Treball final de grau

GRAU DE MATEMÀTIQUES

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

The Quillen-Suslin Theorem

Autor: Nil Garcés de Marcilla Escubedo

Director: Dr. Carlos D'Andrea
Realitzat a: Departament d'Àlgebra i Geometria

Barcelona, 27 de juny de 2018

Acknowledgements

First of all, I would like to thank my tutor Carlos D'Andrea for his willingness to help me whenever I needed it, his interest in this work and his patience responding to my rather long emails. His guidance both on the mathematical and personal level surely account for the final quality of the exposition and for making this learning experience more enriching and enjoyable.
I would also want to thank the professor Santiago Zarzuela for giving me bibliographic references on some topics of the work and for introducing me to polynomial rings and commutative algebra at university, and the professor Joan Carles Naranjo for giving me advice on the more geometric aspects of the memoir.
Finally, thanks to all my family, friends and everyone in general who has given me the motivational support necessary to complete successfully this challenging endeavour, specially my loved companion Clara.

Abstract

The Quillen-Suslin Theorem is usually stated as "Let P be a finitely generated projective module over $k[x_1, \ldots, x_n]$. Then P is free". Before being proven independently and in its full generality by Quillen and Suslin in 1976, this question was usually referred to as the "Serre's Conjecture", and stood as one of the most relevant open problems in algebra and affine algebraic geometry for twenty years.
In this memoir we provide in detail all the algebraic tools needed to have a good understanding of the basic mathematics surrounding this theorem and its more elementary proof by Vaserstein, as well as some algorithms related to it.

2010 Mathematics Subject Classification. 13C10, 13D02, 13P99

Contents

Introduction

In his hugely influential paper *Faisceaux algébriques cohérents* ([11], ca. 1955), J.P. Serre systematically introduced modern sheaf theory into algebraic geometry, a field which experienced an almost entire reformulation during the 1950s, with new language and more advanced tools. On page 243 he wrote, rather innocently, (k being a field): "I ignore if there exist finite(ly generated) projective modules over $k[x_1, \ldots, x_n]$ which are not free", making it quite clear that he intended his statement as an *open problem* in this brand new sheaf-theoretic framework. Nowhere in his published writings had he speculated, one way or another, upon the possible outcome of his question. However, almost from the start a surmised positive answer to Serre's problem became known to the mathematical world as the "Serre's Conjecture". This impression was strengthened when he himself proved, just three years later, that projective modules over $k[x_1, \ldots, x_n]$ are *stably free*.

Somewhat later, the interest in projective modules and this "conjecture" was further heightened by the development of two new and closely related subjects in mathematics: homological algebra and algebraic K-theory. With relevant motivations coming from these two areas, "Serre's Conjecture" entered the 1960s as one of the premier open problems in algebra and affine algebraic geometry.

In the 20-year period 1956-1976, new techniques and new insights were introduced into the study of projective modules- over general rings as well as polynomial rings. Interestingly, during this period Serre's Conjecture was solved in one special case after another, by widely different and inventive methods that *did not* seem to generalize. Finally, culminating almost twenty years of effort by algebraists, D. Quillen and A. Suslin proved independently in January of 1976 the statement in its full generality- that is, that finitely generated projective modules over $k[x_1, \ldots, x_n]$ are, indeed, free, for *all* n, and for *all* fields k. Thus, nowadays this result is usually referred to as the **Quillen-Suslin Theorem**.

Shortly thereafter, some very ingenious shorter and more elementary proofs of it became available, being the one by Vaserstein, the proof we will expose in this work, the most popular of them. Using the technique of extending unimodular rows to invertible matrices, his solution not only made the problem completely accessible to anyone with basic knowledge of graduate algebra, but also established the study of unimodular rows as a new interesting topic for research in commutative ring theory. In fact, the proofs by Quillen and Suslin only meant the end of Serre's problem as it had been originally formulated, as many of its ramifications and generalizations have continued to flourish at a steady pace since then: the list of areas of mathematics in which the theorem has had some kind of repercussion in their development is extensive, ranging from the most abstract to the more computational and algorithmic.

In this memoir we provide in detail all the algebraic tools needed to have a good understanding of the basic mathematics surrounding this problem and its proof by Vaserstein, as well as some algorithms related to it. My first contact with this theorem occurred incidentally one year ago, while looking for some information about free resolutions of algebraic varieties. Exploring it a little more, I was impressed by its evolution and by the fact that a result so

influential and originally difficult could nowadays be understood with relatively simple but powerful algebraic tools. As someone greatly interested in commutative algebra and all the branches that have led to its development, I soon realized the potential that the study of this theorem had as an undergraduate's final project, both for its impact and the amount of interesting and varied topics of algebra it passes through.

Memoir structure

In general, the whole text is mostly self-contained and its tone is kept simple, with the inevitable exceptions of section 2.3 and Appendix B, notably more advanced.

Every ring R in the text is commutative and unitary unless otherwise specified.

- *Appendix A* is a collection of some indispensable concepts and results of commutative algebra that the reader should know before reading the main text.
- In *Chapter 1* we develop four relevant notions of modern commutative algebra that will be necessary later in our main exposition. While the *Splitting lemma* is essential and *Localization* appears several times in many chapters, the other two are required in specific sections and one could postpone their reading until they become necessary.
- In *Chapter 2* we introduce projective modules and give some examples of them. We later prove that finitely generated projective modules over a local ring are free and its easy corollary that, if P is a finitely generated projective R-module, then P is finite locally free. In *Appendix B* we give a demonstration of the *converse* implication, considerably harder to prove, for the skilled reader. In the final section, we outline the quite advanced geometric context in which Serre raised his initial question about finitely generated projective modules over $k[x_1, \dots, x_n]$.
- *Chapter 3* presents the notion of a stably free module, a more restrictive kind of projective module which admits a really practical characterization in terms of invertible matrices. The main object of this chapter are *unimodular rows*, which will allow us to restate the whole problem using a more matrix-theoretical approach and that will play a huge role in our final proof of the Quillen-Suslin Theorem.
- The rather technical *Chapter 4* is entirely devoted to prove that finitely generated projective modules over $k[x_1, \dots, x_n]$ *are* stably free, a result also known as the Hilbert-Serre Theorem. This makes it possible to employ their useful properties presented in Chapter 3 to demonstrate the Theorem this whole work is about.
- In *Chapter 5* we finally prove the Quillen-Suslin Theorem, using all the tools presented so far. In its first section we give a kind of constructive proof of it in the case of one variable, an algorithm that will appear again in the final chapter. After demonstrating the Horrock's Theorem, an intermediate necessary result, we prove our desired Theorem in its generality in the last section.
- The interesting *Chapter 6*, more computational in its spirit, is focused on providing an algorithm for extending any given unimodular row in $\mathbb{C}[x_1, \dots, x_n]$ to an invertible matrix with polynomial entries, using the ideas of the previous chapter.

Chapter 1

Preliminaries

1.1 Splitting lemma

This well-known lemma of homological algebra, applicable in any abelian category, gives a simple but handy criterion in terms of exact sequences for a module to be a direct summand of another module, something which is extremely useful when we deal with projective modules. Its consequences will appear constantly throughout the text:

Lemma 1.1. ***(Splitting lemma):*** *Let $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ be an exact sequence of R-modules. The following statements are equivalent:*

(i) There is an homomorphism $\varphi : M'' \to M$ with $g \circ \varphi = id_{M''}$

(ii) There is an homomorphism $\psi : M \to M'$ with $\psi \circ f = id_{M'}$

If these conditions are satisfied, then we have isomorphisms:

$$M = \mathrm{Ker}(g) \oplus \mathrm{Im}(\varphi), \quad M = \mathrm{Im}(f) \oplus \mathrm{Ker}(\psi), \quad M \cong M' \oplus M'' \tag{1.1}$$

Proof. $i) \implies ii)$: We will prove that under $i)$, we have $M = \mathrm{Ker}(g) \oplus \mathrm{Im}(\varphi)$, so we will have $\mathrm{Im}(\varphi) \cong M''$ (as $g \circ \varphi = id_{M''}$, φ is injective) and, since the sequence is exact, $\mathrm{Ker}(g) = \mathrm{Im}(f) \cong M'$, obtaining $M \cong M' \oplus M''$. Thus, the existence of ψ of $ii)$ will be immediate:

Let $x \in M$. Then $x - \varphi(g(x))$ is in the kernel of g, since

$$g(x - \varphi(g(x))) = g(x) - g(\varphi(g(x))) = g(x) - id(g(x)) = g(x) - g(x) = 0 \tag{1.2}$$

and hence $M = \mathrm{Ker}(g) + \mathrm{Im}(\varphi)$.
This sum is direct, for if $x \in \mathrm{Ker}(g) \cap \mathrm{Im}(\varphi)$, there exists $x' \in M''$ with $\varphi(x') = x$, but $g(\varphi(x')) = 0 = x'$, and φ is injective $\Rightarrow \varphi(x') = x = 0$. ✓

$ii) \implies i)$: Analogously, we will prove that under $ii)$, we have $M = \mathrm{Im}(f) \oplus \mathrm{Ker}(\psi)$, so we will have $\mathrm{Im}(f) \cong M'$ (f injective) and $\mathrm{Ker}(\psi) \cong M''$ (to see this last isomorphism,

take $\bar{g} = g|_{\mathrm{Ker}(\psi)}$: clearly $\bar{g} : \mathrm{Ker}(\psi) \to M''$ is injective because if $\bar{g}(x) = 0 \Rightarrow x \in \mathrm{Ker}(g) \Rightarrow x \in \mathrm{Im}(f) \Rightarrow x = f(x')$, $x' \in M' \Rightarrow \psi(f(x')) = x'$ but $x \in \mathrm{Ker}(\psi) \Rightarrow x' = 0 \Rightarrow x = 0$, and surjective because for any $x' \in M''$, there exists $x \in M$ with $g(x) = x'$, and $x - f(\psi(x)) \in \mathrm{Ker}(\psi)$ (see the formula (1.3) below) and has image x'). Thus, we obtain $M \cong M' \oplus M''$, and the existence of φ of i) will be immediate:

Let $x \in M$. Then $x - f(\psi(x))$ is in the kernel of ψ, since

$$\psi(x - f(\psi(x))) = \psi(x) - \psi(f(\psi(x))) = \psi(x) - id(\psi(x)) = \psi(x) - \psi(x) = 0 \tag{1.3}$$

and hence $M = \mathrm{Ker}(\psi) + \mathrm{Im}(f)$.
Again, this sum is direct, for if $x \in \mathrm{Ker}(\psi) \cap \mathrm{Im}(f)$, there exists $x' \in M'$ with $f(x') = x$, but $\psi(f(x')) = 0 = x'$, and f is injective $\Rightarrow f(x') = x = 0$. ✓

□

Definition 1.2. *If these equivalent conditions hold, the exact sequence is called* ***split exact****, or we say that the sequence* ***splits****. Furthermore, we say that an epimorphism p (resp. monomorphism i)* ***splits*** *if it fits in a split exact sequence.*

1.2 Localization

The process of localization is one of the most important technical tools in modern algebra, and the truly importance of finitely generated projective modules becomes apparent mainly when we think of them locally (sections 2.2 and 2.3, Appendix B), so we better make sure to understand it well. These notions will reappear in Chapter 5, when we prove the Quillen-Suslin Theorem, and in Chapter 6. Roughly speaking, it may be thought of as the process of adding inverses for certain elements of a ring.

