to A \otimes_R B$ that satisfies the following universal property: for every abelian group G and every R-biadditive $f : A \times B \to G$ there exists a unique $\mathbb{Z}$-linear map $\tilde{f} : A \otimes_R B \to G$ such that $f = \tilde{f}h$.

$$\begin{tikzcd}
A \times B \arrow[rr, "h"] \arrow[dr, "f"'] & & A \otimes_R B \arrow[dl, dashed, "\tilde{f}"] \\
& G &
\end{tikzcd}$$

Proposition 1.1.6.4 : Uniqueness of tensor product up to isomorphism

Let R be a ring. Let A be a right R-module and B be a left R-module.
If (G, h) and (G', h') are tensor products of A and B, then $G \cong G'$.

Proof. Apply the universal property of (G, h) to G' and $h' : A \times B \to G'$. Then there exists a unique $\mathbb{Z}$-linear map $\tilde{h}' : G \to G'$ such that $h' = \tilde{h}'h$. Apply now the universal property of (G', h') to G and $h : A \times B \to G$. We thus have a unique $\mathbb{Z}$-linear map $\tilde{h} : G' \to G$ such that $h = \tilde{h}h'$. In other words, the following diagram commutes:

$$\begin{tikzcd}
& G \arrow[d, "\tilde{h}'"] \\
A \times B \arrow[ur, "h"] \arrow[r, "h'"] \arrow[dr, "h"] & G' \arrow[d, "\tilde{h}"] \\
& G
\end{tikzcd}$$

Notice how the unique $\mathbb{Z}$-linear map satisfying the universal property of (G, h) for G and h is the identity id_G. In other words, $\tilde{h}\tilde{h}' = \mathrm{id}_G$. In an analogous manner, one can prove that $\tilde{h}'\tilde{h} = \mathrm{id}_{G'}$. This makes $\tilde{h}$ and $\tilde{h}'$ isomorphisms of $\mathbb{Z}$-modules. Hence, $G \cong G'$. □

Proposition 1.1.6.5 : Existence of tensor product

Let R be a ring. Let A be a right R-module and B be a left R-module.
The tensor product $A \otimes_R B$ of A and B exists.

Proof. Let us give a constructive proof. Take F the free abelian group with basis $A \times B$. Denote by S the subgroup of F generated by the union of the three following sets:

$$X := \{(a + a', b) - (a, b) - (a', b) \in F \mid a, a' \in A \wedge b \in B\}$$
$$Y := \{(a, b + b') - (a, b) - (a, b') \in F \mid a \in A \wedge b, b' \in B\}$$
$$Z := \{(ar, b) - (a, rb) \in F \mid a \in A \wedge b \in B \wedge r \in R\}$$

Consider the quotient group ${}^{F}/_{S}$ and the restriction h of the natural map $\pi : F \to {}^{F}/_{S}$ to the elements in $A \times B$. Let us show that these define a tensor product of A and B.

First, notice that, by construction, every element $a, a' \in A$ and $b \in B$ satisfy the relations:

$$\begin{aligned} &\pi((a+a',b)-(a,b)-(a',b)) = 0 && \text{because the element is in } S \\ &\pi((a+a',b)-(a,b)-(a',b)) = h(a+a',b)-h(a,b)-h(a,b') && \text{because } \pi \text{ is a morphism} \end{aligned}$$

Thus, combining those two and writing $h(c,d) =: c \otimes d$, we get:

$$(a+a') \otimes b = a \otimes b + a' \otimes b$$

In a similar way, we get the following relations, for all $a \in A$, $b, b' \in B$ and $r \in R$:

$$a \otimes (b+b') = a \otimes b + a \otimes b'$$

$$(ar) \otimes b = a \otimes (rb)$$

Hence h is an R-biadditive map.

Now, let G an abelian group and $f : A \times B \to G$ an R-biadditive map.

Denote by $i : A \times B \to F$ the evident inclusion. By extending with linearity, there exists a unique morphism of abelian groups $\varphi : F \to G$ such that the following diagram commutes:

$$\begin{tikzcd} A \times B \arrow[rr, "i"] \arrow[dr, "f"'] & & F \arrow[dl, dashed, "\varphi"] \\ & G & \end{tikzcd}$$

In particular, $\forall (a,b) \in A \times B, f(a,b) = \varphi(a,b)$.

Notice that $S \subseteq \ker \varphi$, because if we take an element in S, it is written as a sum of of elements of elements in $X \cup Y \cup Z$, its image through φ is thus a sum of elements $\varphi(x)$, where $x \in X \cup Y \cup Z$ then each of these elements becomes a sum of elements $\varphi(a,b)$ which thus can be replaced by $f(a,b)$; finally, by biadditivity of f, each of these elements reduces to zero.

We can thus define a morphism of abelian groups $\hat{f} : {}^{F}/_{S} \to G$ as $\forall x \in F, \hat{f}(x+S) := \varphi(x)$. It is indeed well-defined since for any $x, y \in F$, $x+S = y+S$ implies that $x-y \in S$ and thus, $\varphi(x-y) = 0$ because $S \subseteq \ker \varphi$, and hence $\varphi(x) = \varphi(y)$.

Now, let $(a,b) \in A \times B$, then $(\hat{f} \circ h)(a,b) = \hat{f}(a \otimes b) = \hat{f}((a,b)+S) = \varphi(a,b) = f(a,b)$. Therefore, the map $\hat{f}$ makes the following diagram commute:

$$\begin{tikzcd} A \times B \arrow[rr, "h"] \arrow[dr, "f"'] & & F/S \arrow[dl, dashed, "\hat{f}"] \\ & G & \end{tikzcd}$$

The uniqueness of $\hat{f}$ follows from the fact that the elements of the form $a \otimes b$ generate ${}^{F}/_{S}$, therefore taking any other morphism $\tilde{f}$ making the above diagram commute implies that $\hat{f}$ and $\tilde{f}$ agree on the set of generators of ${}^{F}/_{S}$ and are thus equal.

We can thus define the tensor product of A and B as the quotient group $A \otimes_R B := {}^{F}/_{S}$ together with the restriction to $A \times B$ of the natural projection from F to ${}^{F}/_{S}$. $\square$

Proposition 1.1.6.6 : Tensor product of linear maps

Let R be a ring. Let $f : A \to A'$ be a morphism of right R-modules. Let $g : B \to B'$ be a morphism of left R-modules.
There exists a unique morphism of abelian groups:

$$\begin{aligned} f \otimes g \colon A \otimes_R B &\to A' \otimes_R B' \quad . \\ a \otimes b &\mapsto f(a) \otimes g(b) \end{aligned}$$

Proof. Indeed, by constructing the map:

$$\begin{aligned} \varphi \colon A \times B &\to A' \otimes_R B' \\ (a, b) &\mapsto f(a) \otimes g(b) \end{aligned}$$

we notice it is R-biadditive by virtue of the properties in $A' \otimes_R B'$ and the fact that f and g are R-linear maps. Therefore, by the universal property defining $A \otimes_R B$, there exists a unique morphism of abelian groups that happen to coincide with $f \otimes g$ defined above. □

Corollary 1.1.6.7 : Composition of tensored linear maps

Let R be a ring. Let $A \xrightarrow{f} A' \xrightarrow{f'} A''$ be maps of right R-modules and $B \xrightarrow{g} B' \xrightarrow{g'} B''$ be maps of left R-modules.
Then:

$$(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g).$$

Proof. The left-hand and right-hand side both send $a \otimes b$ to $(f' \circ f)(a) \otimes (g' \circ g)(b)$. By uniqueness, we conclude the equality of maps. □

Proposition 1.1.6.8 : Structure on tensor product

Let R and S be rings. Let A be a right R-module and B be a left R-module.
If A is (S, R)-bimodule, then $A \otimes_R B$ can be equipped with a structure of left S-module.
If B is (R, S)-bimodule, then $A \otimes_R B$ can be equipped with a structure of right S-module.
In particular, $A \otimes_R B$ can be seen as a left or right $Z(R)$-module.
In particular, if R is commutative, then $A \otimes_R B$ is a R-module.

Proof. Suppose A is a (S, R)-bimodule. Then define the external law of composition on the abelian group $A \otimes_R B$ as:

$$s \left(\sum_{a,b} a \otimes b \right) := \sum_{a,b} (sa) \otimes b.$$

Then:

$$(s + s')(a \otimes b) = ((s + s')a) \otimes b = (sa + s'a) \otimes b = (sa) \otimes b + (s'a) \otimes b = s(a \otimes b) + s'(a \otimes b).$$

$$s(a \otimes b + a' \otimes b') = (sa) \otimes b + (sa') \otimes b' = s(a \otimes b) + s(a' \otimes b').$$

$$(s's)(a \otimes b) = ((s's)a) \otimes b = (s'(sa)) \otimes b = s'((sa) \otimes b) = s'(s(a \otimes b)).$$

$$1_S(a \otimes b) = (1_S a) \otimes b = a \otimes b.$$

Hence, $A \otimes_R B$ is indeed a left R-module.

The same proof can be applied *mutatis mutandis* to prove the second statement.

The special case follows from Example 1.1.1.20. □

1.1.7 Free, projective and injective modules

Definition 1.1.7.1 : Free module

Let R be a ring.
A *free left R-module* is any left R-module F that has a basis *i.e.* there exists a family $(b_i)_{i\in I}$ of elements of F such that:

$$\forall a \in F, \quad \exists! J \subseteq I, \quad \operatorname{card}(J) < \infty \ \wedge \ \exists! \left(r_j\right)_{j\in J} \in \left(R \setminus \{0\}\right)^J, \quad a = \sum_{j\in J} r_j b_j.$$

Remark 1.1.7.2 : Characterisation of free modules

Looking at the definition of free modules and the definition of direct sum (Definition 1.1.5.2), we detect similarities. Actually, being a free module is equivalent to being isomorphic to a direct sum of "copies" of the ground ring R. What "copy" mean here is any left R-module isomorphic to R as a module over itself. In summary:

$$F \text{ is a free } R\text{-module} \ \Leftrightarrow \ \exists I, \quad F \cong \bigoplus_{i\in I} R.$$

Proposition 1.1.7.3

Let R be a ring. Every left R-module is a quotient of a free left R-module.

Proof. Let M be a left R-module. Take $X \subseteq M$ a generating set of M, *i.e.* $\langle X\rangle = M$. Such a set does exist since M is such one. Consider now F the free module on X, *i.e.* $F := \bigoplus_{x\in X} R$. Denote by $(b_x)_{x\in X}$ the basis of F. Then, since X generates M, the following map extended by linearty is surjective:

$$\begin{aligned} \varphi_X : F &\to M. \\ b_x &\mapsto x \end{aligned}$$

By the first isomorphism theorem (Theorem 1.1.2.11), it follows that $M \cong {}^{F}/_{\ker(\varphi_X)}$, hence the result. □

Definition 1.1.7.4 : Projective module

Let R be a ring.
A *projective left R-module* is any left R-module P such that for any surjective R-linear map $p : A \to B$ and any R-linear map $f : P \to B$, there exists a R-linear map $g : P \to A$ such that $f = p \circ g$.

$$\begin{tikzcd} & P \arrow[d, "f"] \arrow[dl, dashed, "g"'] & \\ A \arrow[r, two heads, "p"'] & B \arrow[r] & 0 \end{tikzcd}$$

Theorem 1.1.7.5 : (Characterisation of projective modules)

Let R be a ring. Let P be a left R-module.
Then, the following conditions are equivalent:

(i) P is projective,

(ii) if $\varepsilon : M \to P$ is a surjective R-linear map, then there exists an R-linear map $\eta : P \to M$ such that $\varepsilon\eta = \mathrm{id}_P$,

(iii) P is a direct summand in every module of which it is a quotient,

(iv) P is a direct summand in a free module.

Proof. A complete proof can be found in [HS97, Theorem 4.7]. □

Remark 1.1.7.6 : Characterisation projective in terms of exactness of Hom functor

Yet another characterisation for being a projective module is expressed in terms of the exactness of the $\mathrm{Hom}_R(P, -)$ functor. However, we have not yet introduced those notions. For later reference, this just means that every short exact sequence:

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

remains an exact sequence under the action of the functor:

$$0 \to \mathrm{Hom}_R(P, A) \xrightarrow{f_*} \mathrm{Hom}_R(P, B) \xrightarrow{g_*} \mathrm{Hom}_R(P, C) \to 0$$

Definition 1.1.7.7 : Injective module

Let R be a ring.
An *injective left R-module* is any left R-module I such that for every injective R-linear map $i : B \to A$ and every R-linear map $f : B \to I$, there exists a R-linear map $g : A \to I$ such that $f = g \circ i$.

$$\begin{tikzcd} 0 \arrow[r] & B \arrow[r, tail, "i"] \arrow[d, "f"] & A \arrow[dl, dashed, "g"] \\ & P & \end{tikzcd}$$

1.2 Non-commutative algebra

1.2.1 Associative unitary algebras

Definition 1.2.1.1 : Associative unitary algebra

Let K be a *commutative* ring.
An *associative unitary K-algebra* is any K-module A whose underlying additive abelian group can also be equipped with a structure of unital ring and that satisfy the following compatibility condition:

$$\forall \lambda \in K, \quad \forall x, y \in A, \quad \lambda(xy) = (\lambda x)y = x(\lambda y)$$

Remark 1.2.1.2 : Axioms versus ring-homomorphism on center

Now, suppose we are given a unital ring A. To define a structure of K-algebra on A one can simply provide a unital-ring-homomorphism $\eta : K \to Z(A)$, where $Z(A)$ is the center of A (see Example 1.1.1.20). Indeed, the scalar multiplication is then given by $\lambda x := \eta(\lambda)x$. Conversely, if the scalar multiplication is defined, construct the unital-ring-homomorphism $\eta(\lambda) := \lambda 1_A$.

Example 1.2.1.3 : (Ring as algebra over itself)

Let K be a commutative ring. As we have seen in Example 1.1.1.7, we can view K as a module over itself. Then, it suffices to show that the compatibility condition is verified which is trivial since the scalar multiplication and the ring multiplication coincide, both are associative and K is commutative.

Example 1.2.1.4 : (Tensor algebra)

Let $\mathbb{K}$ be a field. Let V be a finite-dimensional $\mathbb{K}$-vector space. The *tensor algebra* over V is defined as:

$$T(V) := \mathbb{K} \oplus V \oplus V^{\otimes 2} \oplus V^{\otimes 3} \oplus \cdots = \bigoplus_{n \in \mathbb{N}} V^{\otimes n}.$$

where $V^{\otimes n}$ is the n-fold tensor product on V over $\mathbb{K}$.
The multiplication is given by the tensor product $V^{\otimes i} \otimes V^{\otimes j} \to V^{\otimes i+j}$.
The tensor algebra is a fundamental notion for non-commutative algebra.

Definition 1.2.1.5 : Augmented algebra

Let $\mathbb{K}$ be a field.
An *augmented algebra* over $\mathbb{K}$ is any associative unitary $\mathbb{K}$-algebra A together with a homomorphism of associative unitary $\mathbb{K}$-algebras $\varepsilon : A \to \mathbb{K}$. We then have the vector-space decomposition:

$$A = \mathbb{K}1_A \oplus \ker(\varepsilon).$$

The map ε is then called the *augmentation map* and $\ker(\varepsilon)$ is the *augmentation ideal.*

Definition 1.2.1.6 : Graded connected algebra

Let $\mathbb{K}$ be a field.
A *graded connected* $\mathbb{K}$*-algebra* is any *graded* $\mathbb{K}$-algebra whose zero-component is one-dimensional and generated by the unit element 1_A. What it means to be graded is that there exists a sequence $(A_n)_{n \in \mathbb{N}}$ of $\mathbb{K}$-vector spaces such that:

$$A \cong \bigoplus_{n \in \mathbb{N}} A_n \qquad \text{and} \qquad \forall m, n \in \mathbb{N}, \quad A_n A_m \subseteq A_{n+m}$$

The zero-component A_0 admit 1_A as a basis in such a way that $A_0 \cong \mathbb{K}1_A$.

Remark 1.2.1.7 : Natural augmentation on graded connected algebras

Any graded connected $\mathbb{K}$-algebra can be augmented naturally by the projection of A onto $A_0 \cong \mathbb{K}$. The augmentation ideal is then $A_+ := \bigoplus_{n \geqslant 1} A_n$.

Definition 1.2.1.8 : Homogeneous algebra

Let $\mathbb{K}$ be a field. Let $N \geqslant 2$ be an integer.
An *N-homogeneous $\mathbb{K}$-algebra* is a graded connected algebra $A = \bigoplus_{n\in\mathbb{N}} A_n$ such that there exists a surjective homomorphism of $\mathbb{K}$-algebras $\pi : T(A_1) \to A$ (where $T(A_1)$ is the tensor algebra over A_1) whose kernel is generated as a two-sided ideal by elements of $A_1^{\otimes N}$.

Definition 1.2.1.9 : Quadratic algebra

Let $\mathbb{K}$ be a field.
A *quadratic $\mathbb{K}$-algebra* is a 2-homogeneous $\mathbb{K}$-algebra.

1.2.2 Free algebras

Definition 1.2.2.1 : Construction of free algebra on monoid

Let M be a monoid written multiplicatively. Let K be a commutative ring.
The *free K-algebra over the monoid M* is the set KM of finite formal linear combinations of elements in M with coefficients in K, where addition and scalar multiplication are defined component-wise and the ring multiplication is given by distributivity and the operation on the monoid.

More precisely, denote:

$$KM := \left\{ \sum_{x\in N} \lambda_x x \;\middle|\; N \subseteq M \quad \wedge \quad \mathrm{card}(N) < \infty \quad \wedge \quad \forall x \in N, \quad \lambda_x \in K \right\}$$

the set of finite formal linear combinations of elements in M with coefficients in K.

For any element $a = \sum_{x\in N} \lambda_x x \in KM$ and any element $x \in M$, write $\mathrm{coef}_a(x) := \lambda_x$ the coefficient associated to x in the linear combination describing a if it appears, and 0 otherwise. Then define the *support* of a as the subset of M:

$$\mathrm{supp}(a) := \{x \in M \mid \mathrm{coef}_a(x) \neq 0\}.$$

By definition, it will always be a finite set. It follows that any element $a \in KM$ is written as:

$$a = \sum_{x\in \mathrm{supp}(a)} \mathrm{coef}_a(x)\, x.$$

Then, we define addition on KM as follows:

$$\forall a, b \in KM, \quad a + b := \sum_{x\in \mathrm{supp}(a)\cup\mathrm{supp}(b)} (\mathrm{coef}_a(x) + \mathrm{coef}_b(x))\, x.$$

Scalar multiplication is also defined component-wise as such:

$$\forall a \in KM, \quad \forall \lambda \in K, \quad \lambda a := \sum_{x\in \mathrm{supp}(a)} (\lambda \times \mathrm{coef}_a(x))\, x.$$

Finally, the ring multiplication is given by:

$$\forall a, b \in KM, \quad ab := \sum_{z\in M} \left(\sum_{xy=z} (\mathrm{coef}_a(x) \times \mathrm{coef}_b(y)) \right) z.$$

This is well-defined because for all $z \in M$ there exist only finitely many $x, y \in M$ such that $xy = z$ and $\mathrm{coef}_a(x) \neq 0$ or $\mathrm{coef}_b(y) \neq 0$. Moreover, since $\mathrm{supp}(a)$ and $\mathrm{supp}(b)$ are finite, there will only be finitely many $z \in M$ such that there exist $x, y \in M$ with $xy = z$ and $\mathrm{coef}_a(x) = 0$ or $\mathrm{coef}_b(y) = 0$.

It is then routine to check that those operations define a structure of associative unitary K-algebra on KM.

Example 1.2.2.2 : (Polynomial algebra)

Given $n \in \mathbb{N}^*$ indeterminates $x_1, \cdots, x_n$, we can consider the free commutative monoid:

$$[x_1, \cdots, x_n] := \left\{ \prod_{i=1}^{n} x_i^{e_i} \;\middle|\; \forall i \in [\![1\,..\,n]\!], \quad e_i \in \mathbb{N} \right\}$$

where the operation is defined as:

$$\left(\prod_{i=1}^{n} x_i^{e_i} \right) \left(\prod_{i=1}^{n} x_i^{f_i} \right) := \prod_{i=1}^{n} x_i^{e_i + f_i}.$$

The free algebra on $[x_1, \cdots, x_n]$ is then the *polynomial algebra* $K[x_1, \cdots, x_n]$. We say it is *univariate* if $n = 1$ and *multivariate* otherwise.
No matter the value of n, the polynomial algebra is commutative (*i.e.* the ring multiplication is commutative).

Example 1.2.2.3 : (Polynomial algebra with non-commuting indeterminates (a.k.a. free algebra))

Given a non-empty set X (called *alphabet* in that context) of indeterminates (also called here *letters*), we can construct the free monoid of *words* over X:

$$\langle X \rangle := \{ x_1 \cdots x_n \mid n \in \mathbb{N} \ \wedge \ \forall i \in [\![1\,..\,n]\!], \quad x_i \in X \}.$$

where the operation is defined as the *concatenation* of words:

$$\forall x_1 \cdots x_n, y_1 \cdots y_m \in \langle X \rangle, \quad (x_1 \cdots x_n)(y_1 \cdots y_m) := x_1 \cdots x_n y_1 \cdots y_m.$$

When X is a singleton, the free algebra $K\langle X \rangle$ over the monoid $\langle X \rangle$ is equal to the univariate polynomial algebra.
Otherwise, if X is not a singleton, the free algebra $K\langle X \rangle$ is not commutative because the letters do not commute.
Given any non-empty set X, we call the *free K-algebra over the set X* the free algebra over the monoid $\langle X \rangle$, thus denoted $K\langle X \rangle$.

Proposition 1.2.2.4 : Free algebra and tensor algebra isomorphic

Let $\mathbb{K}$ be a field. Let X be a finite set.
Then, the free $\mathbb{K}$-algebra over X and the tensor algebra over free $\mathbb{K}$-vector space $\mathbb{K}X$ are isomorphic:

$$\mathbb{K}\langle X\rangle \cong T(\mathbb{K}X).$$

Proof. For each $n \in \mathbb{N}$, we have the following isomorphism of vector spaces:

$$\begin{aligned}\varphi_n :\ \mathbb{K}X^{(n)} &\to \mathbb{K}X^{\otimes n}\\ x_1\cdots x_n &\mapsto x_1\otimes\cdots\otimes x_n.\end{aligned}$$

where $X^{(n)}$ is the set of words in $\langle X\rangle$ that are of length n.

Combining those maps into a single map $\bigoplus_{n\in\mathbb{N}}\varphi_n$ we obtain an isomorphism of associative unitary $\mathbb{K}$-algebras. □

Definition 1.2.2.5 : Monomial order

Let M be a monoid written multiplicatively. A *monomial order* on M is any well-order $\prec$ such that it is compatible with left- and right-multiplication of the monoid.
Explicitly, well-order means total order such that every descending sequence is stationary:

$$\forall\,(x_n)_{n\in\mathbb{N}}\,M^{\mathbb{N}},\quad (\forall n\in\mathbb{N},\quad x_{n+1}\preceq x_n)\ \Rightarrow\ \exists n_0\in\mathbb{N},\quad \forall n\geqslant n_0,\quad x_{n_0}=x_n,$$

and compatibility with multiplication means:

$$\forall x,y,u,v\in M,\quad x\prec y\ \Rightarrow\ uxv\prec uyv.$$

Example 1.2.2.6 : (Deglex order)

Given an alphabet X that is equipped with a total order $\prec$, the *degree lexicographic order* (or *deglex order*) is a monomial order defined on $\langle X\rangle$ by:

$$\begin{aligned}x_1\cdots x_n \prec_{\text{deglex}} y_1\cdots y_m \ \Leftrightarrow\ & n<m\ \vee\\ & (n=m\ \wedge\ \exists i_0\in[\![1\,..\,n]\!],\quad \forall i<i_0,\quad x_i=y_i\ \wedge\ x_{i_0}\prec y_{i_0}).\end{aligned}$$

Definition 1.2.2.7 : Leading monomial, leading coefficient

Let K be a commutative ring. Let X be a non-empty set. Let $K\langle X\rangle$ be the free K-algebra over X. Let $\prec$ be a monomial order on $\langle X\rangle$.
For any non-zero $f\in K\langle X\rangle$, define the *leading monomial* of f as:

$$\mathrm{LM}(f) := \max_{\prec}\operatorname{supp}(f),$$

and the *leading coefficient* of f as:

$$\mathrm{LC}(f) := \operatorname{coef}_f(\mathrm{LM}(f)).$$

They exist since $\operatorname{supp}(f)$ is finite, $\prec$ is a total order and f is non-zero.
For any non-empty set F of non-zero polynomials in $K\langle X\rangle$, we let:

$$\mathrm{LM}(F) := \{\mathrm{LM}(f)\mid f\in F\}.$$

1.2.3 Presentations

Proposition 1.2.3.1 : Every algebra is quotient of the free algebra

Let K be a commutative ring. Let A be an associative unitary K-algebra.
Then, there exists a non-empty set X and a two-sided ideal I of $K\langle X\rangle$ such that:

$$A \cong {}^{K\langle X\rangle}/_{I}.$$

Proof. The proof is the same as for free modules (Proposition 1.1.7.3) *mutatis mutandis* swapping free modules with free algebras and the kernel of the map is a two-sided ideal instead of simply a submodule. □

Definition 1.2.3.2 : Presentation of algebras

Let K be a commutative ring. Let A be an associative unitary K-algebra.
A *presentation* (*by generators and relations*) of A is any non-empty set X and any set R of polynomials from $K\langle X\rangle$ together with an isomorphism of K-algebras:

$$A \cong {}^{K\langle X\rangle}/_{I(R)}.$$

where $I(R)$ is the two-sided ideal generated by R in $K\langle X\rangle$.
We denote the presentation by $\langle X|R\rangle$.

