united nations
educational, scientific
and cultural
organization

international atomic
energy agency

the
abdus salam
international centre for theoretical physics

ICTP 40th Anniversary

SMR1563/4

School on Commutative Algebra and Interactions with Algebraic Geometry and Combinatorics

(24 May - 11 June 2004)

On the equations defining the affine curves

L. Badescu
Università di Genova
Dipartimento di Matematica
Via Dodecaneso 35
16146 Genova
Italy

ON THE EQUATIONS DEFINING THE AFFINE CURVES

LUCIAN BĂDESCU

INTRODUCTION

The aim of these notes is to determine the minimal number of equations needed to define a given curve in the 3-dimensional affine space $\mathbb{A}^3$ over an algebraically closed field K. To be more precise we need some definitions. Let $A := K[X_1, ..., X_n]$ be the K-algebra of polynomials in the n indeterminates $X_1, ..., X_n$. To every $I \subset A$ one can associate the subset $\mathcal{V}(I) \subset \mathbb{A}^n$ defined by

$$\mathcal{V}(I) := \{(x_1, ..., x_n) \in \mathbb{A}^n \mid P(x_1, ..., x_n) = 0, \ \forall P \in I\}.$$

The subsets of $\mathbb{A}^n$ of the form $\mathcal{V}(I)$, with I an arbitrary ideal of A, are called algebraic subsets of $\mathbb{A}^n$. On the other hand, to every subset $V \subset \mathbb{A}^n$ one can associate the ideal $\mathcal{I}(V) \subset \mathbb{A}^n$ defined by

$$\mathcal{I}(V) := \{P \in A \mid P(x_1, ..., x_n) = 0, \ \ \forall (x_1, ..., x_n) \in V\}.$$

The ideal $\mathcal{I}(V)$ is called *the ideal* of V. The well-known Hilbert Nullstellensatz states that for every ideal I of A the following equality holds: $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$, where

$$\sqrt{I} := \{P \in A \mid \exists n = n_a > 0 \ : \ a^n \in I\}.$$

Let now $V := \mathcal{V}(I)$ be an algebraic subset of $\mathbb{A}^n$. If J is an ideal of A such that $\mathcal{V}(I) = \mathcal{V}(J)$, then Hilbert's Nullstellensatz yields $\sqrt{I} = \sqrt{J}$ (and conversely). By the a famous theorem of Hilbert the ring A is Noetherian, so that the ideal J is finitely generated. Let $\{f_1, ..., f_m\}$ be a system of generators of the ideal J. Then $f_1, ..., f_m$ are called equations defining the algebraic subset V set-theoretically in $\mathbb{A}^n$. In other words one has the equality

$$(*) \qquad V = \{(x_1, ..., x_n) \in \mathbb{A}^n \mid f_i(x_1, ..., x_n) = 0, \ \forall i = 1, ..., m\}.$$

The general problem we want to study is the following: assuming we are given the algebraic subset $V = \mathcal{V}(I) \subseteq \mathbb{A}^n$, determine the minimal number of equations that define V set-theoretically. In other words, determine the minimal number $m = m(V) \in \mathbb{N}$ such that there exist $f_1, ..., f_m \in A$ such that the equality $(*)$ holds, i.e.

$$\sqrt{I} = \sqrt{Af_1 + \cdots + Af_m}.$$

A general standard fact shows that the number $m = m(V)$ satisfies the following inequality:

$$(**) \qquad m \geq n - \dim(V).$$

If in $(**)$ the equality holds, one says that V is *set-theoretically a complete intersection* in $\mathbb{A}^n$.

If V is a hypersuface, i.e. $\dim(V) = n - 1$, the answer to this question is very simple because in this case the ideal $I = \mathcal{I}(V)$ is principal. This follows from the fact that the polynomial K-algebra $A = K[X_1, ..., X_n]$ is factorial (or UFD); if for example the hypersurface V is irreducible then I is a prime ideal of height one, and thus I is a principal ideal because A is factorial.

But if $\dim(V) \leq n - 2$ the problem becomes a lot more complicated and in fact is an open question for $n \geq 4$. Here we shall restrict ourselves to the case $n = 3$ and $\dim(V) = 1$, i.e. to the case of affine space curves. Our aim is to present (following [K]), and in large part also to prove, the algebraic results which lead to the proof of the following fundamental:

Main theorem. *(Serre-Ferrand-Szpiro) Let V be an affine algebraic curve in the affine 3-dimensional space $\mathbb{A}^3$. If V is a local complete intersection in $\mathbb{A}^3$ (for example, if V is smooth) then V is a set-theoretic complete intersection in $\mathbb{A}^3$, i.e. V is given (set-theoretically) by two equations in $\mathbb{A}^3$.*

Here are the main ingredients of the proof of this result:

1) A criterion due to Serre to recognize when an ideal I which is locally a complete intersection in a Cohen-Macaulay ring A is generated by two elements (see Corollary 4 of section 2).

2) A result of Serre which states that, given a commutative ring A and two projective A-modules P and L such that $\text{rank}(P) > \dim(A)$ and $\text{rank}(L) = 1$, then there exists a surjective homomorphism of A-modules $\varphi : P \to L$ (see Corolary 5 of section 2).

3) A duality theorem concerning the A-module $\text{Ext}^1_A(I, A)$, where $I \subset A$ is an ideal of projective dimension ≤ 1 (see Theorem 4 of section 3).

4) A construction (due to Ferrand) which allows one, starting with an ideal $I \subset A$, to produce another ideal J "with small number of generators" and such that $\sqrt{J} = \sqrt{I}$ (see (3.3) and Theorema 6 of section 4).

5) A fundamental result (conjectured by Serre and) proved independently by Quillen and Suslin which states that every projective module of finite type over the polynomial K-algebra $A = k[X_1, ..., X_n]$ is free (this is the only ingredient not proved in this paper).

We included a preliminary section 1 which presents the main concepts and general results of commutative and homological algebra needed in the subsequent sections. The proof of the main theorem can be found in section 4.

We also inluded three additional sections 5, 6 and 7. In section 5 we prove, following [EE], a result due to Kneser-Eisenbud-Evans according to which every closed algebraic subset of $\mathbb{A}^n$ or of P^n is the set-theoretic intersection of n hypersurfaces (of $\mathbb{A}^n$ or of P^n). In section 6 we prove (following [G] and [H3]) that there some topological constraint for an algebraic subset X of dimension ≥ 2 of $\mathbb{A}^n$ to be a set-theoretic complete intersection.

The material of these two sections complements nicely the above main theorem. Finally, in the last section we use a topological Lefschetz-type theorem for integral homology to produce more examples of subvarieties of the complex projective space that are not set-theoretic complete intersections.

1. Preliminaries

(1.1) Free modules. All rings considered are commutative and unitary (with $1 \neq 0$). If M and N are two A-modules, we shall denote by $\mathrm{Hom}_A(M,N)$ the A-module of all homomorphisms of A-modules defined on M with values in N. An element of $\mathrm{Hom}_A(M,N)$ will be called simply homomorphism, if no danger of confusion is possible. A subset B of an A-module M will be called *basis* of M if B is linearly independent over A as well as a system generators of the A-module M. In other words,

(1.1.1) For every family $\{\lambda_x\}_{x\in B}$ of elements of A of finite support such that $\sum_{x\in B}\lambda_x x = 0$, then necessarly $\lambda_x = 0\ \forall x \in B$ (the linear independence).

(1.1.2) For every element $m \in M$ there exists a family $\{\lambda_x\}_{x\in B}$ of elements of A of finite support such that $m = \sum_{x\in B}\lambda_x x$ (generatedness).

If B is a basis of the A-module M then every element $m \in M$ can be uniquely expressed as a linear combination of elements of B (with coefficients in A) as (1.1.2).

An A-module M is called *free* if M has a basis. For example the A-module A^n (with $n \geq 1$) is free because the subset

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

is a basis of A^n. On the other hand, taking $A = \mathbb{Z}$, then the $\mathbb{Z}$-modules (= the abelian groups) $M = \mathbb{Z}/n\mathbb{Z}$ (with $n \geq 2$), or $M = \mathbb{Q}$ are not free; indeed, in the first case every subset of M linearly dependent, while in the second, every two elements of M are linearly dependent (over $\mathbb{Z}$).

If A is a commutative unitary ring and if X is an arbitrary non-empty set, then there exists a a pair (L_X,φ_X) consisting of a free A-module L_X and of a function $\varphi_X : X \to L_X$, with the following properties:

(1.1.3) For every other function $\psi : X \to M$, with M an arbitrary A-module, there exists a unique homomorphism $\psi' \in \mathrm{Hom}_A(M,N)$ such that $\psi' \circ \varphi_X = \psi$.

A pair (L_X,φ_X) satisfying (1.1.3) is called *the free A-module of basis X*. Any two free A-modules of basis X are canonically isomorphic (as one can easily see). On the other hand, given A and X, we can construct L_X as the set of all functions $\chi : X \to A$ of finite support (i.e. $\chi(x) \neq 0$ only for finitely many $x \in X$). The operations on L_X are defined by $(\chi+\chi')(x) = \chi(x)+\chi'(x)$ and $(\lambda\chi)(x) = \lambda\chi(x)$, $\forall x \in X$ and $\forall \lambda \in A$. Then the function $\varphi_X : X \to L_X$ is defined in the following way: for every $x \in X$, $\varphi_X(x)$ is the characteristic function of x, i.e. $[\varphi_X(x)](y) = 0\ \forall y \neq x$ and $[\varphi_X(x)](x) = 1$. Then it is a simple exercise to check that the pair (L_X,φ_X) satisfies (1.1.3).

(1.2) Projective modules. Let P be an A-module over the commutative unitary ring A. We say that P is a *projective A-module* if for every surjective homomorphism $\varphi \in \mathrm{Hom}_A(M,M'')$ and for every $f \in \mathrm{Hom}_A(P,M'')$, there exists a (not necessarly unique) homomorphism $g \in \mathrm{Hom}_A(P,M)$ such that $f = \varphi \circ g$. In other words, P is projective if for every surjective homomorphism $\varphi : M \to M''$ the induces homomorphism $\varphi' : \mathrm{Hom}_A(P,M) \to \mathrm{Hom}_A(P,M'')$ defined by $\varphi'(g) = \varphi \circ g$, $\forall g \in \mathrm{Hom}_A(P,M)$, is again surjective.

Proposition 1. *Every free A-module is projective.*

Proof. Let P be a free A-module of basis B, $\varphi : M \to M''$ a surjective homomorphism, and $f : P \to M''$ a arbitrary homomorphism. Consider the family $\{f(x)\}_{x\in B}$ of elements of M''; since φ is surjective, there exists a family $\{m_x\}_{x\in B}$ of elements of M such that $\varphi(m_x) = f(x)$, $\forall x \in B$. In this way we get the function $B \to M$ defined by $x \to m_x$. Since B is a basis of the A-module P, this function can be extended to a unique homomorphism of A-modules $g : P \to M$. Then by construction, $f = \varphi \circ g$. □

Proposition 2. *(i) Every A-module M is a quotient of a free A-module, i.e. there exists a free A-module L and a surjective homomorphism of A-modules $f : L \to M$. Moreover, L can be chosen finitely generated if M is finitely generated.*
(ii) Every projective finitely generated A-module P is a direct summand of a free A-module of finite rank. Conversely, if a finitely generated A-module P is a direct summand of a free A-module of finite rank then P is a projective A-module.

Proof. *(i)* Let $G \subseteq M$ be a system of generators of the A-module M, and let $L := L_G$ be the free A-module of basis G. Since $G \subseteq M$, by the universal property (1.1.3), there exists a unique homomorphism $f : L \to M$ such that $f(g) = g$, $\forall g \in G$. Since G is a system of generators of A-module M, the homomorphism f is surjective. If M is a finitely generated A-module we can choose G finite, so that the free A-module $L = L_G$ is also finitely generated.

(ii) Let P be a projective A-module. By *(i)* there exists a free A-module L and a surjective homomorphism $\varphi : L \to P$. Taking $f = \mathrm{id}_P$ and using the fact that P is projective, we deduce the existence of a homomorphism $\psi \in \mathrm{Hom}_A(P, L)$ such that $\varphi \circ \psi = \mathrm{id}_P$.

Conversely, assume that P is a direct summand of the free A-module of finite rank L, i.e. there exist two homomorphisms $\varphi \in \mathrm{Hom}_A(L, P)$ and $\psi \in \mathrm{Hom}_A(P, L)$ such that $\varphi \circ \psi = \mathrm{id}_P$. Let $u : M \to M''$ be an arbitrary surjective homomorphism, and let $f : P \to M''$ be an arbitrary homomorphism. We have to show that there exists a homomorphism $g : P \to M$ such that $f = u \circ g$. Since L is free, by Proposition 1, L is projective, so that there exists a homomorphism $g' : L \to M$ such that $u \circ g' = f \circ \varphi$. Setting $g := g' \circ \psi$, one immediately checks (using $\varphi \circ \psi = \mathrm{id}_P$) that $u \circ g = f$. □

(1.3) Remark. The converse of Proposition 1 is in general false. For example, consider the ring $A = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, with $n \geq 2$. Let $P := \mathbb{Z}/n\mathbb{Z}$, viewed as an A-module via the second projection $p_2 : A \to \mathbb{Z}/n\mathbb{Z}$. In other words, the scalar multiplication on P is given by $(a, b) \cdot x = bx$, $\forall (a, b) \in A$, $\forall x \in P$. Then P is a direct summand of the free A-module A (of rank one); indeed if $\psi : P \to A$ is the homomorphism $x \to (\hat{0}, x)$, then $p_2 \circ \psi = \mathrm{id}_P$. On the other hand, P cannot be a free A-module, because otherwise P would have a basis consisting of m elements, and so P would have $(n^2)^m = n^{2m}$ elements, which is obviously impossible (since P has only n elements).