Definition 1.3. *Given a ring R, we say that $S \subsetneq R$ is a* ***multiplicatively closed subset*** *of R if $1 \in S$ and, for any two $s, t \in S \Rightarrow st \in S$.*

We can then define an equivalence relation in $R \times S$ as

$$(a, s) \sim (b, t) \iff u(at - bs) = 0 \text{ for some } u \in S \tag{1.4}$$

We write $\frac{a}{s}$ for the equivalence class of (a, s) and $S^{-1}R = R \times S/\sim$. $S^{-1}R$ is naturally a commutative and unitary ring with the addition and multiplication defined in the same way as with fractions of elementary algebra,

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} \tag{1.5}$$

It is elementary to see that these operations are indeed independent of the choice of the representatives. Also note that, with the multiplication defined this way, we have that every element of the form $\frac{s}{s'}$ with $s \in S$ becomes a unit in $S^{-1}R$.

Definition 1.4. *Given a commutative ring R, we call* ***spectrum of*** *R the set of its prime ideals, that is,* $\mathrm{Spec}(R) = \{\mathfrak{p} \subset R | \, \mathfrak{p} \text{ is a prime ideal in } R\}$.

Now, given $\mathfrak{p} \in Spec(R)$, it is immediate to see that $S = R\backslash\mathfrak{p}$ is a multiplicatively closed subset of R. We write $R_\mathfrak{p} := S^{-1}R$ in this case. The elements $\frac{a}{s}$ with $a \in \mathfrak{p}$ form an ideal $\mathfrak{m}$ in $R_\mathfrak{p}$. If $\frac{b}{t} \notin \mathfrak{m}$, then $b \notin \mathfrak{p}$, so $b \in S$ and therefore $\frac{b}{t}$ is a unit in $R_\mathfrak{p}$. It follows that, if $\mathfrak{a}$ is an ideal in $R_\mathfrak{p}$ and $\mathfrak{a} \nsubseteq \mathfrak{m}$, then $\mathfrak{a}$ contains a unit and is therefore the whole ring. Hence $\mathfrak{m}$ is the *only* maximal ideal in $R_\mathfrak{p}$.

Definition 1.5. *We say that a ring is local if it only contains one maximal ideal.*

Thus, $R_\mathfrak{p}$ is a local ring, and the process of passing from R to $R_\mathfrak{p}$ is called **localization at** $\mathfrak{p}$. Local rings are easier to study and have very nice properties, and they play a major role in modern algebra- in fact, many important results in this area, including the Quillen-Suslin Theorem as we shall see, have been proved by "glueing together" local rings which satisfy or not a certain characteristic.

The construction of $S^{-1}R$ can be carried through with an R-module M instead of a ring R. Similarly, we define a relation in $M \times S$ as follows:

$$(m, s) \sim (m', s') \iff u(sm' - s'm) \text{ for some } u \in S. \tag{1.6}$$

As before, this is an equivalence relation, and we write $\frac{m}{s}$ for the equivalence class of the pair (m, s). $S^{-1}M$ denotes the set of such fractions, and it can be made into an $S^{-1}R$-module with the obvious definitions of addition and scalar multiplication. Analogously to $R_\mathfrak{p}$, we write $M_\mathfrak{p}$ instead of $S^{-1}M$ when $S = R\backslash\mathfrak{p}$ with $\mathfrak{p}$ a prime ideal of R, and we call this process the **localization of** M **at** $\mathfrak{p}$. In this memoir, we will see that the $R_\mathfrak{p}$-module $M_\mathfrak{p}$ can usually give us information about M as a R-module.

1.3 Finite filtration of a Noetherian module

The concept of filtration appears in many contexts in mathematics, though in this section we refer to a very concrete case: we prove that, over a Noetherian ring R, every finitely generated R-module M admits a finite chain like the one described in Theorem 1.13. This result and the notion of associated prime will be necessary in our proof of the Hilbert-Serre Theorem (section 4.3, Theorem 4.13).

Definition 1.6. *Given two R-modules M, N, with $M \subseteq N$, we define their **ideal quotient** as $(M : N) = \{a \in R |\, aN \subseteq M\}$ (it is immediate to verify that it is an ideal). If we take $M = 0$, we call this ideal the **annihilator of** N, $Ann_R(N) = \{a \in R |\, aN = 0\}$.*

Definition 1.7. *Given a R-module M, we say that $\mathfrak{p} \in Spec(R)$ is **associated to** M if there exists a non-zero element $m \in M$ such that $\mathfrak{p} = Ann_R(m)$ (we write m instead of the R-submodule (m), to simplify). The set of **associated primes of** M is denoted by $Ass_R(M)$.*

Here is a useful criterion to know whether a prime ideal is an associated prime of M:

Lemma 1.8. $\mathfrak{p} \in Ass_R(M) \iff$ *There exists an injective R-morphism $h_\mathfrak{p} : R/\mathfrak{p} \hookrightarrow M$*

Proof. $\Rightarrow$) If $\mathfrak{p} = Ann_R(m)$ for $m \in M$, define the R-linear map $R \to M$, $x \mapsto xm$. It clearly induces an injection $R/\mathfrak{p} \hookrightarrow M$.
$\Leftarrow$) Suppose there is an R-injection $R/\mathfrak{p} \hookrightarrow M$, and let $m \in M$ be the image of 1. Then $\mathfrak{p} = Ann_R(m)$, so $\mathfrak{p} \in Ass_R(M)$. □

Also, these two results guarantee that there always exist associated primes if $M \neq 0$:

Proposition 1.9. *Let R be a ring, M a R-module and $\mathfrak{a}$ an ideal. Then, if $\mathfrak{a}$ is maximal in the set of annihilators of non-zero elements of M, $\mathfrak{a} \in Ass_R(M)$.*

Proof. We just have to see that $\mathfrak{a}$ is prime. Say $\mathfrak{a} := Ann_R(m)$ with $m \neq 0$. Then $1 \notin \mathfrak{a}$, as $m \neq 0$. Suppose $b, c \in R$ with $bc \in \mathfrak{a}$, but $c \notin \mathfrak{a}$. Then $bcm = 0$, but $cm \neq 0$. Clearly, $\mathfrak{a} \subseteq Ann_R(cm)$, so $\mathfrak{a} = Ann_R(cm)$ by maximality. But $b \in Ann_R(cm)$, so $b \in \mathfrak{a}$. This proves that $\mathfrak{a}$ is prime. □

Corollary 1.10. *If R is Noetherian and M a R-module, $M = 0 \iff Ass_R(M) = \emptyset$*

Proof. $\Rightarrow$ is trivial. $\Leftarrow$ follows from the fact that, if R is Noetherian, the set of annihilators of non-zero elements of M has at least one maximal ideal $\mathfrak{p}$ and, by the Proposition 1.9, $\mathfrak{p} \in Ass_R(M)$. □

We just need the following two previous results to prove Theorem 1.13:

Lemma 1.11. *For a ring R and a prime ideal $\mathfrak{p}$, $Ass_R(R/\mathfrak{p}) = \{\mathfrak{p}\}$.*

Proof. $\supseteq$ is trivial. To see $\subseteq$, it is enough to see that for any non-zero element $m \in R/\mathfrak{p}$, $Ann_R(m) = \mathfrak{p}$. To see this, say $m \neq 0$ is the residue of $y \in R$ (so $y \notin \mathfrak{p}$). Let $x \in R$. Then $xm = 0 \iff xy \in \mathfrak{p} \iff x \in \mathfrak{p}$, so $Ann_R(m) = \mathfrak{p}$. □

Proposition 1.12. *For R-modules M_1, M_2 and M_3 and $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ exact, we have $Ass_R(M_1) \subseteq Ass_R(M_2)$ and $Ass_R(M_2) \subseteq Ass_R(M_1) \cup Ass_R(M_3)$.*

Proof. The first inclusion is trivial, as if we have $\mathfrak{p} = Ann_R(m_1)$ with $m_1 \in M_1$, then $\mathfrak{p} = Ann_R(f(m_1))$ (f is injective), so $\mathfrak{p} \in Ass_R(M_2)$.
To prove the second inclusion, suppose we have $\mathfrak{p} \in Spec(R)$ with $h : R/\mathfrak{p} \hookrightarrow M_2$. If $h(R/\mathfrak{p}) \cap f(M_1) \neq \emptyset \Rightarrow \exists m_1 \in M_1$ such that $Ann_R(f(m_1)) = \mathfrak{p}$ by Lemma 1.11 (see its proof), and as f is injective, that means $\mathfrak{p} = Ass_R(m_1)$ and so $\mathfrak{p} \in Ass_R(M_1)$.
If $h(R/\mathfrak{p}) \cap f(M_1) = \emptyset$, then the composition $R/\mathfrak{p} \hookrightarrow M_2 \to M_3$ is injective (as $\mathrm{Im}(f) = \mathrm{Ker}(g)$, no element goes to zero in the second map), and $\mathfrak{p} \in Ass_R(M_3)$ by Lemma 1.8. □

Theorem 1.13. *If R is Noetherian and $M \neq 0$ a finitely generated R-module, there exists a finite chain of R-submodules*

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n = M \tag{1.7}$$

*with $M_{i+1}/M_i \cong R/\mathfrak{p}_i$, with $\mathfrak{p}_i \in Spec(R)$. Such a chain is called a **(finite) filtration of M**.*