Definition 1.2.3.3 : Monomial presentation

Let K be a commutative ring. Let A be an associative unitary K-alegbra.
A presentation $\langle X|R\rangle$ of A is *monomial* if the elements of R are monomials:

$$R \subseteq \langle X\rangle .$$

If such a presentation of A exists, A is said to be a *monomial algebra*.

Definition 1.2.3.4 : Homogeneous presentation

Let K be a commutative ring. Let A be an associative unitary K-alegbra.
A presentation $\langle X|R\rangle$ of A is *homogeneous* if the elements of R are of homogeneous polynomials of same degree:

$$\exists N \geqslant 2, \quad R \subseteq KX^{(N)}$$

where $X^{(N)}$ is the set of monomials of X of degree N.
If such a presentation of A exists, then A is an N-homogeneous algebra (Definition 1.2.1.8).

Definition 1.2.3.5 : Homogeneous monomial presentation

Let K be a commutative ring. Let A be an associative unitary K-alegbra.
A presentation $\langle X|R\rangle$ of A is *homogeneous monomial* if it is both homogeneous and monomial:

$$\exists N \geqslant 2, \quad R \subseteq X^{(N)}$$

where $X^{(N)}$ is the set of monomials on X of degree N.
If such a presentation of A exists, A is said to be a *N-homogeneous monomial algebra*.

1.2.4 Non-commutative Gröbner bases

In this section, we consider associative unitary algebras over a field $\mathbb{K}$. In particular, we fix throughout this subsection, a non-empty set X and the free algebra $\mathbb{K}\langle X\rangle$ on X.

Denote by $m \subseteq m'$ the relation of subwords on $\langle X\rangle$:

$$\forall m, m' \in \langle X\rangle, \quad m \subseteq m' \ \Leftrightarrow\ \exists a, b \in \langle X\rangle, \quad amb = m'.$$

Proposition 1.2.4.1 : Multivariate division algorithm

Let $\prec$ be a monomial order on $\langle X\rangle$. Let $f, g_1, g_2, \cdots, g_n \in \mathbb{K}\langle X\rangle$.
There exists $a_1, \cdots, a_n, b_1, \cdots, b_n \in \mathbb{K}\langle X\rangle$ and $r \in \mathbb{K}\langle X\rangle$ such that:

- $f = r + \sum_{i=1}^{n} \sum_{j=1}^{n_i} a_{i,j} g_i b_{i,j}$,
- $\forall i \in [\![1 \mathinner{..} n]\!], \quad \mathrm{LM}\left(\sum_{j=1}^{n_i} a_{i,j} g_i b_{i,j}\right) \preceq \mathrm{LM}(f)$,
- $\forall m \in \mathrm{supp}(r), \quad \forall i \in [\![1 \mathinner{..} n]\!], \quad \mathrm{LM}(g_i) \not\subseteq m$.

In such a case, we say that f reduces to r through $G := \{g_1, \cdots, g_n\}$ and we denote it $f \xrightarrow[G]{*} r$.

Proof. Consider Algorithm 1. It provides a constructive way of defining the polynomials stated to exist in the proposition.

Algorithm 1: Division algorithm for non-commutative polynomials

---

Input: $f, g_1, \cdots, g_n \in \mathbb{K}\langle X\rangle$, $\prec$ monomial order on $\langle X\rangle$.
Output: $r, (a_{i,j})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n_i}}, (b_{i,j})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n_i}} \in \mathbb{K}\langle X\rangle$ satisfying the conditions of Proposition 1.2.4.1.

$r \leftarrow f$
$(n_1, \cdots, n_n) \leftarrow (0, \cdots, 0)$
while $\exists m \in \mathrm{supp}(r), \exists i \in [\![1 \mathinner{..} n]\!], \exists a, b \in \langle X\rangle, m = a\mathrm{LM}(g_i)\, b$ **do**
  $r \leftarrow r - \dfrac{\mathrm{coef}_r(m)}{\mathrm{LC}(g_i)} a g_i b$
  $a_{i,n_i+1} \leftarrow \dfrac{\mathrm{coef}_r(m)}{\mathrm{LC}(g_i)} a$
  $b_{i,n_i+1} \leftarrow b$
  $n_i \leftarrow n_i + 1$
end
return $r, (a_{i,j})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n_i}}, (b_{i,j})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n_i}}$

□

Definition 1.2.4.2 : Monomial ideal

A *monomial ideal* in $\langle X\rangle$ is a subset $I \subseteq \langle X\rangle$ stable by left- and right-multiplication:

$$\forall m \in I, \quad \forall a, b \in \langle X\rangle, \quad amb \in I.$$

If R is a subset of I such that $\forall m \in I, \exists r \in R, \exists a, b \in \langle X\rangle, m = arb$, then we say that R *generates* I as a monomial ideal.

Example 1.2.4.3 : (Monomial ideal from algebraic ideal)

If I is a two-sided ideal of $\mathbb{K}\langle X\rangle$ and $\prec$ is a monomial order, then the set $\mathrm{LM}(I)$ of leading monomials with respect to $\prec$ of polynomials in I is a monomial ideal.

Definition 1.2.4.4 : Non-commutative Gröbner basis

Let I be a two-sided ideal of $\mathbb{K}\langle X\rangle$. Let $\prec$ be a monomial order on $\langle X\rangle$.
A subset G of I is called a *non-commutative Gröbner basis* of I with respect to $\prec$ if the set $\mathrm{LM}(G)$ generates $\mathrm{LM}(I)$ as a monomial ideal.

Definition 1.2.4.5 : S-polynomial

Let $f, g \in \mathbb{K}\langle X\rangle$.
An *S-polynomial* of f and g is a polynomial S such that there exists $a, b, c \in \langle X\rangle$ with $b \neq 1$ and:

(i) either $\mathrm{LM}(f) = ab$ and $\mathrm{LM}(g) = bc$ in which case $S = \frac{1}{\mathrm{LC}(f)} fc - \frac{1}{\mathrm{LC}(g)} ag$,

(ii) or $\mathrm{LM}(f) = abc$ and $\mathrm{LM}(g) = b$ in which case $S = \frac{1}{\mathrm{LC}(f)} f - \frac{1}{\mathrm{LC}(g)} agc$.

Theorem 1.2.4.6 : (Buchberger criterion, non-commutative case)

Let I be a two-sided ideal of $\mathbb{K}\langle X\rangle$. Let $G \subseteq I$. Let $\prec$ be a monomial order on $\langle X\rangle$.
Then: G is a non-commutative Gröbner basis of I with respect to $\prec$ if and only if for any S-polynomial S between elements of G, we have $S \xrightarrow[G]{*} 0$.

Proof. See [Mor94, Theorem 4.9]. □

Definition 1.2.4.7 : Minimal non-commutative Gröbner basis

Let I be a two-sided ideal of $\mathbb{K}\langle X\rangle$. Let $G \subseteq I$. Let $\prec$ be a monomial order on $\langle X\rangle$.
The set G is a *minimal non-commutative Gröbner basis* of I with respect to $\prec$ if it is a non-commutative Gröbner basis of I w.r.t. $\prec$ and:

$$\forall g_1, g_2 \in G, \quad g_1 \neq g_2 \;\Rightarrow\; \mathrm{LM}(g_1) \not\subseteq \mathrm{LM}(g_2).$$

Proposition 1.2.4.8 : Minimal generating set for leading monomial ideal

Let I be a two-sided ideal of $\mathbb{K}\langle X\rangle$. Let $\prec$ be a monomial order on $\langle X\rangle$.
For any two *minimal* non-commutative Gröbner bases G_1 and G_2 of I w.r.t. $\prec$, we have:

$$\mathrm{LM}(G_1) = \mathrm{LM}(G_2).$$

Proof. By contradiction, suppose there exists a non-zero polynomial $g \in G_1$ with $\mathrm{LM}(g) \notin \mathrm{LM}(G_2)$. Then, we show that the monomial ideals generated by G_1 and by G_2 are different, denoted I_1 and I_2 respectively:

- Suppose there is an element $g' \in G_2$ such that and $\mathrm{LM}(g) \subsetneq \mathrm{LM}(g')$ (resp. $\mathrm{LM}(g') \subsetneq \mathrm{LM}(g)$). By minimality of the bases, $\mathrm{LM}(g) \notin I_2$ (resp. $\mathrm{LM}(g') \notin I_1$). So $I_1 \neq I_2$.
- Suppose there is no element $g' \in G_2$ such that $\mathrm{LM}(g) \subseteq \mathrm{LM}(g')$ nor $\mathrm{LM}(g') \subseteq \mathrm{LM}(g)$. Then, $\mathrm{LM}(g) \notin I_2$. So $I_1 \neq I_2$.

Since G_1 and G_2 are by hypothesis both non-commutative Gröbner bases of I, we were supposed to have $I_1 = \mathrm{LM}(I) = I_2$. But in both cases, $I_1 \neq I_2$. So one of them is not a non-commutative Gröbner basis of I. □

Definition 1.2.4.9 : Reduced non-commutative Gröbner basis

Let I be a two-sided ideal of $\mathbb{K}\langle X\rangle$. Let $G \subseteq I$. Let $\prec$ be a monomial order on $\langle X\rangle$.
The set G is a *reduced non-commutative Gröbner basis* of I with respect to $\prec$ if it is a minimal non-commutative Gröbner basis of I w.r.t. $\prec$ and:

$$\forall g_1, g_2 \in G, \quad g_1 \neq g_2 \quad \Rightarrow \quad \forall m \in \mathrm{supp}(g_2), \quad \mathrm{LM}(g_1) \not\subseteq m.$$

Proposition 1.2.4.10 : Existence and uniqueness of reduced non-commutative Gröbner basis

Let I be a two-sided ideal of $\mathbb{K}\langle X\rangle$. Let $\prec$ be a monomial order on $\langle X\rangle$.
There exists a unique reduced non-commutative Gröbner basis of I w.r.t. $\prec$.

Proof. See [Mor94, Proposition 1.5]. □

Proposition 1.2.4.11 : Decomposition according to a presentation

Let I be a two-sided ideal of $\mathbb{K}\langle X\rangle$. Let $\prec$ be a monomial order on $\langle X\rangle$.
Then, we have the following $\mathbb{K}$-vector space decomposition:

$$\mathbb{K}\langle X\rangle \cong I \oplus \mathbb{K}O(I)$$

where $O(I) := \langle X\rangle \setminus \mathrm{LM}(I)$.

Proof. See [Mor94, Theorem 1.3]. □

Chapter 2

Basics of category theory

Category theory has emerged in parallel of the efforts made towards homology theory in algebraic topology, and later in homological algebra, during the second half of the XX'th century. The birth of the field is attributed to the 1945 article of EILENBERG and MAC LANE [EM45] where they describe the basic definitions of *categories* and *functors* in order to study what they call *natural transformations* and, in particular, *natural equivalences*.

The framework proposed by category theory is particularly well-suited to study algebraic structures in an abstract way, allowing one to enunciate general theorems with only a single proof about different domains of applications such as group theory, ring theory, commutative algebra, etc.

The reference book for a graduate-level introduction to category theory is MAC LANE's own *Categories for the working mathematician* [ML98] originally published in 1971. Another standard resource on the subject containing subsequent topics developed in the field is KASHIWARA's and SCHAPIRA's *Categories and sheaves* [KS06]. In particular, it deals with the concept of *derived categories* which is a concept central in the general understanding of homological algebra.

As it is a perfect example of how powerful category theory can be, I studied the concept of *universal properties* in connection with the *Yoneda lemma* and the theory of *adjoint functors*. The resources best-suited to explore these ideas are [Rie16] for a formal approach and [Per19] for a more intuitive depiction with plenty of concrete examples from different areas of mathematics and even related sciences. However, I fail to have time to make a written account on what I have learnt on that matter.

2.1 Basic definitions

To introduce the basic definitions of category theory, we can place ourselves in standard set theory (ZFC for instance). However, when we are concerned about the foundations of the theory, it is somewhat more interesting to reason in terms of *universes*. These are sets closed under any kind of basic set-theoretic operations. The idea is to rid ourselves of proper classes and work solely in given universes where everything is sets. An element of a universe U is called a *U-set*. Any set in bijection with U-set is called a *U-small set*. In terms of classes and sets, a set is a U-small set and a class is a set in bijection with a subset of U. Every set is class but not every class is a set, hence the existence of proper classes. Even though this presentation with universes is generally more well-suited for deep-dive study of category theory, most resources use the classes terminology and so will we in this thesis.

This discussion is important for what follows as we will often consider proper classes such as the class of all sets, which famously is not a set, the class of all groups, of all topological spaces, etc.

2.1.1 Categories

Definition 2.1.1.1 : Category

A (locally small) *category* consists of:

- a class $\mathcal{C}$ of *objects*,
- a set $\mathrm{Hom}_{\mathcal{C}}(A, B)$ of *morphisms*, for every ordered pair (A, B) of objects,
- a map $\circ : \mathrm{Hom}_{\mathcal{C}}(A, B) \times \mathrm{Hom}_{\mathcal{C}}(B, C) \to \mathrm{Hom}_{\mathcal{C}}(A, C)$ called *composition*, for every ordered triple (A, B, C) of objects,

such that they verify the following axioms:

(i) Hom-sets are pairwise disjoint:

$$\forall A, B, A', B' \in \mathcal{C}, \quad (A \neq A' \ \vee \ B \neq B') \ \Rightarrow \ \mathrm{Hom}(A, B) \cap \mathrm{Hom}(A', B') = \varnothing.$$

(ii) There exists an identity morphism for every object:

$$\forall A \in \mathcal{C}, \quad \exists 1_A \in \mathrm{Hom}(A, A), \quad \forall B \in \mathcal{C}, \forall f \in \mathrm{Hom}(A, B), \forall g \in \mathrm{Hom}(B, A),$$
$$1_A \circ g = g \ \wedge \ f \circ 1_A = f.$$

(iii) The composition is associative:

$$\forall A, B, C, D \in \mathcal{C}, \quad \forall f \in \mathrm{Hom}(A, B), \forall g \in \mathrm{Hom}(B, C), \forall h \in \mathrm{Hom}(C, D),$$
$$h \circ (g \circ f) = (h \circ g) \circ f.$$

We generally denote with the same symbol the category and the class of its objects.
We write $f : A \to B$ instead of $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$.

Example 2.1.1.2 : (Category of all sets)

Denote by **Sets** the category whose objects class is the proper class of all sets and for every sets A and B the set $\mathrm{Hom}_{\mathbf{Sets}}(A, B)$ of morphisms is the set of all maps from A to B. Composition is then given by map composition. The identity 1_A on A is given by the identity map id_A and composition of maps is well-known to be associative.

Example 2.1.1.3 : (Category of all groups)

Denote by **Groups** the category of all groups with morphisms the homomorphisms of groups. Once again, the composition is simply map composition and identities are identity homomorphisms.

Example 2.1.1.4 : (Category of all topological spaces)

Denote by **Top** the category of all topological spaces with morphisms the continuous maps from a space to another. Yet again, the composition is given by map composition and identities are identity maps.

So far, we have only provided examples where objects are just sets with some structure and morphisms maps with some additional properties. Consider now the following example:

Example 2.1.1.5 : (Preorders as categories)

Let $(P, \lesssim)$ be a preordered set *i.e.* $\lesssim$ is reflexive and transitive.
Define the category, also denoted P, whose objects are elements of P and whose morphisms are given as follows:

$$\forall a, b \in P, \quad \mathrm{Hom}_P\left(a, b\right) = \begin{cases} \{(a,b)\} & \text{if } a \lesssim b, \\ \varnothing & \text{otherwise.} \end{cases}$$

Composition is defined by the following rule: $(a, b) \circ (b, c) := (a, c)$.
Identities are guaranteed by reflexivity of $\lesssim$ and associativity is verified thanks to transitivity of $\lesssim$.

Example 2.1.1.6 : (Monoids as categories)

Let $(M, \star)$ be a monoid. We can define the following category, also denoted M, that contains a single object $\bullet$ and the morphisms are given by the elements of M. Composition is then defined by the monoid operation:

$$\forall a, b \in \mathrm{Hom}_M\left(\bullet, \bullet\right), \quad a \circ b := a \star b.$$

The single identity morphism is given by the identity element of the monoid. The associativity of composition follows directly from the associativity of the monoid operation.

Now, let us introduce the main category used in homological algebra:

Example 2.1.1.7 : (Categories of all modules)

Let R be a ring. Denote by ${}_R\mathbf{Mod}$ (resp. $\mathbf{Mod}_R$) the category whose objects are all left (resp. right) R-modules (Definition 1.1.1.1) and whose morphisms are R-linear maps (Definition 1.1.2.1). The composition is given by map composition.
This does form a category since the identity maps are R-linear maps (Example 1.1.2.6) and map composition is associative.
Similarly, if S is a ring, denote by ${}_R\mathbf{Mod}_S$ the category of all (R, S)-bimodules and whose morphisms are left R-linear maps that are also right S-linear.

Definition 2.1.1.8 : Subcategory

Let $\mathcal{C}$ be category.
A *subcategory* of $\mathcal{C}$ consists of:

- a subclass $\mathcal{D}$ of the class of objects in $\mathcal{C}$,
- a subset $\mathrm{Hom}_{\mathcal{D}}\left(A, B\right)$ of $\mathrm{Hom}_{\mathcal{C}}\left(A, B\right)$ for every ordered pair (A, B) of objects in $\mathcal{D}$.

such that:

(i) The identities are kept:

$$\forall A \in \mathcal{D}, \quad 1_A \in \mathrm{Hom}_{\mathcal{D}}\left(A, A\right).$$

(ii) The hom-sets of the subcategory are closed under composition:

$$\forall A, B, C \in \mathcal{D}, \quad \forall (f, g) \in \mathrm{Hom}_{\mathcal{D}}\left(A, B\right) \times \mathrm{Hom}_{\mathcal{D}}\left(B, C\right), \quad g \circ f \in \mathrm{Hom}_{\mathcal{D}}\left(A, C\right).$$

Definition 2.1.1.9 : Full subcategory

A subcategory $\mathcal{D}$ of a category $\mathcal{C}$ is called *full* if:

$$\forall A, B \in \mathcal{D}, \quad \mathrm{Hom}_{\mathcal{D}}(A, B) = \mathrm{Hom}_{\mathcal{C}}(A, B).$$

Example 2.1.1.10 : (Category of all abelian groups)

Recall the category **Groups** of all groups from Example 2.1.1.3. Consider now only the abelian groups with the group-homomorphisms between them. This defines a full subcategory of **Groups** that we denote by **Ab**.

Example 2.1.1.11 : (Submonoid)

Let M be the category associated to a monoid $(M, \star)$ as in Example 2.1.1.6. Then, a non-empty subcategory of M defines a submonoid of $(M, \star)$ and *vice versa*. In particular, this can yield subcategories that are not full.

One powerful concept in category theory is duality, the notion of "reversing all arrows". This starts with the notion of dual category:

Definition 2.1.1.12 : Dual category

Let $\mathcal{C}$ be a category whose composition is denoted by $\circ$.
The *dual category* of $\mathcal{C}$ is the category $\mathcal{C}^{\mathrm{op}}$ whose objects are the same as $\mathcal{C}$, whose morphisms hom-sets are defined as $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(A, B) := \mathrm{Hom}_{\mathcal{C}}(B, A)$ and whose composition $\overset{\mathrm{op}}{\circ}$ is defined as $g \overset{\mathrm{op}}{\circ} f := f \circ g$. To every morphism f in $\mathcal{C}$, write f^{op} for the associated morphism in the dual category.

The main interest of duality is that most definitions in category theory are defined solely in terms of arrows and therefore often admits a dual definition that consists of the same statement but with all arrows reversed. The object from the dual definition corresponds to an object for the original definition but in the dual category. Therefore, proving a theorem for a "dualisable" definition for *all* categories implies that this theorem is also true for the dual category and thus for the dual definition as well.

2.1.2 Functors

Definition 2.1.2.1 : Functor

Let $\mathcal{C}$ and $\mathcal{D}$ be two categories.
A *functor* T from $\mathcal{C}$ to $\mathcal{D}$ consists of:

- a map T of classes that associates to every object $A \in \mathcal{C}$ a unique object $T(A) \in \mathcal{D}$,
- for every $A, B \in \mathcal{C}$, a map $T : \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(T(A), T(B))$.

verifying the axioms:

(i) Identity morphisms are preserved: $\forall A \in \mathcal{C}, \quad T(1_A) = 1_{T(A)}$.

(ii) Composition is preserved:

$$\forall A, B, C \in \mathcal{C}, \quad \forall f \in \mathrm{Hom}(A, B), \forall g \in \mathrm{Hom}(B, C), \quad T(g \circ f) = T(g) \circ T(f).$$

A *contravariant functor* from $\mathcal{C}$ to $\mathcal{D}$ is a functor T from $\mathcal{C}^{\mathrm{op}}$ to $\mathcal{D}$. It defines the maps:

$$T : \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(T(B), T(A)),$$

and verifies the property of reversing composition instead of preserving it:

$$T(g \circ f) = T(f) \circ T(g).$$

When we wish to emphasise that a functor is not contravariant we say that it is *covariant*.

Definition 2.1.2.2 : Full, faithful, essentially surjective

Let $T : \mathcal{C} \to \mathcal{D}$ be a functor between two categories.
It is said that T is:

- *full* if for every $A, B \in \mathcal{C}$, the map $T : \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(T(A), T(B))$ is surjective,
- *faithful* if for every $A, B \in \mathcal{C}$, the map $T : \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(T(A), T(B))$ is injective,
- *fully faithful* if it is both full and faithful,
- *essentially surjective* if for every $X \in \mathcal{D}$, there exists an object $A \in \mathcal{C}$ such that $T(A)$ is isomorphic to X in $\mathcal{D}$.

Example 2.1.2.3 : (Identity functor)

The *identity functor* $\mathrm{I}_{\mathcal{C}}$ on a category $\mathcal{C}$ assigns each object and each morphism to itself. It is covariant. It is fully faithful and essentially surjective.

Example 2.1.2.4 : (Dual functor)

The *dual functor* is defined as the contravariant functor $\mathrm{op} : \mathcal{C} \to \mathcal{C}^{\mathrm{op}}$ defined by the identity of $\mathcal{C}^{\mathrm{op}}$. Thus, it is also fully faithful and essentially surjective.

Example 2.1.2.5 : (Embedding functor)

Let $\mathcal{C}$ be a category and $\mathcal{D}$ be a subcategory.
Then, the restriction of the identity functor to the objects and morphisms of $\mathcal{D}$ yields a new functor, called the *embedding functor* of $\mathcal{D}$ into $\mathcal{C}$. It is faithful. If $\mathcal{D}$ is a full subcategory, it is also full.

Example 2.1.2.6 : (Covariant Hom functor for modules)

Let $A \in {}_R\mathbf{Mod}$ be a left R-module. Define the following functor T_A:

- $\forall B \in {}_R\mathbf{Mod}, \quad T_A(B) := \mathrm{Hom}_R(A, B)$ where $\mathrm{Hom}_R(A, B)$ is the set of R-linear maps from A to B,
- $\forall f : B \to B', T_A(f) =: f_* : \mathrm{Hom}_R(A, B) \to \mathrm{Hom}_R(A, B')\,,\ g \mapsto f_*(g) = f \circ g.$

This defines a covariant functor called *covariant Hom functor* and denoted $\mathrm{Hom}_R(A, -)$. According to Proposition 1.1.2.14, the sets $\mathrm{Hom}_R(A, B)$ for $B \in {}_R\mathbf{Mod}$ are actually $Z(R)$-module. Hence: $\mathrm{Hom}_R(A, -) : {}_R\mathbf{Mod} \to {}_{Z(R)}\mathbf{Mod}$.

Example 2.1.2.7 : (Contravariant Hom functor for modules)

Let $B \in {}_R\mathbf{Mod}$ be a left R-module. Define the following functor T_B:

- $\forall A \in {}_R\mathbf{Mod}, \quad T_B(A) := \mathrm{Hom}_R(A, B)$,
- $\forall f : A \to A', T_B(f) =: f^* : \mathrm{Hom}_R(A', B) \to \mathrm{Hom}_R(A, B)\,,\ g \mapsto f^*(g) = g \circ f$.

This defines a contravariant functor called *contravariant Hom functor* and that we denote by $\mathrm{Hom}_R(-, B)$. Proposition 1.1.2.14 allows us to obtain the functor:

$$\mathrm{Hom}_R(-, B) : {}_R\mathbf{Mod}^{\mathrm{op}} \to {}_{Z(R)}\mathbf{Mod}$$

Example 2.1.2.8 : (Tensor product functor)

Let $A \in \mathbf{Mod}_R$ be a right R-module. Define the functor T_A as:

- $\forall B \in {}_R\mathbf{Mod}, \quad T_A(B) := A \otimes_R B$,
- $\forall f \in \mathrm{Hom}_{{}_R\mathbf{Mod}}(B, B')\,, \quad T_A(f) =: A \otimes f := \mathrm{id}_A \otimes f$ (see Proposition 1.1.6.6).