However, in the "local case" we have the following converse of Proposition 1:

Prososition 3. *Let A be a local Noetherian ring and M a finitely generated A-module. Then M is a projective A-module if and only if M is a free A-module.*

Proof. If M is free then M is projective by Proposition 1. Assume therefore that M projective. Let us denote by m_A the maximal ideal of A and by $k = A/m_A$ the residue field of A. Clearly we may assume $M \neq 0$. Choose a minimal system of generators $G := \{x_1, ..., x_n\}$ of the A-module M and consider the homomorphism $\varphi : A^n \to M$ defined by $\varphi(a_1, ..., a_n) = a_1x_1 + \cdots + a_nx_n$. We shall prove that φ is in fact an isomorfism of A-modules (which obviously will prove our proposition). The fact that G is a set of generators is equivalent is equivalent to the surjectivity of φ. Thus it remains to prove the injectivity of φ. To this end consider the exact sequence

$$0 \to K \to A^n \to M \to 0,$$

where $K := \mathrm{Ker}(\varphi)$. Since M is projective, there exists a homomorphism $\psi : M \to A^n$ such that $\varphi \circ \psi = \mathrm{id}_M$, i.e. the above exact sequence splits (in other words, $A^n \cong M \oplus K$). Since the tensor product is an additive functor (which in particular commutes with the finite direct sums) it follows that the sequence

$$0 \to K \otimes_A k \to A^n \otimes_A k \to M \otimes_A k \to 0$$

is also a split exact sequence, where the third arrow is the homomorphism

$$\varphi \otimes_A k : A^n \otimes_A k \cong k^n \to M \otimes_A k \cong M/m_AM$$

induced by φ.

On the other hand, the minimality of G implies that the map $\varphi \otimes k$ is an isomorphism of k-vector spaces. Then from the second exact sequence it follows $K/m_AK \cong K \otimes_A k = 0$. Since A is Noetherian, K is a finitely generated A-module (as a submodule of the finitely generated A-module A^n). By Nakayama's Lemma we infer that $K = 0$, i.e. φ is an isomorphism. □

Proposition 4. *Let M be a finitely generated A-module over the Noetherian ring A. Then M is a projective A-module if and only if for every maximal ideal m of A the A_m-module M_m is free, where A_m (resp. M_m) is the localization of A (resp. of M) with respect to m (i.e. A_m (resp. M_m) is the fractions ring of A (resp. the fractions module of M) with respect to the multiplicative set $S_m := A \setminus m$).*

Proof. The direct implication is a consequence of Proposition 3. Conversely, assume that M_m is a free A_m-module for every maximal ideal m al lui A. To prove that M is projective we have to prove that for every surjective homomorphism of A-modules $\varphi : N \to N''$, the homomorphism $\varphi' : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, N')$ is also surjective, where φ' is defined by the formula $\varphi'(f) := \varphi \circ f$. To prove the surjectivity of φ' we need the following:

Claim. Let $f : L \to L'$ be a homomorphism of A-modules. Then f is surjective if and only if the induced homomorphisms of A_m-modules $f_m : L_m \to L'_m$ are surjective for every maximal ideal m of A.

Taking this claim for granted for a while, it follows that all we have to prove is the surjectivity of the homomorphisms of A_m-modules

$$\varphi'_m : \mathrm{Hom}_A(M, N)_m \to \mathrm{Hom}_A(M, N')_m,$$

for every maximal ideal m of A. But using a general property (see the exercise below), we have natural identifications

$$\mathrm{Hom}_A(M,N)_m \cong \mathrm{Hom}_{A_m}(M_m,N_m),$$

$$\mathrm{Hom}_A(M,N')_m \cong \mathrm{Hom}_{A_m}(M_m,N'_m).$$

It follows that the surjectivity of φ'_m is equivalent to the surjectivity of the following maps

$$\mathrm{Hom}_{A_m}(M_m,N_m) \to \mathrm{Hom}_{A_m}(M_m,N'_m),$$

for all maximal ideals m of A. But this latter fact is quivalent to the projectivity of the A_m-module M_m, for every maximal ideal m al lui A (M_m is projective because A_m is free by proposition 1). Thus Proposition 4 is proved modulo the above claim.

Proof of the claim. The "only if" implication is a simple consequence of the general fact that the localization functor is exact. Assume therefore that f_m is surjective for every maximal ideal m of A. Let $x' \in L'$ be an arbitrary element of L'. We want to find an element $x \in L$ such that $f(x) = x'$. Since for every m the map f_m is surjective, there are an elements $z_m \in L$ and $s_m \in A \setminus m$ such that

$$f_m(\frac{z_m}{s_m}) = \frac{x'}{1}, \text{ or else, } \frac{f(z_m)}{s_m} = \frac{x'}{1}.$$

Therefore for every m there is an $s'_m \in A \setminus m$ such that $s'_m(f(z_m) - s_m x') = 0$, or else, $f(x_m) = t_m x'$, where $x_m = s'_m z_m$ and $t_m = s'_m s_m \in A \setminus m$ (because m is a maximal ideal). Now the ideal I generated by all elements t_m (where m runs the set $\mathrm{Max}(A)$ of all maximal ideals of A) coincides with A. Indeed, this follows from an general result of Krull because I (by its construction) cannot be contained in any maximal ideal m of A ($t_m \in I \setminus m$). It follows that there are finitely many maximal ideals $m_1,...,m_n$ of A and elements $a_1,...a_n$ such that $\sum_{i=1}^n a_i t_{m_i} = 1$. Setting $x := \sum_{i=1}^n a_i x_{m_i}$, we have

$$f(x) = f(\sum_{i=1}^n a_i x_{m_i}) = \sum_{i=1}^n a_i f(x_{m_i}) = \sum_{i=1}^n a_i t_{m_i} x' = x'.$$

This proves the claim, and thereby Proposition 4. □

Corollary 1. *Let P be a finitely generated projective A-module, with A a Noetherian ring. Then the dual $\mathrm{Hom}_A(P,A)$ of P is also a finitely generated projective A-module, and the canonical map $\alpha_P : P \to P^{**}$ into the bidual is an isomorphism.*

Proof. For the first statement one applies Proposition 4. For the second, one observes that the verification of the bijectivity of α_P is a local question, therefore we may assume that A is a local ring. Then by Proposition 3, P is free of finite rank, and in this case the bijectivity of α_P is well known. □

Lemma 1. *Let A be a local Noetherian ring of maximal ideal $m = m_A$, and M a free A-module of finite rank. Let $x \in M$ be an element such that $x \notin mM$. Then the A-module M/Ax is also free.*

Proof. Consider the non-zero vector $\hat{x} := x \mod mM$ in the finite dimensional k-vector space M/mM, with $k = A/m$. Then there is a basis $\hat{x_1}, \hat{x_2}, ..., \hat{x_n}$ of M/mM, with $x_i \in M$, $\forall i = 1, ..., n$, şi $x_1 = x$. By Nakayama's lemma, $x_1 = x, x_2, ..., x_n$ is a system of generators of the A-module M. On the other hand, let $y_1, ..., y_p$ be a basis of the free A-module M. Then $\hat{y_1}, ..., \hat{y_p}$ is a basis of the k-vector space M/mM. In particular, $p = n$. Since $y_1, ..., y_n$ is a basis of M, there exists an $n \times n$-matrix $\mathcal{A} = |a_{ij}|_{i,j=1,...,n}$ with entries in A such that

$$x_i = \sum_{j=1}^{n} a_{ji} y_j, \quad \forall i = 1, ..., n.$$

Since $x_1, ..., x_n$ is a system of generators of M, there exists a $n \times n$-matrix $\mathcal{B} = |b_{ij}|_{i,j=1,...,n}$ with entries in A such that

$$y_i = \sum_{j=1}^{n} b_{ji} x_j, \quad \forall i = 1, ..., n.$$

Comparing these equalities we get:

$$y_i = \sum_{j=1}^{n} b_{ji} x_j = \sum_{j=1}^{n} b_{ji} \sum_{l=1}^{n} a_{lj} y_l = \sum_{l=1}^{n} (\sum_{j=1}^{n} a_{lj} b_{ji}) y_l, \quad \forall i = 1, ..., n.$$

Because $y_1, ..., y_n$ is a basis of the A-module M we get:

$$\sum_{j=1}^{n} a_{lj} b_{ji} = \delta_{li}, \quad \forall l, i = 1, ..., n.$$

In other words we get the equality $\mathcal{AB} = I_n$ of matrices, or else, $\mathcal{B} = \mathcal{A}^{-1}$. Since $y_1, ..., y_n$ is a basis of M, it follows that $x_1 = x, x_2, ..., x_n$ is also a basis of M. Thus

$$x_2 \mod xM, ..., x_n \mod xM$$

is a basis of the A-module M/Ax, i.e. M/Ax is a free A-module. □

(1.4) Definition. Let M be an A-module. A *projective resolution* of M is by definition a sequence of projective A-modules $\{P_n\}_{n \geq 0}$, a surjective homomorphism $\varepsilon : P_0 \to M$ and a sequence of homomorphisms $\{f_n : P_n \to P_{n-1}\}_{n \geq 1}$ such that the following sequence of A-modules and homomorphisms of A-modules

$$\cdots \xrightarrow{f_{n+1}} P_{n+1} \xrightarrow{f_n} P_n \xrightarrow{f_{n-1}} \cdots \xrightarrow{f_1} P_1 \xrightarrow{f_0} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0,$$

is exact, i.e. $\mathrm{Ker}(f_n) = \mathrm{Im}(f_{n+1})$, $\forall n = 0, 1, ...$ and $\mathrm{Ker}(\varepsilon) = \mathrm{Im}(f_0)$.

Corollary 2. *Every A-module M possesses at least a projective resolution. If moreover the ring A is Noetherian and M is finitely generated over A, then M possesses a projective resolution as in definition* (1.4) *such that P_n is a projective finitely generated A-module $\forall n \geq 0$.*

Proof. By Proposition 2 there exists a surjective homomorphism $\varepsilon : P_0 \to M$, with P_0 a free A-module (hence projective, by Proposition 1). Again by Proposition 1 there exists a surjective homomorphism $g_0 : P_1 \to \mathrm{Ker}(\varepsilon)$, with P_1 projective A-module. If f_0 is the composition of the inclusion $\mathrm{Ker}(\varepsilon) \subseteq P_0$ with g_0, it follows that the sequence

$$P_1 \xrightarrow{f_0} P_0 \xrightarrow{\varepsilon} M \to 0$$

is exact. Repeting this procedure, there exists a surjective homomorphism $g_1 : P_2 \to \mathrm{Ker}(f_0) = \mathrm{Ker}(g_0)$, with P_2 projective A-module. Denoting by f_1 the composition of the inclusion $\mathrm{Ker}(f_0) \subseteq P_1$ cu g_1, we get the exact sequence

$$P_2 \xrightarrow{f_1} P_1 \xrightarrow{f_0} P_0 \xrightarrow{\varepsilon} M \to 0,$$

with P_0, P_1, P_2 projective A-modules. Continuing in this way we get by induction the first statement of the proposition.

For the second statement, because M is finitely generated, by Proposition 2 we can choose the projective A-module P_0 also finitely generated. Since A is Noetherian and P_0 finitely generated peste A, $\mathrm{Ker}(\varepsilon)$ is also finitely generated. Repeting the same argument we can choose the surjective homomorphism $g_1 : P_1 \to \mathrm{Ker}(\varepsilon)$, with P_1 a projective and finitely generated A-module. By induction we get that for every $n \geq 1$ the A-module P_n is projective and finitely generated. □

(1.5) Let $u : M' \to M$ be a homomorphism of A-modules. If N is an arbitrary A-module we shall denote by

$$u' := \mathrm{Hom}_A(N, u) : \mathrm{Hom}_A(N, M') \to \mathrm{Hom}_A(N, M),$$

$$u'' := \mathrm{Hom}_A(u, N) : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M', N)$$

the homomorphisms of A-modules defined by $u'(f) := u \circ f$ and $u''(g) = g \circ u$, $\forall f \in \mathrm{Hom}_A(N, M')$ and $\forall g \in \mathrm{Hom}_A(M, N)$.

Let

$$0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0\,, \tag{1.5.1}$$

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0 \tag{1.5.2}$$

be two exact sequences of A-modules.

Proposition 5. (*i*) *In the notation of* (1.5), *for every exact sequence of the form* (1.5.1) *and for every A-module N the following sequence*

$$0 \longrightarrow \mathrm{Hom}_A(M'', N) \xrightarrow{v''} \mathrm{Hom}_A(M, N) \xrightarrow{u''} \mathrm{Hom}(M', N)$$

is exact.
(*ii*) *For every exact sequence of the form* (1.5.2) *and for every A-module M the following sequence*

$$0 \longrightarrow \mathrm{Hom}_A(M, N') \xrightarrow{f'} \mathrm{Hom}_A(M, N) \xrightarrow{g'} \mathrm{Hom}_A(M, N'')$$

is exact.

Proof. The verification is completely straightforward. □

(1.6) Remark. For a given A-module M it is not true in general that for every surjective homomorphism $g : N \to N''$ the map

$$g' = \mathrm{Hom}_A(M, g) : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, N'')$$

is still surjective. The A-modules M enjoying the property that g' is surjective for every surjective homomorphism $g : N \to N''$ are exactly the projective A-modules (in fact this is precisely the definition of projective modules).

Similarly, it is not true in general that for every injective homomorphism $u : M' \to M$ the map

$$u'' = \mathrm{Hom}_A(u, N) : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M', N)$$

is surjective. The A-modules N enjoying the property that the map u'' is surjective for every injective homomorphism $u : M' \to M$ are called *injective modules.* Although very important in homological algebra, the injective modules will not be used in this paper.

(1.7) The functors Ext^*.

Let M and N be two arbitrary A-modules and let

$$(1.7.1) \quad \cdots \to P_{n+1} \xrightarrow{f_n} P_n \xrightarrow{f_{n-1}} \cdots \longrightarrow P_1 \xrightarrow{f_0} P_0 \xrightarrow{\varepsilon} M \to 0$$

be a projective resolution of the A-module M. The existence of projective resolutions is ensured by Corollary 2. Then we can consider the sequence of A-modules and homomorphisms of A-modules

$$0 \longrightarrow \mathrm{Hom}_A(P_0, N) \xrightarrow{f_0''} \mathrm{Hom}_A(P_1, N) \xrightarrow{f_1''} \mathrm{Hom}_A(P_2, N) \longrightarrow \cdots$$

$$\cdots \xrightarrow{f_{n-1}''} \mathrm{Hom}_A(P_n, N) \xrightarrow{f_n''} \mathrm{Hom}_A(P_{n+1}, N) \xrightarrow{f_{n+1}''} \cdots,$$

in which the homomorphisms are

$$f_n'' := \mathrm{Hom}_A(f_n, N) : \mathrm{Hom}_A(P_n, N) \to \mathrm{Hom}_A(P_{n+1}, N), \quad \forall n \geq 0,$$

and $f''_n = 0$, $\forall n < 0$. Since $f_n \circ f_{n-1} = 0$ then by functoriality we get $f''_n \circ f''_{n-1} = 0$, i.e. $\mathrm{Im}(f''_{n-1}) \subseteq \mathrm{Ker}(f''_n)$, $\forall n \in \mathbb{Z}$. Then we put by definition:

$$\mathrm{Ext}^n_A(M,N) := \mathrm{Ker}(f''_n)/\,\mathrm{Im}(f''_{n-1}), \quad \forall n \geq 0. \tag{1.7.2}$$

One can prove that the definition (1.7.2) of $\mathrm{Ext}^n(M,N)$ depends only on the A-modules M and N, and not on the choice of the projective resolution (1.7.1) of the A-module M. For every $n \geq 0$, $\mathrm{Ext}^n(M,N)$ is an A-module, and $\mathrm{Ext}^n(M,N) = 0$ for every $n < 0$.