Proof. As $Ass_R(M) \neq \emptyset$, by Corollary 1.10 we can take $\mathfrak{p}_1 \in Ass_R(M)$. Then, by Lemma 1.8, there exists $M_1 \subseteq M$ with $M_1 \cong R/\mathfrak{p}_1$ ($M_1 = h_{\mathfrak{p}_1}(R/\mathfrak{p}_1)$). Thus, we have

$$0 = M_0 \subsetneq M_1 \subseteq M \tag{1.8}$$

Now, if $M \neq M_1$, again there exists $\mathfrak{p}_2 \in Ass_R(M/M_1)$ such that $h_{\mathfrak{p}_2} : R/\mathfrak{p}_2 \hookrightarrow M/M_1$, so there exists M_2 with $M_2 \subseteq M, M_1 \subsetneq M_2$ such that $M_2/M_1 \cong R/\mathfrak{p}_2$, and

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subseteq M. \tag{1.9}$$

This can be done repeatedly, obtaining a chain

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subseteq M \tag{1.10}$$

As R is Noetherian and M finitely generated, M is Noetherian and the chain of (1.10) must eventually stabilize, so in this process there exists some n with $M_n = M$, and we get the finite filtration with the desired properties. □

Corollary 1.14. *If R is Noetherian and M a finitely generated R-module, $Ass_R(M)$ is finite.*

Proof. It is enough to prove that $Ass_R(M) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, with $\mathfrak{p}_i$ the prime ideals of the finite filtration. This follows applying Proposition 1.12 inductively to the exact sequence

$$0 \to M_i \to M_{i+1} \to M_{i+1}/M_i \to 0 \tag{1.11}$$

and keeping in mind the Lemma 1.11 in each step and $M_{i+1}/M_i \cong R/\mathfrak{p}_i \; \forall i$. □

1.4 Noether's Normalization Theorem

In this last section, we provide a standard proof of the Noether's Normalization Theorem. However, we are not interested in the result per se, but in the change of variables we have to do to prove it, and Remark 1.20. We will need this very same construction in our final proof of the Quillen-Suslin Theorem and in Chapter 6, when we discuss some algorithmic aspects. We start with some basic definitions:

Definition 1.15. *Let K be an extension field of a field k. Let S be a subset of K. We say that the elements $\{s\}_{s\in S}$ are **algebraically independent over** k if they do not satisfy any non-trivial polynomial equation with coefficients in k.*

Definition 1.16. *If S is a subset of K which is algebraically independent over k and its cardinality is the greatest among all such subsets, then we call this cardinality the **transcendence degree** of K over k. In this case, we say that the elements of S are a **transcendence basis** of K over k.*

It can be proven that any two transcendence bases of K over k have the same cardinality, whether it is finite or infinite, so the transcendence degree is well defined. We arrive now to our most relevant definition:

Definition 1.17. *For a commutative ring B and $A \subseteq B$ a subring, we say that an element $b \in B$ is **integral over** A if b is a root of a monic polynomial with coefficients in A. If every element of B is integral over A, then we say that B is integral over A.*

It can be proven that the set of integral elements $b \in B$ over A forms a subring of B, obviously containing A. We also need this lemma, which we will state without proof, as it is proved in the course of "Commutative Algebra" of our bachelor's degree:

Lemma 1.18. ***(Transitivity of integral extensions):*** *If $A \subseteq B \subseteq C$ are rings and B is integral over A and C is integral over B, then C is integral over A.*

With this in mind, we can now demonstrate our main theorem:

Theorem 1.19. ***(Nother's Normalization Theorem):*** *Let $k[x_1,\dots,x_n] = k[x]$ be a finitely generated integral domain over a field k, and assume that $k(x)$ has transcendence degree r. Then there exist elements $y_1,\dots,y_r$ in $k[x]$ such that $k[x]$ is integral over $k[y_1,\dots,y_r] = k[y]$.*

Proof. As the integral elements form a subring, it is enough that the variables x_i are integral. If they are already algebraically independent over k, then $n = r$ and we are done with $y_i = x_i\ \forall i$. If not, there exists a non-trivial relation

$$\sum_{i\in I} a_i x_1^{\alpha_1^i}\dots x_n^{\alpha_n^i} = 0 \tag{1.12}$$

with $0 \neq a_i \in k$ and I finite, so the sum is taken over a finite number of distinct n-tuples of integers $(\alpha_1^i,\dots,\alpha_n^i)$, $\alpha_j^i \geq 0$. Now let $m_2,\dots,m_n$ be positive integers, and put

$$y_2 = x_2 - x_1^{m_2},\quad \dots\quad , y_n = x_n - x_1^{m_n}. \tag{1.13}$$

Clearly $x_i = y_i + x_1^{m_i}$, $i = 2,\dots,n$, and we can substitute that in (1.12). Using vector notation, we write $(m) = (1, m_2,\dots,m_n)$ and use the dot product $(\alpha^i)\cdot(m)$ for $\alpha_1^i + m_2\alpha_2^i + \dots + m_n\alpha_n^i$. If we expand now the relation of (1.12), we get

$$\sum_{i\in I} c_i x_1^{(\alpha^i)\cdot(m)} + f(x_1, y_2,\dots,y_n) = 0, \tag{1.14}$$

where f is a polynomial in which no pure power of x_1 appears. If we select now $d > \max_{i,j}\{\alpha_j^i\}$ and we take $(m) = (1, d, d^2,\dots,d^n)$, then all the $(\alpha^i)\cdot(m)$ are distinct, so the left sum of (1.14) can not be zero, and thus we obtain an integral equation for x_1 over $k[y_2,\dots,y_n]$ dividing by a certain constant, if necessary (k is a field). Since each x_1, $i > 1$ is clearly integral over $k[x_1, y_2,\dots,y_n]$, all the variables are integral and it follows that $k[x]$ is integral over $k[y_2,\dots,y_n]$. We can now proceed inductively, using the transitivity of integral extensions (Lemma 1.18), to shrink the number of y's until we reach an algebraically independent set of y's, which will have r elements. □

Remark 1.20. *The transcendence degree of $k(x_1,\dots,x_n)$ over k, with the x_i being independent variables (that is, the "usual" polynomial ring) is n, so what the proof of this theorem shows us in this case is that, for any $f \in k[x_1,\dots,x_n]$, it is possible to do a change of variables $x_i \mapsto y_i$ such that the same polynomial written with the variables y_i is* ***monic*** *in y_1. In this situation a "change of variables" means an automorphism of k-algebras $\varphi : k[x_1,\dots,x_n] \to k[x_1,\dots,x_n]$, $x_i \mapsto \varphi(x_i)$, so that we can always recover the unique preimage of $\varphi(f)$ with φ^{-1}. This way, for any $f \in k[x_1,\dots,x_n]$, we can take a change of variables based on the one in (1.13):*

$$y_1 = x_1,\quad y_2 = x_2 - x_1^{m_2},\quad \dots\quad , y_n = x_n - x_1^{m_n}, \tag{1.15}$$

such that f is monic expressed in terms of the y_i, dividing by a certain constant if necessary (it is clear that the k-algebra morphism φ defined on the generators like in (1.15) is an automorphism). This change of variables φ will be important because, later on, we will work with some polynomial matrices with determinant in $k\backslash 0$ in which monic polynomials play a huge role, and as $\varphi|_k = id_k$, the determinant will not change under this change of variables, so we will be able to transform a certain f to a monic $\bar{f}$ conveniently. In this case, if in this "new" matrix we do not manipulate some $\bar{f}$'s, we can always recover a matrix with their initial polynomials f's by applying φ^{-1}.

Chapter 2

Projective modules

Let us introduce right away the main object of this work in its full generality:

2.1 Definition and examples

Proposition 2.1. *Let R be a ring and P a R-module. The following properties are equivalent:*

(i) For all R-modules M, M'', given a homomorphism $f : P \to M''$ and a surjective homomorphism $g : M \to M''$, there exists a homomorphism $h : P \to M$ making the following diagram commutative:

$$\begin{array}{ccccc} & & P & & \\ & \overset{h}{\swarrow} & \downarrow{\scriptstyle f} & & \\ M & \xrightarrow{g} & M'' & \longrightarrow & 0 \end{array} \tag{2.1}$$

(ii) Every exact sequence of R-modules $0 \to M' \to M \to P \to 0$ splits.

(iii) There exists a module M' such that $P \oplus M'$ is free (P is a direct summand of a free module).

Proof. $i) \implies ii)$: Given the exact sequence of $ii)$, take $M'' = P$ and $f = id$ in the diagram,

$$\begin{array}{ccccc} & & P & & \\ & \overset{h}{\swarrow} & \downarrow{\scriptstyle id} & & \\ M & \longrightarrow & P & \longrightarrow & 0 \end{array} \tag{2.2}$$

then h gives the desired splitting of the sequence.

$ii) \implies iii)$: As every module can be represented as a quotient of a free module, there is a surjective homomorphism $r : F \to P$ with F free, and applying $ii)$ to the short exact sequence $0 \to \mathrm{Ker}(r) \xrightarrow{i} F \xrightarrow{r} P \to 0$, we get $F \cong P \oplus M'$, where $M' = \mathrm{Ker}(r)$.

$iii) \implies i)$: First, assume P is free and B a basis of P. The restriction $f|_B$ can be lifted to a map $\gamma : B \to M$ (this means $f|_B = g \circ \gamma$), since $M \to M''$ is surjective (mapping the

elements of B to appropriate pre-images of g). Then, the linear extension $h : P \to M$ of γ fulfills the assertion.
Now let $P \oplus Q$ be free. Then f extends to a linear map $f' : P \oplus Q \to M''$, defined by $(p, q) \mapsto f(p)$. Let $h' : P \oplus Q \to M$ be a lift of f' (just as before, this is done with h' defined by linear extension over a basis of $P \oplus Q$). Then, with $h := h'|_P$, we get $g \circ h = f$. □

Definition 2.2. *A R-module with the equivalent properties of Proposition 2.1 is called* ***projective****.*

The reader could wonder why would someone define a module satisfying these equivalent properties, and we can explain now at least two important reasons that justify the notion of a projective module, both from Homological Algebra:

The first one is trying to find a more arrow-theoretical characterization of free modules; in almost every field of algebra the importance of free modules is unquestionable, but in this concrete branch one is particularly interested in how do certain objects interact with one another using morphisms between them. In this sense, a useful characterization of free modules is that they satisfy a diagram like the one in (2.1) (see implication $iii) \Rightarrow i)$), though it was soon realized that a module does not need to be free to do so- below we will provide some insightful examples in this direction.