This functor is covariant and is called the *tensor product functor by A on the left* and is denoted: $A \otimes_R -$.
Similarly, with $B \in {}_R\mathbf{Mod}$ a left R-module, we can define a covariant called the *tensor product by B on the right* denoted by $- \otimes_R B$.
In summary, according to Proposition 1.1.6.8:

$$A \otimes_R - : {}_R\mathbf{Mod} \to {}_{Z(R)}\mathbf{Mod}, \quad A \otimes_R f := \mathrm{id}_A \otimes f.$$

$$- \otimes_R B : \mathbf{Mod}_R \to {}_{Z(R)}\mathbf{Mod}, \quad f \otimes_R B := f \otimes \mathrm{id}_B\,.$$

Example 2.1.2.9 : (Forgetful functors)

There exists a wide range of functors called *forgetful functors*. The general idea is that it takes objects from some category and remove ("forget") some structure on it. For instance, consider the forgetful functor for groups: **Groups** $\to$ **Sets** that associates to each group its underlying set and to each group-homomorphism the underlying set-theoretic map. Plenty of other forgetful functors, such as:

- **Ab** $\to$ **Groups**,
- ${}_R\mathbf{Mod} \to \mathbf{Ab}$,
- **Top** $\to$ **Sets**.

Proposition 2.1.2.10 : Composition of functors

Let $\mathcal{C}$, $\mathcal{C}'$ and $\mathcal{C}''$ three categories.
If $T : \mathcal{C} \to \mathcal{C}'$ and $S : \mathcal{C}' \to \mathcal{C}''$ are functors, then the following is also a functor:

$$\begin{aligned} S \circ T : \mathcal{C} &\to \mathcal{C}'' \\ A &\mapsto S(T(A)) \quad \text{for objects,} \\ f &\mapsto S(T(f)) \quad \text{for morphisms.} \end{aligned}$$

2.1.3 Natural transformations

Definition 2.1.3.1 : Natural transformations

Let $S, T : \mathcal{C} \to \mathcal{D}$ be functors.
A *natural transformation τ from S to T* is a family $(\tau_A)_{A \in \mathcal{C}}$ of morphisms in $\mathcal{D}$ such that $\tau_A : S(A) \to T(A)$ and for all $f : A \to A'$ in $\mathcal{C}$:

$$T(f) \circ \tau_A = \tau_{A'} \circ S(f)$$

$$\begin{tikzcd}
S(A) \arrow[rrr, "S(f)", ""{name=SF, below}] \arrow[ddd, "\tau_A"'] & & & S(A') \arrow[ddd, "\tau_{A'}"] \\
& A \arrow[r, "f", ""{name=F}] \arrow[ul, dotted, "S"'] \arrow[ddl, dotted, "T"] & A' \arrow[ur, dotted, "S"] \arrow[ddr, dotted, "T"'] & \\
& & & \\
T(A) \arrow[rrr, "T(f)"', ""{name=TF, above}] & & & T(A')
\arrow[from=F, to=SF, dotted, "S"]
\arrow[from=F, to=TF, dotted, "T"']
\end{tikzcd}$$

A *natural equivalence* is a natural transformation $\tau = (\tau_A)_{A \in \mathcal{A}}$ such that for any $A \in \mathcal{C}$ the component τ_A is an isomorphism in $\mathcal{D}$. In such case, we also say that T and S are *naturally isomorphic* and that τ is a *natural isomorphism*.

This idea behind natural transformations is to formalise the notion of "canonical" constructions, *i.e.* constructions that can be performed on all alike objects in the same abstract way and without making use of special "presentations" of the data manipulated.

Example 2.1.3.2 : (Determinant [ML98])

Let K be a commutative ring. Let $n \in \mathbb{N}^*$ be a positive integer.
Denote by $\mathrm{GL}_n(K)$ the set of $n \times n$ invertible matrices with coefficients in K. Write $K^\times$ the set of units for the ring multiplication. The *determinant* of a matrix M is written $\det_K M$.
The determinant is a natural transformation between the following two functors:

$$\mathrm{GL}_n(-) : \mathbf{ComRings} \to \mathbf{Groups} \qquad (-)^\times : \mathbf{ComRings} \to \mathbf{Groups}.$$

$$\begin{tikzcd}
\mathrm{GL}_n(K) \arrow[rrr, "\mathrm{GL}_n f", ""{name=SF, below}] \arrow[ddd, "\det_K"'] & & & \mathrm{GL}_n(K') \arrow[ddd, "\det_{K'}"] \\
& K \arrow[r, "f", ""{name=F}] \arrow[ul, dotted, "\mathrm{GL}_n(-)"'] \arrow[ddl, dotted, "(-)^\times"] & K' \arrow[ur, dotted, "\mathrm{GL}_n(-)"] \arrow[ddr, dotted, "(-)^\times"'] & \\
& & & \\
K^\times \arrow[rrr, "f^\times"', ""{name=TF, above}] & & & (K')^\times
\arrow[from=F, to=SF, dotted, "\mathrm{GL}_n(-)"]
\arrow[from=F, to=TF, dotted, "(-)^\times"']
\end{tikzcd}$$

Example 2.1.3.3 : (Double dual [EM45])

Let $\mathbb{K}$ be a field.
If V is finite-dimensional $\mathbb{K}$-vector space, write $V^{**} = \mathrm{Hom}_{\mathbb{K}}(\mathrm{Hom}_{\mathbb{K}}(V, \mathbb{K}), \mathbb{K})$ its *double dual*. The double dual is functorial (because it is the composition of two contravariant Hom functors).
Eilenberg and Mac Lane have proven in [EM45] that the double dual functor is naturally isomorphic to the identity functor on $\mathbf{Vect}_{\mathbb{K}}$, the category of all finite-dimensional $\mathbb{K}$-vectors

spaces.

What follows is a (somewhat naive) attempt to show that the equivalence between the representations of groups and the structure of modules on the group-algebras as exposed in Example 1.1.1.8 is natural. This was a proof I made at the start of my internship as an exercise. The proof lasts until page 44, it is long and technical, but all steps are routine.

For any k-vector space V,
giving a representation $\rho : G \to \mathrm{Aut}(V)$ of a group G
is naturally equivalent to
equipping V with a structure of $k[G]$-module for that same group G.

where

- $\mathrm{Aut}(V)$ denotes the group of automorphisms on V (equipped with composition)
- $k[G]$ denotes the group-ring of G over k, *i.e.* the set of finite formal linear combinations of elements in G with coefficients in k.

Let us fix k a field and V a k-vector space. They are fixed for the whole duration of the proof. The statement we wish to prove is formalised in terms of a natural equivalence as follows:

The following map is an isomorphism in **Sets**, natural in the group G:

$$\begin{aligned} \tau_G : \mathrm{Hom}\left(G, \mathrm{Aut}(V)\right) &\to \mathrm{ModMul}_L(k[G], V) \\ \rho : G \to \mathrm{Aut}(V) &\mapsto \ell_\rho : \quad k[G] \times V \quad \to V \\ & \qquad \left(\mathbf{g} = \textstyle\sum_g \lambda_g . g, v\right) \mapsto \ell_\rho(\mathbf{g}, v) := \textstyle\sum_g \lambda_g \left[\rho(g)(v)\right] \end{aligned}$$

where

- $\mathrm{Hom}\left(G, \mathrm{Aut}(V)\right)$ denotes the set of homomorphism of groups from G to $\mathrm{Aut}(V)$,
- $\mathrm{ModMul}_L(k[G], V)$ denotes the set of external laws of composition on V over $k[G]$ that satisfy the axioms of the left $k[G]$-module for V and such that if $\ell \in \mathrm{ModMul}_L(k[G], V)$ then $\forall \lambda \in k, \forall v \in V, \ell(\lambda . 1_G, v) = \lambda v$ in V.

Let G be a group.

Let us verify the well-definedness and closure of τ_G (*i.e.* τ_G does take values in the target object). Let $\rho : G \to \mathrm{Aut}(V)$ be a representation of G in V. Then ℓ_ρ is external law of composition (straightforward since V is a k-vector space) and it satisfies the axioms making V a left $k[G]$-module: let $u, v \in V$, $\mathbf{g_1} = \sum_g \lambda_g . g \in k[G]$ and $\mathbf{g_2} = \sum_h \mu_h . h \in k[G]$:

$$\begin{aligned} \ell_\rho\left(\mathbf{g_1}, u + v\right) &= \sum_g \lambda_g \left[\rho(g)(u + v)\right] \\ &= \sum_g \lambda_g \left(\left[\rho(g)\right](u) + \left[\rho(g)\right](v)\right) && \text{for } \rho(g) \text{ is a morphism on } V \\ &= \sum_g \lambda_g \left[\rho(g)\right](u) + \sum_g \lambda_g \left[\rho(g)\right](v) && \text{in } V \\ \ell_\rho\left(\mathbf{g_1}, u + v\right) &= \ell_\rho\left(\mathbf{g_1}, u\right) + \ell_\rho\left(\mathbf{g_1}, v\right) \end{aligned}$$

$$\begin{aligned}
\ell_\rho\left(\mathbf{g}_1+\mathbf{g}_2, u\right) &= \sum_{k \in "g \cup h"} \left(\lambda_k+\mu_k\right)[\rho(k)(u)] && \text{by definition of } \mathbf{g}_1+\mathbf{g}_2 \\
&= \sum_g \lambda_g [\rho(g)(u)] + \sum_h \mu_h [\rho(h)(u)] && \text{in } V \\
\ell_\rho\left(\mathbf{g}_1+\mathbf{g}_2, u\right) &= \ell_\rho\left(\mathbf{g}_1, u\right)+\ell_\rho\left(\mathbf{g}_2, u\right)
\end{aligned}$$

$$\begin{aligned}
\ell_\rho\left(\mathbf{g}_1, \ell_\rho\left(\mathbf{g}_2, u\right)\right) &= \ell_\rho\left(\mathbf{g}_1, \sum_h \mu_h [\rho(h)(u)]\right) \\
&= \sum_g \lambda_g\left[\rho(g)\left(\sum_h \mu_h [\rho(h)(u)]\right)\right] \\
&= \sum_g \lambda_g\left[\sum_h \mu_h [\rho(g)(\rho(h)(u))]\right] && \text{for } \rho(g) \text{ is } k\text{-linear} \\
&= \sum_g \lambda_g\left[\sum_h \mu_h [\rho(gh)(u)]\right] && \text{for } \rho \text{ is a homomorphism} \\
&= \sum_k \left(\sum_{gh=k} \lambda_g \mu_h\right)[\rho(k)(u)] && \text{in } V \\
\ell_\rho\left(\mathbf{g}_1, \ell_\rho\left(\mathbf{g}_2, u\right)\right) &= \ell_\rho\left(\mathbf{g}_1 \mathbf{g}_2, u\right)
\end{aligned}$$

$\Longrightarrow \tau_G$ is therefore a well-defined morphism in **Sets**.

τ_G is indeed an isomorphism in **Sets**. Consider the following map:

$$\begin{aligned}
\sigma_G : \mathrm{ModMul}_L(k[G], V) &\to \mathrm{Hom}\left(G, \mathrm{Aut}(V)\right) \\
\ell : k[G] \times V \to V &\mapsto \rho_\ell : G \to \mathrm{Aut}(V) \\
& \qquad\qquad g \mapsto \rho_\ell(g) := \ell(g, \bullet) : V \to V \\
& \qquad\qquad\qquad\qquad\qquad v \mapsto \ell(g, v)
\end{aligned}$$

This is a well-defined closed map because for any $\ell \in \mathrm{ModMul}_L(k[G], V)$, ρ_ℓ has values in $\mathrm{Aut}(V)$ ($\rho_\ell(g)$ has $\rho_\ell(g^{-1})$ as a two-sided inverse and is therefore an automorphism on V) and is a morphism of groups: indeed let $g, h \in G$, let $v \in V$:

$$\begin{aligned}
\left[\rho_\ell(gh)\right](v) &= \ell(gh, v) && \text{with } gh = g \times h \text{ in } k[G] \\
&= \ell(g, \ell(h, v)) && \text{because } \ell \text{ is compatible with } \times \text{ in } k[G] \\
&= \left[\rho_\ell(g)\right]\left(\left[\rho_\ell(h)\right](v)\right) \\
\left[\rho_\ell(gh)\right](v) &= \left[\rho_\ell(g) \circ \rho_\ell(h)\right](v)
\end{aligned}$$

i.e. $\rho_\ell(gh) = \rho_\ell(g) \circ \rho_\ell(h)$ so ρ_ℓ is indeed a morphism of groups.

σ_G is thus a morphism in **Sets**. Let us show that it is a two-sided inverse of τ_G.

- Let $\rho : G \to \mathrm{Aut}(V)$ be a representation of G in V. We have $(\sigma_G \circ \tau_G)(\rho) = \sigma_G(\ell_\rho) = \rho_{\ell_\rho}$. Show that $\rho_{\ell_\rho} = \rho$. Let $g \in G$ and $v \in V$:

$$\begin{aligned}
\left[\rho_{\ell_\rho}(g)\right](v) &= \left[\ell_\rho(g, \bullet)\right](v) && \text{by definition of } \ell_{\rho_\ell} \text{ in } \sigma_G \\
&= \ell_\rho(g, v) && \text{by definition of } \ell_\rho(g, \bullet) \text{ in } \sigma_G \\
\left[\rho_{\ell_\rho}(g)\right](v) &= [\rho(g)](v) && \text{by definition of } \ell_\rho \text{ in } \tau_G
\end{aligned}$$

Therefore $\sigma_G \circ \tau_G = \mathrm{id}_{\mathrm{Hom}(G, \mathrm{Aut}(V))}$.

- Let $\ell \in \mathrm{ModMul}_L(k[G], V)$. We have $(\tau_G \circ \sigma_G)(\ell) = \tau_G(\rho_\ell) = \ell_{\rho_\ell}$. Let us show that $\ell_{\rho_\ell} = \ell$.

Let $\mathbf{g} = \sum_g \lambda_g.g \in k[G]$ and $v \in V$:

$$\begin{aligned}
\ell_{\rho_\ell}(\mathbf{g}, v) &= \sum_g \lambda_g \left[\rho_\ell(g)(v)\right] && \text{by definition of } \ell_{\rho_\ell} \text{ in } \tau_G \\
&= \sum_g \lambda_g \left[\ell(g, \bullet)(v)\right] && \text{by definition of } \rho_\ell \text{ in } \sigma_G \\
&= \sum_g \lambda_g \left[\ell(g, v)\right] && \text{by definition of } \ell(g, \bullet) \text{ in } \sigma_G \\
&= \ell\left(\sum_g \lambda_g.1_G, \ell(g, v)\right) && \text{because } \lambda v = \ell(\lambda.1_G, v) \text{ in } V \\
&= \ell\left(\sum_g \lambda_g.g, v\right) && \text{because } \ell \text{ satisfies axioms of left } k[G]\text{-modules} \\
\ell_{\rho_\ell}(\mathbf{g}, v) &= \ell(\mathbf{g}, v)
\end{aligned}$$

Hence, $\tau_G \circ \sigma_G = \mathrm{id}_{\mathrm{ModMul}_L(k[G], V)}$.

$\implies \tau_G$ and σ_G are isomorphisms in **Sets**.

Let G not be a fixed group anymore. We now proceed to show that τ_G is natural in the group G.

Consider the following two contravariant functors:

$$\begin{aligned}
S: \quad \textbf{Groups} \quad &\to \textbf{Sets} \\
G \quad &\mapsto \mathrm{Hom}\,(G, \mathrm{Aut}(V)) \\
f: G \to G' &\mapsto f^*: \mathrm{Hom}\,(G', \mathrm{Aut}(V)) \to \mathrm{Hom}\,(G, \mathrm{Aut}(V)) \\
&\qquad\qquad \rho' \qquad\qquad \mapsto f^*(\rho') := \rho' \circ f
\end{aligned}$$

$$\begin{aligned}
T: \quad \textbf{Groups} \quad &\to \textbf{Sets} \\
G \quad &\mapsto \mathrm{ModMul}_L(k[G], V) \\
f: G \to G' &\mapsto \overline{f}: \mathrm{ModMul}_L(k[G'], V) \to \mathrm{ModMul}_L(k[G], V) \\
&\qquad\qquad \ell' \qquad\qquad \mapsto \overline{f}(\ell')
\end{aligned}$$

where:

$$\begin{aligned}
\overline{f}(\ell'): \qquad k[G] \times V \qquad &\to V \\
\left(\mathbf{g} = \textstyle\sum_g \lambda_g.g, v\right) &\mapsto \left[\overline{f}(\ell')\right](\mathbf{g}, v) := \ell'\left(\textstyle\sum_g \lambda_g.f(g), v\right)
\end{aligned}$$

Those are indeed contravariant functors:

- S being a really basic Hom contravariant functor, there is nothing to prove, apart from the (almost trivial) closure/well-definedness of f^*, since both f and ρ' are homomorphisms of groups (f because in **Groups**, ρ' because it is a representation of a group)
- For T, we must prove three things :

1. $\overline{f}(\ell')$ is indeed in $\mathrm{ModMul}_L(k[G], V)$

2. Identities are preserved by T (straightforward)

3. Composition is reversed, *i.e.* if $G \xrightarrow{f} G' \xrightarrow{f'} G''$, then $\overline{f' \circ f} = \overline{f} \circ \overline{f'}$

1. Let $f: G \to G'$ be a homomorphism of groups and ℓ' be an external law of composition on V over $k[G']$ satisfying the axioms of the $k[G']$-modules. By construction (see definition of T), it is clear that $\overline{f}(\ell')$ is a well-defined external law of composition on V over $k[G]$. Let us show that it

satisfies the required axioms. Let $u, v \in V$, $\mathbf{g_1} = \sum_g \lambda_g.g \in k[G]$ and $\mathbf{g_2} = \sum_h \mu_h.h \in k[G]$:

$$\begin{aligned}
\left[\overline{f}(\ell')\right](\mathbf{g_1}, u+v) &= \ell'\left(\sum_g \lambda_g.f(g), u+v\right) \\
&= \ell'\left(\sum_g \lambda_g.f(g), u\right) + \ell'\left(\sum_g \lambda_g.f(g), u\right) && \text{for } \ell' \text{ is right-additive} \\
\left[\overline{f}(\ell')\right](\mathbf{g_1}, u+v) &= \left[\overline{f}(\ell')\right](\mathbf{g_1}, u) + \left[\overline{f}(\ell')\right](\mathbf{g_1}, v)
\end{aligned}$$

$$\begin{aligned}
\left[\overline{f}(\ell')\right](\mathbf{g_1}+\mathbf{g_2}, u) &= \ell'\left(\sum_{k\in ``g\cup h"} (\lambda_k+\mu_k).f(k), u\right) \\
&= \ell'\left(\sum_g \lambda_g.f(g) + \sum_h \mu_h.f(h), u\right) && \text{by distributivity} \\
&= \ell'\left(\sum_g \lambda_g.f(g), u\right) + \ell'\left(\sum_h \mu_h.f(h), u\right) && \text{for } \ell' \text{ is left-additive} \\
\left[\overline{f}(\ell')\right](\mathbf{g_1}+\mathbf{g_2}, u) &= \left[\overline{f}(\ell')\right](\mathbf{g_1}, u) + \left[\overline{f}(\ell')\right](\mathbf{g_2}, u)
\end{aligned}$$

$$\begin{aligned}
\left[\overline{f}(\ell')\right]\left(\mathbf{g_1}, \left[\overline{f}(\ell')\right](\mathbf{g_2}, u)\right) &= \left[\overline{f}(\ell')\right]\left(\mathbf{g_1}, \ell'\left(\sum_h \mu_h.f(h), u\right)\right) \\
&= \ell'\left(\sum_g \lambda_g.f(g), \ell'\left(\sum_h \mu_h.f(h), u\right)\right) \\
&= \ell'\left(\left(\sum_g \lambda_g.f(g)\right)\left(\sum_h \mu_h.f(h)\right), u\right) && \text{for } \ell' \text{ is compatible} \\
&= \ell'\left(\sum_k \sum_{gh=k} (\lambda_g\mu_h).f(g)f(h), u\right) \\
&= \ell'\left(\sum_k \left(\sum_{gh=k} \lambda_g\mu_h\right).f(k), u\right) && \text{for } f \text{ is a morphism} \\
\left[\overline{f}(\ell')\right]\left(\mathbf{g_1}, \left[\overline{f}(\ell')\right](\mathbf{g_2}, u)\right) &= \left[\overline{f}(\ell')\right](\mathbf{g_1}\mathbf{g_2}, u)
\end{aligned}$$

Hence, $\overline{f}(\ell')$ satisfy the axioms making V a $k[G]$-module.

2. The identities are preserved *i.e.* for $\mathrm{id}_G : G \to G$, $\overline{\mathrm{id}_G} = \mathrm{id}_{\mathrm{ModMul}_L(k[G],V)}$. This is completely straightforward with the definition of $\overline{f}$ (see definition of T).

3. Let $G \xrightarrow{f} G' \xrightarrow{f'} G''$ be homomorphisms of groups. Let $\ell'' \in \mathrm{ModMul}_L(k[G''], V)$.

Let $\mathbf{g} = \sum_g \lambda_g.g \in k[G]$ and $v \in V$, then:

$$
\begin{aligned}
\left[\left(\overline{f} \circ \overline{f'}\right)(\ell'')\right](\mathbf{g}, v) &= \left[\overline{f}\left(\overline{f'}(\ell'')\right)\right](\mathbf{g}, v) \\
&= \left[\overline{f}(\ell')\right](\mathbf{g}, v) && \text{by letting } \ell' := \overline{f'}(\ell'') \\
&= \ell'\left(\sum_g \lambda_g.f(g), v\right) && \text{by definition of } \overline{f}(\ell') \\
&= \left[\overline{f'}(\ell'')\right]\left(\sum_g \lambda_g.f(g), v\right) && \text{substituting back} \\
&= \ell''\left(\sum_g \lambda_g.f'(f(g)), v\right) && \text{by definition of } \overline{f'}(\ell'') \\
&= \ell''\left(\sum_g \lambda_g.(f' \circ f)(g), v\right) \\
\left[\left(\overline{f} \circ \overline{f'}\right)(\ell'')\right](\mathbf{g}, v) &= \left[\overline{(f' \circ f)}(\ell'')\right](\mathbf{g}, v)
\end{aligned}
$$

Thus, composition is reversed by T.

$\Longrightarrow$ S and T are contravariant functors from **Groups** to **Sets**.

Let us finally show that τ_G is natural in G, *i.e.* let us prove the commutativity of:

$$
\begin{tikzcd}
\mathrm{Hom}(G, \mathrm{Aut}(V)) \arrow[dd, "\tau_G"'] & & {} & & \mathrm{Hom}(G', \mathrm{Aut}(V)) \arrow[llll, "f^*"'] \arrow[dd, "\tau_{G'}"] \\
& G \arrow[ul, dotted, "S"'] \arrow[dl, dotted, "T"] \arrow[rr, "f"] & {} \arrow[u, dotted, "S"] \arrow[d, dotted, "T"] & G' \arrow[ur, dotted, "S"'] \arrow[dr, dotted, "T"] & \\
\mathrm{ModMul}_L(k[G], V) & & {} & & \mathrm{ModMul}_L(k[G'], V) \arrow[llll, "\overline{f}"]
\end{tikzcd}
$$

Let $\rho' : G' \to \mathrm{Aut}(V)$ be a morphism of groups. Let $\mathrm{g} = \sum_g \lambda_g.g \in k[G]$ and $v \in V$:

$$
\begin{aligned}
\left[\left(\tau_G \circ f^*\right)(\rho')\right](\mathbf{g}, v) &= \left[\tau_G\left(\rho' \circ f\right)\right](\mathbf{g}, v) && \text{by definition of } f^* \\
&= \ell_{\rho' \circ f}(\mathbf{g}, v) && \text{by definition of } \tau_G \\
\left[\left(\tau_G \circ f^*\right)(\rho')\right](\mathbf{g}, v) &= \sum_g \lambda_g\left[(\rho' \circ f)(g)(v)\right] && \text{by definition of } \ell_{\rho' \circ f}
\end{aligned}
$$

$$
\begin{aligned}
\left[\left(\overline{f} \circ \tau_{G'}\right)(\rho')\right](\mathbf{g}, v) &= \left[\overline{f}\left(\ell_{\rho'}\right)\right](\mathbf{g}, v) && \text{by definition of } \tau_{G'} \\
&= \ell_{\rho'}\left(\sum_g \lambda_g.f(g), v\right) && \text{by definition of } \overline{f}\left(\ell_{\rho'}\right) \\
&= \sum_g \lambda_g\left[(\rho'(f(g)))(v)\right] && \text{by definition of } \ell_{\rho'} \\
\left[\left(\overline{f} \circ \tau_{G'}\right)(\rho')\right](\mathbf{g}, v) &= \sum_g \lambda_g\left[(\rho' \circ f)(g)(v)\right]
\end{aligned}
$$

$\Longrightarrow$ $\tau = (\tau_G)_{G \in \mathbf{Groups}}$ is a natural equivalence between S and T in **Sets**.

This is a rather naive approach to the problem. However, it does bring up the fact that there exists a natural isomorphism between notions related to this. Indeed, there is an *adjunction of functors* between the group-algebra construction:

$$\mathbb{K}[-] : \mathbf{Groups} \to \mathbb{K}\text{-}\mathbf{Alg}$$

and the group of units for an algebra:

$$(-)^{\times} : \mathbb{K}\text{-}\mathbf{Alg} \to \mathbf{Groups}.$$

This is indeed almost equivalent to what the previous proof shows because we have essentially proven that there is an natural equivalence between:

$$\mathrm{Hom}_{\mathbf{Groups}}\left(G, \mathrm{Aut}(V)\right)$$

and:

$$\mathrm{Hom}_{k-\mathbf{Alg}}\left(k[G], \mathrm{End}(V)\right).$$

Let us continue with another example of a natural equivalence in categories related to modules.

Consider the category ${}_R\mathbf{Mod}^*$:

- whose objects are non-empty families $(B_i)_{i\in I}$ of left R-modules and
- whose morphisms σ between two non-empty families $(B_i)_{i\in I}$ and $(C_j)_{j\in J}$ of left R-modules consist of a function $\sigma : I \to J$ and a family $\left(\sigma_{i,\sigma(i)} : B_i \to C_{\sigma(i)}\right)_{i\in I}$ of left R-maps and
- whose composition between $\sigma : I \to J$ and $\sigma' : J \to I'$ is defined as $\sigma'' := \sigma' \circ \sigma$.