If the A-module M admits a projective resolution

$$0 \longrightarrow P_n \xrightarrow{f_{n-1}} P_{n-1} \xrightarrow{f_{n-2}} \cdots \xrightarrow{f_0} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0, \tag{1.7.1.1}$$

in other words, if $P_m = 0$, $\forall m > n$, we will say that the A-module M has the *projective dimension* $\leq n$, and will shall write $\mathrm{dh}_A(M) \leq n$. In general, *the projective dimension*, $\mathrm{dh}_A(M)$, of an A-module M is defined as the minimum of all non-negative integers $n \geq 0$ for which there exists a projective resolution (1.7.1.1) with $P_n \neq 0$. In such a case we shall write $\mathrm{dh}_A(M) = n$. For example $\mathrm{dh}_A(M) = 0$ if and only if M is a projective A-module. However, it might well happen that for a given A-module M a projective resolution (1.7.1) for which $P_m = 0$ for for some $m > 0$, does not exist. In such a case we shall write $\mathrm{dh}_A(M) = \infty$, and we will say that M has infinite projective dimension. Clearly, if $\mathrm{dh}_A(M) \leq n$, $\mathrm{Ext}^m_A(M,N) = 0$, for every $m > n$ and for every A-module N. Moreover, $\mathrm{dh}_A(M) = 0$ if and only if M is a projective module, and an A-module M has projective dimension ≤ 1 (i.e. $\mathrm{dh}_A(M) \leq 1$) if and only if M admits a projective projective resolution of the form

$$0 \longrightarrow P_1 \xrightarrow{f_0} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0.$$

The A-modules M with $\mathrm{dh}_A(M) = 1$ will play a crucial role in the proof of the Main Theorem of the introduction. First examples of such A-modules can be found at (2.2).

Properties of the functors Ext^n. For every two A-modules M and N, $\mathrm{Ext}^n_A(M,N)$ is an A-module and

$$\mathrm{Ext}^0_A(M,N) = \mathrm{Hom}_A(M,N). \tag{1.7.3}$$

(1.7.3) follows immediately from the definitions and from proposition 5.

(1.7.4) For every homomorphism $f \in \mathrm{Hom}_A(M',M)$ and for every $n \geq 0$ there exists a well defined homomorphism of A-modules

$$\mathrm{Ext}^n_A(f,N) \in \mathrm{Hom}_A(\mathrm{Ext}^n_A(M,N), \mathrm{Ext}^n_A(M',N)),$$

such that $\mathrm{Ext}^n_A(\mathrm{id}_M,N) = \mathrm{id}_{\mathrm{Ext}^n_A(M,N)}$, and if $g \in \mathrm{Hom}_A(M'',M')$ is another homomorphism, then

$$\mathrm{Ext}^n_A(f \circ g, N) = \mathrm{Ext}^n_A(g,N) \circ \mathrm{Ext}^n_A(f,N).$$

In other words, for every A-module N and for every $n \geq 0$ the assignment

$$M \longrightarrow \mathrm{Ext}^n_A(M, N)$$

defines a contravariant functor on the category of A-modules in itself.

(1.7.5) For every homomorphism $u \in \mathrm{Hom}_A(N, N')$ and for every $n \geq 0$ there exists a well-defined homomorphism

$$\mathrm{Ext}^n_A(M, u) \in \mathrm{Hom}_A(\mathrm{Ext}^n_A(M, N), \mathrm{Ext}^n_A(M, N'))$$

such that $\mathrm{Ext}^n_A(M, \mathrm{id}_N) = \mathrm{id}_{\mathrm{Ext}^n_A(M,N)}$, and if $v \in \mathrm{Hom}_A(N', N'')$ is another homomorfism, the following equality holds:

$$\mathrm{Ext}^n_A(M, v \circ u) = \mathrm{Ext}^n_A(M, v) \circ \mathrm{Ext}^n_A(M, u).$$

In other words, for every A-module M and for every $n \geq 0$ the assignment

$$N \longrightarrow \mathrm{Ext}^n_A(M, N)$$

defines a covariant functor on the category of A-modules in itself.

We shall explain how to get the homomorphisms $\mathrm{Ext}^n(f, N)$ and $\mathrm{Ext}^n(M, u)$ of (1.7.4) and (1.7.5) below (when we shall introduce the concept of cochain complexes).

(1.7.6) For every projective A-module M and for every A-module N, one has

$$\mathrm{Ext}^n_A(M, N) = 0, \quad \forall n \geq 1.$$

Indeed, if M is projective, one can take the projective resolution

$$0 \longrightarrow P_0 \xrightarrow{\varepsilon} M \longrightarrow 0,$$

with $P_0 = M$ and $\varepsilon = \mathrm{id}_M$.

(1.7.7) For every exact sequence of A-modules

$$0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0,$$

for every A-module N, and for every $n \geq 0$ there exists a canonical homomorphism (called the boundary homomorphism)

$$\delta_n : \mathrm{Ext}^n_A(M', N) \to \mathrm{Ext}^{n+1}_A(M'', N),$$

such that the first exact sequence of proposition 5 fits into a long exact sequence of cohomology

$$\begin{aligned}
0 \to \mathrm{Hom}_A(M'', N) \to \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M', N) \to \\
\to \mathrm{Ext}^1_A(M'', N) \to \mathrm{Ext}^1_A(M, N) \to \mathrm{Ext}^1_A(M', N) \to \\
\to \mathrm{Ext}^2_A(M'', N) \to \mathrm{Ext}^2_A(M, N) \to \mathrm{Ext}^2_A(M', A) \to \cdots \\
\cdots \to \mathrm{Ext}^{n-1}_A(M', N) \to \mathrm{Ext}^n_A(M'', N) \to \mathrm{Ext}^n_A(M, N) \to \cdots,
\end{aligned}$$

in which the arrows are those obtained by functoriality from u and v (see (1.7.4)) or the boundary homomorphisms δ_n.

We sketch now the idea of how to get this cohomology exact sequence. For this we need some preparatory lemae.

Lemma 2. (*Snake's lemma.*) *Let*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & N' & \xrightarrow[w]{} & N & \xrightarrow[t]{} & N'' & \longrightarrow & 0 \end{array}$$

be a commutative diagram of A-modules and homomorphisms of A-modules, with exact rows. Then the homomorphisms u, v, f', f, f'', w, t induce a canonical exact sequence

$$\begin{aligned} 0 \longrightarrow \operatorname{Ker}(f') \xrightarrow{u'} \operatorname{Ker}(f) \xrightarrow{v'} \operatorname{Ker}(f'') \xrightarrow{\delta} \\ \xrightarrow{\delta} \operatorname{Coker}(f') \xrightarrow{w'} \operatorname{Coker}(f) \xrightarrow{t'} \operatorname{Coker}(f'') \longrightarrow 0 \end{aligned}$$

Proof. We restrict ourselves to defining the homomorphism $\delta : \operatorname{Ker}(f'') \to \operatorname{Coker}(f')$ (the rest of the proof consisting in a straightforward verification). Let then $x'' \in \operatorname{Ker}(f'')$. Since v is surjective, there exists an $x \in M$ such that $v(x) = x''$. From the commutativity of the second square it follows that $f(x) \in \operatorname{Ker}(t) = \operatorname{Im}(w)$. Thus there exists a (unique) $y' \in N'$ such that $w(y') = f(x)$. Then we put by definition

$$\delta(x'') := y' \bmod \operatorname{Im}(f') \in N'/\operatorname{Im}(f') = \operatorname{Coker}(f').$$

The definition of δ is correct because if $x_1 \in M$ is another element of M such that $v(x_1) = x''$, then $v(x - x_1) = 0$, i.e. $x - x_1 \in \operatorname{Ker}(v) = \operatorname{Im}(u)$. Thus there exists an element $z' \in M'$ such that $u(z') = x - x_1$. If $y_1' \in N'$ is such that $w(y_1') = f(x_1)$, from the commutativity of the first square we get $y' - y_1' = f'(z')$, i.e. the elements y' şi y_1' define the same class in $N'/\operatorname{Im}(f') = \operatorname{Coker}(f')$. □

Lemma 3. *Let*

$$0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$$

be an exact sequence of A-modules. Assume that there are projective resolutions:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P_1' & \xrightarrow{f'} & P_0' & \xrightarrow{\varepsilon'} & M' & \longrightarrow & 0 \\ 0 & \longrightarrow & P_1'' & \xrightarrow{f''} & P_0'' & \xrightarrow{\varepsilon''} & M'' & \longrightarrow & 0 \end{array}$$

Then there exists a commutative diagram of A-modules with exact rows and the colums

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_1' & \xrightarrow{f'} & P_0' & \xrightarrow{\varepsilon'} & M' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow u & & \\
0 & \longrightarrow & P_1 & \xrightarrow{f} & P_0 & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow v & & \\
0 & \longrightarrow & P_1'' & \xrightarrow{f''} & P_0'' & \xrightarrow{\varepsilon''} & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

in which the middle horizontal row is a projective resolution of M. In particular, $\mathrm{dh}_A(M) \leq 1$.

Proof. Set $P_0 := P_0' \oplus P_0''$ and consider the exact sequence

$$0 \to P_0' \to P_0 \to P_0'' \to 0,$$

in which the map $P_0' \to P_0$ is given by $x \to (x, 0)$, and the map $P_0 \to P_0''$ by $(x, y) \to y$. Since P_0' and P_0'' are projective, $P_0 = P_0' \oplus P_0''$ is also projective. We have to show that there exists homomorphism $\varepsilon : P_0 \to M$ which makes the two right squares of the diagram commutative. Since P_0'' is a projective A-module and v is surjective, there exists a homomorphism $\eta : P_0'' \to M$ such that $v \circ \eta = \varepsilon''$. Then define the homomorphism $\varepsilon : P_0 \to M$ by $\varepsilon(x, y) = u(\varepsilon'(x)) + \eta(y)$. One checks immediately the commutativity of the two squares. Then set $P_1 := \mathrm{Ker}(\varepsilon)$. By the snake lemma (Lemma 2) the (already constructed) commutative diagram containing the two right squares yields the exact sequence

$$0 \to P_1' \to P_1 \to P_1'' \to 0,$$

which makes commutative also the two left squares. Moreover, since P_1' and P_1'' are projective A-modules, from this exact sequence it follows that P_1 is also projective. □

Remark. Lemma 3 holds true in a more general form (with essentially the same proof), namely starting with two projective resolutions

$$\cdots P_2' \to P_1' \to P_0' \to M' \to 0,$$

$$\cdots P_2'' \to P_1'' \to P_0'' \to M'' \to 0,$$

one can construct a projective resolution

$$\cdots P_2 \to P_1 \to P_0 \to M \to 0,$$

which can be included in a commutative diagram, similar to the one of Lemma 3. In other words, one gets the exact sequence of projective resolutions

$$0 \to P'_* \to P_* \to P''_* \to 0.$$

Taking into account that for every $n \geq 0$ the exact sequence (which is nothing but the component of order n of the above exact sequence of resolutions)

$$0 \to P'_n \to P_n \to P''_n \to 0$$

consists only of projective modules, this latter exact sequence splits. This observation allows one to deduce the exactness of the following sequence

$$0 \to \mathrm{Hom}_A(P''_n, N) \to \mathrm{Hom}_A(P_n, N) \to \mathrm{Hom}_A(P'_n, N) \to 0.$$

It follows that we get the exact sequence of cochain complexes (see the definition below)

$$0 \to \mathrm{Hom}_A(P''_*, N) \to \mathrm{Hom}_A(P_*, N) \to \mathrm{Hom}_A(P'_*, N) \to 0. \tag{1.7.7.1}$$

Since by definition $\mathrm{Ext}^*_A(M, N)$ is the cohomology of the chain complex $\mathrm{Hom}_A(P_*, N)$, the cohomology exact sequence comes from a general technical result. To state it we need some further definitions and notation. Let us denote by X^* the following sequence of A-modules and homomorphisms of A-modules

$$0 \longrightarrow X^0 \xrightarrow{d_0} X^1 \xrightarrow{d_1} \cdots \xrightarrow{d_{n-1}} X^n \xrightarrow{d_n} X^{n+1} \xrightarrow{d_{n+1}} \cdots$$

We will say that X^* is a cochain complex if for every $n \in \mathbb{Z}$ one has $d_n \circ d_{n-1} = 0$, where by convention we put $d_n = 0$ if $n < 0$. An element of X^n is called *cochain of dimension* n of X^*. The condition that $d_n \circ d_{n-1} = 0$ is equivalent to $\mathrm{Im}(d_{n-1}) \subseteq \mathrm{Ker}(d_n)$. If X^* is a cochain complex and n is a fixed integer we put $Z^n(X^*) := \mathrm{Ker}(d_n)$ and $B^n(X^*) := \mathrm{Im}(d_{n-1})$. An element of $Z^n(X^*)$ is called *cocycle of dimension* n of X^*, while an element of $B^n(X^*)$ is called *coboundary of dimension* n of the cochain complex X^*. We have $B^n(X^*) \subseteq Z^n(X^*)$, $\forall n \in \mathbb{Z}$. Thus it makes sense to associate to every cochain complex X^* the following A-modules

$$H^n(X^*) := Z^n(X^*)/B^n(X^*), \text{ for every } n \in \mathbb{Z}.$$

Then $H^n(X^*)$ is called the *cohomology module of dimension* n of the cochain complex X^* ($n \in \mathbb{Z}$). From the definition we see that $H^n(X^*)$ measures the "deviation" from the exactness of the complex X^* at X^n. For example, the projective resolution (1.7.1) of the A-module M produces the cochain complex X^*, with $X^n := \mathrm{Hom}_A(P_n, N)$ and $d_n := f'_n = \mathrm{Hom}_A(f_n, N)$, $\forall n \in \mathbb{Z}$ (see (1.7.2)). Therefore the cohomology module of dimension n of this cochain complex is just $\mathrm{Ext}^n_A(M, N)$.