The second one, more "technical" but very likely more important, comes from the functorial viewpoint: in Homological Algebra and Category Theory, functors are one of the most basic and ubiquitous objects, and probably the most frequent ones are the covariant and the contravariant Hom functors. The reader may know that in general neither kind is exact- they are only left-exact. Projective modules are precisely the kind of modules which make the covariant Hom functor exact, something very remarkable in this context, although we will not prove it nor use it in our main text (nevertheless, we will use it in Appendix B). That is, a fourth property in Proposition 2.1 could be:

(iv) The functor $\mathrm{Hom}_A(P, -)$ *is* ***exact****.*

All this being said, since their appearance 50 years ago, projective modules have also showed up frequently in other branches of mathematics as well, such as algebraic number theory, K-theory and algebraic geometry- in fact, in the section 3 of this chapter we will explore the geometrical context in which Serre raised his famous conjecture.

In practice, one must think of projective modules as modules closely related to free modules, as they are direct summands of them. However, there do exist projective modules which are not free. Here we present some illustrative examples of projective modules, the first two exploring the case just mentioned:

1. Suppose R_1 and R_2 are non-trivial rings. Then the product ring $R = R_1 \times R_2$ admits non-free projective R-modules. Indeed, take P the ideal $R_1 \times \{0\}$ and Q the ideal $\{0\} \times R_2$. Since $R = P \oplus Q$, P and Q are projective. On the other hand, P cannot be free, because taking $e := (0, 1) \in R$, we have $eP = 0$, whereas $eF \neq 0$ for any non-zero free R-module (for F free, $Ann_R(F) = 0$). Similarly, Q is not free either.

Based in this construction, we can give a more familiar example: $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are projective non-free $\mathbb{Z}/6\mathbb{Z}$-modules, since $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

2. If we can find in a domain R two comaximal non-principal ideals I and J (comaximal means $I + J = R$) with IJ principal, then I and J are finitely generated projective non-free R-modules (a non-principal ideal will never be free as an R-module).
   Indeed, first we recall that, for I and J comaximal, $IJ = I \cap J$ ($\subseteq$ trivial, $\supseteq$ follows from the fact that $(I + J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ + IJ = IJ$ and $(I + J) = R$).
   We have the natural short exact sequence

$$0 \to I \cap J \to I \oplus J \to R \to 0 \tag{2.3}$$

   and since R is free, it's also projective and the sequence (2.3) splits, thus giving the isomorphism $I \oplus J \cong IJ \oplus R$. Finally, a non-zero principal ideal in a domain is isomorphic as an R-module to R itself, so if IJ is principal, $I \oplus J \cong R^2$ and I and J are both direct summands of a free module.
   Again, based in this construction: we can take $R = \mathbb{Z}[\sqrt{-5}]$ and $I = (3, 1 + \sqrt{-5})$ and $J = (3, 1 - \sqrt{-5})$. It's not hard to show that both are non-principal (using the common argument with the multiplicative norm $a + b\sqrt{-5} \mapsto a^2 + 5b^2$), and they are comaximal, since $R/I \cong R/J \cong \mathbb{Z}/3\mathbb{Z}$ ($\mathbb{Z}/3\mathbb{Z}$ a field, so I and J are maximal), and $I \neq J$. From the fact that $IJ = (3)$, principal, we deduce that both I and J are projective non-free R-modules.

3. If P_1 and P_2 are projective R-modules, $P_1 \oplus P_2$ is also a projective module, for if $P_1 \oplus Q_1$ and $P_2 \oplus Q_2$ are free for some Q_1 and Q_2, we have the free module $(P_1 \oplus Q_1) \oplus (P_2 \oplus Q_2) \cong (P_1 \oplus P_2) \oplus (Q_1 \oplus Q_2)$. The converse is also true, almost trivially: if $(P_1 \oplus P_2) \oplus Q$ is free for some R-module Q, $P_1 \oplus (P_2 \oplus Q)$ fulfills the condition for P_1, and similarly for P_2.
   This argument can be generalized easily: $\bigoplus_{i \in I} P_i$ is projective iff each P_i is projective.

It is clear that, for any ring R, a free R-module is always projective, and that both notions are fairly close to each other- these previous examples show that it is not immediate to find non-free projective modules. Ever since their appearance, algebraists have explored for which rings R projective modules are *necessarily* free. This question is very hard to answer, in general. The Quillen-Suslin Theorem proves that, over $k[x_1, \ldots, x_n]$ (k being a field), this is indeed the case if the projective module is finitely generated.

2.2 Finitely generated projective modules

As the Theorem this memoir is about is concerned with finitely generated projective modules (over $k[x_1, \ldots, x_n]$), it is convenient to study now some of their properties. Actually, the main goal of this section is to study how do finitely generated projective modules behave under localization, and which is the relation between f.g. projective modules and locally free modules. A locally free module is defined in the obvious way having in mind the exposition of section 1.2:

Definition 2.3. *A R-module M is locally free if $M_\mathfrak{p}$ is $R_\mathfrak{p}$-free $\forall \mathfrak{p} \in Spec(R)$.*

We also recall from Definition 1.5 that $R_\mathfrak{p}$ is a local ring $\forall \mathfrak{p} \in Spec(R)$- that is, it only has one maximal ideal. Changing the notation a little bit temporarily, if a ring A is local we usually write $(A, \mathfrak{m})$, where $\mathfrak{m}$ denotes its maximal ideal. Note that $A/\mathfrak{m}$ is a field because $\mathfrak{m}$ is maximal. We call it the **residue field** of A. The first goal of this section is to prove that, in a local ring A, any finitely generated projective A-module is indeed free. To do so we will need the well-known Nakayama's Lemma and its consequences. But first:

Definition 2.4. *We say that a generating set of a module is **minimal** if no proper subset of it generates the module.*

The number of elements of a minimal generating set for an arbitrary R-module need not be unique, and it usually is not. However, if M is finitely generated, there obviously exist minimal generating sets with finite cardinal, and the infimum of these is uniquely determined by M. Before going with Nakayama's Lemma:

Remark 2.5. *In a local ring $(A, \mathfrak{m})$, $x \notin \mathfrak{m} \iff x$ is a unit. $\Leftarrow$ is trivial (otherwise $\mathfrak{m} = A$!), while $\Rightarrow$ can be deduced from the fact that every non-unit element of a ring is contained in some maximal ideal (using Zorn's Lemma), and if A is local, it must be $\mathfrak{m}$.*

Lemma 2.6. ***(Nakayama's Lemma):*** *Let M be a finitely generated A-module, $(A, \mathfrak{m})$ a local ring. Then $\mathfrak{m}M = M \implies M = 0$.*

Proof. Suppose $M \neq 0$ and $\{u_1, \dots, u_n\}$ a minimal generating set of M. As $\mathfrak{m}M = M$, we have $u_n \in \mathfrak{m}M$, and there is an equation $u_n = a_1u_1 + \cdots + a_nu_n$ with $a_i \in \mathfrak{m}$. Thus

$$(1 - a_n)u_n = a_1u_1 + \cdots + a_{n-1}u_{n-1}. \tag{2.4}$$

As $a_n \in \mathfrak{m}$, $(1 - a_n) \notin \mathfrak{m}$ and by Remark 2.5, it is a unit in A. Thus u_n belongs to $(u_1, \dots, u_{n-1})$, in contradiction with the minimality of the generating set. □

Corollary 2.7. *If M is a f.g. A-module and $N \subseteq M$ is such that $M = \mathfrak{m}M + N$, then $N = M$.*

Proof. M/N is finitely generated, and we have $\mathfrak{m}(M/N) = (\mathfrak{m}M + N)/N = M/N$. By Nakayama's Lemma, this implies $M/N = 0 \implies M = N$. □

Now, for any ring R and $I \subsetneq R$ an ideal, M/IM is naturally a R/I-module with multiplication defined as $\bar{a}\bar{m} = \overline{am}$. Clearly, for any generating set $\{m\}_{i\in I}$ of M as a R-module, $\{\overline{m}_i\}_{i\in I}$ is a generating set of M/IM as a R/I-module, so if M is a finitely generated R-module, M/IM is a finitely generated R/I-module. In the case where $(A, \mathfrak{m})$ is local and M finitely generated, $M/\mathfrak{m}M$ is an $A/\mathfrak{m}$-vector space with finite dimension.

Proposition 2.8. *Let $(A, \mathfrak{m})$ be a local ring, $k = A/\mathfrak{m}$ and M a finitely generated A-module. Then any minimal generating set $\{m_1, \dots, m_n\}$ of M forms a k-basis $\{\overline{m}_1, \dots, \overline{m}_n\}$ for $M/\mathfrak{m}M$. In particular, every minimal generating set has the same number of elements, $\mu(M) = \dim_k M/\mathfrak{m}M$.*

Proof. We just have to prove that if $\{m_1, \dots, m_n\}$ is a minimal generating set of M, then $\{\overline{m}_1, \dots, \overline{m}_n\}$ are linearly independent in k (they are naturally a generating set). If they were not, we could take wlog $\{\overline{m}_2, \dots, \overline{m}_n\}$ as a generating set for $M/\mathfrak{m}M$. But then $M = \sum_{i=2}^n Am_i + \mathfrak{m}M$, and by Corollary 2.7 we would have $M = \sum_{i=2}^n Am_i$, in contradiction with the minimality of the initial generating set! Thus they are linearly independent. The

second part follows from the fact that two minimal finite generating sets with different cardinality would form two k-basis with a different number of elements, which is clearly impossible, since the number of elements of a basis of a finite vector space is unique. □

With this we arrive finally to our desired result:

Proposition 2.9. *Supose $A = (A, \mathfrak{m})$ is a local ring and M is a finitely generated projective A-module. Then M is free.*

Proof. By Proposition 2.8, if we take $\{m_1, \dots, m_n\}$ a minimal generating set of M, their projection in $M/\mathfrak{m}M$ forms a basis for $M/\mathfrak{m}M$ as a k-module. Define now $\varphi : A^n \to M$ by sending the ith basis vector to m_i; as it is surjective and M is projective, we have an isomorphism $A^n \xrightarrow{\cong} M \oplus \mathrm{Ker}(\varphi)$, with $\mathrm{Ker}(\varphi)$ finitely generated, as there exists an split epimorphism $\phi : A^n \hookrightarrow \mathrm{Ker}(\varphi)$. Reducing $\mod \mathfrak{m}$, we get $k^n \xrightarrow{\cong} (M/\mathfrak{m}M) \oplus (\mathrm{Ker}(\phi)/\mathfrak{m}\,\mathrm{Ker}(\phi))$, but we know that the map is an isomorphism on the first factor, as it matches up the basis vectors. Thus, the second factor must be trivial, so $\mathrm{Ker}(\varphi) = \mathfrak{m}\,\mathrm{Ker}(\varphi)$. But, as $\mathrm{Ker}(\varphi)$ is a finitely generated A-module, Nakayama's Lemma implies that $\mathrm{Ker}(\phi) = 0$, and hence the original φ is an isomorphism and M is free. □

Actually, I. Kaplansky proved that the finite generation of M is not required, and the result holds for arbitrary projective modules over A. Thus, local rings are also one of the kind of rings for which projective modules are necessarily free. From this we will deduce easily the other important result of this section, Proposition 2.12, although we will have to prove a simple lemma before, Lemma 2.11.