Let R be a ring and B be a left R-module.

Consider the contravariant functor $S_B : {}_R\mathbf{Mod}^* \to {}_{Z(R)}\mathbf{Mod}$ such that:

- an object $(A_i)_{i\in I}$ is mapped to the left $Z(R)$-module $\mathrm{Hom}\left(\bigoplus_{i\in I} A_i, B\right)$
- a morphism $\sigma : (A_i)_{i\in I} \to (D_j)_{j\in J}$ is mapped to the morphism $\sigma^* : \mathrm{Hom}\left(\bigoplus_{j\in J} D_j, B\right) \to \mathrm{Hom}\left(\bigoplus_{i\in I} A_i, B\right)$ defined such that if $f : \bigoplus_{j\in J} D_j \to B$ is a left R-map then:

$$\begin{aligned} \sigma^*(f) \colon \bigoplus_{i\in I} A_i &\to B \\ (a_i)_{i\in I} &\mapsto f\left(\left(\sum_{i\in\sigma^{-1}(j)} \sigma_{i,j}(a_i)\right)_{j\in J}\right) \end{aligned}$$

Consider now the contravariant functor $T_B : {}_R\mathbf{Mod}^* \to {}_{Z(R)}\mathbf{Mod}$ such that:

- an object $(A_i)_{i\in I}$ is mapped to the left $Z(R)$-module $\prod_{i\in I} \mathrm{Hom}\left(A_i, B\right)$
- a morphism $\sigma : (A_i)_{i\in I} \to (D_j)_{j\in J}$ is mapped to the morphism $\overline{\sigma} : \prod_{j\in J} \mathrm{Hom}\left(D_j, B\right) \to \prod_{i\in I} \mathrm{Hom}\left(A_i, B\right)$ such that if $\left(f_j : D_j \to B\right)_{j\in J}$ is a family of left R-maps then we associate to it the family $\left(g_i : A_i \to B\right)_{i\in I}$ such that for any $i \in I$, we have:

$$\begin{aligned} g_i \colon A_i &\to B \\ a_i &\mapsto g_i(a_i) := (f_{\sigma(i)} \circ \sigma_{i,\sigma(i)})(a_i) \end{aligned}$$

Example 2.1.3.4

Let R be a ring.
Consider $\tau = (\tau_{\mathfrak{a}})_{\mathfrak{a}\in {}_R\mathbf{Mod}^*}$ the family of morphisms in ${}_{Z(R)}\mathbf{Mod}$ such that:

$$\forall \mathfrak{a} = (A_i)_{i\in I} \in {}_R\mathbf{Mod}^*, \quad \begin{aligned} \tau_{\mathfrak{a}} \colon \mathrm{Hom}\left(\bigoplus_{i\in I} A_i, B\right) &\to \prod_{i\in I} \mathrm{Hom}\left(A_i, B\right) \\ f &\mapsto (f\alpha_i)_{i\in I} \end{aligned}$$

where $\alpha_i : A_i \to \bigoplus_{i'\in I} A_{i'}$ is the usual injection and $f\alpha_i := f \circ \alpha_i$.s
Then, τ is a natural equivalence between S_B and T_B, *i.e.*

$$\begin{tikzcd}
\mathrm{Hom}\left(\bigoplus_{i\in I} A_i, B\right) \arrow[dd, hook, two heads, "\tau_{\mathfrak{a}}"'] & & & \mathrm{Hom}\left(\bigoplus_{j\in J} D_j, B\right) \arrow[lll, "\sigma^*"'] \arrow[dd, hook, two heads, "\tau_{\mathfrak{d}}"] \\
& \mathfrak{a} = (A_i)_{i\in I} \arrow[ul, dotted, mapsto, "S_B"'] \arrow[dl, dotted, mapsto, "T_B"] \arrow[r, "\sigma"] & \mathfrak{d} = (D_j)_{j\in J} \arrow[ur, dotted, mapsto, "S_B"] \arrow[dr, dotted, mapsto, "T_B"'] & \\
\prod_{i\in I} \mathrm{Hom}(A_i, B) & & & \prod_{j\in J} \mathrm{Hom}(D_j, B) \arrow[lll, "\overline{\sigma}"]
\end{tikzcd}$$

Proof. First prove that for any $\mathfrak{a} = (A_i)_{i\in I} \in {}_R\mathbf{Mod}^*$, $\tau_{\mathfrak{a}}$ is a $Z(R)$-isomorphism.

For any $f, g \in \mathrm{Hom}\left(\bigoplus_{i\in I} A_i, B\right)$ and $r \in Z(R)$ we have:

$$\begin{aligned}
\tau_{\mathfrak{a}}(f + rg) &= ((f + rg)\alpha_i)_{i\in I} \\
&= ((f\alpha_i) + ((rg)\alpha_i))_{i\in I} && \text{by distributivity of composition over addition} \\
&= ((f\alpha_i) + r(g\alpha_i))_{i\in I} && \text{by homogeneity} \\
&= (f\alpha_i)_{i\in I} + r\,(g\alpha_i)_{i\in I} && \text{by definition in the product of } Z(R)\text{-modules} \\
\tau_{\mathfrak{a}}(f + rg) &= \tau_{\mathfrak{a}}(f) + r\tau_{\mathfrak{a}}(g)
\end{aligned}$$

Hence, $\tau_{\mathfrak{a}}$ is a left $Z(R)$-map.

Let $(f_i)_{i\in I} \in \prod_{i\in I} \mathrm{Hom}\,(A_i, B)$. Define the map:

$$\begin{aligned}
f \colon \textstyle\bigoplus_{i\in I} A_i &\to B \\
(a_i)_{i\in I} &\mapsto \textstyle\sum_{i\in I} f_i(a_i)
\end{aligned}$$

It is well defined because the family $(a_i)_{i\in I}$ is of finite support and $f_i(0) = 0$. It is evidently a left R-map for f_i are left R-maps. It is trivial to notice that for any $i \in I$, $f \circ \alpha_i = f_i$. Therefore, $\tau_{\mathfrak{a}}$ is surjective.

Take $f, g \in \mathrm{Hom}\left(\bigoplus_{i\in I} A_i, B\right)$. Assume that for any $i \in I$, we have $f\alpha_i = g\alpha_i$. This means f and g agree on every element of the form $a^{(i_0)} := (a_i)_{i\in I}$ where $a_i = 0, \forall i \in I \setminus \{i_0\}$, for any $i_0 \in I$. Since every element of $\bigoplus_{i\in I} A_i$ is a finite sum of such elements, then because f and g are left R-maps, it follows that f and g agree on all elements of $\bigoplus_{i\in I} A_i$, *i.e.* $f = g$. So $\tau_{\mathfrak{a}}$ is injective.

Let us now proceed to show that τ is natural. Let $\mathfrak{a} = (A_i)_{i\in I}$ and $\mathfrak{d} = (D_j)_{j\in J}$ in ${}_R\mathbf{Mod}^*$. Let $\sigma : \mathfrak{a} \to \mathfrak{d}$ be a morphism, *i.e.* we have $\sigma : I \to J$ and a family $\left(\sigma_{i,\sigma(i)} : A_i \to D_{\sigma(i)}\right)_{i\in I}$ of left R-maps. Show that the diagram commutes.

Let $f : \bigoplus_{j\in J} D_j \to B$ be a left R-map. The goal is to show that for any $i \in I$:

$$((\tau_{\mathfrak{a}} \circ \sigma^*)(f))_i = ((\overline{\sigma} \circ \tau_{\mathfrak{d}})(f))_i$$

We will denote:

- for any $i \in I$, $p_i : \bigoplus_{i'\in I} A_{i'} \to A_i$ the usual projection.
- for any $j \in J$, $q_j : \bigoplus_{j'\in J} D_{j'} \to D_j$ the usual projection.
- for any $i \in I$, $\alpha_i : A_i \to \bigoplus_{i'\in I} A_{i'}$ the usual injection.
- for any $j \in J$, $\beta_j : D_j \to \bigoplus_{j'\in J} D_{j'}$ the usual injection.

Let $i \in I$.

- Counterclockwise, we have:

$$\begin{aligned}((\tau_{\mathfrak{a}} \circ \sigma^*)(f))_i &= (\tau_{\mathfrak{a}}\left[\sigma^*(f)\right])_i \\ &= \left(\tau_{\mathfrak{a}}\left[f \circ \beta_{\sigma(i)} \circ \sigma_{i,\sigma(i)} \circ p_i\right]\right)_i \\ &= f \circ \beta_{\sigma(i)} \circ \sigma_{i,\sigma(i)} \circ p_i \circ \alpha_i \\ ((\tau_{\mathfrak{a}} \circ \sigma^*)(f))_i &= f \circ \beta_{\sigma(i)} \circ \sigma_{i,\sigma(i)}\end{aligned}$$

- Clockwise, we get:

$$\begin{aligned}((\overline{\sigma} \circ \tau_{\mathfrak{d}})(f))_i &= (\overline{\sigma}\left[\tau_{\mathfrak{d}}(f)\right])_i \\ &= \left(\overline{\sigma}\left[(f \circ \beta_j)_{j \in J}\right]\right)_i \\ ((\overline{\sigma} \circ \tau_{\mathfrak{d}})(f))_i &= f \circ \beta_{\sigma(i)} \circ \sigma_{i,\sigma(i)}\end{aligned}$$

This concludes the proof that τ is a natural equivalence between S_B and T_B. □

Similarly, we give the following example of a natural equivalence whose proof is similar to the previous.

Let A be a left R-module.

Consider the functor $S_A : {}_R\mathbf{Mod}^* \to {}_{Z(R)}\mathbf{Mod}$ such that:

- an object $(B_i)_{i \in I}$ is mapped to the left $Z(R)$-module $\operatorname{Hom}\left(A, \prod_{i \in I} B_i\right)$
- a morphism $\sigma : (B_i)_{i \in I} \to (C_j)_{j \in J}$ is mapped to the morphism $\sigma_* : \operatorname{Hom}\left(A, \prod_{i \in I} B_i\right) \to \operatorname{Hom}\left(A, \prod_{j \in J} C_j\right)$

defined such that if $f : A \to \prod_{i \in I} B_i$ is a left R-map then:

$$\begin{aligned}\sigma_*(f) \colon A &\to \textstyle\prod_{j \in J} C_j \\ a &\mapsto \left(\textstyle\sum_{i \in \sigma^{-1}(j)} (\sigma_{i,j} p_i f)(a)\right)_{j \in J}\end{aligned}$$

Consider now the functor $T_A : {}_R\mathbf{Mod}^* \to {}_{Z(R)}\mathbf{Mod}$ such that:

- an object $(B_i)_{i \in I}$ is mapped to the left $Z(R)$-module $\prod_{i \in I} \operatorname{Hom}(A, B_i)$
- a morphism $\sigma : (B_i)_{i \in I} \to (C_j)_{j \in J}$ is mapped to the morphism $\tilde{\sigma} : \prod_{i \in I} \operatorname{Hom}(A, B_i) \to \prod_{j \in J} \operatorname{Hom}(A, C_j)$

defined such that if $\left(f_i : A \to B_i\right)_{i \in I}$ is a family of left R-maps then we associate to it the family $\left(g_j : A \to C_j\right)_{j \in J}$ such that for any $j \in J$ we have:

$$\begin{aligned}g_j \colon A &\to C_j \\ a &\mapsto g_j(a) := \textstyle\sum_{i \in \sigma^{-1}(j)} (\sigma_{i,j} f_i)(a)\end{aligned}$$

Example 2.1.3.5

Let R be a ring.

Consider $\tau = (\tau_{\mathfrak{b}})_{\mathfrak{b} \in {}_R\mathbf{Mod}^*}$ the family of morphisms in ${}_{Z(R)}\mathbf{Mod}$ such that:

$$\forall \mathfrak{b} = (B_i)_{i \in I} \in {}_R\mathbf{Mod}^*, \quad \begin{aligned}\tau_{\mathfrak{b}} \colon \operatorname{Hom}\left(A, \textstyle\prod_{i \in I} B_i\right) &\to \textstyle\prod_{i \in I} \operatorname{Hom}(A, B_i) \\ f &\mapsto (p_i f)_{i \in I}\end{aligned}$$

where $p_i : \prod_{i' \in I} A_{i'} \to A_i$ is the usual projection.

Then, τ is a natural equivalence between S_A and T_A, *i.e.*

$$\begin{tikzcd}
\mathrm{Hom}\left(A,\prod_{i\in I}B_i\right) \arrow[rrr, "\sigma_*"] \arrow[d, hook, two heads, "\tau_{\mathfrak{b}}"'] & & & \mathrm{Hom}\left(A,\prod_{j\in J}C_j\right) \arrow[d, hook, two heads, "\tau_{\mathfrak{c}}"] \\
 & \mathfrak{b}=(B_i)_{i\in I} \arrow[ul, dotted, mapsto, "S_A"'] \arrow[dl, dotted, mapsto, "T_A"] \arrow[r, "\sigma"] & \mathfrak{c}=(C_j)_{j\in J} \arrow[ur, dotted, mapsto, "S_A"] \arrow[dr, dotted, mapsto, "T_A"'] & \\
\prod_{i\in I}\mathrm{Hom}(A,B_i) \arrow[rrr, "\tilde{\sigma}"'] & & & \prod_{j\in J}\mathrm{Hom}(A,C_j)
\end{tikzcd}$$

These two examples establish the equivalence between:

- Giving a map from a direct sum is like giving a family of maps from each summand of the direct sum.
- Giving a map to a direct product is like giving a family of maps to each factor of the direct product.

2.2 Abelian categories

2.2.1 Pre-additive and additive categories

Definition 2.2.1.1 : Pre-additive category

A category $\mathcal{C}$ is called *preadditive* if, for every $A, B \in \mathcal{C}$ the hom-set $\mathrm{Hom}_{\mathcal{C}}(A, B)$ has a structure of (additive) abelian group such that composition is bilinear:

$$\forall A, B, C \in \mathcal{C}, \quad \forall f, g \in \mathrm{Hom}_{\mathcal{C}}(A, B), \quad \forall h, k \in \mathrm{Hom}_{\mathcal{C}}(B, C),$$
$$h \circ (f + g) = h \circ f + h \circ g \ \wedge \ (h + k) \circ f = h \circ f + k \circ f.$$

Example 2.2.1.2

If R is a ring, then the category ${}_R\mathbf{Mod}$ of left R-modules is pre-additive. Indeed, according to Proposition 1.1.2.12, the hom-sets $\mathrm{Hom}_R(A, B)$ are equipped with a structure of ablelian groups. One can routinely verify that composition is then bilinear.

Definition 2.2.1.3 : Additive functor

Let $\mathcal{C}$ and $\mathcal{D}$ be two pre-additive categories.
A functor $T : \mathcal{C} \to \mathcal{D}$ is said to be *additive* if the maps $\mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(T(A), T(B))$ are actually group-homomorphisms with respect to the additive abelian group structure on the hom-sets.

Example 2.2.1.4

If R is any ring, then the tensor products functors on the category of R-modules and the Hom functors on that same category are additive.

Proposition 2.2.1.5

Let $\mathcal{C}$ be a pre-additive category.
Any finite product in $\mathcal{C}$ is also a finite coproduct. We call them *biproducts*.

Definition 2.2.1.6 : Initial object

Let $\mathcal{C}$ be a category.
An object $I \in \mathcal{C}$ is said to be *initial* if for every object $A \in \mathcal{C}$ there exists a unique morphism from I to A. All initial objects are therefore isomorphic.

Definition 2.2.1.7 : Terminal object

Let $\mathcal{C}$ be a category.
An object $T \in \mathcal{C}$ is said to be *terminal* if for every object $A \in \mathcal{C}$ there exists a unique morphism from A to T. All terminal objects are therefore isomorphic.

Definition 2.2.1.8 : Zero object

Let $\mathcal{C}$ be a category.
An object $Z \in \mathcal{C}$ is called a *zero object* if it is both initial and terminal. Then, between every two objects A and B in $\mathcal{C}$ there exists a morphism called the *zero morphism* $A \to Z \to B$.

Definition 2.2.1.9 : Additive category

A category $\mathcal{C}$ is said to be *additive* if it is pre-additive, it has a zero object and every finite biproduct exist.

Example 2.2.1.10

If R is a ring, the categories ${}_R\mathbf{Mod}$ and $\mathbf{Mod}_R$ are additive. Their zero object is the trivial module (Example 1.1.1.14) and their finite biproduct is the finite direct sum (which coincides with the finite direct product).

Proposition 2.2.1.11

Let $\mathcal{C}$ and $\mathcal{D}$ be additive categories. Let $T : \mathcal{C} \to \mathcal{D}$ be a functor.
Then: T is additive if, and only if, T preserves all biproduct diagrams (*i.e.* biproducts are sent on biproducts and injections/projections are sent to injections/projections).

2.2.2 Pre-abelian and abelian categories

Definition 2.2.2.1 : Equaliser

Let $\mathcal{C}$ be a category. Let $X, Y \in \mathcal{C}$ and $f, g \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$.
The *equaliser* of f and g consists of an object $E \in \mathcal{C}$ and a morphism $\mathrm{eq} \in \mathrm{Hom}_{\mathcal{C}}(E, X)$ such that:

- $f \circ \mathrm{eq} = g \circ \mathrm{eq}$,
- for any object $O \in \mathcal{C}$ and morphism $m \in \mathrm{Hom}_{\mathcal{C}}(O, X)$ with $f \circ m = g \circ m$ there exists a unique morphism $u \in \mathrm{Hom}_{\mathcal{C}}(O, E)$ such that $m = \mathrm{eq} \circ u$.

$$\begin{tikzcd} E \arrow[r, "\mathrm{eq}"] & X \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & Y \\ O \arrow[u, dashed, "u"] \arrow[ur, "m"'] & & \end{tikzcd}$$

The dual definition is called *coequaliser*.

Definition 2.2.2.2 : Kernel, Cokernel

Let $\mathcal{C}$ be a category with a zero object. Let $X, Y \in \mathcal{C}$ and $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$.
The *kernel* (resp. *cokernel*) of f is the equaliser (resp. *coequaliser*) between f and the zero morphism between X and Y.

Definition 2.2.2.3 : Pre-abelian category

A category $\mathcal{C}$ is called *pre-abelian* if it is additive and the kernel, as well as the cokernel, of every morphism in $\mathcal{C}$ exist in $\mathcal{C}$.

Example 2.2.2.4

If R is any ring, the categories ${}_R\mathbf{Mod}$ and $\mathbf{Mod}_R$ are pre-abelian. The kernel (resp. cokernel) of f is given by $\ker(f)$ (resp. $\mathrm{coker}(f)$) (Definition 1.1.2.3) together with the canonical injection from $\ker(f)$ (resp. the canonical projection onto $\mathrm{coker}(f)$).

Definition 2.2.2.5 : Left- and right-exact functors

Let $\mathcal{C}$ and $\mathcal{D}$ be pre-abelian categories.
A functor $T : \mathcal{C} \to \mathcal{D}$ is called *left-exact* (resp. *right-exact*) if it is additive and it preserves all kernels (resp. all cokernels).

Example 2.2.2.6

Let us place ourselves once again in the category of R-modules where R is a ring. Then the covariant and contravariant Hom functor are left-exact and the tensor product functors are right-exact.

Definition 2.2.2.7 : Monomorphism and epimorphism

Let $\mathcal{C}$ be a category.
A morphism $f \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ is called a *monomorphism* (resp. *epimorphism*) if it is left-cancellable (resp. right-cancellable) that is to say, for any $g_1, g_2 \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ (resp. $h_1, h_2 \in \mathrm{Hom}_{\mathcal{C}}(C, D)$) we have:

$$f \circ g_1 = f \circ g_2 \;\Rightarrow\; g_1 = g_2,$$

$$h_1 \circ f = h_2 \circ f \;\Rightarrow\; h_1 = h_2.$$

Definition 2.2.2.8 : Abelian category

A category $\mathcal{C}$ is said to be *abelian* if it is pre-abelian and every monomorphism is a kernel of some morphism and every epimorphism is a cokernel of some morphism.

Example 2.2.2.9

For any ring R, the categories ${}_R\mathbf{Mod}$ and $\mathbf{Mod}_R$ are abelian. The monomorphisms (resp. epimorphisms) are exactly the R-linear maps that are injective (resp. surjective).

Chapter 3

Elements of homological algebra

Homology theory originated from the field of algebraic topology at the end of the XIX'th century. It was in particular used to study the concept of "holes" inside topological spaces. The area extended as time went on. Practices first seen in algebraic topology make appearances in algebra. A few different homology theories in algebra arose during the first half of the XX'th century: namely, the cohomology of groups, the cohomology of associative algebras and the cohomology of Lie algebras. To unify those theories, Cartan and Eilenberg introduced the concept of projective modules together with the use of derived functors in their 1956 book [CE56], named *Homological Algebra* that marks the birth of the discipline of the same name.

For a complete account on the history of homological algebra, see [Wei99].

The standard references for studying homological algebra are [Rot09, HS97, Wei94, ML95].

3.1 Modern homological algebra

3.1.1 Chain complexes

Definition 3.1.1.1 : Chain complex

Let $\mathcal{A}$ be an abelian category.
A *chain complex* $(C., d.)$ in $\mathcal{A}$ is any family indexed by $\mathbb{Z}$ of morphisms called *differentials*:

$$\cdots \to C_{n+1} \overset{d_{n+1}}{\to} C_n \overset{d_n}{\to} C_{n-1} \to \cdots$$

such that for any $n \in \mathbb{Z}$ we have $d_n d_{n+1} = 0$ (the zero morphism).

Remark 3.1.1.2

In the abelian category $\mathcal{A} = {}_R\mathbf{Mod}$ where R is a ring, saying that $d_n d_{n+1} = 0$ is equivalent to saying that $\mathrm{im}(d_{n+1}) \subseteq \ker(d_n)$. Hence, it follows that exact sequences (Definition 1.1.3.1) are chain complexes.

Proposition 3.1.1.3

Let $\mathcal{A}$ and $\mathcal{A}'$ be abelian categories. Let $F : \mathcal{A} \to \mathcal{A}'$ be an additive functor.
If $(C., d.)$ is a chain complex in $\mathcal{C}$, then $(FC., Fd.) := (FC_n, Fd_n)_{n\in\mathbb{Z}}$ is a chain complex in $\mathcal{A}'$.

Definition 3.1.1.4 : Homology of a complex

Let $\mathcal{A}$ be an abelian category. Let $\mathbf{C} := (C_\cdot, d_\cdot)$ be a chain complex in $\mathcal{A}$.
For every $n \in \mathbb{Z}$, define the set of *n-chains* as C_n, the set of *n-cycles* as $Z_n(\mathbf{C}) := \ker(d_n)$ and the set of *n-boundaries* as $B_n(\mathbf{C}) := \operatorname{im}(d_{n+1})$.
The n'th *homology* of $\mathbf{C}$ if defined as:

$$H_n(\mathbf{C}) := {}^{Z_n(\mathbf{C})}/_{B_n(\mathbf{C})}.$$

3.1.2 Chain maps

Definition 3.1.2.1 : Chain map

Let $\mathcal{A}$ be an abelian category. Let $(C_\cdot, d_\cdot)$ and $(C'_\cdot, d'_\cdot)$ be chain complexes in $\mathcal{A}$.
A *chain map* f between $(C_\cdot, d_\cdot)$ and $(C'_\cdot, d'_\cdot)$ is any sequence of morphisms $\left(f_n : C_n \to C'_n\right)_{n\in\mathbb{Z}}$ in $\mathcal{A}$ such that for all $n \in \mathbb{Z}$, we have $d'_n \circ f_n = f_{n-1} \circ d_n$.

$$\begin{tikzcd}
\cdots \arrow[r] & C_{n+1} \arrow[r, "d_{n+1}"] \arrow[d, "f_{n+1}"] & C_n \arrow[r, "d_n"] \arrow[d, "f_n"] & C_{n-1} \arrow[r] \arrow[d, "f_{n-1}"] & \cdots \\
\cdots \arrow[r] & C'_{n+1} \arrow[r, "d'_{n+1}"] & C'_n \arrow[r, "d'_n"] & C'_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

Remark 3.1.2.2

Chain maps can be composed in an obvious way, namely, a chain map f from $(C_\cdot, d_\cdot)$ to $(C'_\cdot, d'_\cdot)$ and a chain map g from $(C'_\cdot, d'_\cdot)$ to $(C''_\cdot, d'_\cdot)$ define:

$$g \circ f := (g_n \circ f_n)_{n\in\mathbb{Z}}\,.$$

It actually follows that, for any abelian category, the chain complexes in $\mathcal{A}$ together with chain maps between them and their composition form a category, denoted $\mathbf{Comp}(\mathcal{A})$.

Proposition 3.1.2.3

If $\mathcal{A}$ is an abelian category, then $\mathbf{Comp}(\mathcal{A})$ is an abelian category.

Proof. See [Rot09, Proposition 5.100]. □

Proposition 3.1.2.4

If $\mathcal{A}$ is an abelian category, then we can define an induced map from chain maps in such a way that $H_n : \mathbf{Comp}(\mathcal{A}) \to \mathcal{A}$ is an additive functor for each $n \in \mathbb{Z}$.