Let $X^* = \{X^n, d^X_n : X^n \to X^{n+1}\}_{n\in\mathbb{Z}}$ and $Y^* = \{Y^n, d^Y_n : Y^n \to Y^{n+1}\}_{n\in\mathbb{Z}}$ be two cochain complexes. A homomorphism $f : X^* \to Y^*$ of cochain complexes is by definition a sequence $\{f_n\}_{n\in\mathbb{Z}}$ of homomorphisms of A-module $f_n : X^n \to Y^n$ such

that $f_{n+1} \circ d_n^X = d_n^Y \circ f_n$, $\forall n \in \mathbb{Z}$. One verifies immediately that every homomorphism $f : X^* \to Y^*$ of cochain complexes induces a well defined homomorphism

$$H^n(f) : H^n(X^*) \to H^n(Y^*), \quad \forall n \in \mathbb{Z}.$$

In fact, if c_n is an element of $H^n(X^*)$ represented by the cocycle $z_n \in Z^n(X^*)$, then by definition $H^n(f)(c_n)$ is the class of $f_n(z_n)$ modulo $B^n(Y^*)$; indeed, from $f_{n+1} \circ d_n^X = d_n^Y \circ f_n$ it follows that $d_n^Y(f_n(z_n)) = f_{n+1}(d_n^X(z_n)) = f_{n+1}(0) = 0$, i.e. $f_n(z_n) \in Z^n(Y^*)$.

At this point we can explain how to get the functorial homomorphism $\mathrm{Ext}_A^n(f, N) : \mathrm{Ext}_A^n(M, N) \to \mathrm{Ext}_A^n(M', N)$ associated to an arbitrary $f \in \mathrm{Hom}_A(M', N)$ (see (1.7.4)). To this extent, choose projective resolutions

$$\cdots \longrightarrow P_2' \xrightarrow{a_1'} P_1' \xrightarrow{a_0'} P_0' \xrightarrow{\varepsilon'} M' \longrightarrow 0\,,$$

$$\cdots \longrightarrow P_2 \xrightarrow{a_1} P_1 \xrightarrow{a_0} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0$$

of M' and M respectively. We claim that there exists a sequence $\{f_n\}_{n \geq 0}$ of homomorphisms $f_n \in \mathrm{Hom}_A(P_n', P_n)$ such that the following diagram

$$\text{(f)} \qquad \begin{array}{ccccccccccc} \cdots & \longrightarrow & P_2' & \xrightarrow{a_1'} & P_1' & \xrightarrow{a_0'} & P_0' & \xrightarrow{\varepsilon'} & M' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f} & & \\ \cdots & \longrightarrow & P_2 & \xrightarrow{a_1} & P_1 & \xrightarrow{a_0} & P_0 & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \end{array}$$

is commutative. Indeed, since P_0' is projective and ε surjective, there exists a (not necessarily unique) homomorphism $f_0 \in \mathrm{Hom}_A(P_0', P_0)$ such that $\varepsilon \circ f_0 = f \circ \varepsilon'$. Moreover, since $\varepsilon \circ f_0 \circ a_0' = f \circ (\varepsilon' \circ a_0') = f \circ 0 = 0$, $\mathrm{Im}(f_0 \circ a_0') \subseteq \mathrm{Ker}(\varepsilon) = \mathrm{Im}(a_0)$. Then, using the fact that P_1' is projective and the surjection $a_0 : P_1 \to \mathrm{Im}(a_0)$, we infer that there exists a (not necessarily unique) $f_1 \in \mathrm{Hom}_A(P_1', P_1)$ such that $a_0 \circ f_1 = f_0 \circ a_0'$ (here we used the fact that $\mathrm{Im}(f_0 \circ a_0') \subseteq \mathrm{Im}(a_0)$!). Continuing in this way by induction we proved the claim.

Now, the commutative diagram (f) yields the homomorphism of cochain complexes

$$F : X^* := \mathrm{Hom}_A(P_*, N) \to Y^* := \mathrm{Hom}_A(P_*', N),$$

whose component of order n is

$$F_n := \mathrm{Hom}_A(f_n, N) \ : \ X^n = \mathrm{Hom}_A(P_n, N) \to Y^n = \mathrm{Hom}_A(P_n', N).$$

Then, according to the definition of Ext's, the desired homomorphism $\mathrm{Ext}_A^n(f, N) : \mathrm{Ext}_A^n(M, N) \to \mathrm{Ext}_A^n(M', N)$ is by definition the map $H^n(f) : H^n(X^*) \to H^n(Y^*)$. Of course, here one has to check that this definition is correct in the sense that it does not depend of several choices (resolutions, the maps f_n, see [CE] for details).

The definition of the map $\mathrm{Ext}^n_A(M,u) : \mathrm{Ext}^n_A(M,N) \to \mathrm{Ext}^n(M,N')$ associated to an arbitrary homomorphism $u \in \mathrm{Hom}_A(N,N')$ (see (1.7.5)) is even simpler. In fact, one choose a projective resolution

$$\cdots \longrightarrow P_2 \xrightarrow{a_1} P_1 \xrightarrow{a_0} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0$$

of M as above, and then we get the homomorphism of cochain complexes

$$U : X^* := \mathrm{Hom}_A(P_*, N) \to Y^* := \mathrm{Hom}_A(P_*, N'),$$

whose component of order n is $U_n := \mathrm{Hom}(P_n, u) : \mathrm{Hom}_A(P_n, N) \to \mathrm{Hom}_A(P_n, N')$. Then, according to the definition of Ext's, the desired map $\mathrm{Ext}^n_A(M,u)$ is $H^n(U) : H^n(X^*) \to H^n(Y^*)$.

Let now X^*, Y^* şi Z^* be three cochain complexes and $f = \{f_n\}_n : X^* \to Y^*$ and $g = \{g_n\}_n : Y^* \to Z^*$ two homomorphisms of cochain complexes. One says that the sequence

$$0 \longrightarrow X^* \xrightarrow{f} Y^* \xrightarrow{g} Z^* \longrightarrow 0$$

is exact if for every $n \in \mathbb{Z}$ the sequence

$$0 \longrightarrow X^n \xrightarrow{f_n} Y^n \xrightarrow{g_n} Z^n \longrightarrow 0$$

is an exact sequence of A-modules. With these definitions one has:

Proposition 6. *Let*

$$0 \longrightarrow X^* \xrightarrow{f} Y^* \xrightarrow{g} Z^* \longrightarrow 0$$

be an exact sequence of cochain complexes of A-modules. Then for every $n \in \mathbb{Z}$ there exists a canonical homomorphism $\delta_n : H^n(Z^*) \to H^{n+1}(X^*)$ such that the following sequence of A-modules and homomorphisms of A-modules

$$\cdots \xrightarrow{\delta_{n-1}} H^n(X^*) \xrightarrow{H^n(f)} H^n(Y^*) \xrightarrow{H^n(g)} H^n(Z^*) \xrightarrow{\delta_n}$$

$$\xrightarrow{\delta_n} H^{n+1}(X^*) \xrightarrow{H^{n+1}(f)} H^{n+1}(Y^*) \xrightarrow{H^{n+1}(g)} H^{n+1}(Z^*) \xrightarrow{\delta_{n+1}} \cdots$$

is exact.

Proof. We only indicate how to get the maps δ_n ($n \in \mathbb{Z}$). Consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & X^{n-1} & \xrightarrow{f_{n-1}} & Y^{n-1} & \xrightarrow{g_{n-1}} & Z^{n-1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d^X_{n-1}} & & \downarrow{\scriptstyle d^Y_{n-1}} & & \downarrow{\scriptstyle d^Z_{n-1}} & & \\
0 & \longrightarrow & X^n & \xrightarrow{f_n} & Y^n & \xrightarrow{g_n} & Z^n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d^X_n} & & \downarrow{\scriptstyle d^Y_n} & & \downarrow{\scriptstyle d^Z_n} & & \\
0 & \longrightarrow & X^{n+1} & \xrightarrow{f_{n+1}} & Y^{n+1} & \xrightarrow{g_{n+1}} & Z^{n+1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d^X_{n+1}} & & \downarrow{\scriptstyle d^Y_{n+1}} & & \downarrow{\scriptstyle d^Z_{n+1}} & & \\
0 & \longrightarrow & X^{n+2} & \xrightarrow{f_{n+2}} & Y^{n+2} & \xrightarrow{g_{n+2}} & Z^{n+2} & \longrightarrow & 0
\end{array}$$

Let $\xi_n \in H^n(Z^*)$ be an arbitrary cohomology class, which is represented by a cocycle $z_n \in Z^n(Z^*)$. Since g_n is surjective, there is an element $y_n \in Y^n$ such that $g_n(y_n) = z_n$. Then

$$g_{n+1}(d_n^Y(y_n)) = d_n^Z(g_n(y_n)) = d_n^Z(z_n) = 0,$$

and therefore $d_n^Y(y_n) \in \mathrm{Ker}(g_{n+1}) = \mathrm{Im}(f_{n+1})$. Thus there is a (unique) element $x_{n+1} \in X^{n+1}$ such that $f_{n+1}(x_{n+1}) = d_n^Y(y_n)$.

Now, one observes that $d_{n+1}^X(x_{n+1}) = 0$, $x_{n+1} \in Z^{n+1}(X^*)$. Indeed, since f_{n+2} is injective this is equivalent to $f_{n+2}(d_{n+1}^X(x_{n+1})) = 0$. But

$$f_{n+2}(d_{n+1}^X(x_{n+1})) = d_{n+1}^Y(f_{n+1}(x_{n+1})) = d_{n+1}^Y(d_n^Y(y_n)) = 0,$$

because $d_{n+1}^Y \circ d_n^Y = 0$. Then we put by definition

$$\delta_n(\xi_n) := \text{class of } x_{n+1} \text{ in } H^{n+1}(X^*) = Z^{n+1}(X^*)/B^{n+1}(X^*).$$

A simple diagram chase over the above diagram shows that if we take another $y'_n \in Y_n$ such that $g_n(y'_n) = g_n(y_n) = z_n$, then the element x'_{n+1} got in a similar way has the property that $x'_{n+1} - x_{n+1} \in \mathrm{Im}(d_n^X) = Z^{n+1}(X^*)$, whence x'_{n+1} and x_{n+1} define the same class in $H^{n+1}(X^*)$.

The rest of the proof is a somehow long (but rather straightforward) verification of the exactness. □

Definition. The long exact sequence from Proposition 6 is called *the cohomology exact sequence* associated to the short exact sequence cochain complexes (of Proposition 6).

Combining Proposition 6 with Lemma 3 (under the form of the remark following it, especially the exact sequence (1.7.7.1)) we get the cohomology exact sequence (1.7.7) of the Ext's.

(1.7.8) For every exact sequence of A-modules

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0,$$

for every A-module M and for every $n \geq 0$, there exists a canonical homomorphism

$$d_n : \mathrm{Ext}_A^n(M, N'') \to \mathrm{Ext}_A^{n+1}(M, N'),$$

such that the second exact sequence of Proposition 5 can be included in the following (second) cohomology exact sequence of Ext's:

$$\begin{aligned}
0 \to \mathrm{Hom}_A(M, N') \to \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, N'') \to \\
\to \mathrm{Ext}_A^1(M, N') \to \mathrm{Ext}_A^1(M, N) \to \mathrm{Ext}_A^1(M, N'') \to \\
\to \mathrm{Ext}_A^2(M, N') \to \mathrm{Ext}_A^2(M, N) \to \mathrm{Ext}_A^2(M, N'') \to \cdots \\
\cdots \to \mathrm{Ext}_A^{n-1}(M, N'') \to \mathrm{Ext}_A^n(M, N') \to \mathrm{Ext}_A^n(M, N) \to \cdots,
\end{aligned}$$

in which the rest of the arrows are induced by f and g (using the functoriality). The proof is similar and is based on again on Proposition 6. Specifically, let

$$P_* : \quad \cdots \to P_2 \to P_1 \to P_0 \to M \to 0$$

be a projective resolution of M. Then we get the complexes of cochains

$$X^* = \mathrm{Hom}_A(P_*, N') : \quad 0 \to \mathrm{Hom}_A(P_0, N') \to \mathrm{Hom}_A(P_1, N') \to \mathrm{Hom}_A(P_2, N') \to \cdots,$$

$$Y^* = \mathrm{Hom}_A(P_*, N) : \quad 0 \to \mathrm{Hom}_A(P_0, N) \to \mathrm{Hom}_A(P_1, N) \to \mathrm{Hom}_A(P_2, N) \to \cdots,$$

$$Z^* = \mathrm{Hom}_A(P_*, N'') : \quad 0 \to \mathrm{Hom}_A(P_0, N'') \to \mathrm{Hom}_A(P_1, N'') \to \mathrm{Hom}_A(P_2, N'') \to \cdots,$$

Moreover, we also get (by functoriality) the maps $X^* \to Y^*$ and $Y^* \to Z^*$ of complexes such that the sequence of cochain complexes

$$0 \to X^* \to Y^* \to Z^* \to 0$$

is exact. The exactness in dimension n amounts to the verification of the exactness of the following exact sequence

$$0 \to \mathrm{Hom}_A(P_n, N') \to \mathrm{Hom}_A(P_n, N) \to \mathrm{Hom}_A(P_n, N'') \to 0,$$

which follows from Proposition 5, (ii), and from the fact that the A-module P_n is projective. Then one applies Proposition 6.