In section 1.2 there is the explanation on how, given a multiplicatively closed set $S \subsetneq R$, one can form $S^{-1}M$, a $S^{-1}R$-module in a natural way. Going further, it is easy to prove that localization at S can be thought of as a *functor* $S^{-1} : Mod_R \to Mod_{S^{-1}R}$ by sending a R-morphism $f : M \to N$ to the naturally defined $S^{-1}R$-morphism

$$\begin{aligned} S^{-1}f : S^{-1}M &\to S^{-1}N \\ \frac{m}{1} &\mapsto \frac{f(m)}{1} \end{aligned} \tag{2.5}$$

In fact, it is an **exact functor**, in the sense of Proposition 2.10. The reader unfamiliar with the language of functors may just "believe" this result. As it is presented in the course "Introduction to Commutative Algebra" of our bachelor's degree and it is straightforward to demonstrate, we shall just state it without proof:

Proposition 2.10. *Applying the functor S^{-1} to an exact sequence of R-modules*

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0 \tag{2.6}$$

yields an exact sequence

$$0 \to S^1M_1 \xrightarrow{S^1f} S^1M_2 \xrightarrow{S^1g} S^1M_3 \to 0 \tag{2.7}$$

Lemma 2.11. *Localization preserves finite direct sums- that is, given a finite family of R-modules $\{M_1, \dots M_n\}$, one has $S^{-1}(\bigoplus_{i=1}^n M_i) \cong \bigoplus_{i=1}^n S^{-1}M_i$ as $S^{-1}R$-modules.*

Proof. As S^{-1} is an exact functor, from Proposition 2.10, for any two R-modules M and N one has two natural exact sequences of $S^{-1}R$-modules

$$\begin{aligned} 0 \to S^{-1}M \to S^{-1}(M \oplus N) \to S^{-1}N \to 0 \\ 0 \to S^{-1}M \to S^{-1}M \oplus S^{-1}N \to S^{-1}N \to 0. \end{aligned} \tag{2.8}$$

One can now apply the Five Lemma (Lemma A.16) in the obvious way between both to see that $S^{-1}(M \oplus N) \cong S^{-1}M \oplus S^{-1}N$. For an arbitrary finite direct sum the result follows by induction. □

This lemma has as simple corollaries that the localization of a f.g. free R-module, $\bigoplus_{i=1}^{n} R$, is always a f.g. free $S^{-1}R$-module, and the same applies to f.g. projective R-modules. This will look clearer in the proof of our desired result:

Proposition 2.12. *If P is a finitely generated projective R-module, then P is locally free.*

Proof. As P is finitely generated, there exists a R-module Q such that $R^n \cong P \oplus Q$ for some $n \in \mathbb{N}$. Now localizing at any $\mathfrak{p} \in Spec(R)$, $S = R \backslash \mathfrak{p}$, by Lemma 2.11 one has $(S^{-1}R)^n \cong S^{-1}(R^n) \cong S^{-1}(P \oplus Q) \cong S^{-1}P \oplus S^{-1}Q$- that is, $(R_\mathfrak{p})^n \cong P_\mathfrak{p} \oplus Q_\mathfrak{p}$. Thus, $P_\mathfrak{p}$ is a direct summand of a free $R_\mathfrak{p}$-module, so it is a projective $R_\mathfrak{p}$-module. As it is obviously finitely generated and $R_\mathfrak{p}$ is a local ring, by Proposition 2.9 $P_\mathfrak{p}$ is free $\forall \mathfrak{p} \in Spec(R)$, and thus P is locally free. □

It is clear that, since P is finitely generated, $P_\mathfrak{p}$ is finitely generated as a $R_\mathfrak{p}$-module $\forall \mathfrak{p} \in Spec(R)$, so one could easily write "*finite* locally free" in the proposition above. For any $\mathfrak{p} \in Spec(R)$, one defines the **rank** of projective R-module P at $\mathfrak{p}$ as $rk_\mathfrak{p}(P) := rank_{R_\mathfrak{p}} P_\mathfrak{p}$. It is a natural question to ask how does the function $rk(P) : Spec(R) \to \mathbb{Z}$ vary with $\mathfrak{p} \in Spec(R)$. The complete but "hard" answer to this question is that it is continuous with respect to the Zarisky topology on $Spec(R)$. For those unfamiliar with this terminology, an "easy" and sufficient answer to it in our case (and a direct consequence of its "hard" counterpart, as in this case $Spec(R)$ is connected) could be Proposition 2.13, when R is a (commutative) integral domain, the usual case in algebraic geometry:

Proposition 2.13. *If R is an integral domain, then any f.g. projective R-module has constant rank.*

Now, the remarkable fact about Proposition 2.12 is that, by imposing this condition on $rk_\mathfrak{p} P$ (that is, $rk_\mathfrak{p} P$ is continuous with respect to the Zarisky topology/ constant if R integral domain), **the converse implication also holds**. So, in an integral domain, one has

Proposition 2.14. *If P is a finitely generated module being finite locally free with $rk_\mathfrak{p} P$ constant over $Spec(R)$, then P is a finitely generated projective R-module.*

Proposition 2.14 is significantly harder to prove than its reciprocal, and doing so requires more advanced techniques, so one may just assume its validity and continue to section 3. Nevertheless, the interested reader will find a detailed demonstration of it in Appendix B, though many well-known but quite technical results of commutative algebra will be taken for granted in it.

Thus, together with the previous four discussed in section 1, Propositions 2.12 and 2.14 give yet a fifth characterization of projective modules in the case in which they are finitely generated (and R is commutative and an integral domain). In fact, this property is the one which really gives finitely generated projective modules their geometric value, as we shall see in the following.

2.3 Geometric motivation of the Serre's problem

A curious fact about the Quillen-Suslin Theorem is that it can be treated (and solved) without any reference to algebraic geometry nor having a strong knowledge of it, despite it solving a problem which was originally formulated in a geometric context- in fact, the content of this section will not appear for the rest of the text. Nevertheless, our treatment of the Theorem would not be complete without comprehending what geometric intuition led Serre to formulate the question in the first place. The purpose of this section is to sketch this geometric origin, following the original paper of Serre.
Although we will keep the exposition simple and without proofs, it will take us some pages of definitions to finally arrive to the geometric meaning of our problem. Some prior knowledge of standard algebraic geometry will be inevitably assumed, and the first pages will be devoted to providing an introduction to sheaf theory.

In retrospective, *Faisceaux algébriques cohérents* ("Coherent algebraic sheaves") might be the most influential paper in 20th century abstract algebraic geometry. In it, Serre not only introduced sheaves into this field, but developed systematically and in great detail many of the sheaf-theoretic methods that are still in use today, most importantly sheaf cohomology, which has been proven to be an incredibly powerful tool. His far-reaching approach led to a reformulation of the entire subject during the 1950s and 1960s, mostly headed by A. Grothendieck. Nowadays, FAC is still a reference article by many geometers and sheaves are ubiquitous in modern algebraic geometry- in fact, they are necessary even to define the notion of *scheme*, its main object of study.

Despite the importance of the article, the aim of this section is more modest, and we will only treat the notions necessary to understand our problem, which are actually a lot. Unsurprisingly, it is inevitable to define what is a *sheaf* and, before, a *presheaf*:

Definition 2.15. *Let X be a topological space. A **presheaf** $\mathfrak{F}$ of abelian groups on X consists of the data*

a) for every open set $U \subseteq X$, an abelian group $F(U)$.

b) for every inclusion $V \subseteq U$ of open sets, a morphism of abelian groups $\rho_{UV} : \mathfrak{F}(U) \to \mathfrak{F}(V)$

subject to the conditions

(0) $\mathfrak{F}(\emptyset) = 0$, where $\emptyset$ is the empty set,

(1) $\rho_{UU} : \mathfrak{F}(U) \to \mathfrak{F}(U)$ is the identity map, and

(2) if $W \subseteq V \subseteq U$ are three open sets, then $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$.

We define a presheaf of rings replacing the word "abelian group" in the definition by "ring". These will be important later. Also, as a matter of terminology, if $\mathfrak{F}$ is a presheaf on X, we also refer to $\mathfrak{F}(U)$ as the *sections* of the presheaf $\mathfrak{F}$ over the open set U. We also call the maps ρ_{UV} *restriction* maps, and sometimes write $s|_V$ instead of $\rho_{UV}(s)$, if $s \in \mathfrak{F}(U)$.
A sheaf is, roughly speaking, a presheaf whose sections are determined by local data:

Definition 2.16. *A presheaf $\mathfrak{F}$ on a topological space X is a **sheaf** if it satisfies the following supplementary conditions:*

(3) if U is an open set, $\{V_i\}$ is an open covering of U and $s \in \mathfrak{F}(U)$ is an element such that $s|_{V_i} = 0$ for all i, then $s = 0$;

(4) if U is an open set, $\{V_i\}$ is an open covering of U, and we have elements $s_i \in F(V_i)$ for each i with the property that, for each i, j, $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$, then there is an element $s \in \mathfrak{F}(U)$ such that $s|_{V_i} = s_i$ for each i (and (3) implies s is unique).