Proof. See [Rot09, Proposition 6.8].
The functor's action on morphisms is defined as follows:

$$\begin{aligned} H_n(f) : H_n(\mathbf{C}) &\to H_n(\mathbf{C}') \\ \operatorname{cls}(z_n) &\mapsto \operatorname{cls}(f_n z_n) \end{aligned}\quad.$$

□

3.1.3 Homotopy

Definition 3.1.3.1 : Homotopy between chain maps

Let $\mathcal{A}$ be an abelian category. Let $(C_., d_.)$ and $(C'_., d'_.)$ be chain complexes in $\mathcal{A}$.
Two chains maps $f, g : (C_., d_.) \to (C'_., d'_.)$ are said to be *homotopic* if for all $n \in \mathbb{Z}$ there exists a morphism $s_n : C_n \to C'_{n+1}$ such that:

$$f_n - g_n = d'_{n+1} s_n + s_{n-1} d_n.$$

In which case, we write $f \simeq g$. We say that f is *null-homotopic* if $f \simeq 0$ where 0 is the zero morphism.

Theorem 3.1.3.2

Let $\mathcal{A}$ be an abelian category. Let $\mathbf{C} := (C_., d_.)$ and $\mathbf{C}' := (C'_., d'_.)$ be chain complexes in $\mathcal{A}$.
Let f and g be chain maps between $(C_., d_.)$ and $(C'_., d'_.)$.
If $f \simeq g$, then for all $n \in \mathbb{Z}$ the induced maps $H_n(f)$ and $H_n(g)$ are equal.

Proof. Let $z \in Z_n$ be an n-cycle. Hence, we have by homotopy:

$$f_n z - g_n z = d'_{n+1} s_n z + s_{n-1} d_n z = d'_{n+1} s_n z$$

since by definition of z, we have $d_n z = 0$.
It follows that $f_n z - g_n z \in B_n(\mathbf{C}')$ from which we deduce $H_n(f) = H_n(g)$. □

Definition 3.1.3.3 : Contracting homotopy

Let $\mathcal{A}$ be an abelian category.
A chain complex $\mathbf{C} = (C_., d_.)$ in $\mathcal{A}$ is said to have a *contracting homotopy* if the identity morphism $1_{\mathbf{C}}$ is null-homotopic.
In other words, for every $n \in \mathbb{Z}$ there exists a morphism $s_n : C_n \to C_{n+1}$ such that:

$$d_{n+1} s_n + s_{n-1} d_n = 1_{C_n}.$$

Proposition 3.1.3.4

Let $\mathcal{A}$ be an abelian category. Let $\mathbf{C}$ be a chain complex in $\mathcal{A}$.
If $\mathbf{C}$ has a contracting homotopy, then it is *acyclic*, that is to say:

$$\forall n \in \mathbb{Z}, \quad H_n(\mathbf{C}) = 0.$$

3.1.4 Resolutions

The notions of projective and injective modules extend to any abelian category.

Definition 3.1.4.1 : Projective and injective objects

Let $\mathcal{A}$ be an abelian category.
An object P is *projective* if for every epimorphism $p : A \to B$ and any morphism $f : P \to B$ there exists a morphism $g : P \to A$ such that $f = p \circ g$.

$$\begin{tikzcd} & P \arrow[dl, dashed, "g"'] \arrow[d, "f"] \\ A \arrow[r, two heads, "p"'] & B \end{tikzcd}$$

The dual definition by reversing arrows and considering monomorphisms instead of epimorphisms yield the notion of injective object.

Definition 3.1.4.2 : Projective resolution

Let $\mathcal{A}$ be an abelian category. Let $A \in \mathcal{A}$ be an object.
A *projective resolution* of A in the category $\mathcal{A}$ is an exact sequence:

$$\mathbf{P} := \cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} A \to 0$$

where each P_n is projective in $\mathcal{A}$.

Definition 3.1.4.3 : Deleted projective resolution

Let $\mathcal{A}$ be an abelian category. Let $A \in \mathcal{A}$.
A *deleted projective resolution* of a projective resolution $\mathbf{P}$ of A is the complex:

$$\mathbf{P}_A := \cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to 0.$$

Giving a projective resolution is equivalent to giving a deleted projective resolution since we can recover A by computing $\operatorname{coker}(d_1)$.

Proposition 3.1.4.4

Let $\mathcal{A}$ be an abelian category.
If $\mathcal{A}$ has *enough projectives* ($\forall A \in \mathcal{A}$, there exists a projective P and an epimorphism from P to A), then every object in $\mathcal{A}$ has a projective resolution.

Proof. See [Rot09, Corollary 6.3]. □

Remark 3.1.4.5

In the category ${}_R\mathbf{Mod}$ where R is a ring, the projectives are the projective modules (Definition 1.1.7.4) and the category "has enough projectives". Free modules are projective modules. For any left R-module M, we can actually construct a *free resolution* of M, by an iterative process on taking presentations on free modules.

Definition 3.1.4.6 : Injective resolution

Let $\mathcal{A}$ be an abelian category. Let $A \in \mathcal{A}$ be an object.
An *injective resolution* of A in the category $\mathcal{A}$ is an exact sequence:

$$\mathbf{E} := 0 \to A \xrightarrow{\eta} E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} E^2 \to \cdots$$

where each E^n is injective in $\mathcal{A}$.

Definition 3.1.4.7 : Deleted injective resolution

Let $\mathcal{A}$ be an abelian category. Let $A \in \mathcal{A}$.
A *deleted injective resolution* of an injective resolution $\mathbf{E}$ of A is the complex:

$$\mathbf{E}^A := 0 \to E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} E^2 \to \cdots .$$

Once again, having a deleted injective resolution instead of its injective resolution does not lose information since we can recover A by computing $\ker(d^0)$.

The dual statement of Proposition 3.1.4.4 is also true, *i.e.* every object has an injective resolution when the abelian category has enough injectives. For instance, the category ${}_R\mathbf{Mod}$ for any ring R has enough injectives.

3.2 Derived functors

3.2.1 Left-derived functors and Tor

Theorem 3.2.1.1 : (Comparison theorem)

Let $\mathcal{A}$ be an abelian category. Let $f : A \to A'$ be a morphism in $\mathcal{A}$.
Consider the diagram:

$$\begin{tikzcd}
\cdots \arrow[r] & P_2 \arrow[r, "d_2"] \arrow[d, dashed, "\hat{f}_2"] & P_1 \arrow[r, "d_1"] \arrow[d, dashed, "\hat{f}_1"] & P_0 \arrow[r, "\varepsilon"] \arrow[d, dashed, "\hat{f}_0"] & A \arrow[r] \arrow[d, "f"] & 0 \\
\cdots \arrow[r] & P_2' \arrow[r, "d_2'"] & P_1' \arrow[r, "d_1'"] & P_0' \arrow[r, "\varepsilon'"] & A \arrow[r] & 0
\end{tikzcd}$$

where the rows are chain complexes.
If the P_i in the top row are projective and if the bottom row is exact, then there exists a chain map $\hat{f}$ between the chain complexes after removing A and A' such that the diagram commutes and such that $f \circ \varepsilon = \varepsilon' \circ f_0$. Moreover, any two such chain maps are homotopic.

Let us define the notion of *left-derived functors*.

Let $T : \mathcal{A} \to \mathcal{C}$ be a covariant functor between abelian categories. We assume that $\mathcal{A}$ has enough projectives.

For now, for every object $A \in \mathcal{A}$, fix a projective resolution $\mathbf{P}$. Define:

$$\forall n \in \mathbb{Z}, \quad (L_n T)A := H_n(T\mathbf{P}_A)$$

where $\mathbf{P}_A$ is the deleted projective resolution associated with the fixed projective resolution $\mathbf{P}$ for A.

Now, for a morphism $f : A \to A'$ in $\mathcal{A}$, define:

$$\forall n \in \mathbb{Z}, \quad (L_n T)f := H_n(T\hat{f})$$

where $\hat{f} : \mathbf{P}_A \to \mathbf{P}'_{A'}$ is a chain map obtained from the Comparison theorem (Theorem 3.2.1.1) for f with $\mathbf{P}_A$ (resp. $\mathbf{P}'_{A'}$) the deleted projective resolution associated to the fixed projective resolution for A (resp. for A').

Explicitly, we have $(L_nT)f : z + \mathrm{im}(Td_{n+1}) \mapsto (T\hat{f}_n)z + \mathrm{im}(Td'_{n+1})$.

Theorem 3.2.1.2 : (Left-derived functors)

Let $\mathcal{A}$ and $\mathcal{C}$ two abelian categories. Let $T : \mathcal{A} \to \mathcal{C}$ be an additive covariant functor.
If $\mathcal{A}$ has enough projectives, then, for every $n \in \mathbb{Z}$, $(L_n)T : \mathcal{A} \to \mathcal{C}$ is an additive covariant functor. The family $(L_nT)_{n\in\mathbb{Z}}$ is called the family of *left-derived functors* of T.

Proof. The well-definedness of the functor on morphism follows from the Comparison theorem, since it states that the chain map $\hat{f}$ we picked is unique up to homotopy, and therefore taking another one yields the same induced map once we take the map through the homology functor. The rest just follows from the fact that H_n is an additive covariant functor. □

Proposition 3.2.1.3

Let $\mathcal{A}$ and $\mathcal{C}$ be abelian categories. Let $T : \mathcal{A} \to \mathcal{C}$ be an additive covariant functor.
Suppose $\mathcal{A}$ has enough projectives. Construct a new family of left-derived functors $(\tilde{L_n}T)$ of T by fixing a new projective resolution for every object $A \in \mathcal{A}$.
Then, for every $n \in \mathbb{Z}$, the functors L_nT and $\tilde{L_n}T$ are naturally isomorphic.
In particular, for all object $A \in \mathcal{A}$, the objects $(L_nT)A$ are independent of the choice of projective resolution for A.

Proof. See [Rot09, Proposition 6.20]. □

Let us now introduce the main left-derived functors in the category ${}_R\mathbf{Mod}$.

Definition 3.2.1.4 : Tor functors

Let R be a ring. Let A be a right R-module.
The left-derived functors of the additive covariant functor $A \otimes_R -$ are denoted $\mathrm{Tor}_n^R(A, -)$, and called Tor functors.
Similarly, if B is a left R-module, the left-derived functors of the additive covariant functor $- \otimes_R B$ are denoted $\mathrm{Tor}_n^R(-, B)$.

The notation is the same for the two functors because, according to [Rot09, Theorem 6.32], the abelian groups constructed from $\mathrm{Tor}_n^R(A, -)$ and $\mathrm{Tor}_n^R(-, B)$ respectively applied to B and A are isomorphic, for any $n \in \mathbb{Z}$.

3.2.2 Right-derived functors and Ext

There is an analogous procedure to construct right-derived functors of a covariant additive functor: instead of projective resolutions, one has to fix injective resolutions, then take homology of the deleted injective resolution through the functor and finally, since the dual statement of the Comparison theorem (Theorem 3.2.1.1) is also true, define the right-derived functors on morphisms by using the chain map whose existence is asserted in the dual of the Comparison theorem.

The right-derived functors of a covariant additive functor T are denoted by R^nT.

Definition 3.2.2.1 : Covariant Ext functors

Let R be a ring. Let A be a left R-module.
The right-derived functors of the additive covariant Hom functor $\mathrm{Hom}_R(A, -)$ are denoted $\mathrm{Ext}_R^n(A, -)$ and called Ext functors.

Now, let us take interest in the right-derived functors of an additive contravariant functor T. By contravariance, a *positive* chain complex (*i.e.* a chain complex $(C_\cdot, d_\cdot)$ for which for every $n < 0$, we have $C_n = 0$) is sent through T to a *negative* chain complex (for all $n > 0$, $C_n = 0$). Hence, one needs to start from a projective resolution of A that will later be sent to a negative chain complex through T.

Here is now how we define the right-derived functors of the additive contravariant functor T:

- For every object $A \in \mathcal{A}$, fix a projective resolution of A.
- Then define, for every object $A \in \mathcal{A}$:

$$(R^n T)A := H^n(T\mathbf{P}_A)$$

where $\mathbf{P}_A$ is the deleted projective resolution associated to the projective resolution fixed for A and $H^n(-)$ is the homology functor on negative chain complexes.

- Finally, for every morphism $f : A \to A'$ in $\mathcal{A}$ define:

$$(R^n T)f := H^n(T\hat{f})$$

where $\hat{f}$ is a chain map (unique up to homotopy) that satisfies the condition of the Comparison theorem (Theorem 3.2.1.1) between the deleted projective resolutions associated with the projective resolutions fixed for A and A'.

The proof of independence of the choice of projective resolutions for the aforementioned right-derived functors can be found in [Rot09, Proposition 6.56].

Definition 3.2.2.2 : Contravariant Ext functors

Let R be a ring. Let B be a left R-module.
The right-derived functors of the additive contravariant Hom functor $\mathrm{Hom}_R(-, B)$ are denoted $\mathrm{Ext}_R^n(-, B)$ and are also called Ext functors.

It is indeed again a result [Rot09, Theorem 6.67] that the abelian groups formed by the functors $\mathrm{Ext}_R^n(-, B)$ and $\mathrm{Ext}_R^n(A, -)$ applied respectively to A and B are isomorphic.

Chapter 4

Anick resolution and Koszul complex

4.1 Anick resolution

When it comes to the homology of associative algebras, one is concerned about the ability of constructing projective or free resolutions that enables the computation of homological invariants such as the $\mathrm{Tor}_n^A(\mathbb{K}, \mathbb{K})$ groups where $\mathbb{K}$ is a field and A an augmented $\mathbb{K}$-algebra. Indeed classification theorems of algebraic structures, for instance, can be enunciated through the lens of such invariants. One such resolution always exists: it is called the *bar resolution* (see [EM53, ML95]). However, it is usually too big of a resolution to be used in practice. Ideally, one would have a *minimal resolution* (see Subsection 4.1.5), but there are no such effective constructions for any associative algebra in general. An alternative has been proposed for augmented algebras A by David J. Anick in 1986 [Ani86]: it consists of a free resolution of the ground field in the category of right A-modules. The n'th module in the resolution is generated by a certain construction called *n-chains* (see Subsection 4.1.2), first introduced by Anick in [Ani85] then reformulated in [Ani86]. The n-chains are built on top of the notion of *obstructions*. As subsequent resources on the matter present it (see for instance [Ufn95, DMR99, Chapter 7]), these obstructions can be understood as the leading monomials of a minimal non-commutative Gröbner basis of the ideal of relations of a given presentation. We refer the reader to the preprint [ML23] (from which some parts in this section are taken) where the relation between the original setting and the interpretation in terms of non-commutative Gröbner bases is explored in details. Efforts towards generalising the pattern behind the Anick resolution and its connections to non-commutative Gröbner bases theory have arisen. See for instance the algorithmic approaches in [GS07] and in [DMR99, Chapter 2] to construct projective resolutions of path algebras using Gröbner bases.

4.1.1 Setting

Let $\mathbb{K}$ be a field and A an augmented associative unitary $\mathbb{K}$-algebra (Definition 1.2.1.5). Denote by $\varepsilon : A \to \mathbb{K}$ the augmentation map and by $\eta : \mathbb{K} \to A$ the unique section of ε satisfying $\eta(1_{\mathbb{K}}) = 1_A$.

Let $\langle X|R\rangle$ be a presentation of A (Definition 1.2.3.2) and $\prec$ be a monomial order on $\langle X\rangle$ (Definition 1.2.2.5). Denote by $I := I(R)$ the ideal of relations and by $O(I) := \langle X\rangle \setminus \mathrm{LM}(I)$. Notice how $O(I)$ depends on chosen the monomial order $\prec$. The elements of the set $O(I)$ are known as *normal words*. Recall from Proposition 1.2.4.11 the decomposition as vector spaces:

$$\mathbb{K}\langle X\rangle = I \oplus \mathbb{K}O(I),$$

where $\mathbb{K}O(I)$ is the vector space spanned by the set of normal words. This is equivalent to saying that ${}^{\mathbb{K}\langle X\rangle}/_{I} \cong \mathbb{K}O(I)$. It follows that A and $\mathbb{K}O(I)$ are isomorphic as vector spaces. We will denote by $\overline{r}$ the image in A of any polynomial $r \in \mathbb{K}\langle X\rangle$ through the canonical projection $\mathbb{K}\langle X\rangle \to {}^{\mathbb{K}\langle X\rangle}/_{I}$ induced by the presentation $\langle X|R\rangle$.

We can suppose that R is a non-commutative Gröbner basis of I with respect to $\prec$ (Definition 1.2.4.4). Indeed, if it is not, we can construct, for instance using the Buchberger procedure ([Mor94, Section 5.4]), a new presentation $\langle X|G\rangle$, that gives the same quotient algebra isomorphic to A, but in which G is a non-commutative Gröbner basis of the ideal of relations with respect to the monomial order $\prec$. This is the case because a non-commutative Gröbner basis of the ideal I (here generated by R) generates that same ideal I.

Moreover, we can assume R to be minimal, or even reduced, as a non-commutative Gröbner basis since we can apply the procedure of reduction presented in Proposition 1.2.4.10.

Remark 4.1.1.1

Note that the set $\mathrm{LM}(R)$ is independent of the choice of the minimal non-commutative Gröbner basis R according to Proposition 1.2.4.8.

Definition 4.1.1.2 : Obstructions

If R is a minimal non-commutative Gröbner basis of the ideal it generates, then call the monomials in $\mathrm{LM}(R)$ *obstructions*. With Remark 4.1.1.1 in mind, denote by $V := \mathrm{LM}(R)$ the set of obstructions.

In the literature, obstructions are also sometimes called *tips* ([Far92, NWW19]).

In terms of rewriting theory over associative algebras [Mal19], the obstructions are exactly the monomials defining the rewriting rules. Thus, they are exactly the elements from which the *critical branchings* [Mal19] arise. We will now define a subset of those critical branchings, called the *n-chains*.

4.1.2 n-chains

The concept of n-chains can be defined in several ways:

- the definition in terms of *tails* as in [Ani85, Mal19, Far92],
- the definition in terms of a *graph* as in [Ufn95, NWW19],
- the definition in terms of *obstructions* as in [Ani86].

It has be shown in the preprint [ML23, Proposition 2.6] that the definition in terms of obstructions and in terms of a graph are equivalent. We will show in Proposition 4.1.2.6 that they are actually all equivalent by proving that the definition in terms of a graph is also equivalent to the one in terms of tails.

Different numberings can be found in the literature. The one used originally by Anick starts from (-1) and can be considered as “counting” the number of obstructions contained within the chain. The other one starts from 0 and can be viewd as “counting” the number of tails that the chain contains. It also has the convenient advantage to match the homology degrees once we concern ourselves with the resolution. We will use the latter one in this thesis.

Let us introduce all of them and show that they are indeed equivalent after giving some examples.

Definition 4.1.2.1 : n-chains in terms of obstructions

Let $w = x_1 \cdots x_\ell$ be a word in $\langle X \rangle$. Let $n \geqslant 2$.
We say that w is an *n-prechain* if there exists two $(n-1)$-tuples $(a_1, \cdots, a_{n-1})$ et $(b_1, \cdots, b_{n-1})$ of integers such that:

$$1 = a_1 < a_2 \leqslant b_1 < a_3 \leqslant b_2 < a_4 \leqslant b_3 < \cdots < a_{n-1} \leqslant b_{n-2} < b_{n-1} = \ell$$

and

$$\forall m \in [\![1 \mathinner{..} n-1]\!], \quad x_{a_m} x_{a_m+1} \cdots x_{b_m-1} x_{b_m} \in V.$$

An n-prechain is called a *n-chain* if:

$$\forall m \in [\![1 \mathinner{..} n-1]\!], \quad \forall i \in [\![1 \mathinner{..} b_m - 1]\!], \quad x_1 x_2 \cdots x_i \text{ is not an } (m+1)\text{-prechain.}$$

Denote by C_n^O the set of n-chains according to that definition.

In this definition, unlike for the other two, we must fix, *by convention*, the set of 0-chains to $\{1\}$ and the set of 1-chains to X.

Definition 4.1.2.2 : n-chains in terms of a graph

Construct a simple directed graph Q whose nodes are:

$$Q_0 = \{1\} \cup X \cup \{s \in \langle X \rangle \mid s \text{ is a proper suffix of an obstruction}\}.$$

The directed edges are defined as follows:

$$Q_1 = \{(1, x) \mid x \in X\} \cup \left\{(s, t) \in (Q_0 \setminus \{1\})^2 \;\middle|\; st \text{ contains only one obstruction and it is a suffix}\right\}.$$

For any non-negative integer $n \in \mathbb{N}$, we define the set of n-chains by this definition as:

$$C_n^G := \left\{ \prod_{i=0}^{n} w_i \;\middle|\; (1 = w_0, w_1, \cdots, w_n) \text{ are nodes in a walk with } n \text{ edges in } Q \text{ starting at } 1 \right\}.$$

This graph can be constructed as soon as the set V of obstructions is explicitly known, and we will show that we can extract some precious information from it.

Notice that the only walk of length 0 starting at 1 is 1 itself. Therefore, $C_0^G = \{1\}$. Note also that the only nodes directly connected to 1 are all the letters of X. Therefore, we have $C_1^G = X$.

Let us now introduce the last definition in terms of tails:

Definition 4.1.2.3 : n-chains in terms of tails

Define, for $n \in \mathbb{N}$, the set C_n^T of *n-chains* and their tails inductively as follows.

- The only 0-chain is the empty word 1 and its tail is itself.
- The 1-chains are the letters in X, and a letter is its own tail.
- Assume the set of n-chains and their tails has been defined. Define an $(n+1)$-chain, for $n \geqslant 1$, as a word wt such that:
    1. w is an n-chain,
    2. t is a normal word (*i.e.* $t \in O(I)$) called the *tail* of the $(n+1)$-chain,
    3. $t't$, where t' is the tail of w, contains a unique obstruction (*i.e.* an element from V) and it is a suffix.

This last definition allows one to decompose uniquely any n-chain $c^{(n)} \in C_n^T$ as $c^{(n)} = t_1 t_2 \cdots t_n$ where the t_i's are the successive tails. We will write $c^{(n)} =: [t_1, t_2, \cdots, t_n]$.

Remark 4.1.2.4

It is worthwhile to notice that the tails being normal words, it means that the obstruction contained in any $t't$ (where t' and t are consecutive tails in a chain) necessarily overlaps on t' in addition to being a suffix of $t't$.

Let us proceed to give some examples.

Example 4.1.2.5

Consider the alphabet $X = \{x, y, z\}$.
Suppose we have the set of obstructions $V = \{xxx, xxyx, yxz\}$.
The word $xxxx$ is:

- in C_3^O because we can view it as the overlap of the obstructions $\underline{x\overline{xx}}\overline{x}$ defined through the tuples $(a_1, a_2) := (1, 2)$ and $(b_1, b_2) := (3, 4)$
- in C_3^G because there is a walk with 3 edges $1 \to x \to xx \to x$ in the graph given in Figure 4.1.
- in C_3^T because $xxxx = [x, xx, x]$ satisfying the tails conditions.

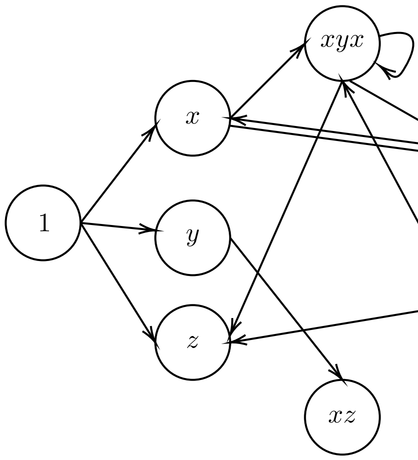
On the other hand, $xxxxx$ is:

- not in C_3^O (even though it is a 3-prechain as seen by $\underline{xx\overline{x}}\overline{xx}$) because $xxxx$ is a 3-prechain smaller and contained in $xxxxx$. It also not a 4-prechain because it does not contain 3 obstructions that satisfy the overlapping conditions. Therefore, $xxxxx$ is not in C_4^O either.
- not in C_3^G because the only walk with two edges that matches the start of the word in Figure 4.1 is $1 \to x \to xx$. We would thus need an edge from xx to itself to complete the walk of three edges giving the word $xxxxx$ which is not the case. Also, one could hope to get a walk of four edges starting with $1 \to x \to xx \to x$ but once again there are no looping edge on the node x, and so we cannot get $xxxxx$. Hence $xxxxx$ is not in C_4^G either.
- not in C_3^T because the first tail t_1 has to be x (first letter of the word), thus the second tail t_2 as to be xx to have an obstruction in $t_1 t_2$ that also matches the start of the word. Then, we would have needed to have xx as third tail t_3 to complete the word with 3 tails; however this is impossible because it would violate the condition that $t_2 t_3 = xxxx$ contains only one obstruction. Similarly, if we try in 4 tails, we could get $t_3 = x$ working, but we would stumble against the impossibility of defining $t_4 = x$ since we would have $t_3 t_4$ that does not contain an obstruction. Thus, $xxxxx$ is not in C_4^T either.

In the same manner, one can show that $\underline{x\overline{xx}}\overline{yx} = [x, xx, yx]$ is in C_3^O, C_3^G and C_3^T but $\underline{xx\overline{x}}\overline{xyx}$, even though it is 3-prechain, is not a 3-chain by any definition.
An example of a 4-chain for all three definitions is for instance $\underline{xxy\overline{x}}\overline{x\underline{yx}}\underline{z} = [x, xyx, xyx, z]$.

Let us now show that the three definitions are indeed equivalent.

Figure 4.1: n-chains graph for Example 4.1.2.5



Proposition 4.1.2.6

For all $n \in \mathbb{N}$, we have $C_n^O = C_n^G = C_n^T$.

Proof. It is shown in [ML23, Proposition 2.6] that the definitions in terms of obstructions and in terms of a graph match, *i.e.* $\forall n \in \mathbb{N}, C_n^O = C_n^G$. Let us show now that the definition in terms of tails matches with the one in terms of a graph.