An interpretation of $\mathrm{Ext}^1_A(M, N)$**.** Let M be an A-module, let $\varepsilon : P \to M$ be a surjective homomorphism from a projective A-module P (Proposition 2, (i)), and set $M' := \mathrm{Ker}(\varepsilon)$. We get an exact sequence

$$0 \longrightarrow M' \xrightarrow{f} P \xrightarrow{\varepsilon} M \longrightarrow 0. \tag{1.7.9}$$

In particular, if M is an A-module such that $\mathrm{dh}_A(M) \leq 1$, there exists even a projective resolution of M of the form

$$0 \longrightarrow P_1 \xrightarrow{f_0} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0. \tag{1.7.10}$$

Then writing a part of the cohomology exact sequence (1.7.7) associated to (1.7.9) we get the exact sequence for every A-module N:

$$\mathrm{Hom}_A(P, N) \xrightarrow{f''} \mathrm{Hom}_A(M', N) \xrightarrow{\delta_0} \mathrm{Ext}^1_A(M, N) \longrightarrow \mathrm{Ext}^1_A(P, N).$$

Since P is projective, $\mathrm{Ext}^1_A(P, N) = 0$ by (1.7.6). Therefore get the exact sequence

$$\mathrm{Hom}_A(P, N) \xrightarrow{f''} \mathrm{Hom}_A(M', N) \xrightarrow{\delta_0} \mathrm{Ext}^1_A(M, N) \longrightarrow 0, \tag{1.7.11}$$

where $f'' := \mathrm{Hom}_A(f, N) : \mathrm{Hom}_A(P, N) \to \mathrm{Hom}_A(M', N)$ is the homomorphism induced by f. If there is a resolution of the form (1.7.10), we can write (1.7.11) by taking $M' = P_1$. The exact sequence (1.7.11) gives in particular a direct definition of the A-module $\mathrm{Ext}^1_A(M, N)$ (as the cokernel of the map f'').

Ext^n and localisation. Let M, N be two finitely generated A-modules over the Noetherian ring A. If S is a multiplicative system of A then for every $n \geq 0$ one has a canonical isomorphism

$$S^{-1}\,\mathrm{Ext}^n_A(M,N) \cong \mathrm{Ext}^n_{S^{-1}A}(S^{-1}M, S^{-1}N). \tag{1.7.12}$$

For every Noetherian ring A let us denote by $\mathrm{Max}(A)$ the set of all maximal ideals of A. Then we have the following formula (see e.g. [CE], or [S2]):

$$\mathrm{dh}_A(M) = \sup_{m \in \mathrm{Max}(A)} \mathrm{dh}_{A_m}(M_m). \tag{1.7.13}$$

In particular, if for a natural number n we have the inequalities $\mathrm{dh}_{A_m}(M_m) \leq n$ for every $m \in \mathrm{Max}(A)$ then one also has $\mathrm{dh}_A(M) \leq n$. We are going to prove (1.7.13) in a special case, which will be enough for our purposes (see (3.1)). Namely, assume that $\mathrm{dh}_{A_m}(M_m) \leq 1$ for all $m \in \mathrm{Max}(A)$. Then we claim that for every exact sequence

$$0 \to X \to P_0 \to M \to 0, \tag{1.7.14}$$

with P_0 projective (such an exact sequence always exists by Proposition 2), then X is necessarily a projective A-module.

Indeed for every A-module N the exact sequence (1.7.14) yields the following cohomology sequence of Ext's (see (1.7.7)):

$$\mathrm{Ext}^1_A(P_0,N) \longrightarrow \mathrm{Ext}^1_A(X,N) \xrightarrow{\delta_0} \mathrm{Ext}^2_A(M,N) \longrightarrow \mathrm{Ext}^2(P_0,N),$$

in which the extreme A-modules vanish because P_0 is projective (see (1.7.6)). It follows that the map

$$\delta_0 : \mathrm{Ext}^1_A(X,N) \to \mathrm{Ext}^2(M,N)$$

is an isomorphism. On the other hand, $\mathrm{Ext}^2_A(M,N) = 0$. Indeed, it will be sufficient to show that $\mathrm{Ext}^2_A(M,N)_m = 0$ for every $m \in \mathrm{Max}(A)$. But by (1.7.12),

$$\mathrm{Ext}^2_A(M,N)_m \cong \mathrm{Ext}^2_{A_m}(M_m, N_m),$$

and since the right hand side vanishes for every $m \in \mathrm{Max}(A)$ (because by hypothesis $\mathrm{dh}_{A_m}(M_m) \leq 1$), we get that $\mathrm{Ext}^2_A(M,N)_m = 0$, as stated. Therefore $\mathrm{Ext}^2_A(M,N) = 0$, and since δ_0 is an isomorphism we also get that

$$\mathrm{Ext}^1_A(X,N) = 0 \text{ for every } A\text{-module } N. \tag{1.7.15}$$

Finally, (1.7.15) implies that X is a projective A-module. Indeed, for every exact sequence of A-modules

$$0 \to N' \to N \to N'' \to 0$$

we get the cohomology sequence of Ext's (see (1.7.8))

$$0 \to \mathrm{Hom}_A(X,N') \to \mathrm{Hom}_A(X,N) \to \mathrm{Hom}_A(X,N'') \to \mathrm{Ext}^1_A(X,N') = 0,$$

which proves that X is projective.

(1.8) Fibered sum of modules. We recall that, given two homomorphisms of A-modules $f : M \to P$ and $g : M \to N$ (both defined on the same A-module M), the *fibered sum* $P \sqcup_M N$ of P and N with respect to f and g is by definition an A-module $P \sqcup_M N$ together with two homomorphisms of A-modules $\alpha : P \to P \sqcup_M N$ and $\beta : N \to P \sqcup_M N$ such that $\alpha \circ f = \beta \circ g$, which verify the following universal property: for every two homomorphisms of A-modules $\alpha' : P \to X$ and $\beta' : N \to X$ such that $\alpha' \circ f = \beta' \circ g$, then there exists a unique homomorphism of A-modules $u : P \sqcup_M N \to X$ such that $u \circ \alpha = \alpha'$ and $u \circ \beta = \beta'$.

Proposition 7. *Let $f : M \to P$ and $g : M \to N$ be two homomorphisms of A-modules. Then there exists a fibered sum $P \sqcup_M N$ of P and N with respect to f and g.*

Proof. Set $S' := P \oplus N$, and set

$$E := \{(f(m), -g(m)) \mid m \in M\}.$$

Then E is an A-submodule of S'. If we put $P \sqcup_M N := (P \oplus N)/E$, $\alpha : P \to P \sqcup_M P$ and $\beta : N \to P \sqcup_M N$ the homomorphisms defined by

$$\alpha(p) := (p, 0) \bmod E, \quad \beta(n) := (0, n) \bmod E,$$

then it is easy to see that the triple $(P \sqcup_M N, \alpha, \beta)$ verifies the universal property of the fibered sum. □

Corollary 3. *Assume that $S = P \sqcup_M N$ is the fibered sum of P and N with respect to $f : M \to P$ and $g : M \to N$, and let $\alpha : P \to S$ and $\beta : N \to S$ be the canonical homomorphisms. Then*
(i) $S = \alpha(P) + \beta(N)$.
(ii) $\mathrm{Ker}(\alpha) = f(\mathrm{Ker}(g))$ and $\mathrm{Ker}(\beta) = g(\mathrm{Ker}(f))$. In particular, if g is one-to-one then α is also one-to-one.

Proof. Everything is a straightforward verification. □

(1.9) Ext^1 and extensions. Let M' and M'' be two A-modules. An *extension of M'' by M'* is by definition an exact sequence (of A-modules and homomorphisms of A-modules)

$$0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0 \tag{1.9.1}$$

One says that the extension (1.9.1) and the extension

$$0 \longrightarrow M' \xrightarrow{f} N \xrightarrow{g} M'' \longrightarrow 0$$

(of M'' by M') are *isomorphic* if there exists homomorphism of A-modules such that the following diagram

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

is commutative. Then it follows easily that φ is an isomorphism of A-modules. This fact explains the terminology.

We shall denote by $\mathrm{Ex}_A(M'', M')$ the set of all isomorphism classes of extensions of M'' by M'. We define a canonical map

$$\omega : \mathrm{Ex}_A(M'', M') \to \mathrm{Ext}^1_A(M'', M')$$

in the following way. Consider an isomorphism class of extensions $e \in \mathrm{Ex}_A(M'', M')$ of M'' by M' which is represented by the exact sequence (1.9.1). In the cohomology exact sequence (1.7.7) associated to (1.9.1) we have the boundary homomorphism

$$\delta_0 : \mathrm{Hom}_A(M', M') \to \mathrm{Ext}^1_A(M'', M').$$

Then define

$$\omega(e) := \delta_0(\mathrm{id}_{M'}). \tag{1.9.2}$$

Then we have the following result which will be used in the sequel:

Theorem 2. *In the above notation and hypotheses, the canonical map ω defined by (1.9.2) is bijective.*

Proof. To check the bijectivity of ω one constructs its inverse

$$\beta : \mathrm{Ext}^1_A(M'', M') \to \mathrm{Ex}_A(M'', M')$$

using the interpretation of $\mathrm{Ext}^1(M'', M')$ given at (1.7.11). Specifically pick an exact sequence

$$0 \longrightarrow N \xrightarrow{\alpha} P \xrightarrow{\varepsilon} M'' \longrightarrow 0,$$

with P a projective A-module. Then we get the exact sequence of cohomology

$$\mathrm{Hom}_A(P, M') \xrightarrow{\alpha^*} \mathrm{Hom}_A(N, M') \longrightarrow \mathrm{Ext}^1_A(M'', M') \longrightarrow 0. \tag{1.9.3}$$

Let now ξ be an element of $\mathrm{Ext}^1_A(M'', M')$ which is represented (via (1.9.3)) by the class of a map $g \in \mathrm{Hom}_A(N, M')$. Then we put $M_g := P \sqcup_N M'$ via the maps $\alpha : N \to P$ and $g : N \to M'$. In other words we get the commutative square

$$\begin{array}{ccc} N & \xrightarrow{\alpha} & P \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle w_g} \\ M' & \xrightarrow[u_g]{} & M_g \end{array}$$

By Corollary 3 the map u_g is injective because α is so. Using the maps $\varepsilon : P \to M''$ and $0 : M' \to M''$ together with the universal property of the fibered sum we get a unique map $v_g : M_g \to M''$. One easily verifies that in this way we get the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{\alpha} & P & \xrightarrow{\varepsilon} & M'' & \longrightarrow & 0 \\ & & {\scriptstyle g}\downarrow & & {\scriptstyle w_g}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_{M''}} & & \\ 0 & \longrightarrow & M' & \xrightarrow{u_g} & M_g & \xrightarrow{v_g} & M'' & \longrightarrow & 0 \end{array}$$

which is commutative with exact rows. So the bottom exact sequence of this diagram defines an extension $e(g) \in \mathrm{Ex}_A(M'', M')$. We put by definition

$$\beta(\xi) := e(g).$$

We have to check that this definition does not depend on the representative g of ξ. Assume therefore $\xi = \hat{g} = \hat{h}$, with $h \in \mathrm{Hom}(N, M')$. Then (1.9.4) implies that there exists an $f \in \mathrm{Hom}_A(P, M')$ such that $h - g = \alpha^*(f) = f \circ \alpha$. Let

$$\text{(e(h))} \qquad 0 \longrightarrow M' \xrightarrow{u} M_h \xrightarrow{v} M'' \longrightarrow 0$$

be the extension associated (similarly) to h. We have to construct a map $f : M_g \to M_h$ such that the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{u_g} & M_g & \xrightarrow{v_g} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_{M'}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}_{M''}} & & \\ 0 & \longrightarrow & M' & \xrightarrow{u_h} & M_h & \xrightarrow{v_h} & M'' & \longrightarrow & 0 \end{array}$$

is commutative. For this let $\varphi' : P \oplus M' \to P \oplus M'$ be the homomorphism defined by

$$\varphi'(p, m') := (p, m' - f(p)), \quad \forall (p, m') \in P \oplus M'.$$

Clearly φ is a homomorphism of A-modules such that

$$\varphi(\alpha(n), -g(n)) = (\alpha(n), -g(n) - f(\alpha(n)) = (\alpha(n), -h(n)), \quad \forall n \in N.$$

Then using the definition of the fibered sum, φ' yields the desired homomorphism $\varphi : M_g \to M_h$ which makes the last diagram commutative. This shows that the extensions $e(g)$ and $e(h)$ are isomorphic, which proves that the definition of β is correct. The verification that β is the inverse of α is straightforward and is left to the reader (cf. [CE], chap. XIV, Theorem 1.1). □

(1.10) Definition. Let A be a commutative unitary ring and let $f_1, ..., f_r \in A$ be r elements of A. We shall say that $\{f_1, ..., f_r\}$ is an *A-sequence* if f_1 is not a zero-divisor of A, and for every i such that $1 \leq i \leq r-1$, $f_{i+1} \mod Af_1 + \cdots + Af_i$ is not a zero-divisor $A/Af_1 + \cdots + Af_i$.

For example, let $A := K[X_1, ..., X_n]$ be the polynoamial K-algebra (with K a field) in n indeterminates and let f_1, $f_2 \in A$ be two non-constant polynomials. Then, using the factoriality of A (Gauss' theorem) one immediately checks that f_1, f_2 is an A-sequence if and only if f_1 şi f_2 have no common prime factors.

(1.11) Definition. Let A be a local Noetherian ring of maximal ideal m. We define the depth of A, denoted depth(A), as the maximal integer $r \geq 0$ for which there exists an A-sequence $f_1, ..., , f_r \in m$. In general we have the inequality depth$(A) \leq \dim(A)$. A local ring (A, m) is called *Cohen-Macaulay* if depth$(A) = \dim(A)$. If A is an arbitrary commutative Noetherian ring, A is called Cohen-Macaulay if for every $m \in \mathrm{Max}(A)$, the local ring A_m is Cohen-Macaulay. Let $g_1, ..., g_d \in m$ be d elements belonging to the maximal ideal of a local Noetherian ring A of dimension d. Then $g_1, ...g_d$ is called *system of parameters of A* if $\sqrt{Ag_1 + \cdots + Ag_d} = m$, i.e. every element of m raised to a certain power belongs to the ideal $Ag_1 + \cdots + Ag_d$. A general result concerning the local Cohen-Macaulay rings shows that A is Cohen-Macaulay if and only if every system of parameters of A is an A-sequence (see e.g. [AM]).

2. Two theorems of Serre

The first theorem of Serre proved in this section is the following important criterion to recognize when the middle A-module in an extension (see (1.9.1)) is free. Precisely we have the following:

Theorem 3. *(Serre) Let A be a local Noetherian ring, $I \subset A$ an ideal of A which admits a projective (free) resolution of the form*

$$0 \longrightarrow A^p \longrightarrow A^q \xrightarrow{\varphi} I \longrightarrow 0.$$

Let $e \in \mathrm{Ext}^1_A(I, A)$ be the element associated (via the bijective map ω of theorem 2) to the extension given by an exact sequence of the form

$$0 \longrightarrow A \xrightarrow{\alpha} M \xrightarrow{\beta} I \longrightarrow 0. \tag{2.0}$$

Then M is a free A-module if and only if the element e generates the A-module $\mathrm{Ext}^1_A(I, A)$.