Example 2.17. *Let G be an abelian group and denote by $\mathfrak{F}_U$ the set of functions on U with values in G; for $U \subseteq V$, define $\phi_{VU} : \mathfrak{F}_V \to \mathfrak{F}_U$ the restriction of such functions. We thus obtain a system $(\mathfrak{F}_U, \phi_{VU})$ and hence a sheaf $\mathfrak{F}(X)$, **the sheaf of germs of functions** with values in G.*

Now, sheaves are defined on open sets, but it is convenient to attempt to isolate the behaviour of a sheaf at a single fixed point of X. If $\mathfrak{F}$ is a presheaf on X and $P \in X$, we define the **stalk** $\mathfrak{F}_P$ of $\mathfrak{F}$ at P to be the *direct limit* of the groups $\mathfrak{F}(U)$ for all open sets U containing P, via the restriction maps ρ. That is,

Definition 2.18.

$$\mathfrak{F}_P = \varinjlim_{U_i \ni P} \mathfrak{F}(U_i) = \bigsqcup_{U_i \ni P} \mathfrak{F}(U_i) / \sim \tag{2.9}$$

where, for $x_i \in \mathfrak{F}(U_i)$ and $x_j \in \mathfrak{F}(U_j)$, $x_i \sim x_j$ iff there is some $\mathfrak{F}(U_k)$ with $\mathfrak{F}(U_k) \subseteq \mathfrak{F}(U_i)$, $\mathfrak{F}(U_k) \subseteq \mathfrak{F}(U_j)$ such that $\rho_{U_i U_k}(x_i) = \rho_{U_j U_k}(x_j)$. (Intuitively, two elements of the disjoint union are equivalent iff they "eventually become equal" by further restriction).

Thus, any element of $\mathfrak{F}_P$ is represented by a pair (U, s), where U is an open neighbourhood of P and $s \in \mathfrak{F}_P$, and such that any two pairs (U, s) and (V, s) define the same element in $\mathfrak{F}_P$ iff there is an open neighbourhood W of P with $W \subseteq U \cap V$ with $s|_W = t|_W$. (One can carry out all the basic definitions about sheaves by using stalks instead of open sets and, in fact, Serre originally did it that way).

We arrive now to the important notion of a *sheaf of $\mathfrak{A}$-modules*, which actually includes the other two kinds of sheaves exposed so far:

Definition 2.19. *Given a sheaf of rings $\mathfrak{A}$ on X, $\mathfrak{F}$ is a sheaf of $\mathfrak{A}$-modules on X if*

(1) for each open set $U \subseteq X$, the group $\mathfrak{F}(U)$ is an $\mathfrak{A}(U)$-module, and

(2) for each inclusion of open sets $V \subseteq U$, the restriction homomorphism $\mathfrak{F}(U) \to \mathfrak{F}(V)$ is compatible with the module structures via the ring homomorphism $\mathfrak{A}(U) \to \mathfrak{A}(V)$.

One may obtain many different kinds of sheaves of $\mathfrak{A}$-modules using various constructions: subsheaves, quotient sheaves, direct sum of sheaves, tensor product of sheaves... These constructions can be enlarged when one allows *morphisms* between them come into play, which can be defined quite naturally and are very useful in practice:

Definition 2.20. *Let $\mathfrak{A}$ be a sheaf of rings and $\mathfrak{F}$ and $\mathfrak{G}$ two sheaves of $\mathfrak{A}$-modules. Then $\phi : \mathfrak{F} \to \mathfrak{G}$ is an $\mathfrak{A}$-homomorphism if for each open set $U \subseteq X$, $\phi_U : \mathfrak{F}(U) \to \mathfrak{G}(U)$ is a homomorphism of $\mathfrak{A}(U)$-modules and, whenever $V \subseteq U$ is an inclusion, we get the following commutative diagram:*

$$\begin{array}{ccc} \mathfrak{F}(U) & \xrightarrow{\phi_U} & \mathfrak{G}(U) \\ \downarrow{\scriptstyle \rho_{UV}} & & \downarrow{\scriptstyle \rho_{UV}} \\ \mathfrak{F}(V) & \xrightarrow{\phi_V} & \mathfrak{G}(V) \end{array} \tag{2.10}$$

It is easy to see that the kernel and the cokernel of a morphism are again sheaves. Finally,

Definition 2.21. *A sheaf of $\mathfrak{A}$-modules $\mathfrak{F}$ is said to be **coherent** if*

(a) $\mathfrak{F}$ is of finite type- that is, it is locally generated by a finite number of its sections, so for each $U \subseteq X$, there is an epimorphism $\mathfrak{A}(U)^p \twoheadrightarrow \mathfrak{F}(U)$, and

(b) for any $s_1, \ldots, s_p \in \mathfrak{F}(U)$, the sheaf of relations between the s_i ($\mathrm{Ker}(\phi : A(U)^p \to \mathfrak{F}(U))$ with $\phi(e_i) = s_i \, \forall i$) is of finite type.

It is easy to see that every coherent sheaf of $\mathfrak{A}$-modules $\mathfrak{F}$ is locally isomorphic to the cokernel of a homomorphism $\mathfrak{A}^q \to \mathfrak{A}^p$.

All this being said, now it is time to connect a little all these terms to algebraic geometry. From now on, k will denote any commutative algebraically closed field.
Let $X = \mathbb{A}_k^r$ be the *affine space* of dimension r over the field k. We equip X with the *Zarisky topology*, so a subset of X is closed iff it is the zero set of a family of polynomials in $k[x_1, \ldots, x_r]$. For an open set U of X, we denote by $\mathcal{O}_U = \{\frac{p}{q}, p, q \in k[x_1, \ldots, x_r] | \, q(x) \neq 0 \, \forall x \in U\}$. Any fraction like this is said to be *regular* in U, and for all points $x \in X$ for which $q(x) \neq 0$, $x \mapsto \frac{p(x)}{q(x)}$ defines a continuous function with values in k (k being given the Zarisky topology). It can be easily proven that the $\{\mathcal{O}_U\}_{U \subseteq X}$ form a subsheaf $\mathcal{O}$ of the sheaf $\mathfrak{F}(X)$ of germs of functions on X with values in k (Example 2.17), particularly a sheaf of rings. Note that the stalk of $\mathcal{O}$ at x for any $x \in X$, $\mathcal{O}_x$, is the *local ring* of x in X. This is why the sheaf $\mathcal{O}$ is called the *sheaf of local rings*.
This can be generalized to any locally closed subspace Y of X ($Y = U \cap F$, with U (resp. F) an open (resp. closed) subspace of X) by taking the sheaf of germs of functions on Y with values in k and restricting $\mathfrak{F}(X)_x \to \mathfrak{F}(Y)_x$ for each $x \in Y$. In this case, the ring $\mathcal{O}_{x,Y}$ is isomorphic to the localization of $k[x_1, \ldots, x_n]/I(F)$ in the maximal ideal defined by the point x. In this way, one can associate this sheaf to any "classical" algebraic variety, both affine and projective.
In fact, having this in mind, Serre "redefined" and enlarged the concept of algebraic variety, taking a definition which is quite close to that of a scheme, in retrospective:

Definition 2.22. *An algebraic variety over k is a set X equipped with*

(1) a topology (the Zarisky topology), and

(2) a subsheaf $\mathcal{O}_X$ of the sheaf $\mathfrak{F}(X)$ of germs of functions on X with values in k (the sheaf of local rings),

this data being subject to axioms:

(a) There exists a finite open covering $\{V_i\}_{i\in I}$ of the space X such that each V_i, equipped with the structure induced from X, is isomorphic to a locally closed subspace U_i of an affine space, equipped with the sheaf $\mathcal{O}_{U_i}$ defined before- that is, there is an homeomorphism of V_i to U_i which transforms $\mathcal{O}_{V_i}$ to $\mathcal{O}_{U_i}$ (also called a "chart").

(b) The diagonal $\Delta = \{(x,x)|\, x \in X\}$ of $X \times X$ is closed in $X \times X$ (the topology in $X \times X$ being the product topology and having in mind (a)).

With this notion of algebraic variety, one can prove that, for any algebraic variety V, the sheaf $\mathcal{O}_V$ is a coherent sheaf of rings on V. Then, an **algebraic sheaf** on V is any sheaf of $\mathcal{O}_V$-modules, and it is said to be **coherent** if it satisfies Definition 2.21. Also, V is said to be *affine* if it is directly isomorphic to a closed subvariety of an affine space. For two algebraic varieties X and Y, $\phi : X \to Y$ is said to be a morphism between them if ϕ is continuous and if for any $x \in X$ and $f \in \mathcal{O}_{\phi(x),Y}$, then $f \circ \phi \in \mathcal{O}_{x,X}$.

After all this way, our last two steps to understand the geometric intuition behind Serre's problem are the notions of *algebraic vector bundle* and *sheaf associated to a module M*:

- An **algebraic vector bundle** over k of rank r with base (a variety) V is an algebraic variety E together with a surjective morphism of algebraic varieties $p : E \to V$ such that, for each point $x \in V$, $p^{-1}(x) \cong k^r$ and which is locally trivial in the sense that, for each point $x \in V$, there exists an open neighbourhood U of x such that $p^{-1}(U) = E|_U \cong U \times k^r$, and such that the two isomorphisms over an intersection $U_i \cap U_j$ differ by a linear automorphism (of vector spaces).
One must think of algebraic vector bundles as "vector spaces parametrized by an algebraic variety". The reader may be more familiar with topological vector bundles; the ones just defined are their analogous but in the context of algebraic geometry, so we require the fiber space to be an algebraic variety and the morphism between it and the base V to be a morphism of algebraic varieties. Also, we say that E is a **trivial bundle** if it is isomorphic to the product $E \times k^r$.
Now, if U is an open subset of V, one can consider $\mathfrak{J}(E)_U$ the *set of regular sections of E on U*, and for $U \subseteq W$, we have the restriction homomorphism $\rho_{WU} : \mathfrak{J}(E)_W \to \mathfrak{J}(E)_U$. These form a sheaf $\mathfrak{J}(E)$, called the **sheaf of germs of sections** of E, and since E is a vector bundle, each $\mathfrak{J}(E)_U$ is a $\Gamma(U, \mathcal{O}_V)$-module and $\mathfrak{J}(E)$ is an algebraic sheaf on E which is *locally isomorphic to* $\mathcal{O}_V^r$ (and in particular, coherent). Conversely, it is easily seen that any algebraic sheaf $\mathfrak{F}$ on V which is locally isomorphic to $\mathcal{O}_V^r$ is isomorphic to a sheaf $\mathfrak{J}(E)$, where E is determined up to isomorphism.