We have already pointed out that $C_0^G = \{1\} = C_0^T$ and $C_1^G = X = C_1^T$.

Remains only the induction step. Let n be a certain integer greater than 0 such that $C_n^G = C_n^T$ and the tail of an element w associated to the walk $1 \to w_1 \to \cdots \to w_n$ is w_n.

Let $w \in C_{n+1}^G$. It is therefore associated with a walk with $(n+1)$ edges $1 \to w_1 \to \cdots \to w_n \to w_{n+1}$ such that $w = w_1 \cdots w_{n+1}$. Removing the last node w_{n+1} we obtain an element in C_n^G. By inductive hypothesis, we thus have $w_1 \cdots w_n \in C_n^T$ with w_n its tail. First, w_{n+1} is a normal word because it is a node in the graph and thus a subword of an obstruction (even if it is a letter, since it is in a path of length $\geqslant 2$). Then, since there is an edge between w_n and w_{n+1} there exists exactly one obstruction $w_n w_{n+1}$, and it is a suffix. Hence, $w \in C_{n+1}^T$.

Let $[t_1, \cdots, t_n, t_{n+1}] \in C_{n+1}^T$. By inductive hypothesis $t_1 \cdots t_n \in C_n^G$, that is to say, there is a walk $1 \to t_1 \to \cdots \to t_n$. Now since $t_n t_{n+1}$ contains an obstruction that overlaps on t_n, and it is suffix, it follows that t_{n+1} is a proper suffix of an obstruction and thus a node in the graph. Moreover, this also means there is an edge from t_n to t_{n+1} completing the walk $1 \to t_1 \to \cdots \to t_n \to t_{n+1}$. Hence, $t_1 \cdots t_{n+1} \in C_{n+1}^G$. □

Remark 4.1.2.7

With Proposition 4.1.2.6 and [ML23, Proposition 2.6], we can safely drop the superscripts when writing the sets of n-chains since all three definitions define the same sets. Then, let us denote by C_n the set of n-chains according to any of Definition 4.1.2.1, Definition 4.1.2.2 or Definition 4.1.2.3. Notice also that the proof of the previous proposition allows us to interpret the nodes of a walk in the graph as the successive tails of the associated chain.

Remark 4.1.2.8

Notice that no matter what the set of obstructions V is and no matter the alphabet X, we will always have:

$$C_0 = \{1\} \qquad C_1 = X \qquad C_2 = V$$

4.1.3 The resolution

The modules in the Anick resolution are of the form $\mathbb{K}C_n \otimes_{\mathbb{K}} A$ where C_n is the set of n-chains as defined in Remark 4.1.2.7. Before presenting the resolution, we need to introduce a last ingredient: the *high-term*.

Definition 4.1.3.1 : High-term

Let $n \in \mathbb{N}$ and $P := \sum_i \lambda_i c_i^{(n)} \otimes \overline{r_i} \in \mathbb{K}C_n \otimes_{\mathbb{K}} A$.
The *high-term* of P is defined as the following monomial:

$$\mathrm{LM}\,(P) := \mathrm{LM}\left(\sum_i \lambda_i \left(c_i^{(n)} \widehat{r_i}\right)\right),$$

where $\widehat{r_i}$ is the unique normal form of r_i with respect the non-commutative Gröbner basis.

Theorem 4.1.3.2 : (Anick resolution [Ani86, Theorem 1.4])

Let $\mathbb{K}$ be a field. Let A be a $\mathbb{K}$-algebra augmented by ε with the section defined by $\eta(1_{\mathbb{K}}) = 1_A$. Let $\langle X | R \rangle$ be a presentation of A such that R is a minimal non-commutative Gröbner basis according to the monomial order $\prec$. Let I be the two-sided ideal generated by R. Let $O(I) := \langle X \rangle \setminus \mathrm{LM}\,(I)$ be the set of normal words. Let $V := \mathrm{LM}\,(R)$ be the set of leading monomials in R. For any $n \in \mathbb{N}$, let C_n denote the set of n-chains on V.
There is a free resolution of $\mathbb{K}$ in the category of right A-modules:

$$\cdots \rightleftarrows \mathbb{K}C_{n+1} \otimes_{\mathbb{K}} A \underset{i_n}{\overset{d_{n+1}}{\rightleftarrows}} \mathbb{K}C_n \otimes_{\mathbb{K}} A \underset{i_{n-1}}{\overset{d_n}{\rightleftarrows}} \mathbb{K}C_{n-1} \otimes_{\mathbb{K}} A \rightleftarrows \cdots \rightleftarrows \mathbb{K}C_1 \otimes_{\mathbb{K}} A \underset{i_0}{\overset{d_1}{\rightleftarrows}} \mathbb{K}C_0 \otimes_{\mathbb{K}} A \underset{\eta}{\overset{\varepsilon}{\rightleftarrows}} \mathbb{K} \to 0$$

where for $n \geqslant 1$, the map of right A-modules d_n satisfies:

$$\forall c^{(n)} := [t_1, \cdots, t_n] \in C_n, \quad d_n\left([t_1, \cdots, t_n] \otimes 1_A\right) := [t_1, \cdots, t_{n-1}] \otimes \overline{t_n} + \omega_{c^{(n)}},$$

with either $\omega_{c^{(n)}} = 0$ or its high-term verifies $\mathrm{LM}\,(\omega_{c^{(n)}}) \prec c^{(n)}$.

Proof. The proof can be found in its entirety in [Ani86] or in [ML23] with slightly more details. Alternative ways of proving the theorem are proposed in [NWW19] and in [Far92].

We shall recall here the definitions of the differentials and of the contracting homotopy:

- $\forall x \in X, \quad d_1(x \otimes 1_A) := 1 \otimes \overline{x} - 1 \otimes \eta\varepsilon(\overline{x})$.
- $\forall y = x_1 \cdots x_\ell \in O(I), \quad i_0(1 \otimes (\overline{y} - \eta\varepsilon(\overline{y}))) := \sum_{j=1}^{\ell} \varepsilon(x_1 \cdots x_{j-1}) x_j \otimes \overline{x_{j+1} \cdots x_\ell}$.
- $\forall n \in \mathbb{N}^*, \forall c^{(n+1)} = [t_1, \cdots, t_n, t_{n+1}] \in C_{n+1}$

$$d_{n+1}\left([t_1, \cdots, t_n, t_{n+1}] \otimes 1_A\right) := [t_1, \cdots, t_n] \otimes \overline{t_{n+1}} - i_{n-1} d_n\left([t_1, \cdots, t_n] \otimes \overline{t_{n+1}}\right).$$

- $\forall n \in \mathbb{N}^*, \forall v = \sum_i \lambda_i c_i^{(n)} \otimes \overline{s_i} \in \mathbb{K}C_n \otimes_{\mathbb{K}} A$

$$i_n(v) := \begin{cases} \mathrm{LC}\,(v)\, c^{(n+1)} \otimes \overline{t} - i_n\left(v - \mathrm{LC}\,(v)\, d_{n+1}\left(c^{(n+1)} \otimes \overline{t}\right)\right) & \text{if } v \in \ker(d_n) \setminus \{0\} \\ 0 & \text{otherwise} \end{cases},$$

where $c^{(n+1)} t = \mathrm{LM}\,(v)$, $c^{(n+1)} \in C_{n+1}$ and $t \in O(I)$.

$\square$

Example 4.1.3.3

Let us consider the algebra presented by $\langle X|R\rangle$, where $X = \{x, y, z\}$ and the relations are $R = \{xxyx, xxx - xx, yxz - yx\}$ with the deglex monomial order induced by $x \succ y \succ z$ augmented with the evaluation of polynomials at zero. We have $V := \mathrm{LM}(R) = \{xxyx, xxx, yxz\}$ and the graph of n-chains is given in Figure 4.1. We have, for all $\zeta \in X$ and $x_1 \cdots x_\ell \in O(I)$:

$$d_1(\zeta \otimes \overline{1}) = \overline{\zeta}$$
$$i_0(\overline{x_1 \cdots x_\ell}) = x_1 \otimes \overline{x_2 \cdots x_\ell}$$

Then:

$$\begin{aligned} d_2(xxx \otimes \overline{1}) &= x \otimes \overline{xx} - i_0 d_1(x \otimes \overline{xx}) && \text{definition of } d_2 \\ &= x \otimes \overline{xx} - i_0(\overline{xxx}) && \text{definition of } d_1 \\ &= x \otimes \overline{xx} - i_0(\overline{xx}) && \text{reduction} \\ &= x \otimes \overline{xx} - x \otimes \overline{x} && \text{definition of } i_0 \end{aligned}$$

Similarly, we compute:

$$d_2(xxyx \otimes \overline{1}) = x \otimes \overline{xyx}$$
$$d_2(yxz \otimes \overline{1}) = y \otimes \overline{xz} - y \otimes \overline{x}$$

The 3-chains are $\{xxyxxyx, xxyxxx, xxyxz, xxxyx, xxxx\}$. Then:

$$\begin{aligned} d_3(xxxyx \otimes \overline{1}) &= xxx \otimes \overline{yx} - i_1 d_2(xxx \otimes \overline{yx}) && \text{definition of } d_3 \\ &= xxx \otimes \overline{yx} - i_1(x \otimes \overline{xxyx} - x \otimes \overline{xyx}) && \text{definition of } d_2 \\ &= xxx \otimes \overline{yx} - i_1(x \otimes 0 - x \otimes \overline{xyx}) && \text{reduction} \\ &= xxx \otimes \overline{yx} + xxyx \otimes \overline{1} && \text{definition of } i_1 \end{aligned}$$

In an analoguous manner, we compute:

$$d_3(xxyxxyx \otimes \overline{1}) = xxyx \otimes \overline{xyx}$$
$$d_3(xxyxxx \otimes \overline{1}) = xxyx \otimes \overline{xx} - xxyx \otimes \overline{x}$$
$$d_3(xxyxz \otimes \overline{1}) = xxyz \otimes \overline{z} - xxyx \otimes \overline{1}$$
$$d_3(xxxx \otimes \overline{1}) = xxx \otimes \overline{x}$$

The 4-chains are:

$$\{xxyxxyxxyx, xxyxxyxxx, xxyxxyxz, xxyxxxyx, \\ xxyxxxx, xxxyxxyx, xxxyxxx, xxxyxz, xxxxxyx, xxxxxx\}$$

We thus have:

$$\begin{aligned}
d_4(xxxyxxx \otimes \overline{1}) &= xxxyx \otimes \overline{xx} - i_2 d_3(xxxyx \otimes \overline{xx}) && \text{definition of } d_4 \\
&= xxxyx \otimes \overline{xx} - i_2(xxx \otimes \overline{yxxx} + xxyx \otimes \overline{xx}) && \text{definition of } d_3 \\
&= xxxyx \otimes \overline{xx} - i_2(xxx \otimes \overline{yxx} + xxxyx \otimes \overline{xx}) && \text{reduction} \\
&= xxxyx \otimes \overline{xx} - xxxyx \otimes \overline{x} - i_2(xxyx \otimes \overline{xx} - xxyx \otimes \overline{x}) && \text{definition of } i_2 \\
&= xxxyx \otimes \overline{xx} - xxxyx \otimes \overline{x} - xxyxxx \otimes \overline{1} && \text{definition of } i_2
\end{aligned}$$

We compute in the same way:

$$\begin{aligned}
d_4(xxyxxyxxyx \otimes \overline{1}) &= xxyxxyx \otimes \overline{xyx} \\
d_4(xxyxxyxxx \otimes \overline{1}) &= xxyxxyx \otimes \overline{xx} - xxyxxyx \otimes \overline{x} \\
d_4(xxyxxyxz \otimes \overline{1}) &= xxyxxyx \otimes \overline{z} - xxyxxyx \otimes \overline{1} \\
d_4(xxyxxxyx \otimes \overline{1}) &= xxyxxx \otimes \overline{yx} + xxyxxyx \otimes \overline{1} \\
d_4(xxyxxxx \otimes \overline{1}) &= xxyxxx \otimes \overline{x} \\
d_4(xxxyxxyx \otimes \overline{1}) &= xxxyx \otimes \overline{xyx} - xxyxxyx \otimes \overline{1} \\
d_4(xxxyxz \otimes \overline{1}) &= xxxyx \otimes \overline{z} - xxxyx \otimes \overline{1} - xxyxz \otimes \overline{1} \\
d_4(xxxxxyx \otimes \overline{1}) &= xxxx \otimes \overline{xyx} \\
d_4(xxxxxx \otimes \overline{1}) &= xxxx \otimes \overline{xx} - xxxx \otimes \overline{x}
\end{aligned}$$

We can compute in that fashion any differential, by computing all the previous ones that are needed.

4.1.4 Applications

The Anick resolution is useful in practice to compute homological invariants of the algebra A and other constructions built on top of those invariants.

For instance, in [Ani86], the Anick resolution is shown to provide an efficient way of computing the *Hilbert series* [Ani82] for monommial algebras (and more generally any graded algebra for which the resolution is minimal), via the formula:

$$H_A(z) = \left(1 - \sum_{n=0}^{\infty} (-1)^n H_{\mathbb{K}C_n}(z)\right)^{-1},$$

where $H_{\mathbb{K}C_n}(z) = \sum_{k=0}^{\infty} \operatorname{card}\left\{c^{(n)} \in C_n \;\middle|\; \left|c^{(n)}\right| = k\right\} z^k$. The simplifications that Anick resolution offer for the computation of the Hilbert series are exploited in the Bergman package developped in [CU97].

In [Ufn95], it is stated that if A is a monomial algebra, then the *double Poincaré series* as defined in [Ufn95, page 60] of A exists and satisfies the equation:

$$P_A(s,t) = 1 + \sum_{n=0}^{\infty} H_{\mathbb{K}C_n}(t) s^{n+1}$$

It is also asserted that the finiteness of the resolution for a monomial algebra, *i.e.* the existence of an $n \in \mathbb{N}$ such that $C_n = 0$, is equivalent n being an upper bound for the *global dimension* of A [Eil56], *i.e.* $\text{gl.dim} A \leqslant n$. Furthermore, for a general connected graded algebra $A = \langle X | R \rangle$, we can consider its associated monomial algebra $\overline{A} = \langle X | V \rangle$ where V is the set of obstructions (*i.e.*

the leading monomials of a minimal non-commutative Gröbner basis of the ideal generated by R). We have then the coefficient-wise inequality $P_A(s,t) \leqslant P_{\overline{A}}(s,t)$ for the double Poincaré series of the two algebras. This means in particular that if X and V are finite, then the Poincaré series exists. Moreover, assuming there is an $n \in \mathbb{N}$ such that $C_n = 0$, then the global dimension of the graded algebra A is bounded by n above, gl.dim$A \leqslant n$.

A particular corollary case discussed in [Ani86, Ufn95] of these results is, if no leading monomial of the minimal non-commutative Gröbner basis G of the ideal of relations overlaps with another leading monomial of an element G, then $\mathrm{Tor}_n^A(\mathbb{K},\mathbb{K}) = 0$ for $n \geqslant 3$ and thus $P_A(s,t) = 1 + H_X s + H_R s^2$.

Finally, in [NWW19], the authors use the Anick resolution and show that it is equivalent to a tensor product of three complexes that they use to prove that cohomology rings of certain Hopf algebras are finitely generated.

4.1.5 Properties

In [Ani86], Anick specialises Theorem 4.1.3.2 to the case of graded algebras and shows that, assuming the monomial order is graded by some degree map on the generators (for instance the *deglex* monomial order), the differentials of the resolution are homogeneous maps of graded-algebras.

The Anick resolution is not minimal in general. However, in the case of monomial algebras, it is always minimal ([Ani86, Lemma 3.3], [Ufn95, Page 60]). Indeed, writing $(r_n)_{n\in\mathbb{N}}$ the sequence defined by $r_n := \mathrm{card}(C_n)$, since each A-module $\mathbb{K}C_n \otimes_{\mathbb{K}} A$ ($n \in \mathbb{N}$) is free of rank r_n, it is isomorphic to the r_n-fold direct sum of the base ring A:

$$\mathbb{K}C_n \otimes_{\mathbb{K}} A \cong A^{r_n} := \bigoplus_{i=1}^{r_n} A. \tag{4.1}$$

On the other hand, we have the isomorphism:

$$\begin{aligned} \varphi : A \otimes_A \mathbb{K} &\to \mathbb{K} \\ a \otimes \lambda\ &\mapsto a \cdot \lambda = \varepsilon(a)\lambda, \end{aligned} \tag{4.2}$$

that induces a sequence of isomorphisms $\left(\varphi^{r_n} : A^{r_n} \otimes_A \mathbb{K} \to \mathbb{K}^{r_n}\right)_{n\in\mathbb{N}}$ because the tensor product is an additive functor and thus commutes with direct sums.

Therefore, applying the functor $- \otimes_A \mathbb{K}$ on the Anick resolution, we obtain by (4.1) and (4.2) the following commutative diagram, writing $F_n := \mathbb{K}C_n \otimes_{\mathbb{K}} A$ for all $n \in \mathbb{N}$:

$$\begin{tikzcd}
\cdots \arrow[r] & F_n \otimes_A \mathbb{K} \arrow[r, "d_n\otimes \mathrm{id}_{\mathbb{K}}"] \arrow[d, tail, two heads] & F_{n-1}\otimes_A \mathbb{K} \arrow[r] \arrow[d, tail, two heads] & \cdots \arrow[r] & F_1 \otimes_A \mathbb{K} \arrow[r, "d_1\otimes \mathrm{id}_{\mathbb{K}}"] \arrow[d, tail, two heads] & F_0 \otimes_A \mathbb{K} \arrow[r, "\varepsilon\otimes \mathrm{id}_{\mathbb{K}}"] \arrow[d, tail, two heads] & \mathbb{K}\otimes_A \mathbb{K} \arrow[r] \arrow[d, equal] & 0 \\
\cdots \arrow[r] & A^{r_n} \otimes_A \mathbb{K} \arrow[r] \arrow[d, tail, two heads, "\varphi^{r_n}"] & A^{r_{n-1}} \otimes_A \mathbb{K} \arrow[r] \arrow[d, tail, two heads, "\varphi^{r_{n-1}}"] & \cdots \arrow[r] & A^{r_1} \otimes_A \mathbb{K} \arrow[r] \arrow[d, tail, two heads, "\varphi^{r_1}"] & A \otimes_A \mathbb{K} \arrow[r] \arrow[d, tail, two heads, "\varphi"] & \mathbb{K}\otimes_A \mathbb{K} \arrow[r] \arrow[d, equal] & 0 \\
\cdots \arrow[r] & \mathbb{K}^{r_n} \arrow[r, "\overline{d_n}"] & \mathbb{K}^{r_{n-1}} \arrow[r] & \cdots \arrow[r] & \mathbb{K}^{r_1} \arrow[r, "\overline{d_1}"] & \mathbb{K} \arrow[r, "\overline{d_0}"] & \mathbb{K}\otimes_A \mathbb{K} \arrow[r] & 0
\end{tikzcd}$$

By definition, the Anick resolution is therefore said to be *minimal* [Eil56] if $\overline{d_n} = 0$ for all $n \in \mathbb{N}$. But, we have explicitly for all $(\lambda_1, \cdots, \lambda_{r_n}) \in \mathbb{K}^{r_n}$:

$$\begin{aligned}
\overline{d_n}(\lambda_1, \cdots, \lambda_{r_n}) &= \varphi^{r_{n-1}} \circ (d_n \otimes \mathrm{id}_{\mathbb{K}}) \circ \left(\varphi^{-1}\right)^{r_n} (\lambda_1, \cdots, \lambda_{r_n}) \\
&= \varphi^{r_{n-1}} \circ (d_n \otimes \mathrm{id}_{\mathbb{K}}) \left(\eta(\lambda_1), \cdots, \eta(\lambda_{r_n})\right) \otimes 1_{\mathbb{K}}) \\
&= \varphi^{r_{n-1}}(d_n(\eta(\lambda_1), \cdots, \eta(\lambda_{r_n})) \otimes 1_{\mathbb{K}}) \\
&= \left(\varepsilon\left(d_n^{(1)}(\eta(\lambda_1), \cdots, \eta(\lambda_{r_n}))\right), \cdots, \varepsilon\left(d_n^{(r_{n-1})}(\eta(\lambda_1), \cdots, \eta(\lambda_{r_n}))\right)\right),
\end{aligned}$$

where $d_n^{(i)} = p_n^{(i)} d_n$ with $p_n^{(i)}$ the projection on the i'th component.

But as we will see in Proposition 4.3.2.2, $\omega_{c^{(n)}} = 0$ in the statement of Theorem 4.1.3.2, for any n-chain and any $n \in \mathbb{N}$. Then, $d_n(\eta(\lambda_1), \cdots, \eta(\lambda_{r_n}))$ is a $\mathbb{K}$-linear combination of $c^{(n-1)} \otimes \bar{t}$ where t is not the empty word. Thus, the $d_n^{(i)}(\eta(\lambda_1), \cdots, \eta(\lambda_{r_n}))$ are either zero or of the form $\mu c^{(n-1)} \otimes \bar{t}$ with t not the empty word and $\mu \in \mathbb{K}$. It follows that applying the augmentation map yields 0 for each component since they belong in the augmentation ideal A_+. Hence, the resolution is indeed minimal if A is monomial.

Now recall the definition of n-chains in terms of a graph, denote by $Q = (Q_0, Q_1)$ the graph of Definition 4.1.2.2. Suppose that the set V of obstructions is finite (that is to say, the reduced non-commutative Gröbner basis of the ideal of relations is finite). This happens for instance when the algebra A is of finite $\mathbb{K}$-dimension, according to [Far92]. Suppose also that the set X of generators is finite. Then, it entails that the set Q_0 of vertices is finite. We can thus construct the adjacency matrix M of the graph Q:

$$M := \left(\begin{cases} 1 & \text{if there is an edge } s \to t \\ 0 & \text{otherwise} \end{cases} \right)_{\substack{s \in Q_0 \\ t \in Q_0}},$$

where Q_0 is ordered in a fixed way (by identifying it to the set of integers $[\![1 \mathinner{..} \operatorname{card}(Q_0)]\!]$).

This matrix is read as follows: each line is associated with a vertex $s \in Q_0$. A 1 in column associated with vertex $t \in Q_0$ means that there is an edge going from s to t. Hence, M is symmetric if and only if for each edge $s \to t$ the edge $t \to s$ exists. Also, a non-zero diagonal coefficient at row and column $s \in Q_0$ means that there is a loop edge on s.

Example 4.1.5.1

For instance, considering again Example 4.1.2.5 whose graph is given in Figure 4.1 we get the adjacency matrix:

$$M = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

where the set of vertices is ordered as $(1, x, y, z, xyx, xx, yx, xz)$.

Recall that the coefficient at $(s, t) \in Q_0 \times Q_0$ of the n'th power of the adjacency matrix gives the number of n-walks (*i.e.* walks with n edges) starting from s and finishing on t. Hence, since, for $n \in \mathbb{N}$, the n-chains have been defined has the n-walks starting from 1, to know exactly the rank of the n'th free A-module $\mathbb{K}C_n \otimes_{\mathbb{K}} A$ in the Anick resolution, one just has to compute M^n and take the sum of the coefficients in row associated with the monomial 1. This observation entails the following proposition:

Proposition 4.1.5.2

Let $A = \langle X|R\rangle$ be a monomial algebra where the set X of generators and the set $V = R$ of obstructions are finite. Let $Q = (Q_0, Q_1)$ be the associated graph and M the adjacency matrix.
Define the sequence $(s_n)_{n\in\mathbb{N}}$ as $s_n := \sum_{v\in Q_0} m_{1,v}$ where $M^n =: (m_{s,t})_{\substack{s\in Q_0\\ t\in Q_0}}$. Then:

$$\forall n \in \mathbb{N}, \quad \mathrm{Tor}_n^A(\mathbb{K}, \mathbb{K}) \cong \mathbb{K}^{s_n}.$$

This proposition remains true when considering other algebras, not necessarily monomial, in the event where the Anick resolution is also minimal for those algebras.

Notice also that, by definition, no edges can reach the vertex 1. Therefore, any walk involving the vertex 1 starts at 1 (and, incidentally, does not pass through it again). Furthermore, to get the set of n-chains from the graph, one has only to consider the connected component of the vertex 1, that is to say, all those vertices that have a walk passing through 1. Hence, considering the adjacency matrix $\hat{M}$ of that restricted graph, it follows that $\hat{M}$ is nilpotent, *i.e.* there exists $n \in \mathbb{N}$ such that $\hat{M}^n = 0$, if and only if, the Anick resolution is finite. Indeed, nilpotence of the adjacency matrix is equivalent to the non-existence of walks in the graph that goes through the same vertex twice (because the graph is finite under our assumptions, so the only way to have walks of arbitrary length is to have a walk that goes through the same vertex twice, somewhat similar to what we would call a loop). And since, by restriction on the connected component, every walk starts from vertex 1, then there is a bijection between the n-chains and the n-walks. Finally, the claim follows from the fact that there will be no $(n+1)$ chains if there are no n-chains (this is deduced from the inductive Definition 4.1.2.3).