Proof. The exact sequence (2.0) yields by (1.7.7) the cohomology sequence of Ext's

$$\mathrm{Hom}_A(A, A) \xrightarrow{\delta_0} \mathrm{Ext}^1_A(I, A) \longrightarrow \mathrm{Ext}^1_A(M, A) \longrightarrow \mathrm{Ext}^1_A(A, A).$$

By definition $e = \delta_0(\mathrm{id}_A)$ (cf (1.9)). On the other hand, A is a free A-module (whence projective, by proposition 1), whence by (1.7.6)

$$\mathrm{Ext}^1_A(A, A) = 0.$$

Taking into account that $\mathrm{Hom}_A(A, A) \cong A$, from the above cohomology sequence it follows that e generates $\mathrm{Ext}^1(I, A)$ if and only if $\mathrm{Ext}^1_A(M, A) = 0$. Then the proof of our theorem is a consequence of the following:

Claim. $\mathrm{Ext}^1_A(M, A) = 0$ if and only if M is a free A-module.

It remains therefore to prove the claim. If M is free then $\mathrm{Ext}^1_A(M, A) = 0$ by (1.7.6). Conversely, assume that $\mathrm{Ext}^1_A(M, A) = 0$. Since the A-module A^q is projective, from the surjective homomorphism $\beta : M \to I$ we infer the existence of a homomorphism $\Phi \in \mathrm{Hom}_A(A^q, M)$ such that $\varphi = \beta \circ \Phi$. Then define the homomorphism

$$\psi : A \oplus A^q = A^{q+1} \to M$$

by the formula $\psi(x, y) = \alpha(x) + \Phi(y)$, $\forall (x, y) \in A \oplus A^q$. In this way we get the commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & A^{q+1} & \xrightarrow{\pi} & A^q & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_A} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \varphi} & & \\ 0 & \longrightarrow & A & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & I & \longrightarrow & 0 \end{array} \tag{2.1}$$

in which the homomorphisms i and π are defined by $i(x) = (x, 0)$ and $\pi(x, y) = y$, $\forall x \in A$ and $\forall y \in A^q$. Applying the snake's lemma (Lemma 2) to the diagram (2.1) we get:

$$\mathrm{Ker}(\psi) \cong \mathrm{Ker}(\varphi) = A^p,$$

as well as the surjectivity of ψ. In other words, we get an exact sequence of the form

$$0 \to A^p \to A^{q+1} \to M \to 0.$$

Now, the hypothesis that $\mathrm{Ext}^1_A(M, A) = 0$ implies that $\mathrm{Ext}^1_A(M, A^p) = 0$, because the functor $X \longrightarrow \mathrm{Ext}^1(M, X)$ is additive and commutes with finite direct sums. Therefore the above exact sequence yields the cohomology exact sequence (see (1.7.8))

$$\mathrm{Hom}_A(M, A^{q+1}) \xrightarrow{\eta} \mathrm{Hom}_A(M, M) \xrightarrow{d_0} \mathrm{Ext}^1_A(M, A^p) = 0.$$

It follows that the homomorphism $\eta : \mathrm{Hom}_A(M, A^{q+1}) \to \mathrm{Hom}_A(M, M)$ is surjective. In particular, there exists an homomorphism $u \in \mathrm{Hom}_A(M, A^{q+1})$ such that $\psi \circ u = \mathrm{id}_M$, i.e. the A-module M is a direct summand of the free A-module A^{q+1}. By Proposition 2 it follows then that M is a projective A-module. Finally, since A is a local Noetherian ring and M is a finitely generated A-module, the fact that M is projective implies that M is free by Proposition 3. □

(2.2) Example. Let A be a local Noetherian ring and I an ideal of A which is generated by the A-sequence $\{f_1, f_2\}$ (consisting of two elements, see the definition (1.9)). We shall produce a free (in particular, projective) resolution of the form

$$0 \longrightarrow A \xrightarrow{\psi} A^2 \xrightarrow{\varphi} I \longrightarrow 0 \tag{2.2.1}$$

of the ideal I. To this end, consider the (obviously surjective) homomorphism $\varphi : A^2 \to I$ given by $\varphi(a, b) = af_1 + bf_2$, $\forall (a, b) \in A^2$. Consider also the homomorphism $\psi : A \to A^2$ given by $\psi(c) = (-cf_2, cf_1)$, $\forall c \in A$. Clearly, ψ is injective and $\varphi \circ \psi = 0$. In particular, $\mathrm{Im}(\psi) \subseteq \mathrm{Ker}(\varphi)$. Let now $(a, b) \in \mathrm{Ker}(\varphi)$, i.e. $af_1 + bf_2 = 0$. From the equality $bf_2 = -af_1$ it follows (taking into account that $\hat{f}_2$ is not a zero-divisor of A/Af_1) that there is $c \in A$ such that $b = cf_1$. Then the euqality $af_1 + bf_2 = 0$ becomes $f_1(a + cf_2) = 0$, and since f_1 is not a zero-divisor of A, we get $a + cf_2 = 0$. Therefore $(a, b) = (-cf_2, cf_1) = \psi(c) \in \mathrm{Im}(\psi)$.

In this way we checked the exactness of the sequence (2.2.1), which in particular is a concrete example of a free resolution of I. This resolution is in fact a very special case of a general resolution, known as *the Koszul complex* that can be associated to an A-sequence $\{f_1, ..., f_r\}$ of arbitrary length $r \geq 2$.

(2.3) Definition. Let $p \subset A$ be a prime ideal of a commutative ring A. A strictly increasing sequence of prime ideals

$$p_0 \subset p_1 \subset \cdots \subset p_r \tag{2.3.1}$$

($r \geq 0$) is said to be saturated either if $r = 0$, or if $r \geq 1$ and for every $i = 0, 1, ..., r-1$ the only prime ideals containing p_i and contained in p_{i+1} are p_i and p_{i+1}. The number r of a chain of prime ideals (2.3.1) is called the length of the chain. The height of a prime ideal p of A is the maximum of the lengths r of all saturated prime ideals of type (2.3.1) such that $p_r = p$. Let now A be a Cohen-Macaulay (not necessarily local) ring, and let $I \subset A$ ($I \neq A$) be an ideal of A. We sall say that I has height r if all minimal prime ideals of A containing I have height r. The ideal I of height $r \geq 1$ is said to be *local complete intersection* if for every maximal ideal m of A such that $I \subseteq m$, the ideal $I_m = IA_m$ is generated by an A_m-sequence $\{f_1, ..., f_r\}$ of length r.

An important consequence of theorem 3 is the following global result:

Corollary 4. *Let A be a Cohen-Macaulay (not necessarily local) ring, and let $I \subset A$ be an ideal of height 2 which is a local complete intersection. Assume that every projective A-module of rank ≤ 2 is free. Then the following two conditions are equivalent:*
(i) The ideal I is generated by two elements.
(ii) The A-module $\mathrm{Ext}^1_A(I, A)$ is generated by one element.

Proof. Assume that *(ii)* holds, and let u be a generator of $\mathrm{Ext}^1_A(I, A)$. Then by Theorem 2, u corresponds to an extension I by A of the form

$$0 \to A \to M \to I \to 0. \tag{2.2.2}$$

Let m be an arbitrary maximal ideal of A. Then by (1.9.1),

$$\mathrm{Ext}^1_A(I, A)_m \cong \mathrm{Ext}^1_{A_m}(I_m, A_m).$$

In particular, the latter A_m-module is generated by one element. If $I \subseteq m$ then by hypothesis I_m is generated by an A_m-sequence $\{f_1, f_2\}$, and therefore by example (2.2), there exists a resolution of the form

$$0 \to A_m \to A_m^2 \to I_m \to 0.$$

Then we can apply Theorem 3 to the local ring A_m and to the ideal I_m and deduce that in the extension

$$0 \to A_m \to M_m \to I_m \to 0$$

the A_m-module M_m is free. If $I \not\subseteq m$ then $I_m = A_m$, whence M_m is free also in this case. In fact, in this case we get the exact sequence

$$0 \to A_m \to M_m \to A_m \to 0,$$

which splits because the third non-zero A_m-module is free. Applying Proposition 4 we infer that M is a projective A-module (of rank 2). Then by hypotheses M is a free A-module, i.e. $M \cong A^2$. Then the exact sequence (2.2.2) together with this latter isomorphism imply that I is generated by two elements.

Conversely, assume that *(i)* holds, i.e. the ideal I is generated by two elements f_1 and f_2. Then we may consider the homomorphism $\varphi : A^2 \to I$ defined by $\varphi(a_1, a_2) =$

$a_1 f_1 + a_2 f_2$. Since f_1 and f_2 generate I, φ is surjective. We can also consider the homomorphism $\psi : A \to A^2$ defined by $\psi(c) = (-cf_2, cf_1)$. Then it is easy to see that ψ is injective (this is obvious if A is a domain, which will the case in which we will apply Corollary 4; but the injectivity holds in general, check this!). Therefore we get the following (*a priori* not necessarily exact) sequence (analogous to (2.2.1)):

$$0 \longrightarrow A \xrightarrow{\psi} A^2 \xrightarrow{\varphi} I \longrightarrow 0, \tag{2.2.3}$$

in which ψ is injective, φ is surjective and $\varphi \circ \psi = 0$ (i.e. $\mathrm{Im}(\psi) \subseteq \mathrm{Ker}(\varphi)$).

Since I is a local complete intersection ideal of A of height 2 in the Cohen-Macaulay ring A it follows that for every maximal ideal m of A containing I, the ideal I_m of the local ring A_m of height two, which is generated by f_1 and f_2. Since A_m is also Cohen-Macaulay, this implies that $\{f_1, f_2\}$ is an A_m-sequence. Then applying Example (2.2) we infer that the sequence (2.2.3) localized at m is exact.

On the other hand, for obvious reasons (2.2.3) becomes exact also when is localized at a maximal ideal m such that $I \not\subseteq m$. Indeed, in this case $I_m = A_m$, and since I_m is generated by f_1 and f_2, either f_1 or f_2 is invertible in A_m. Assume for example that f_1 is invertible in A_m. Then we can easily prove that $\mathrm{Ker}(\varphi_m) \subseteq \mathrm{Im}(\psi_m)$. Indeed, pick an arbitrary $(a_1, a_2) \in \mathrm{Ker}(\varphi_m)$. Then $a_1 f_1 + a_2 f_2 = 0$, whence $a_1 = -(a_2 f_1^{-1}) f_2$. Taking $c := a_2 f_1^{-1}$ we get $a_1 = -cf_2$ and $a_2 = cf_1$. In other words, $(a_1, a_2) = \psi(c) \in \mathrm{Im}(\psi)$.

In conclusion the sequence (2.2.3) is exact. Then we write a part of the cohomology exact sequence (1.7.7) associated to (2.2.3) to get the exact sequence

$$\mathrm{Hom}_A(A, A) \cong A \to \mathrm{Ext}^1_A(I, A) \to \mathrm{Ext}^1_A(A^2, A).$$

Since A^2 is a free A-module, $\mathrm{Ext}^1_A(A^2, A) = 0$ (see (1.7.6)). It follows that $\mathrm{Ext}^1_A(I, A)$ is a quotient of $\mathrm{Hom}_A(A, A) \cong A$, and therefore is generated by one element. □

(2.4) Remark. If I is an ideal of A, then the exact sequence

$$0 \to I \to A \to A/I \to 0$$

induces the cohomologie exact sequence (see (1.7.7))

$$\mathrm{Ext}^1_A(A, A) \longrightarrow \mathrm{Ext}^1_A(I, A) \xrightarrow{\alpha} \mathrm{Ext}^2_A(A/I, A) \longrightarrow \mathrm{Ext}^2_A(A, A).$$

Since A is a free A-module, the first and the fourth Ext are zero (see (1.7.6)), therefore for every ideal I of A there exists a canonical isomorphism

$$\alpha : \mathrm{Ext}^1_A(I, A) \cong \mathrm{Ext}^2_A(A/I, A). \tag{2.4.1}$$

Proposition 8. *Le A be a Cohen-Macaulay ring and let $I \subset A$ be an ideal which is a local complete intersection of height 2. Then $\mathrm{Ext}^1_A(I, A)$ is a projective A/I-module of rank one.*

Proof. By remark (2.4), $\mathrm{Ext}^1_A(I, A) \cong \mathrm{Ext}^2_A(A/I, A)$, and since the second A-module has a structure of an A/I-module, it follows that $\mathrm{Ext}^1_A(I, A)$ becomes an A/I-module. To

prove that this A/I-module is projective of rank one, by Proposition 4 it will be sufficient to show that for every maximal ideal m of A/I, $\mathrm{Ext}^1_A(I,A)_m \cong \mathrm{Ext}^1_{A_m}(I_m, A_m)$ is a free $(A/I)_m$-module of rank 1. In other words, we may assume that A is local and I is generated by an A-sequence $\{f_1, f_2\}$. Then I has the free resolution (2.2.1), and so applying (1.7.11) we get the exact sequence

$$(A^2)^* \xrightarrow{\psi^*} A^* \longrightarrow \mathrm{Ext}^1_A(I,A) \longrightarrow \mathrm{Ext}^1(A^2, A) = 0,$$

where by M^* we denoted the dual $\mathrm{Hom}_A(M,A)$ of an A-module M. Recalling the definition of ψ, it follows immediately that the dual map

$$\psi^* : (A^2)^* \cong A^2 \to A^* \cong A$$

can be identified to the map $(a_1, a_2) \to -a_1 f_2 + a_2 f_1$, and therefore $\mathrm{Im}(\psi^*) = I$, i.e. $\mathrm{Ext}^1_A(I,A) \cong A/I$. $\square$

We shall also need another result due to Serre:

Theorem 4. (*Serre*) *Let A be a reduced finitely generated K-algebra over the algebraically closed field K, and let P be a projective finitely generated A-module of constant rank r (i.e. for every maximal ideal m of A one has $r = dim_{k(m)} P \otimes_A k(m)$, where $k(m) = A/m$). Assume $r > \dim(A)$. Then there is a surjective homomorphism of A-modules $P \to A$ (in particular, A este un sumand direct al lui P).*

Proof. Let $p_1, ..., p_N$ be a minimal system of generators of the A-module P (in particular, $p_1, ..., p_N$ are linearly independent over K), and denote by $\varphi : A^N \to P$ the surjective homomorphism defined by $\varphi(a_1, ..., , a_N) = \sum_{i=1}^N a_i p_i$. Set $P' := \mathrm{Ker}(\varphi)$. Then we get the exact sequence

$$0 \longrightarrow P' \longrightarrow A^N \xrightarrow{\varphi} P \longrightarrow 0.$$

Since P is projective, there exist an $N > 0$ and a homomorphism $\psi : P \to A^N$ such that $\varphi \circ \psi = \mathrm{id}_P$. It follows that $A^N \cong P \oplus P'$. By Proposition 2, P' is also a projective A-module. Moreover, $\mathrm{rank}(P') = N - \mathrm{rank}(P) = N - r$, i.e. P' is a projective A-module of constant rank $s := N - r$.