- If we take V an affine variety and $\mathcal{O}$ the sheaf of local rings of V, the ring $\mathfrak{F}(V) = \Gamma(V, \mathcal{O})$, also called *the ring of coordinates* of V, is an algebra over k with no non-zero nilpotent elements (if V is embedded as a closed subvariety of k^r, A is identified with the quotient algebra of $k[x_1, \ldots, x_n]$ by the ideal of polynomials vanishing on V, and is a f.g. k-algebra). Conversely, if A is a commutative k-algebra with no non-zero nilpotent elements which is f.g., there exists a (unique) variety V such that A is isomorphic to $\Gamma(V, \mathcal{O})$.
Now let M be an A-module. M defines a constant sheaf on V, which we denote again

by M; the same way, A defines a constant sheaf, and the sheaf M can be considered as a sheaf of A-modules. Define $\mathfrak{A}(M) = \mathcal{O} \otimes_A M$, the sheaf $\mathcal{O}$ also being considered as a sheaf of A-modules; then it is clear that $\mathfrak{A}(M)$ is a sheaf of $\mathcal{O}$-modules (by "extension of scalars") and thus an algebraic sheaf on V, and if M is f.g., it is coherent. We call it **the sheaf associated to** M. Note that the stalk of $\mathfrak{A}(M)$ at any point $x \in X$ is isomorphic to $\mathcal{O}_x \otimes_A M \cong M_x$ (localized at x).

Now, by what we proved in the previous section, if we take M to be a finitely generated A-module, *M is projective if and only if the $\mathcal{O}_x$-module $\mathcal{O}_x \otimes_A M$ is free for every $x \in V$.*
Note that if $\mathfrak{F}$ is a coherent algebraic sheaf on V and if $\mathfrak{F}_x$ is isomorphic to $\mathcal{O}_x^p$, $\mathfrak{F}$ is isomorphic to $\mathcal{O}^p$ in a neighbourhood of x; if this property is satisfied in every $x \in V$, the sheaf $\mathfrak{F}$ is thus locally isomorphic to the sheaf $\mathcal{O}^p$, the integer p being constant on every connected component of V. Hence,

Proposition 2.23. *For $\mathfrak{F}$ a coherent algebraic sheaf on a connected affine variety V, the following two properties are equivalent:*

(1) $\mathfrak{F}(V)$ is a projective A-module.

(2) $\mathfrak{F}(V)$ is isomorphic to the sheaf of germs of sections of a vector bundle with base V

In other words, the mapping $E \mapsto \mathfrak{J}(E)$ gives a bijective correspondence between classes of algebraic vector bundles over V and classes of finitely generated projective A-modules, and in this correspondence, a *trivial bundle* corresponds to a *free* modules and conversely.

Finally, going back to our problem, we want to consider the total affine space, that is, $X = \mathbb{A}_k^r$ and $\mathcal{O}$ the natural sheaf of local rings, so $\Gamma(X, \mathcal{O}) = k[x_1, \ldots, x_r]$. By what we have said so far, there is a bijective correspondence between finitely generated projective $k[x_1, \ldots, x_r]$-modules and algebraic vector bundles over $\mathbb{A}_k^r$ of finite rank. Thus, Serre's problem can be restated in geometric terms as

Is every algebraic vector bundle over the affine space $\mathbb{A}_k^r$ a trivial bundle? (for all $r \in \mathbb{N}$).

It is a standard result in topology that, if X is a contractible space, every topological vector bundle over it is trivial, so any **topological** vector bundle over $\mathbb{A}_k^r$, with k being the more familiar $\mathbb{R}$ or $\mathbb{C}$, is always trivial. Thus, the motivation of Serre's question was to know whether this was still true in the geometric setting (that is, for **algebraic** vector bundles) and for any field k, with the "moral impulse" that $\mathbb{A}_k^r$ should still behave like a "contractible" space. When Quillen and Suslin proved that finitely generated projective modules over $k[x_1, \ldots, x_n]$ are necessarily free, it was proved that this is indeed the case.

Chapter 3

Stably free modules

We have seen that, in one of its many equivalent criteria, an R-module P is projective iff there is a R-module Q such that $P \oplus Q$ is free. It has been shown that this does not necessarily imply that P itself is free. Remarkably, even if Q is finitely generated and free and $P \oplus Q$ is free, P need not be free. This motivates the concept of a stably free module, a more restrictive kind of projective module with useful and interesting properties which will be key in our demonstration of the Quillen-Suslin Theorem, once we prove, in Chapter 4, that any finitely generated projective module over $k[x_1, \ldots, x_n]$ *is* stably free.

3.1 Definition and characterization

Definition 3.1. *An R-module P is said to be **stably free of type** m ($0 \leq m < \infty$) if $P \oplus R^m$ is free. A module is said to be **stably free** if it is stably free of type m for some m. (Such a module P is, of course, projective, and if $m = 0$, P is free.)*

Remark 3.2. *This terminology is a little bit informal, since the type of P is not a uniquely determined integer (if P has type m, then it also has type $m + k$ for any $k \geq 0$). If we want to associate a uniquely defined non-negative integer to P, we can define its "minimal type" to be the smallest integer $m \geq 0$ such that $P \oplus R^m$ is free.*

Thus, every free module is stably free (of type 0). As we anticipated in the introduction of this chapter, there do exist stably free modules which are not free. We will give an example of one in the next section, once we have introduced the concept of *unimodular row*, which will make the example look less artificial.

Also, there is a good reason why we want to restrict the m above to be a *finite* cardinal number. In fact, if we don't impose such a restriction, *any* projective module P would satisfy the definition. The proof of this is a famous trick of S. Eilenberg:

Proof. Let $P \oplus Q \cong E$ with E free, and let $F = E \oplus E \oplus E \dots$ (also free). Then:

$$\begin{aligned} P \oplus F &\cong P \oplus E \oplus E \dots \\ &\cong P \oplus (Q \oplus P) \oplus (Q \oplus P) \dots \\ &\cong (P \oplus Q) \oplus (P \oplus Q) \dots \\ &\cong E \oplus E \dots \\ &\cong F! \end{aligned} \tag{3.1}$$

□

Another relevant observation is that a stably free module P is of interest mainly in the case when it is finitely generated. That's due to another beautiful trick found by M. Gabel, which shows that:

Proposition 3.3. *If P is stably free but not finitely generated, then P is actually free.*

Proof. Say $P \oplus R^m \cong F$, where F is free with basis $e_i, i \in I$. Since P is not finitely generated, I must be an infinite set (otherwise, it would be finitely presented $\iff$ finitely generated). P can then be viewed as $\mathrm{Ker}(f : F \twoheadrightarrow R^m)$ for some epimorphism f. As R^m is finitely generated, for a sufficiently large finite subset $I_0 \subset I$, we have $F_0 = \sum_{e_i \in I_0} e_i \cdot R \xrightarrow{f} R^m$ already onto. Thus, $F = P + F_0$. Writing $Q = P \cap F_0$, we have two short exact sequences:

$$\begin{aligned} 0 \to Q \to P \to P/Q \to 0 \\ 0 \to Q \to F_0 \to R^m \to 0 \end{aligned} \tag{3.2}$$

the first one trivially and the second one from the fact that $\mathrm{Ker}(f|_{F_0}) = P \cap F_0$. Now, by the Second Isomorphism Theorem (for two modules S and T, $(S+T)/T \cong S/(S \cap T)$), we get $P/Q = P/(P \cap F_0) \cong (P + F_0)/F_0 = F/F_0 \cong \sum_{i \in I \setminus I_0} e_i \cdot R$. Since $I \setminus I_0$ is infinite, we can write $P/Q \cong R^m \oplus F_1$ for some free module F_1. Now, as in both of the sequences of (3.2) the module on the right is free (thus projective), both split, so

$$P \cong Q \oplus (P/Q) \cong Q \oplus (R^m \oplus F_1) \cong (Q \oplus R^m) \oplus F_1 \cong F_0 \oplus F_1 = \text{free},$$

as we wanted to prove.

□

In view of this, we shall henceforth restrict more justifiably our attention to finitely generated stably free modules, the ones we are really interested in.

In this case, the definition of a stably free module P (of type m) is equivalent to the existence of a short exact sequence

$$0 \to R^m \xrightarrow{g} R^n \to P \to 0 \tag{3.3}$$

for some suitable $m, n \in \mathbb{N}$.
As the sequence splits, we get that P is stably free of type m iff $P \cong \mathrm{Ker}(f : R^n \twoheadrightarrow R^m)$ for a suitable (split) epimorphism f. Now, note that if M is the matrix associated with

f (recall Remark A.14), then M is right invertible, i.e. there exists an $n \times m$ matrix N such that $MN = I_m$ (N would be the matrix associated to the homomorphism g, so that $f \circ g = id_{R^m}$). Conversely, any right invertible $m \times n$ matrix M *defines* a f.g. stably free R-module P of type m, namely

$$P = \{\alpha = (a_1 \dots a_n)^T | M \cdot \alpha = 0\} \qquad \text{(The also called 'solution space' of } M\text{)} \tag{3.4}$$

The following criterion for the freeness of $P = \mathrm{Ker}(R^n \xrightarrow{f} R^m)$ will be extremely important to restate the problem in other (and more useful) terms:

Proposition 3.4. *$P = \mathrm{Ker}(R^n \xrightarrow{f} R^m)$ is free if and only if f can be lifted to an isomorphism $f' : R^n \to R^m \oplus R^r$ for some r, such that $\pi_1 \circ f' = f$, where π_1 is the projection onto the first factor (so the following diagram commutes):*

$$\begin{array}{ccc} & & R^m \oplus R^r \\ & \overset{f'}{\nearrow} & \big\downarrow \pi_1 \\ R^n & \xrightarrow{f} & R^m \end{array} \tag{3.5}$$

Proof. Suppose P is free, so there exists $g : P \xrightarrow{\cong} R^r$. Then one may write $R^n = Q \oplus P$ in such a way that the restriction of f to Q gives an isomorphism $f_0 : Q \to R^m$. Then $f_0 \oplus g : R^n \to R^m \oplus R^r$ clearly gives the desired isomorphism.