4.2 Koszul complex

The *Koszul complex* as we will present it here is the outcome of several generalisation procedures. Starting from the work of Koszul in [Kos50] in which the homology of Lie algebras is studied, Tate describes in [Tat57] how to construct in theory generally smaller resolutions than the bar resolution (see [EM53, ML95]). This process is now known as the *Koszul-Tate resolution*. Inspired by these ideas, Priddy introduces the concept of *Koszul algebras* in [Pri70] for quadratic algebras (Definition 1.2.1.9). In this paper is introduced the *Koszul complex* of a quadratic algebra. It is then a theorem that the Koszul property for a quadratic algebra is equivalent to the acyclity of its Koszul complex. It is also a result [Ber01] that the Koszul complex then becomes a minimal resolution of the ground field. After studying the Koszul property of quadratic algebras in terms of confluence and lattice theory in [Ber98a, Ber98b], Berger introduces in [Ber01] a generalisation of the Koszul property for the case of homogeneous algebras of degree $\geqslant 2$ (Definition 1.2.1.8) as well as describes explicitly the associated Koszul complex for these algebras. In this paper, Berger goes on to prove that the Koszul property for these algebras is also equivalent to the acyclity of the associated Koszul complex. He also gives a sufficient condition in terms of the *distributivity* [Ber01] of the algebra in addition to a certain property called *extra-condition* (see Theorem 4.2.3.6). A more abstract and fundamental approach to obtaining the Koszul complex for quadratic algebras is connected to the notion of Koszul duality [BGS88]. In [BDVW03], the authors go into details about the generalisation of this duality for non-quadratic homogeneous algebras and explain how to recover the explicit definition of the Koszul complex as originally presented in [Ber01].

4.2.1 Koszul duality

Fix throughout this section $\mathbb{K}$ a field and $N \geqslant 2$ an integer. The tensor product is taken over field $\mathbb{K}$ unless specified otherwise, so we allow ourselves to drop the subscript, *i.e.* $\otimes := \otimes_{\mathbb{K}}$.

In this subsection, we give an overview of Koszul duality for homogeneous algebras of arbitrary degree as it is presented in [BDVW03].

First, let us recall the definition of homogeneous algebra (Definition 1.2.1.8) but put it in terms of tensor algebras:

Definition 4.2.1.1 : Homogeneous algebra (Tensor algebra)

An *N-homogeneous $\mathbb{K}$-algebra* is any associative unitary $\mathbb{K}$-algebra A for which there exist a finite-dimensional $\mathbb{K}$-vector space E and a subspace R of $E^{\otimes N}$ such that there is the isomorphism of $\mathbb{K}$-algebras:

$$A \cong {}^{T(E)}\!/\!_{I(R)},$$

where $T(E)$ is the tensor algebra on E and $I(R)$ is the two-sided ideal generated by R. In that case, we write $A(E, R) := A$.

Every N-homogeneous algebra A is a graded connected algebra generated in degree 1 where we have:

$$A = \bigoplus_{n \in \mathbb{N}} A_n \quad \text{with} \quad A_n := \begin{cases} E^{\otimes n} & \forall n < N, \\ \dfrac{E^{\otimes n}}{\sum_{i+j+N=n} E^{\otimes i} \otimes R \otimes E^{\otimes j}} & \forall n \geqslant N. \end{cases}$$

Definition 4.2.1.2 : Homomorphism of homogeneous algebras

Let $A(E, R)$ and $A'(E', R')$ be two N-homogeneous $\mathbb{K}$-algebras. A *homomorphism of N-homogeneous algebras* is the map induced by any map $f : E \to E'$ such that $f^{\otimes N}(R) \subseteq R'$.

The N-homogeneous algebras together with their homomorphisms form a subcategory, denoted in [BDVW03] by $\mathbf{H}_N\mathbf{Alg}$, of the graded connected algebras category. One can define a contravariant endofunctor on that category:

Definition 4.2.1.3 : Homogeneous dual

Let $A := A(E, R)$ be an N-homogeneous $\mathbb{K}$-algebra. We define its dual as being the N-homogeneous algebra $A^! := A(E^*, R^\perp)$ where $E^* := \mathrm{Hom}_{\mathbb{K}}(E, \mathbb{K})$ is the dual vector space of E and $R^\perp$ is the annihilator of R under the natural pairing, that is to say:

$$R^\perp = \left\{ \varphi \in \left(E^{\otimes N}\right)^* \;\middle|\; \forall x \in R, \quad \varphi(x) = 0 \right\}$$

identifying $\left(E^{\otimes N}\right)^*$ with $(E^*)^{\otimes N}$ since E is finite-dimensional.

Notice that $\left(A^!\right)^! \cong A$ for any N-homogeneous algebra A.

Now, if $f : E \to E'$ is the underlying map defining a homomorphism, also denoted f, of N-homogeneous algebras between $A := A(E, R)$ and $A' := A(E', R')$, then we define the dual of that map as the transpose of f such that:

$$\begin{aligned} f^! : (A')^! &\to A^! \\ u &\mapsto f^!(u) := u \circ f. \end{aligned}$$

The association of the dual for N-homogeneous $\mathbb{K}$-algebras and of the dual for their homomorphisms yields a well-defined contravariant endofunctor on $\mathbf{H}_N\mathbf{Alg}$.

Referring the reader to [BDVW03] for more details, one can define two "tensor products", $\circ$ and $\bullet$, on $\mathbf{H}_N\mathbf{Alg}$ in the sense that if it is equipped:

- with $\circ$ then it is a *tensor category* with unit object $\mathbb{K}[t]$, the univariate polynomial algebra,
- with $\bullet$ then it is also a tensor category but with unit object $\mathbb{K}[t]^!$.

See [DM82] for details concerning tensor categories, also called *monoidal categories*.

A certain natural isomorphism in the category of $\mathbb{K}$-vector spaces is shown to entail (see [BDVW03, Theorem 2]), as it is the case for quadratic algebras, the natural isomorphism in $\mathbf{H}_N\mathbf{Alg}$:

$$\operatorname{Hom}(A \bullet B, C) \cong \operatorname{Hom}\left(A, B^! \circ C\right). \tag{4.3}$$

The unit object $\mathbb{K}[t]^!$ is isomorphic as N-homogeneous algebra to $A(\mathbb{K}, \mathbb{K}^{\otimes N})$ which in turn can be written $\wedge_N\{d\} := {}^{\mathbb{K}[d]}/_{I(d^N)}$, the univariate polynomial algebra in the indeterminate d modulo the relation $d^N = 0$. Setting A to that object in (4.3) results in the natural isomorphism:

$$\operatorname{Hom}(B, C) \cong \operatorname{Hom}\left(\wedge_N\{d\}, B^! \circ C\right). \tag{4.4}$$

Then, if one is given $f \in \operatorname{Hom}(B, C)$, then there is a unique $g \in \operatorname{Hom}\left(\wedge_N\{d\}, B^! \circ C\right)$ associated to f through the isomorphism (4.4). Write $\xi_f := g(d)$ the element in $B^! \circ C$ that is the image of the indeterminate d through g.

As for the case with quadratic algebras, there exists an injective homomorphism of algebras $i : A \circ A' \to A \otimes A'$ whose image is $\bigoplus_{n\in\mathbb{N}} A_n \otimes A'_n$ (see [BDVW03, Proposition 1]). Then, defining ∂ as the left multiplication by $i(\xi_f)$ in $B^! \otimes C$, we obtain with the proper graduation a cochain N-complex $(B^! \otimes C, \partial)$, denoted $L(f)$. A cochain (N-)complex is th dual notion of a chain (N-)complex, the indices are increasing instead of decreasing. In the particular case where $B = C$ and f is the identity, we write $L(B)$.

There also exists a chain N-complex $K(f) = \left(C \otimes \left(B^!\right)^*, \partial\right)$ (where $\left(B^!\right)^*$ denotes the graded dual, that is $\bigoplus_{n\in\mathbb{N}} \left(B^!_n\right)^*$) obtained by partial dualisation of the cochain N-complex $L(f)$, by applying $\operatorname{Hom}_C(-, C)$ on each module in $L(f)$ and by identifying, thanks to the finite dimension, $\operatorname{Hom}_C\left(B^!_n \otimes C, C\right)$ with $C \otimes \left(B^!\right)^*$. Once again, if $B = C$ and f is the identity, then one writes $K(B)$ instead.

The Koszul complex we are interested in this thesis is derived from the chain N-complex $K(A)$ where A is the N-homogeneous algebra at study. We describe a more explicit way of obtaining it in the next section, that ultimately corresponds to the way Berger presented it in [Ber01].

4.2.2 Koszul complex

Let $A := A(E, R)$ be an N-homogeneous $\mathbb{K}$-algebra. Then, we can give an explicit description of the dual $A^!$:

$$A^! \cong \bigoplus_{n\in\mathbb{N}} A^!_n \quad \text{with} \quad A^!_n := \begin{cases} \left(E^*\right)^{\otimes n} & \forall n < N, \\ \dfrac{\left(E^*\right)^{\otimes n}}{\sum_{i+j+N=n} \left(E^*\right)^{\otimes i} \otimes R^\perp \otimes \left(E^*\right)^{\otimes j}} & \forall n \geqslant N, \end{cases}$$

where E^* and $R^\perp$ are the same as in Definition 4.2.1.3.

Now, let us describe the graded dual of the algebra $A^!$:

$$\left(A^!\right)^* \cong \bigoplus_{n\in\mathbb{N}} \left(A^!_n\right)^* \quad \text{with} \quad \left(A^!_n\right)^* := \begin{cases} E^{\otimes n} & \forall n < N, \\ \bigcap_{i+j+N=n} E^{\otimes i} \otimes R \otimes E^{\otimes j} & \forall n \geqslant N, \end{cases}$$

since $\left(\dfrac{V}{W}\right)^* \cong W^{\perp}$ for every vector space V and subspace W.

For all $n \in \mathbb{N}$ and $i, j \in \mathbb{N}$ such that $n = i + j$, there exists canonical injections:

$$\iota_{i,j} : \left(A^!_n\right)^* \to \left(A^!_i\right)^* \otimes \left(A^!_j\right)^*,$$

by splitting the input word into two appropriate chunks.

Then, the chain N-complex $K(A)$ is given by:

$$\cdots \longrightarrow A \otimes \left(A^!_n\right)^* \xrightarrow{\partial} A \otimes \left(A^!_{n-1}\right)^* \longrightarrow \cdots \longrightarrow A \otimes \left(A^!_1\right)^* \xrightarrow{\partial} A \longrightarrow 0,$$

where ∂ is the A-linear map induced by the canonical injection $\iota_{1,n-1}$. Indeed, since $N \geqslant 2$, we have $\left(A^!_1\right)^* \cong A_1 \subseteq A$, thus, because (A_n) is injected into $\left(A^!_1\right)^* \otimes \left(A^!_{n-1}\right)^*$ via $\iota_{1,n-1}$, it can be injected into $A \otimes \left(A^!_{n-1}\right)^*$.

From that chain N-complex, we can construct a family $C_{p,r}$ of chain complexes as defined in Definition 3.1.1.1 that ranges over $(r, p) \in [\![0 \,..\, N-2]\!] \times [\![r+1 \,..\, N-1]\!]$ and are defined by:

$$\cdots \xrightarrow{\partial^{N-p}} A \otimes \left(A^*_{N+r}\right) \xrightarrow{\partial^{p}} A \otimes \left(A^!_{N-p+r}\right)^* \xrightarrow{\partial^{N-p}} A \otimes \left(A^!_r\right)^* \xrightarrow{\partial^{p}} 0.$$

It is shown in [BDVW03] that the exactness of any chain complexes $C_{p,r}$ for $(p, r) \neq (N-1, 0)$ implies that the algebra A is trivial, in the sense that either $R = 0$ or $R = E^{\otimes N}$.

The chain complex $C_{N-1,0}$ on the other hand is of particular interest since it is proven in [Ber01] that its acyclicity is equivalent to the Koszul property of the algebra A. We call that chain complex $C_{N-1,0}$ the *Koszul complex* of the N-homogeneous algebra A. Let us now proceed to give an explicit definition of that chain complex.

Definition 4.2.2.1 : Diagonal sequence

Let $N \geqslant 2$ be an integer.

The *diagonal sequence* associated to N, denoted by ℓ_N, is defined as:

$$\ell_N(n) := \begin{cases} kN & \text{if } n = 2k, \\ kN + 1 & \text{if } n = 2k+1. \end{cases}$$

Notice how the diagonal sequence associated with 2 is just the identity sequence.

Notice also that, no matter the value of $N \geqslant 2$, the sequence is strictly increasing.

Example 4.2.2.2

We have:

$$\ell_3 = (0, 1, 3, 4, 6, 7, 9, 10, \cdots),$$
$$\ell_4 = (0, 1, 4, 5, 8, 9, 12, 13, \cdots),$$
$$\ell_5 = (0, 1, 5, 6, 10, 11, 15, 16, \cdots).$$

Remark 4.2.2.3

For all $n \in \mathbb{N}$, we have:

(i) $\ell_N(n+1) - \ell_N(n) = 1$ if n is even,

(ii) $\ell_N(n+1) - \ell_N(n) = N-1$ if n is odd,

(iii) $\ell_N(n+2) - \ell_N(n) = N$ regardless of the parity of n.

Let $A = \langle X|R\rangle$ be an N-homogeneous algebra according to Definition 1.2.1.8. Define:

$$J_0 := \mathbb{K} \qquad J_1 := \mathbb{K}X \qquad J_2 = \mathbb{K}R \tag{4.5}$$

and:

$$\forall n \geqslant 3, \quad J_n := \bigcap_{i=0}^{\ell_N(n)-N} \mathbb{K}X^{(i)} \otimes \mathbb{K}R \otimes \mathbb{K}X^{(\ell_N(n)-N-i)} \subseteq \mathbb{K}X^{(\ell_N(n))} \tag{4.6}$$

where $\mathbb{K}X^{(j)} := \mathbb{K}X^{\otimes j}$ for all $j \in \mathbb{N}$.

Definition 4.2.2.4 : Koszul complex

Let $A = \langle X|R\rangle$ be an N-homogeneous algebra.
The *Koszul complex* of A is the complex in the category of left A-modules:

$$\cdots \to A \otimes_{\mathbb{K}} J_{n+1} \overset{\partial_{n+1}}{\to} A \otimes_{\mathbb{K}} J_n \overset{\partial_n}{\to} A \otimes_{\mathbb{K}} J_{n-1} \to \cdots \to A \otimes_{\mathbb{K}} \mathbb{K}R \overset{\partial_2}{\to} A \otimes_{\mathbb{K}} \mathbb{K}X \overset{\partial_1}{\to} A \otimes_{\mathbb{K}} \mathbb{K} \to 0$$

where the J_n are as defined in (4.5) and (4.6) and ∂_{n+1} is defined for $n \in \mathbb{N}$ as the restriction of the following map to $A \otimes J_{n+1}$:

$$\begin{aligned} A \otimes_{\mathbb{K}} \mathbb{K}X^{(\ell_N(n+1))} &\to A \otimes_{\mathbb{K}} \mathbb{K}X^{(\ell_N(n))} \\ 1_A \otimes w \quad &\mapsto \overline{w_1} \otimes w_2, \end{aligned}$$

with $w_1 \in \mathbb{K}X^{(\ell_N(n+1)-\ell_N(n))}$ and $w_2 \in \mathbb{K}X^{(\ell_N(n))}$ the unique words such that $w = w_1 w_2$.

Remark 4.2.2.5

So far, we have worked with the Koszul complex of left A-modules, but we could just as well work with the chain complex of right A-modules by tensoring the J_n by A on the right:

$$\cdots \to J_{n+1} \otimes_{\mathbb{K}} A \overset{\partial_{n+1}}{\to} J_n \otimes_{\mathbb{K}} A \overset{\partial_n}{\to} J_{n-1} \otimes_{\mathbb{K}} A \to \cdots \to \mathbb{K}R \otimes_{\mathbb{K}} A \overset{\partial_2}{\to} \mathbb{K}X \otimes_{\mathbb{K}} A \overset{\partial_1}{\to} \mathbb{K} \otimes_{\mathbb{K}} A \to 0$$

and defining ∂_{n+1} for $n \in \mathbb{N}$ as the restriction of the following map to $J_{n+1} \otimes A$:

$$\begin{aligned} \mathbb{K}X^{(\ell_N(n+1))} \otimes_{\mathbb{K}} A &\to \mathbb{K}X^{(\ell_N(n))} \otimes_{\mathbb{K}} A \\ w \otimes 1_A \quad &\mapsto w_1 \otimes \overline{w_2}, \end{aligned}$$

with $w_1 \in \mathbb{K}X^{(\ell_N(n))}$ and $w_2 \in \mathbb{K}X^{(\ell_N(n+1)-\ell_N(n))}$ the unique words such that $w = w_1 w_2$.

4.2.3 Koszul property

Depending on the author, the Koszul property for N-homogeneous algebras can be stated in different ways. For instance, Berger defines it as a purity condition on the Tor vector spaces. To understand this definition, let us start by explaining how the Tor groups can be endowed with a graded vector space structure when the resolution is taken in the category of graded A-modules.

If $(P_\bullet, \partial)$ is a projective resolution of $\mathbb{K}$ in the category of left (or right) A-modules, then tensoring by $\mathbb{K}$ over A to obtain the complex $(\mathbb{K} \otimes_A P_\bullet, \mathrm{id}_\mathbb{K} \otimes_A \partial)$ yields a complex of $\mathbb{K}$-vector spaces, since $\mathbb{K}$ can be seen as a $(\mathbb{K}, A)$-bimodule (or as a $(A, \mathbb{K})$-bimodule for the right A-modules variant) and since the differentials are $\mathbb{K}$-linear in particular, then the homology of that complex, known as the Tor groups, can be equipped with a structure of $\mathbb{K}$-vector space.

Moreover, if the A-modules in the resolution $(P_\bullet, \partial)$ are graded and the differentials are graded maps of degree 0, then a graduation can be canonically defined on the tensored complex $(\mathbb{K} \otimes_A P_\bullet, \mathrm{id}_\mathbb{K} \otimes_A \partial)$. It follows that the Tor vector spaces can be graded:

$$\mathrm{Tor}_n^A(\mathbb{K}, \mathbb{K}) = \bigoplus_{m \in \mathbb{N}} \mathrm{Tor}_{n,m}^A(\mathbb{K}, \mathbb{K}).$$

Before we express the Koszul property as Berger did in [Ber01], notice the following result:

Proposition 4.2.3.1 : [BM06, Proposition 2.1]

Let A be an N-homogeneous $\mathbb{K}$-algebra. Then:

$$\forall n \in \mathbb{N}, \quad \forall m < \ell_N(n), \quad \mathrm{Tor}_{n,m}^A(\mathbb{K}, \mathbb{K}) = 0.$$

The Koszul property is said expressed as the following purity condition:

Definition 4.2.3.2 : Koszul property

Let A be an N-homogeneous $\mathbb{K}$-algebra.
Then, A is a *Koszul algebra* if the graded Tor vector spaces are pure in degree given by the diagonal sequence, that is to say, if:

$$\forall n \in \mathbb{N}, \quad \forall m \neq \ell_N(n), \quad \mathrm{Tor}_{n,m}^A(\mathbb{K}, \mathbb{K}) = 0.$$

It is shown in [Ber01] and in [YZ03] that the following theorem is true:

Theorem 4.2.3.3 : ([Ber01, YZ03])

Let A be an N-homogeneous algebra.
Then, A is a Koszul algebra if and only if the Koszul complex as defined in 4.2.2.4 is a deleted resolution of $\mathbb{K}$ under the natural augmentation of graded connected algebras.

Another way to characterise the Koszulity of an algebra is by enforcing conditions on the *Yoneda algebra* as put forward in [BF85] for quadratic algebras but generalisable to homogeneous algebras:

Theorem 4.2.3.4 : ([BF85])

Let A be an N-homogeneous $\mathbb{K}$-algebra.
Then, A is a Koszul algebra if and only if $\mathrm{Ext}_A^{i,j}(\mathbb{K}, \mathbb{K}) = 0$ for all $\ell_N(i) \neq j$.

Yet another characterisation, also in terms of the Yoneda algebra, is presented in [HL05] and in [CS08]:

Theorem 4.2.3.5 : ([HL05, CS08])

Let A be an N-homogeneous $\mathbb{K}$-algebra.
Then, A is a Koszul algebra if and only if the bi-graded Yoneda algebra $\mathrm{Ext}_A(\mathbb{K},\mathbb{K})$ is generated as an algebra by $\mathrm{Ext}^1_A(\mathbb{K},\mathbb{K})$ and $\mathrm{Ext}^2_A(\mathbb{K},\mathbb{K})$.

Finally, when the algebra is *distributive* (see [Ber01, Section 3]), then the Koszulity is equivalent to the extra-condition of Berger:

Theorem 4.2.3.6 : ([Ber01])

Let $\mathcal{A} = A(E,R)$ be an N-homogeneous $\mathbb{K}$-algebra.
Suppose that $\mathcal{A}$ is distributive. Then, $\mathcal{A}$ is a Koszul algebra if only if it satistfies the *extra-condition* which is equivalent to:

$$\forall m \in [\![2\,..\,N-1]\!], \quad (E^{(m)} \otimes R) \cap (R \otimes E^{(m)}) \subseteq (E^{(m-1)} \otimes R \otimes E)$$

Notice how the extra-condition is an empty condition when $N = 2$.

4.3 Special case of homogeneous monomial algebras

4.3.1 Overlap property of homogeneous monomial presentations

This section is dedicated to the main result of this thesis: the Anick resolution (Theorem 4.1.3.2) and the Koszul complex (Definition 4.2.2.4) are the same when considering the case of homogeneous monomial algebras (Definition 1.2.3.5) satisfying the *overlap property*.

It is a result of [Ber01] that monomial algebras are distributive and that the extra-condition is equivalent to the so-called overlap property for homogeneoous monomial algebras described thereafter. It follows by Theorem 4.2.3.6 that homogeneous monomial algebras satisfying the overlap property are Koszul.

Definition 4.3.1.1 : Overlap property

Let $N \geqslant 2$ be an integer. Let $\langle X|R\rangle$ be a N-homogeneous monomial presentation of an algebra A.
The presentation $\langle X|R\rangle$ is said to satisfy the *overlap property* when, if $w \in \langle X\rangle$ is a word of length in $[\![N+2\,..\,2N-1]\!]$ that has a relation in R as a prefix as well as a relation in R as a suffix, then every subword of w of length N is a relation in R. In symbols:

$$\forall m \in [\![2\,..\,N-1]\!], \quad RX^{(m)} \cap X^{(m)}R \subseteq \bigcap_{i+j=m} X^{(i)}RX^{(j)}$$

To prove the result we have described at the start of this subsection we establish a few intermediary results in the next subsections. We begin by showing the special form the Anick resolution takes when considering monomial algebras. Then, we show that for any homogeneous monomial algebra, the Koszul complex is a subcomplex of the Anick resolution. Finally, we show in the last subsection that assuming the overlap property to be true implies that the Anick resolution and Koszul complex are equal.

4.3.2 Anick resolution for monomial algebras

In this subsection, we fix $\langle X|R\rangle$ a monomial presentation (Definition 1.2.3.3) of a homogeneoous monomial algebra (Definition 1.2.3.5) over a field $\mathbb{K}$. We take as augmentation for this algebra the naturally induced augmentation map induced by the graduation.

We can assume that R is an anti-chain for the subword relation, *i.e.* there are no relation in R that is a proper subword of another relation in R. Indeed, any relation being a proper superword of another is superfluous for the generated ideal and can therefore be omitted. In particular, if the presentation is also homogeneous, then R is an anti-chain since all relations are of the same length and thus cannot be proper subwords of other relations.

It follows that, since R are monomials, all the S-polynomials (Definition 1.2.4.5) of the relations necessarily reduce to zero and therefore R is a *minimal* non-commutative Gröbner basis (Definition 1.2.4.7) of the ideal generated by R.

Hence, we have the following proposition:

Proposition 4.3.2.1

Let $\langle X|R\rangle$ be a monomial presentation with R an anti-chain for the subword relation. The set of obstructions for the Anick resolution is exactly the set R of relations.

The differentials in the Anick resolution also admit a special form in that context:

Proposition 4.3.2.2

Let A be a monomial algebra presented with a monomial presentation $\langle X|R\rangle$. Write C_n the set of n-chains for $n\in\mathbb{N}$. Then:

$$\forall n\geqslant 1,\quad \forall c^{(n)}=[t_1,\cdots,t_n]\in C_n,\quad d_n\left([t_1,\cdots,t_n]\otimes 1_A\right)=[t_1,\cdots,t_{n-1}]\otimes\overline{t_n},$$

where $[t_1,\cdots,t_{n-1}]=1$ if $n=1$ and d_n are the differentials of the Anick resolution (Theorem 4.1.3.2).

Proof. For $n=1$, we have: $d_1(x\otimes 1_A)=1\otimes\overline{x}-\eta\varepsilon(\overline{x})$ but $\overline{x}$ is of degree 1 in the graduation of A which is augmented with the natural augmentation induced by the graduation. Hence, $\varepsilon(\overline{x})=0$ for all $x\in X$. It follows that $d_1(x\otimes 1_A)=1\otimes\overline{x}$.

Suppose the property is true for a certain $n\geqslant 1$. Let $c^{(n+1)}=[t_1,\cdots,t_{n+1}]\in C_{n+1}$. We have:

$$d_{n+1}\left([t_1,\cdots,t_{n+1}]\otimes 1_A\right)=[t_1,\cdots,t_n]\otimes\overline{t_{n+1}}-i_{n-1}d_n\left([t_1,\cdots,t_n]\otimes\overline{t_{n+1}}\right).$$

By induction hypothesis, we have:

$$d_n\left([t_1,\cdots,t_n]\otimes\overline{t_{n+1}}\right):=[t_1,\cdots,t_{n-1}]\otimes\overline{t_nt_{n+1}}.$$

But, since t_n and t_{n+1} are two consecutive tails in a $(n+1)$-chain with $n\geqslant 1$, then t_nt_{n+1} contains an obstruction (as a suffix). Since the presentation is monomial, the obstruction reduces to zero and thus $\overline{t_nt_{n+1}}=0$.