Let E (resp. E') be the sheaf on $X = \mathrm{Spec}(A)$ associated to the A-module P (resp. P'). Then E and E' are locally free sheaves of constant ranks r and $s = N - r$ respectively. Geometrically speaking, E' is a vector subbundle of rank s of the trivial vector bundle $X \times V$ of rank N over X (where V is the K-vector space $Kp_1 + \cdots + Kp_N$) such that the quotient bundle $(X \times V)/E'$ is isomorphic to E. Set $d := \dim(V)$. Since the canonical evaluation morphism $X \times V \to E$, defined by $\varphi(x,s) := s(x)$, is a surjective smooth morphism such that every fibre of φ is a k-vector subspace of V of dimension $N - r$.

Let C be the zero section of the canonical projection $\pi : E \to X$, so that $C \cong X$, and in particular, $\dim(C) = \dim(X) = d$. By dimension theorem, $\varphi^{-1}(C) = \{(x,s) \mid s(x) = 0\}$ is a closed irreducible subset of $X \times V$ of dimension $d + N - r$, and since by hypothesis $d < r$, we get $\dim(\varphi^{-1}(C)) < N$.

Let $p : X \times V \to V = \mathbb{A}^N$ be the second projection of $X \times V$, and let us denote by Y the closure of $p(\varphi^{-1}(C))$ in V. Then $\dim(Y) \leq \dim(\varphi^{-1}(C)) < N$, by the dimension theorem. In particular, $Y \neq V$. Then taking $t = a_1 p_1 + \cdots + a_N p_N \in V \setminus Y$ (and this happens for a general point $a = (a_1, ..., a_N) \in K^N$), it follows that $p^{-1}(t) \cap \varphi^{-1}(C) = \emptyset$. Since on the other hand $p^{-1}(t) \cap \varphi^{-1}(C) \cong \{x \in X \mid t(x) = 0\}$, it follows that $t(x) \neq 0$ for every closed point (i.e. maximal ideal of A) $x \in X$.

Set $M := At \subseteq P$. By construction, $t \in M$, $M \cong A$, and $t(x) \neq 0$, i.e. $t \notin m_x M_x$, for every closed point $x \in \mathrm{Spec}(A)$ (i.e. for every maximal ideal of A). Since P is a projective A-module , P_x is a free A_x-module for every closed point $x \in \mathrm{Spec}(A)$, and therefore, by Lemma 1, P_x/M_x is a free A_x-module. Then by Proposition 4 we infer that P/M is a projective A-module. In particular, $P \cong (P/M) \oplus M$, whence there exists a surjective homomorphism $P \to M \cong A$. □

Corollary 5. *Let P be a finitely generated projective module of constant rank r over the finitely generated K-algebra A such that $r > \dim(A)$. Let L be a finitely generated projective A-module of rank 1. Then there exists a surjective homomorphism of A-modules $\varphi : P \to L$.*

Proof. Set $P_1 := P \otimes L^*$, where $L^* := \mathrm{Hom}_A(L, A)$ is the dual of L. Then P_1 is a (finitely generated) projective A-module of constant rank r (one applies Proposition 3 together with the fact that for every maximal ideal m of A, $L_m \cong A_m$, because L is of rank 1). Therefore by Theorem 3 there exists a surjective homomorphism of A-modules $P_1 \to A$. Tensorizing by L, taking into account that the tensor product is a right exact functor and using the canonical isomorphism $L \otimes L^* \cong A$, we get a surjective homomorphism of A-modules $P \to L$. □

3. Three fundamental results

(3.1) Let A be a Cohen-Macaulay domain and $I \subset A$ ($I \neq A$) a local complete intersection ideal of height 2 of A. Then by Example (2.2) and (1.7.13) there exists projective resolution of the ideal I of length ≤ 1 of the form

$$0 \longrightarrow P_1 \xrightarrow{\alpha} P_0 \xrightarrow{\varepsilon} I \longrightarrow 0. \tag{3.1.1}$$

Set

$$E(I) := \mathrm{Ext}^1_A(I, A).$$

From the cohomology sequence of Ext's (see (1.7.7)) together with (1.7.6) (or just take $M = I$ and $N = A$ in (1.7.11)), we get the following exact sequence

$$0 \longrightarrow I^* \xrightarrow{\varepsilon^*} P_0^* \xrightarrow{\alpha^*} P_1^* \longrightarrow E(I) \longrightarrow 0, \tag{3.1.2}$$

where $M^* := \mathrm{Hom}_A(M, A)$ is the dual of an A-module M, and if $u : M \to N$ is a homomorphism of A-modules, then $u^* : N^* \to M^*$ is the dual homomorphism of u defined by $u^*(f) = f \circ u$, $\forall f \in N^*$. By Corollary 1 the A-modules P_0^* and P_1^* are both projective.

The first fundamental result of this section is the following duality result:

Theorem 5. *In the notation of* (3.1), *the A-module $K := \mathrm{Im}(\alpha^*)$ admits a projective resolution of length ≤ 1 and $E(K) := \mathrm{Ext}^1_A(K, A)$ is isomorphic to A/I.*

Proof. Step 1. If $i : I \to A$ is the inclusion of I in A, then $i^* = \mathrm{id}_A$, with i^* is the dual of i.

Indeed, by Proposition 5 we get the exact sequence

$$0 \longrightarrow (A/I)^* \longrightarrow A^* \xrightarrow{i^*} I^*$$

Since I contains non-zero divisors, $(A/I)^* = 0$, whence i^* is one-to-one. It remains to prove that i^* is also onto. Since this verification is a local problem, we may localize at an arbitrary maximal ideal m of A. If $I \not\subseteq m$, then $I_m = A_m$ and we have nothing to verify in this case. If $I \subseteq m$ then I_m is generated by an A_m-sequence $\{f_1, f_2\}$. In other words, we have to prove that every linear form $\lambda : I_m \to A_m$ is the multiplication by a suitable $r \in A_m$. This follows in the following way: from the obvious equality $f_1\lambda(f_2) - f_2\lambda(f_1) = 0$ (with f_1, f_2 an A_m-sequence) we get that there exists an $r \in A_m$ such that $\lambda(f_i) = rf_i$, $i = 1, 2$. It follows that λ is the restriction to I_m of the map $r : A_m \to A_m$ of multiplication by r. Step 1 is proved.

An immediate consequence of step 1 is that the canonical map $I \to I^{**}$ into bidual can be identified to the inclusion $I \subset A$.

Step 2. By step 1, the exact sequence (3.1.2) yields the exact sequence

$$0 \to I^* \cong A \to P_0^* \to K \to 0, \tag{3.1.3}$$

and taking into account that P_0^* is a projective A-module, (3.1.3) becomes a projective resolution of K of length ≤ 1. Dualizing (3.1.3) and taking into account of the definition of $E(K)$, we get the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & I & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & K^* & \longrightarrow & P_0^{**} & \longrightarrow & I^{**} & \longrightarrow & E(K) \longrightarrow 0 \end{array}$$

in which the vertical arrows are the canonical maps into biduals. The first vertical map is by Corollary 1 an isomorphism, and the second vertical map is by step 1 identified with the inclusion $I \subset A$. This proves the last part of the theorem. □

(3.2) The second fundamental result used in the sequel is the following:

Theorem 6. *(Quillen-Suslin) Let $K[X_1, ..., X_n]$ be the polynomial K-algebra in n indeterminates over a field K. Then every projective finitely generated $K[X_1, ..., X_n]$-module is free.*

Theorem 6, which had been conjectured by Serre in [S1] in 1955, has been proved independently by Quillen and Suslin in 1976. We shall not prove this result here, but we refer the reader to [K] for a proof. Geometrically, theorem 6 says that every vector bundle of rank $r \geq 1$ on the affine space $\mathbb{A}^n(K)$ is trivial.

Proposition 9. *Let A be a Cohen-Macaulay ring and $I \subset A$ a local complete intersection ideal of A of height 2. Then the A/I-module I/I^2 is projective of constant rank 2.*

Proof. Clearly, the A-module I/I^2 has the property that $\lambda \cdot \hat{x} = 0$, $\forall \lambda \in I$ and $\forall \hat{x} \in I/I^2$. Therefore the A-module structure of I/I^2 yields a natural A/I-module structure of I/I^2. To prove that I/I^2 is actually a projective A/I-module of constant rank 2 it will be sufficient to show that for every maximal ideal m of A which contains I (i.e. for every maximal ideal of A/I) the A_m/IA_m-module $(I/I^2)_m \cong I_m/I_m^2$ is free of rank 2 (see Proposition 4). Then the proof of proposition 9 will be a consequence the following more precise and general result:

Lemma 4. *Let A be a commutative unitary ring and I an ideal of A generated by an A-sequence $f_1, ..., f_r$. Then $\hat{f}_1, ..., \hat{f}_r$ is a basis of the A/I-module I/I^2.*

Proof. Since I is generated by $f_1, ..., f_r$, I/I^2 is generated (as an A-module, whence also as an A/I-module) by $\hat{f}_1, ..., \hat{f}_r$, with $\hat{f}_i := f_i \mod I^2$, $\forall i = 1, ..., r$.

It remains to prove that $\hat{f}_1, ..., , \hat{f}_r$ are linearly independent over A/I. To do this we proceed by induction on r. If $r = 1$, from $\overline{a} \cdot \hat{f}_1 = 0$, with $\overline{a} = a \mod I$, it follows that $af_1 = bf_1^2$, with $b \in A$. Since f_1 is not a zero-divisor of A, we get $a = bf_1$, i.e. $\overline{a} = 0$.

Assume now that $r \geq 2$ and the statement true for the A-sequence $f_1, ..., f_{r-1}$. Let $a_1, ..., a_r \in A$ be such that $\sum_{i=1}^r \overline{a_i} \cdot \hat{f}_i = 0$ in I/I^2. We may assume that $\sum_{i=1}^r a_i f_i = 0$ in A because otherwise $\sum_{i=1}^r a_i f_i = \sum_{i=1}^r u_i f_i$, with $u_i \in I$, and we can replace a_i by $a_i - u_i$ (without changing $\overline{a_i}$).

Since f_r is not a zero-divisor in the ring $A/Af_1+\cdots+Af_{r-1}$, from $a_rf_r = -\sum_{i=1}^{r-1} a_if_i$ it follows that there exist $b_1, ..., b_{r-1} \in A$ such that $a_r = \sum_{i=1}^{r-1} b_if_i$ (with $b_i \in A$), whence $\sum_{i=1}^{r-1}(a_i + b_if_r)f_i = 0$. By the induction hypothesis, $a_i + b_if_r \in Af_1 + \cdots + Af_{r-1}$, $\forall i = 1, ..., r-1$, from which it follows that $a_i \in I$, i.e. $\overline{a_i} = \overline{0}$, for every $i = 1, ..., r-1$. Since $a_r = \sum_{i=1}^{r-1} b_if_i$, we have $\overline{a_r} = \overline{0}$ as well. □

(3.3) A fundamental construction. Let $I \subset A$ be an ideal of the Cohen-Macaulay ring A, P a finitely generated projective A/I-module of rank 1, and $\pi : I/I^2 \to P$ a *surjective* homomorphism of A/I-modules. Then it makes sense to speak about the fibered sum $S := P \sqcup_{I/I^2} A/I^2$ with respect to the homomorphisms of A-modules $\pi : I/I^2 \to P$ and the canonical inclusion $i : I/I^2 \to A/I^2$. Let

$$0 \longrightarrow I/I^2 \xrightarrow{i} A/I^2 \xrightarrow{\varepsilon} A/I \longrightarrow 0$$

be the canonical exact sequence of A-modules. Since $\varepsilon \circ i = 0$, by the universal property of the fibered sum, there exists a unique homomorphism of A-modules $u : S \to A/I$ such that $u \circ \alpha = \varepsilon$ and $u \circ \beta = 0$, where $\alpha : A/I^2 \to S$ and $\beta : P \to S$ are the canonical maps into the fibered sum. Since ε is surjective, u is also surjective. Moreover, by Corollary 3, β is injective (since i is injective), and one easily checks that $\mathrm{Im}(\beta) = \mathrm{Ker}(u)$. In other words, we get the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I/I^2 & \xrightarrow{i} & A/I^2 & \xrightarrow{\varepsilon} & A/I & \longrightarrow & 0 \\ & & \pi\downarrow & & \alpha\downarrow & & \downarrow \mathrm{id}_{A/I} & & \\ 0 & \longrightarrow & P & \xrightarrow[\beta]{} & S & \xrightarrow[u]{} & A/I & \longrightarrow & 0 \end{array}$$

Then by the snake's lemma (Lemma 2), since the first and the third vertical maps are surjective, the map α is also surjective. It follows that there exists an ideal $J \subset A$ such that $S = A/J$ and $I^2 \subseteq J \subseteq I$. In particular, $\mathcal{V}(I) = \mathcal{V}(J)$, where for every ideal $I' \subset A$ we set

$$\mathcal{V}(I') := \{m \in \mathrm{Max}(A) \mid I' \subseteq m\}.$$

Proposition 10. *In the hypotheses and notation of* (3.3), *assume that the ideal I is a local complete intersection of height r. Then the ideal J is also a local complete intersection of height r.*

Proof. The problem being local, we can replace A by the localisation A_m (with m a maximal ideal of A), and therefore we may assume that A is a local ring with the ideal I generated by an A-sequence $f_1, ..., , f_r$, where r is the height of I ($= \dim(A) - \dim(A/I)$, because A is Cohen-Macaulay). Then by Lemma 4, I/I^2 is a free A/I-module (generated by $\hat{f}_1, ..., \hat{f}_r$). Since P is a free A/I-module of rank 1 and the homomorphism $\pi : I/I^2 \to P$ is surjective, we can choose a system of generators $g_1, ..., g_r$ of the ideal I such that $\hat{g}_1, ..., \hat{g}_r$ is a basis of I/I^2 and $\hat{g}_2, ..., , \hat{g}_r$ is a basis of $\mathrm{Ker}(\pi)$ over A/I(here we implicitly used Nakayama's lemma). Since $I = Ag_1 + \cdots + Ag_r$ and r is the height of I, we get in particular that $g_1, ..., g_r$ is a part of a system of parameters A. Recalling that A

is Cohen-Macaulay, it follows that $g_1, ..., g_r$ is an A-sequence. On the other hand, by Corolary 5 (or also by the snake's lemma) we have

$$J/I^2 = \mathrm{Ker}(A/I^2 \to S) \cong \mathrm{Ker}(\pi),$$

whence $J = Ag_2 + \cdots + Ag_r + I^2 = Ag_1^2 + Ag_2 + \cdots + Ag_r$. Since I and J have the same height r, and $g_1^2, g_2, ..., g_r$ is an A-sequence (because $g_1, ..., g_r$ is an A-sequence), J is a local complete intersection of height r. $\square$

4. Applications to the affine space curves

(4.1) We will apply the fundamental construction from (3.3) to the following situation (that will be assumed throughout this section): A a finitely generated Cohen-Macaulay K-algebra of dimension 3 for which every projective A-module of rank ≤ 2 is free (with K an algebraically closed field), and $I \subset A$ a local complete intersection ideal of height 2. (The standard example one should keep in mind is the polynomial K-algebra $A = K[X_1, X_2, X_3]$ in three variables; then by Theorem 6 of Quillen-Suslin, every projective A-module of finite rank is free.)

By Proposition 4 the A/I-module I/I^2 is projective of rank 2. Also, by Proposition 8 the A/I-module $E(I) := \mathrm{Ext}^1_A(I, A)$ is projective of rank 1. Since I/I^2 is a projective A/I-module of rank 2, $\dim(A/I) = \dim(A) - ht(I) = 3 - 2 = 1$ (where by $ht(I)$ we denoted the height of the ideal I); moreover, since $E(I)$ is a projective A/I-module of rank 1, we may apply Corollary 5 to deduce that there exists a surjective homomorphism $\pi : I/I^2 \to E(I)$ of A/I-modules.

In other words we may apply the fundamental construction from (3.3) to deduce that there exists an ideal $J \subset A$ such that $I^2 \subseteq J \subseteq I$, which yields the exact sequence

$$0 \to E(I) \to A/J \to A/I \to 0.$$

In particular, $E(I) \cong I/J$. Now we are in position to prove the the following fundamental result (from which the Main Theorem of the introduction follows):

Theorem 7. *Under the hypotheses and notation of* (4.1), *for every local complete intersection ideal $I \subset A$ of height 2 of the finitely generated Cohen-Macaulay K-algebra A for which every projective A-module of rank ≤ 2 is free, the ideal J (coming from the fundamental construction* (3.3)*) is generated by two elements. In particular, there exist two elements $f_1, f_2 \in I$ such that $\sqrt{I} = \sqrt{(f_1, f_2)}$.*

Proof. Since $I^2 \subseteq J \subseteq I$ and the height of I is two, the height of J is also two. By Proposition 10 the ideal J is a local complete intersection. Then by (1.7.13) and the example (2.2), we deduce that $\mathrm{dh}_A(J) \leq 1$. In particular, there exists a projective resolution of J of the form

$$0 \to G_1 \to G_0 \to J \to 0.$$

To prove that J is generated by two elements we shall apply Serre's criterion (Corollary 4), according to which it is sufficient to check that $E(J) := \mathrm{Ext}^1_A(J, A)$ is generated by one element.

On the other hand, if

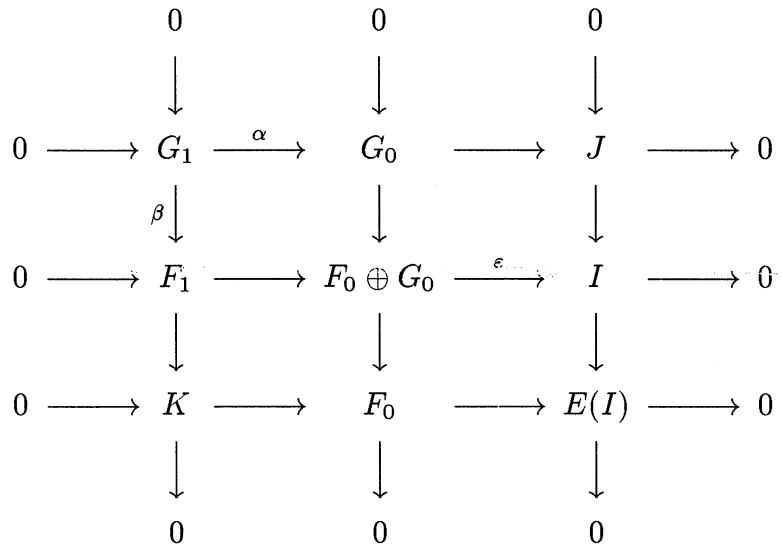
$$0 \longrightarrow P_1 \xrightarrow{u} P_0 \longrightarrow I \longrightarrow 0$$

is a projective resolution of I, we may consider the exact sequence

$$0 \to K \to F_0 = P_1^* \to E(I) \to 0$$

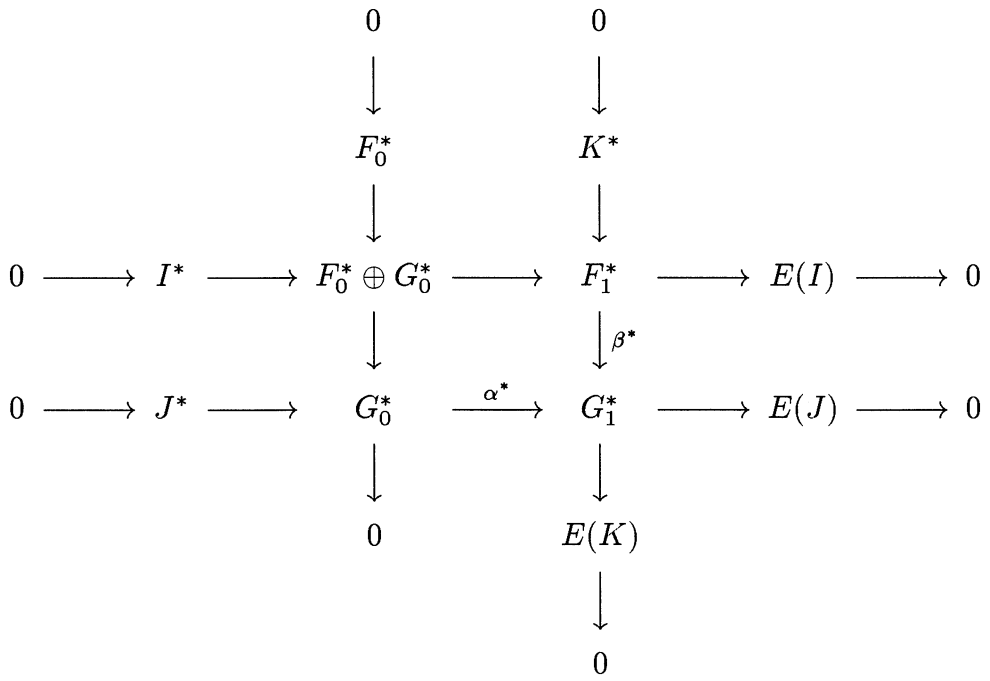
given by Theorem 5, where K is the image of the dual homomorphism $u^* : P_0^* \to P_1^*$. Then by Theorem 5, $\mathrm{dh}_A(K) \leq 1$ and $E(K) \cong A/I$.

At this point we can consider the commutative diagram with exact rows and colums



which can be obtained exactly as in the proof of Lemma 3. More precisely, the map ε can be constructed as in the proof of Lemma 3, and $F_1 := \mathrm{Ker}(\varepsilon)$. Since $\mathrm{dh}_A(I) \leq 1$ and $F_0 \oplus G_0$ is projective, F_1 is also projective. In particular, it follows that the first column is a projective resolution of K, provided it is an exact sequence. But by construction all the three lines and the last two columns are exact sequences. Then the exactness of the first column follows from the snake's lemma (Lemma 2).

Dualizing we get the commutative diagram with exact rows and colums:



Since $\mathrm{Im}(\alpha^*) \subseteq \mathrm{Im}(\beta^*)$, the surjective map $G_1^* \to E(K)$ yields the surjective map $\psi_0 : E(J) \to E(K) \cong A/I$. Denote by $\psi : E(J) \to A/I$ the surjective map gotten by

composition. Since $E(J)$ and A/I are A/J-modules, there exists a homomorphism of A/J-modules $\chi : A/J \to E(J)$ (not necessarily unique) such that the canonical homomorphism $c : A/J \to A/I$ (given by the inclusion $J \subseteq I$) coincides to the composition

$$A/J \xrightarrow{\chi} E(J) \xrightarrow{\psi} A/I.$$

Indeed, since ψ is surjective there exists an element $x \in E(J)$ such that $\psi(x)$ is the class of 1 in A/I. Since $E(J)$ is an A/J-module, J annihilates x, and then we can take χ the unique homomorphism of A/J-modules $\chi : A/J \to E(J)$ which maps the class of 1 in A/J in x.

To finish the proof of the theorem it will be sufficient to show that the map χ is an isomorphism (of A-modules). Since the bijectivity of χ is a local problem, we may replace A by A_m, for an arbitrary maximal ideal m of A, and therefore we may assume that A is a local ring. Then by Proposition 10, J is generated by an A-sequence of length two (because I is generated by an A-sequence of length two), and therefore by Proposition 8 we deduce that $E(J) \cong A/J$. In other words, the canonical surjective homomorphism $c : A/J \to A/I$ can be decomposed as $c = \psi \circ \chi$, with $\psi : A/J \to A/I$ and $\chi : A/J \to A/J$. If χ would not be an isomorphism (i.e. if $\chi(1)$ would be non-invertible in A/J), then $\psi(\chi(1)) = c(1) = 1$ would be non-invertible in A/I (because A is local), a contradiction. Therefore $\psi(1)$ is invertible in A/J. This implies that the map $\psi : A/J \to E(J)$ is (globally) an isomorphism, i.e. $E(J)$ is an A-module generated by one element. □

(4.2) Theorem 7 can be applied to every local complete intersection ideal I of height 2 of the polynomial K-algebra $A = K[X_1, X_2, X_3]$ in three variables over an algebraically closed field K. Indeed, by the result of Quillen-Suslin (theorem 6), in this case every projective A-module of finite rank is free. Geometrically speaking, the local complete intersection ideals $I \subset A$ of height 2 correspond to the affine curves contained in the affine 3-dimensional space $\mathbb{A}^3 = \mathbb{A}^3(K)$, which are locally complete intersection in $\mathbb{A}^3$. For example, every irreducible smooth curve C of $\mathbb{A}^3$ are example of such curves. This follows from the following elementary result of local algebra (exercise, or see [AM] for the algebraic formulation, or [Sh], or [H1] for the geometric formulation):

Proposition 11. *Let A be a regular local ring of dimension $n \geq 2$, and let $I \subset A$ be an ideal of A such that the quotient ring A/I is regular of dimension d. Then there exists an A-sequence $f_1, ..., f_{n-d} \in I$ such that $I = Af_1 + \cdots + Af_{n-d}$.*

Theorem 7 implies therefore the Main Theorem of the introduction:

Theorem 8. *(Serre-Ferrand-Szpiro) Let K be an algebrically closed field and let C be a local complete intersection curve of the affine 3-dimensional space $\mathbb{A}^3 = \mathbb{A}^3(K)$. Then C is defined by two equations in $\mathbb{A}^3$, i.e. there exist two polynomials $f, g \in K[X_1, X_2, X_3]$ such that*

$$C = \{(x_1, x_2, x_3) \in \mathbb{A}^3 \mid f(x_1, x_2, x_3) = g(x_1, , x_2, x_3) = 0\}.$$

In particular, every smooth irreducible affine curve C in $\mathbb{A}^3$ is defined by two equations.

(4.3) Remark. Theorem 8 of Serre-Ferrand-Szpiro says nothing about the number of generators of the ideal $\mathcal{I}(C)$ of a local complete intersection curve C in $\mathbb{A}^3$, where $\mathcal{I}(C)$ is the ideal defined by:

$$\mathcal{I}(C) := \{P \in K[X_1,,X_2,X_3] \mid P(x) = 0,\ \forall x \in C\}.$$

This result only asserts that there exists an ideal J of $K[X_1,X_2,X_3]$ which is generated by two polynomials of $K[X_1,X_2,X_3]$ such that $\mathcal{I}(C)^2 \subseteq J \subseteq \mathcal{I}(C)$. These inclusions imply that the zero locus $\mathcal{V}(J)$ of J coincides to $\mathcal{V}(\mathcal{I}(C)) = C$. In other words, the local complete intersection curve C of $\mathbb{A}^3$ is given only *set-theoretically* $\mathbb{A}^3$ by two polynomials. The curves C of $\mathbb{A}^3$ with this latter property are called *set-theoretic complete intersection affine space curves.* A curve C of $\mathbb{A}^3$ for which even the ideal $\mathcal{I}(C)$ is generated by two polynomials is called a *scheme-theoretic complete intersection affine space curve.*

Finally, we should emphasize that the hypothesis that C is a local complete intersection curve in $\mathbb{A}^3$ is essential in theorem 8. Indeed, there are examples of (non local complete intersection) curves in $\mathbb{A}^3$ that are not given by two equations in $\mathbb{A}^3$.

(4.4) Remark. The analogous problem concerning the number of (homogeneous) equations defining a (smooth) projective curve C of the 3-dimensional projective space $\mathbb{P}^3$ is completely open. In other words, it is not known whether every smooth irreducible projective curve C of $\mathbb{P}^3$ can be given by two (homogeneous) equations (i.e. homogeneous polynomials of the polynomial K-algebra $K[X_0,X_1,X_2,X_3]$).