It follows that $d_{n+1}\left([t_1,\cdots,t_{n+1}]\otimes 1_A\right)=[t_1,\cdots,t_n]\otimes\overline{t_{n+1}}$ by linearity of d_n and i_{n-1}. □

As discussed previously in the section of properties of the Anick resolution, this special form of the differentials imply that the Anick resolution is minimal for monomial algebras.

4.3.3 Koszul is a subcomplex of Anick for homogeneous monomial algebras

Fix throughout this subsection an integer $N \geqslant 2$, a field $\mathbb{K}$, an N-homogeneous monomial $\mathbb{K}$-algebra A and $\langle X|R\rangle$ a homogeneous monomial presentation of A (Definition 1.2.3.5). We assume that A is augmented with the natural augmentation map induced by the graduation.

Consider the Anick resolution (Theorem 4.1.3.2):

$$\cdots \rightleftarrows \mathbb{K}C_{n+1} \otimes_{\mathbb{K}} A \underset{i_n}{\overset{d_{n+1}}{\rightleftarrows}} \mathbb{K}C_n \otimes_{\mathbb{K}} A \underset{i_{n-1}}{\overset{d_n}{\rightleftarrows}} \mathbb{K}C_{n-1} \otimes_{\mathbb{K}} A \rightleftarrows \cdots \rightleftarrows \mathbb{K}C_1 \otimes_{\mathbb{K}} A \underset{i_0}{\overset{d_1}{\rightleftarrows}} \mathbb{K}C_0 \otimes_{\mathbb{K}} A \underset{\eta}{\overset{\varepsilon}{\rightleftarrows}} \mathbb{K} \to 0 \tag{4.7}$$

and the Koszul complex of right A-modules (Remark 4.2.2.5) with the augmentation:

$$\cdots \to J_{n+1} \otimes_{\mathbb{K}} A \overset{\partial_{n+1}}{\to} J_n \otimes_{\mathbb{K}} A \overset{\partial_n}{\to} J_{n-1} \otimes_{\mathbb{K}} A \to \cdots \to J_1 \otimes_{\mathbb{K}} A \overset{\partial_1}{\to} J_0 \otimes_{\mathbb{K}} A \overset{\varepsilon}{\to} \mathbb{K} \to 0. \tag{4.8}$$

We will use the words "obstruction" and "relation" interchangeably in the sequel since we deal with a monomial presentation with R an anti-chain (see Proposition 4.3.2.1).

Denote by B_n for any $n \in \mathbb{N}$ the basis of the vector space J_n defined as follows, from the definitions of the J_n in (4.5) and (4.6):

$$B_0 = \{1\}, \qquad B_1 = X, \qquad B_2 = R, \tag{4.9}$$

and:

$$\forall n \geqslant 3, \quad B_n = \bigcap_{i=0}^{\ell_N(n)-N} X^{(i)} R X^{(\ell_N(n))-N-i}, \tag{4.10}$$

where ℓ_N denotes the diagonal sequence (Definition 4.2.2.1).

Remark 4.3.3.1

It follows from the definition of B_n for $n \geqslant 3$ in (4.10) that we have the following equivalence:

$$\forall w \in \langle X \rangle, \quad w \in B_n \quad \Leftrightarrow \begin{cases} w \text{ is of length } \ell_N(n) \text{ and,} \\ \text{any subword of } w \text{ of length } N \text{ is a relation in } R. \end{cases}$$

Theorem 4.3.3.2 : (Koszul complex is a subcomplex of Anick resolution)

Let $N \geqslant 2$ be an integer. Let $A = \langle X|R\rangle$ be an N-homogeneous monomial algebra presented with a homogeneous monomial presentation.

Then, the Koszul complex (4.8) is a subcomplex of the Anick resolution (4.7). In other words, we have:

$$\forall n \in \mathbb{N}, \quad J_n \otimes_{\mathbb{K}} A \subseteq \mathbb{K}C_n \otimes_{\mathbb{K}} A$$

and:

$$\forall n \geqslant 1, \quad \forall \omega \in J_n \otimes_{\mathbb{K}} A, \quad d_n(\omega) = \partial_n(\omega).$$

Proof. It suffices to show that the basis B_n of J_n is contained in the basis of $\mathbb{K}C_n$, for each $n \in \mathbb{N}$.

Combining the Remark 4.1.2.8 with the result of Proposition 4.3.2.1 and comparing with (4.9), we obtain that:

$$C_0 = \{1\} = B_0, \qquad C_1 = X = B_1, \qquad C_2 = R = B_2.$$

Let $n \geqslant 3$. Write $\ell := \ell_N(n)$. Let $w := x_1 \cdots x_\ell \in B_n$.

Define $t_1, \cdots, t_n$ as:

$$t_m := \begin{cases} x_{kN+1} & \text{if } \exists k \in \mathbb{N}, m = 2k+1, \\ x_{(k-1)N+2} \cdots x_{kN} & \text{if } \exists k \in \mathbb{N}, m = 2k, \end{cases} \tag{4.11}$$

for $m \in [\![1 \,..\, n]\!]$.

Notice how $w = t_1 \cdots t_n$. Indeed, we have:

- $t_1 = x_1$,
- $t_2 = x_2 \cdots x_N$,
- $t_3 = x_{N+1}$,
- $t_4 = x_{N+2} \cdots x_{2N}$ and so on, up until:
- $t_n = \begin{cases} x_{kN+1} & \text{if } n = 2k+1 \text{ (note that } \ell = \ell_N(2k+1) = kN+1), \\ x_{(k-1)N+2} \cdots x_{kN} & \text{if } n = 2k \text{ (note that } \ell = \ell_N(2k) = kN). \end{cases}$

If m is odd, t_m is of length 1, and if m is even, t_m is of length $N-1$. In both cases, t_m will always be shorter than $N \geqslant 2$ which means that $t_m \in O(I)$. Moreover, for all $m \in [\![1 \,..\, n-1]\!]$, $t_m t_{m+1}$ is a subword of w of length N. By Remark 4.3.3.1, we deduce that $t_m t_{m+1}$ is an obstruction. In particular, $t_m t_{m+1}$ contains a unique obstruction which is a suffix. That satisfies all the requirements for w to be considered an n-chain according to Definition 4.1.2.3. Thus: $B_n \subseteq C_n$.

Let $n \geqslant 1$. Let us now show that the restriction of the differentials d_n to $J_n \otimes_{\mathbb{K}} A$ corresponds exactly to ∂_n. Since the differentials are both A-linear, it suffices to show that they agree on all input of the form $w_n \otimes 1_A$ where $w_n \in B_n$.

Let $w_n \in B_n$. Denote by $w \in X^{(\ell_N(n-1))}$ and $t \in X^{(\ell_N(n)-\ell_N(n-1))}$ the unique words such that $w_n = wt$. By definition of the differentials for the Koszul complex, we have:

$$\partial_n(w_n \otimes 1_A) = w \otimes \bar{t}.$$

We have just shown that $B_n \subseteq C_n$. Thus, $w_n = [t_1, \cdots, t_n] \in C_n$ where the tails t_m are the ones defined in (4.11). So, on one hand, according to Proposition 4.3.2.2, we have:

$$d_n(w_n \otimes 1_A) = [t_1, \cdots, t_{n-1}] \otimes \overline{t_n},$$

and, on the other hand, we have $\text{length}(t_n) = \ell_N(n) - \ell_N(n-1)$ by definition of t_n and Remark 4.2.2.3. Hence, t_n is a suffix of w_n of the same size of t. By uniqueness, it follows that $t_n = t$, which in turn implies that $[t_1, \cdots, t_{n-1}] = w$. Hence, the result. $\square$

4.3.4 Overlap property implies equality

In this subsection, we use the same assumptions stated at the start of the last subsection (and the same notations), but we suppose furthermore that the presentation $\langle X|R\rangle$ verifies the overlap property (Definition 4.3.1.1).

First, notice the following result:

Proposition 4.3.4.1

Consider the assumptions of this subsection.
Let $n \in \mathbb{N}$. Let $c^{(n+1)} = c^{(n)}t \in C_{n+1}$ where $c^{(n)}$ is an n-chain and t is the tail of $c^{(n+1)}$.

$$\operatorname{length}(t) = \begin{cases} 1 & \text{if } n \text{ even,} \\ N-1 & \text{if } n \text{ odd.} \end{cases}$$

In particular, for any $n \in \mathbb{N}$, every n-chain is of length $\ell_N(n)$.

Proof. Let us proceed by induction on n.

For $n = 0$, an $(n+1)$-chain is by definition a letter and is its own tail, therefore its tail is of length 1.

Let $n \in \mathbb{N}$ such that $c^{(n+1)} = c^{(n)}t \in C_{n+1}$ with the tail t of the length stated in the proposition. Let $c^{(n+2)} = c^{(n+1)}t' \in C_{n+2}$ be an $(n+2)$-chain with t' as a tail.

By Remark 4.1.2.4, tt' contains a unique obstruction that both is a suffix and overlaps on t.

If n is even, then t is of length 1. Hence, t' is of length exactly $N-1$, otherwise the obstruction would not overlap on t.

If n is odd, then t is of length $N-1$. By contradiction, suppose t' is of length $\ell > 1$. Necessarily, we have $\ell < N$ since the suffix of tt' of length N must overlap with t. Hence, the word tt' is of length $N - 1 + \ell \in [\![N+1 \mathinner{..} 2N-2]\!]$. Since $n > 0$, we can take $c^{(n)} = c^{(n-1)}t''$ with t'' of length 1 (by strong induction) and $t''t$ an obstruction. Hence, the word $t''tt'$ of length in $[\![N+2 \mathinner{..} 2N-1]\!]$ starts and ends in an obstruction. By the overlap property it follows that the prefix of length N in the word tt' is an obstruction which is different from the obstruction which is a suffix of tt': this contradicts the uniqueness of the obstruction contained in tt'. Hence, $\ell = 1$.

For the last result of the proposition, reason step by step: an n-chain $c^{(n)}$ is the succession of n tails $t_1, \cdots, t_n$. Then, from the first result, the n-chain $c^{(n)}$ is of length:

$$1 + (N-1) + 1 + (N-1) + \cdots + \operatorname{length}(t_n) = \begin{cases} kN & \text{if } \exists k \in \mathbb{N}, n = 2k, \\ kN+1 & \text{if } \exists k \in \mathbb{N}, n = 2k+1, \end{cases}$$

which is exactly equal to $\ell_N(n)$ by definition of the diagonal sequence (Definition 4.2.2.1). □

Remark 4.3.4.2

It follows from the assumptions of this subsection that the algebra A is Koszul, which means that the Koszul complex (4.8) is a resolution of $\mathbb{K}$ in the category of right A-modules. Moreover, it is a result in [Ber01] that this resolution is minimal.
On the other hand, we have already established that the Anick resolution is minimal for monomial algebras. Hence, in our present context, the Koszul complex and the Anick resolution are isomorphic. We proceed to show that, even more than that, they are actually equal.

Before that, let us introduce the contracting homotopy $h_n : J_n \otimes_{\mathbb{K}} A \to J_{n+1} \otimes_{\mathbb{K}} A$ of the Koszul complex as presented in [Che16] for Koszul homogeneous monomial algebras but adapted for right A-modules:

$$\forall w \in B_n, \quad \forall s \in O(I), \quad h_n(w \otimes \overline{s}) = \begin{cases} wp \otimes \overline{t} & \text{if } \exists p, t \in \langle X \rangle, s = pt \text{ and } wp \in B_{n+1}, \\ 0 & \text{otherwise.} \end{cases} \tag{4.12}$$

Lemma 4.3.4.3

Let $n \in \mathbb{N}$. Let $c^{(n)} = [t_1, \cdots, t_n] \in C_n$ and $s \in O(I)$. Then:

$c^{(n)} \otimes \overline{s} \in \ker(d_n) \setminus \{0\} \quad \Leftrightarrow \quad \exists t_{n+1} \in O(I), \quad t_{n+1}$ is a prefix of s and $[t_1, \cdots, t_{n+1}] \in C_{n+1}$,

where $d_0 := \varepsilon$ and $[t_1, \cdots, t_n] = 1$ if $n = 0$.

Proof. By exactness, belonging in $\ker(d_n)$ is equivalent to belonging in $\mathrm{im}(d_{n+1})$. By definition of the image, this means:

$$\exists c_i^{(n+1)} \in C_{n+1}, \quad \exists s_i \in O(I), \quad c^{(n)} \otimes \overline{s} = d_{n+1}\left(\sum_i c_i^{(n+1)} \otimes \overline{s_i}\right),$$

which is equivalent to, by Proposition 4.3.2.2:

$$\exists c_i^{(n+1)} = \left[t_1^{(i)}, \cdots, t_{n+1}^{(i)}\right] \in C_{n+1}, \quad \exists s_i \in O(I), \quad c^{(n)} \otimes \overline{s} = \sum_i \left[t_1^{(i)}, \cdots, t_n^{(i)}\right] \otimes \overline{t_{n+1}^{(i)} s_i}.$$

Now since $\langle X | R \rangle$ is a monomial presentation, if $t_{n+1}^{(i)} s_i$ is not a normal form, then the corresponding term $\left[t_1^{(i)}, \cdots, t_n^{(i)}\right] \otimes \overline{t_{n+1}^{(i)} s_i}$ equals 0. Hence, we can assume that all the $t_{n+1}^{(i)} s_i$ are in normal form, *i.e.* are in $O(I)$.

But since the set $\left\{c'^{(n)} \otimes \overline{s'} \;\middle|\; c'^{(n)} \in C_n, s' \in O(I)\right\}$ is a basis of $\mathbb{K}C_n \otimes_{\mathbb{K}} A$, then the decomposition in linear combination of terms of this form is unique. Therefore, this is equivalent to:

$$\exists c^{(n+1)} = [t'_1, \cdots, t'_{n+1}] \in C_{n+1}, \quad \exists s' \in O(I), \quad c^{(n)} \otimes \overline{s} = [t'_1, \cdots, t'_n] \otimes \overline{t'_{n+1} s'}.$$

By identification, it follows that $t_i = t'_i$ for all $i \in [\![1 \mathinner{..} n]\!]$ and, since both s and $t'_{n+1} s'$ are in normal form, t'_{n+1} is a prefix of s that satisfy the statement of the lemma. □

Let us now prove the main theorem.

Theorem 4.3.4.4 : (Koszul equals Anick)

Let $N \geqslant 2$ be an integer. Let $A = \mathbb{K}\langle X | R \rangle$ be an N-homogeneous monomial algebra presented with a homogeneous monomial presentation that satisfies the overlap property.
Then, the Koszul complex (4.8) and the Anick resolution (4.7) are equal.
Moreover, the respective contracting homotopies are equal.

Proof. We have shown in Theorem 4.3.3.2 that the Koszul complex is a subcomplex of the Anick resolution, which means that $J_n \otimes_{\mathbb{K}} A \subseteq \mathbb{K}C_n \otimes_{\mathbb{K}} A$ for all $n \in \mathbb{N}$ and that the restriction of d_n to $J_n \otimes_{\mathbb{K}} A$ is equal to ∂_n for all $n \geqslant 1$. For this purpose, we have proven that $B_n \subseteq C_n$ for all $n \in \mathbb{N}$. To prove the equality of the resolutions, it suffices to show the converse inclusion.

We have already established that $B_n = C_n$ for $n \in \{0, 1, 2\}$. Let us show by induction on n that is true for $n \geqslant 3$.

For $n = 3$, let $w \in C_3$. Then by Proposition 4.3.4.1 it follows that w if of length $\ell_N(3) = N + 1$. It starts and ends with obstructions of length N, thus it trivially satisfies the condition in Remark 4.3.3.1 to belong to B_3.

Suppose that for a certain n we have $C_n \subseteq B_n$. Let $w \in C_{n+1}$. By Proposition 4.3.4.1, it is of length $\ell_N(n+1)$ and the prefix p of w of length $\ell_N(n)$ is an n-chain. Therefore, $p \in B_n$ by induction hypothesis. This means that all subwords of p of length N are obstructions. It only remains to show that the subwords of length N that start at the $(\ell_N(n) - N + 1)$'th letter or after in w are also obstructions.

Consider thus the suffix s of w that start on the $(\ell_N(n) - N)$'th letter. It is therefore of length: $\ell_N(n+1) - \ell_N(n) + N \in \{N+1, 2N-1\}$. If it is of length $N+1$, the result is trivial since it starts with the second-to-last obstruction and ends with the last obstruction and those are the only two subwords of length N. Otherwise, if it is of length $2N-1$, we can apply the overlap property to conclude that all the subwords of s of length N are obstructions.

Hence, w is of length $\ell_N(n+1)$ and all its subwords of length N are obstructions. It follows by Remark 4.3.3.1 that $w \in B_{n+1}$ and thus $C_{n+1} \subseteq B_{n+1}$.

Let us now show that the respective contracting homotopies i_n (Theorem 4.1.3.2) and h_n (4.12) are equal. Since we have $B_n = C_n$ for all $n \in \mathbb{N}$, the Lemma 4.3.4.3 actually proves that the conditions stated in the definition of i_n and h_n are equivalent. Indeed, identifying respectively $c^{(n)}$ with w, s with s and t_{n+1} with p from Lemma 4.3.4.3 to the definition of h_n in (4.12), the condition t_{n+1} (which equals p) is a prefix of s is equivalent to the existence of t such that $s = pt$ and the condition that $[t_1, \cdots, t_{n+1}]$ (which is equal to $c^{(n)}t_{n+1}$ and thus wp) is in C_{n+1} is equivalent to $wp \in B_{n+1}$, since the sets are equal.

Finally, then, it suffices to show that i_n and h_n agree whenever they are not zero.

Let $w = [t_1, \cdots, t_n] \in C_n = B_n$ and $s \in O(I)$ such that there exists $t_{n+1} \in O(I)$ prefix of s (that is to say $s = t_{n+1}t$ for a certain $t \in O(I)$) and $wt_{n+1} \in C_{n+1} = B_{n+1}$. Then:

$$\begin{aligned}
i_n(w \otimes \overline{s}) &= wt_{n+1} \otimes \overline{t} + i_n\left(w \otimes \overline{s} - d_{n+1}\left([t_1, \cdots, t_{n+1}] \otimes \overline{t}\right)\right) && \text{by definition of } i_n \\
&= wt_{n+1} \otimes \overline{t} + i_n\left(w \otimes \overline{s} - [t_1, \cdots, t_n] \otimes \overline{t_{n+1}t}\right) && \text{by Proposition 4.3.2.2} \\
&= wt_{n+1} \otimes \overline{t} && \text{by the assumptions on } w \text{ and } s \\
i_n(w \otimes \overline{s}) &= h_n(w \otimes \overline{s}) && \text{by definition of } h_n
\end{aligned}$$

□

Bibliography

[Ani82] David J Anick. Non-commutative graded algebras and their Hilbert series. *Journal of Algebra*, 78(1):120–140, September 1982.

[Ani85] David J. Anick. On monomial algebras of finite global dimension. *Transactions of the American Mathematical Society*, 291:291–310, 1985.

[Ani86] David J. Anick. On the homology of associative algebras. *Transactions of the American Mathematical Society*, 296:641–659, 1986.

[BDVW03] Roland Berger, Michel Dubois-Violette, and Marc Wambst. Homogeneous algebras. *Journal of Algebra*, 261(1):172–185, 2003.

[Ber98a] Roland Berger. Confluence and Koszulity. *Journal of Algebra*, 201(1):243–283, 1998.

[Ber98b] Roland Berger. Weakly confluent quadratic algebras. *Algebras and Representation Theory*, 1(3):189–213, 1998.

[Ber01] Roland Berger. Koszulity for nonquadratic algebras. *Journal of Algebra*, 239(2):705–734, 2001.

[BF85] Jörgen Backelin and Ralf Fröberg. Koszul algebras, Veronese subrings and rings with linear resolutions. *Revue Roumaine de Mathématiques Pures et Appliquées*, 30:85–97, 1985.

[BGS88] A. A. Beilinson, V. A. Ginsburg, and V. V. Shekhtman. Koszul duality. *Journal of Geometry and Physics*, 5(3):317–350, 1988.

[BM06] Roland Berger and Nicolas Marconnet. Koszul and Gorenstein properties for homogeneous algebras. *Algebras and Representation Theory*, 9(1):67–97, 2006.

[CE56] Henri Cartan and Samuel Eilenberg. *Homological algebra*, volume 19 of *Princeton Math. Ser.* Princeton University Press, Princeton, NJ, 1956.

[Che16] Cyrille Chenavier. *Le treillis des opérateurs de réduction : applications aux bases de Gröbner non commutatives et en algèbre homologique. (The lattice of reduction operators: applications to noncommutative Gröbner bases and homological algebra).* PhD thesis, Paris Diderot University, France, 2016.

[CS08] Thomas Cassidy and Brad Shelton. Generalizing the notion of Koszul algebra. *Mathematische Zeitschrift*, 260(1):93–114, 2008.

[CU97] S. Cojocaru and V. Ufnarovski. BERGMAN under MS-DOS and Anick's resolution. *Discrete Mathematics and Theoretical Computer Science. DMTCS*, 1(2):139–147, 1997.

[DM82] Pierre Deligne and J. S. Milne. Tannakian categories. Hodge cycles, motives, and Shimura varieties, Lect. Notes Math. 900, 101-228 (1982)., 1982.

[DMR99] P. Dräxler, G. O. Michler, and C. M. Ringel, editors. *Computational methods for representations of groups and algebras. Proceedings of the Euroconference in Essen, Germany, April 1–5, 1997*, volume 173 of *Prog. Math.* Basel: Birkhäuser, 1999.

[Eil56] Samuel Eilenberg. Homological dimension and syzygies. *Annals of Mathematics. Second Series*, 64:328–336, 1956.

[EM45] Samuel Eilenberg and Saunders MacLane. General theory of natural equivalences. *Transactions of the American Mathematical Society*, 58(2):231–294, sep 1945.

[EM53] Samuel Eilenberg and Saunders MacLane. On the groups $H(\Pi, n)$. I. *Annals of Mathematics. Second Series*, 58:55–106, 1953.

[Far92] Daniel R. Farkas. The Anick resolution. *Journal of Pure and Applied Algebra*, 79(2):159–168, 1992.

[GS07] Edward L. Green and Øyvind Solberg. An algorithmic approach to resolutions. *Journal of Symbolic Computation*, 42(11-12):1012–1033, 2007.

[HL05] Ji-Wei He and Di-Ming Lu. Higher Koszul algebras and A-infinity algebras. *Journal of Algebra*, 293(2):335–362, 2005.

[HS97] P. J. Hilton and U. Stammbach. *A course in homological algebra.*, volume 4 of *Grad. Texts Math.* New York, NY: Springer, 2nd ed. edition, 1997.

[Kos50] Jean-Louis Koszul. Homologie et cohomologie des algèbres de Lie. *Bulletin de la Société Mathématique de France*, 78:65–127, 1950.

[KS06] Masaki Kashiwara and Pierre Schapira. *Categories and sheaves*, volume 332 of *Grundlehren Math. Wiss.* Berlin: Springer, 2006.

[Mal19] Philippe Malbos. Noncommutative linear rewriting: applications and generalizations. In *Two algebraic byways from differential equations: Gröbner bases and quivers*, volume 28 of *Algorithms and Computations in Mathematics*. Springer, 2019. Lecture note of the Kobe-Lyon summer school 2015.

[ML95] Saunders Mac Lane. *Homology.* Class. Math. Berlin: Springer-Verlag, reprint of the 3rd corr. print. 1975 edition, 1995.

[ML98] Saunders Mac Lane. *Categories for the working mathematician.*, volume 5 of *Grad. Texts Math.* New York, NY: Springer, 2nd ed edition, 1998.

[ML23] Adya Musson-Leymarie. On Anick resolution: from the original setting to the language of non-commutative Groebner bases, July 2023.

[Mor94] Teo Mora. An introduction to commutative and noncommutative Gröbner bases. *Theoretical Computer Science*, 134(1):131–173, 1994.

[NWW19] Van C. Nguyen, Xingting Wang, and Sarah Witherspoon. Finite generation of some cohomology rings via twisted tensor product and Anick resolutions. *Journal of Pure and Applied Algebra*, 223(1):316–339, 2019.

[Per19] Paolo Perrone. Notes on category theory with examples from basic mathematics. December 2019.

[Pri70] Stewart B. Priddy. Koszul resolutions. *Transactions of the American Mathematical Society*, 152:39–60, 1970.

[Rie16] Emily Riehl. *Category theory in context.* Mineola, NY: Dover Publications, 2016.

[Rot09] Joseph J. Rotman. *An introduction to homological algebra.* Universitext. Berlin: Springer, 2nd ed. edition, 2009.

[Ser77] Jean-Pierre Serre. *Linear representations of finite groups. Translated from the French by Leonard L. Scott*, volume 42 of *Grad. Texts Math.* Springer, Cham, 1977.

[Tat57] John Tate. Homology of Noetherian rings and local rings. *Illinois Journal of Mathematics*, 1:14–27, 1957.

[Ufn95] V. A. Ufnarovskij. Combinatorial and asymptotic methods in algebra. In *Algebra VI. Combinatorial and asymptotic methods of algebra. Non- associative structures. Transl. from the Russian by R. M. Dimitrić*, pages 1–196. Berlin: Springer-Verlag, 1995.

[Wei94] Charles A. Weibel. *An Introduction to Homological Algebra*, volume 38 of *Camb. Stud. Adv. Math.* Cambridge: Cambridge University Press, apr 1994.

[Wei99] Charles A. Weibel. History of homological algebra. In *History of topology*, pages 797–836. Amsterdam: Elsevier, 1999.

[YZ03] Yu Ye and Pu Zhang. Higher Koszul complexes. *Science in China. Series A*, 46(1):118–128, 2003.