Conversely, if an isomorphism f' with $\pi_1 \circ f' = f$ exists, then $P = \mathrm{Ker}(f) \cong \mathrm{Ker}(\pi_1) = R^r$, so it is free. □

In the situation of (3.5), we are interested in having $R^n \cong R^m \oplus R^r \implies n = m + r$. It could strike the inexperienced algebraist that this is not always the case- indeed, there do exist some rings A for which $A^m \cong A^n \not\Longrightarrow m = n$. When a ring satisfies it we say that it has the *invariant basis number (IBN)* property. Fortunately, every commutative, unitary, non-trivial ring R (our case) has the IBN property, as the proposition below shows:

Proposition 3.5. *If R is a commutative ring with identity $1 \neq 0$, then R has the IBN property.*

Proof. Assume there exists an R-module isomorphism $f : A^m \to A^n$. Let $e_1, \dots, e_m$ be the canonical basis of A^m. By Krull's Theorem (every non-trivial commutative ring R contains at least one maximal proper ideal, using the Zorn's Lemma), we can take a a maximal ideal $I \subsetneq A$. Then, as f is an A-morphism, if $(i_1, \dots, i_m) \in I^m$, $f(i_1, \dots, i_m) = \sum_{k=0}^{m} i_k f(e_k) \in I^n$, as each $i_k \in I$. Thus, f induces an A/I-module morphism $f' : (\frac{A}{I})^m \to (\frac{A}{I})^n$, which is actually an isomorphism. Since I is maximal, A/I is a field and f' is an isomorphism between finite-dimensional vector spaces, which can only occur for $n = m$. □

This being proved, we can now give an insightful matrix theoretic interpretation of the previous Proposition 3.4: Let M denote the $m \times n$ matrix corresponding to f, and N the $(m + r) \times n = n \times n$ matrix corresponding to f' (if such a f' exists). The condition $\pi_1 \circ f' = f$ says that M is a *submatrix* of N, particularly its first m rows. The condition of f' being an isomorphism says that N is an invertible matrix; that is, there exists another

matrix N' of size $n \times n$ such that $NN' = I_{m+r}$ and $N'N = I_n$.We denote the set of all $n \times n$ invertible matrices with coefficients in R by $GL_n(R)$. We state the very same Proposition 3.4 in this new matrix theoretic context:

Proposition 3.6. *For any right invertible $m \times n$ matrix M with coefficients in R, $m < n$, the (stably free) solution space of M is free if and only if M can be extended to an invertible $n \times n$ matrix by adding a suitable number of new rows.*

Remark 3.7. *As in a commutative ring R we can compute the determinant and the **adjugate** of a matrix without problem, with the general formula $M^{-1} = \frac{1}{\det(M)} adj(M)$, we have that*

$$M \in GL_n(R) \iff \det(M) \in R^* \text{ (here } R^* \text{ denotes the set of invertible elements of } R) \quad (3.6)$$

3.2 Unimodular rows

Pursuing further this "matrix completion" perspective, we introduce the concept of "unimodular row", very important from now on:

Definition 3.8. *We say that $(v_1, \ldots, v_n) \in R^n$ is a **unimodular row** if $\sum_{i=1}^{n} v_i R = R$. The set of all unimodular rows of length m with entries in R is denoted by $Um_n(R)$.*

Remark 3.9. *A row $(v_1, \ldots, v_n) \in Um_n(R)$ iff there are $w_i \in R$ such that $\sum v_i wi = 1$. Therefore, if $w = (w_1, \ldots, w_n)$, then $vw^T = 1$.*

Remark 3.10. *A row, considered as a $(1 \times n)$-matrix, describes a surjective linear map of modules $R^n \to R$ (via left-multiplication) $\iff$ the row is unimodular.*

This proposition below will give us our new key criterion for a f.g. stably free module to be free:

Proposition 3.11. *For any ring R, the following statements are equivalent:*

(i) Any finitely generated stably free R-module is free

(ii) Any finitely generated stably free R-module of type 1 is free

(iii) Any unimodular row over R can be extended to an invertible matrix by adding a suitable number of new rows.

Proof. $ii) \iff iii)$: Follows from Proposition 3.6, when we gave a freeness criterion in matrix-completion terms.

$i) \implies ii)$: Is obvious.

$ii) \implies i)$: We prove the result by induction on m, where $P \oplus R^m$ is free. For $m = 1$ it follows by hypothesis from $ii)$. Now assume the result for $m - 1$, and let P be a finitely generated stably free R-module of type m. Then $P \oplus R^m \cong R^n$, so $(P \oplus R^{m-1}) \oplus R \cong R^n$, and this implies $P \oplus R^{m-1}$ is stably free of type 1. By $ii)$, it is free. Thus $P \oplus R^{m-1} \cong R^k$ for some k. By induction, P is free. □

Remark 3.12. *In light of this proposition, if we want to see that a f.g. stably free R-module is free, it is enough to prove that any unimodular row over R can be extended to an invertible matrix by adding a suitable number of new rows. We will apply this to $k[x_1, \ldots, x_n]$ in the future.*
Alternatively, we may see that the f.g. stably free R-module associated to the solution space of a unimodular row (seen as the matrix of a surjective homomorphism $R^n \to R$) is not free by proving that the row can not be extended to an invertible matrix. This will be used in the example below.

Definition 3.13. *A unimodular row which satisfies the condition iii) above is called* ***completable****.*

We are now ready to give an interesting example of a f.g. stably free module which is not free. For this, consider the coordinate rings of the real n-shpere,

$$R_n = \mathbb{R}[x_0, \ldots, x_n]/(x_0^2 + \cdots + x_n^2 - 1), \tag{3.7}$$

and take for each the unimodular row $\tau_n = (x_0, \ldots, x_n) \in Um_n(R_n)$ (which clearly belongs to $Um_n(R_n)$, as $\tau_n \tau_n^T = 1$ in R_n- we think of the x_i as representatives of the residue class of x_i in (3.7), in each case). Then the solution space P_n associated to each unimodular row τ_n is a f.g. stably free module, but it is only free for $n = 1, 3$ and 7. Indeed, below we show explicitly an invertible (sub)matrix for each of these three cases, all with determinant 1 and constructed considering the multiplication rule in the complex numbers, the quaternions and the Cayley numbers, respectively:

$$\begin{pmatrix}
x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \\
\underline{x_1} & \underline{-x_0} & x_3 & -x_2 & x_5 & -x_4 & -x_7 & x_6 \\
x_2 & -x_3 & -x_0 & x_1 & x_6 & x_7 & -x_4 & -x_5 \\
\underline{x_3} & \underline{x_2} & \underline{-x_1} & \underline{-x_0} & x_7 & -x_6 & x_5 & -x_4 \\
x_4 & -x_5 & -x_6 & -x_7 & -x_0 & x_1 & x_2 & x_3 \\
x_5 & x_4 & -x_7 & x_6 & -x_1 & -x_0 & -x_3 & x_2 \\
x_6 & x_7 & x_4 & -x_5 & -x_2 & x_3 & -x_0 & -x_1 \\
x_7 & -x_6 & x_5 & x_4 & -x_3 & -x_2 & x_1 & -x_0
\end{pmatrix} \tag{3.8}$$

Nevertheless, using a bit of topology, it can be shown that for $n = 2$ this is not possible: suppose the row (x_0, x_1, x_2) can be extended to an invertible matrix $\sigma \in GL_3(R_2)$, with $e_1\sigma = (x_0, x_1, x_2)$. We can think of σ_{ij}, $\det(\sigma)$ as "functions" on the real 2-sphere

$$S^2 = \{(v_0, v_1, v_2) \in \mathbb{R}^3 | \quad v_0^2 + v_1^2 + v_2^2 = 1\} \tag{3.9}$$

Now, for any point of S^2 we can define a tangent vector as follows: if $v \in S^2$, consider

$$\varphi(v) = (\sigma_{12}^{-1^T}(v), \sigma_{22}^{-1^T}(v), \sigma_{32}^{-1^T}(v)) \in \mathbb{R}^3, \tag{3.10}$$

where $\sigma_{ij}^{-1^T}$ denotes the ij-entry of the matrix $\sigma^{-1^T} \in GL_3(R_2)$. Clearly $\langle v, \varphi(v) \rangle = 0$ (it corresponds to multiply the first row of σ by the second column of σ^{-1}, which is 0, as $\sigma\sigma^{-1} = Id_3$), and so $\varphi(v)$ is a tangent vector to S^2 at the point v. Since $\sigma_{i2}^{-1^T}$ are polynomials, the map $\varphi : S^2 \to \mathbb{R}^3$ is a differentiable function. As $\sigma^{-1^T} \in GL_n(A)$, the vector $\varphi(v)$ can never be the zero vector. Thus φ is a nowhere zero vector field on S^2, but this

is well-known to be impossible by the famous Hairy Ball Theorem, a standard result in Algebraic Topology proved in our bachelor's degree, which states that such a continuous tangent vector field on S^2 can not exist- it must vanish somewhere ("in any attempt to comb a hairy ball flat, there will always be at least one tuft of hair at one point on the ball").

In fact, this Theorem states further that there is no non-vanishing continuous tangent vector field on even-dimensional n-spheres, so by the same argument it follows that the solution space associated to the unimodular row τ_n is not free for any n even.
The remaining odd cases for n are considerably harder to prove, and we will not explore here how to do it. Anyway, it can be proven that τ_n is completable only in the cases in which the manifold S^n is *parallelizable*, that is, that its tangent bundle is a trivial bundle. A deep and difficult topological result of Bott, Milnor and Kervaire states that S^n is parallelizable iff $n = 1, 3, 7$, so τ_n is completable only in these three cases.

3.3 Action of $GL_n(R)$ on $Um_n(R)$

The group $GL_n(R)$ of invertible $n \times n$ matrices over R acts on the set $Um_n(R)$ of unimodular rows in the following natural manner: for $v \in Um_n(R), \sigma \in GL_n(R)$,

$$v \mapsto v\sigma \tag{3.11}$$

Indeed, if $w \in M_{1\times n}(R)$ is such that $vw^T = 1$, then $v\sigma(w(\sigma^{-1})^T)^T = 1$, so $v\sigma \in Um_n(R)$ and the map above is well defined as an action of $GL_n(R)$ on $Um_n(R)$. If $v' = v\sigma$ for some $\sigma \in GL_n(R)$, we say that v' and v are conjugate under this action, and we write $v \sim v'$. The equivalence classes of $Um_n(R)$ under $\sim$ are the orbits of this $GL_n(R)$-action.

The proposition below has a nice consequence in terms of conjugate unimodular rows:

Proposition 3.14. *The orbits of $Um_n(R)$ under the $GL_n(R)$-action are in one to one correspondence with the R-modules P for which $P \oplus R \cong R^n$. Under this correspondence, the orbit of $(1, 0, \ldots, 0)$ corresponds to the free module R^{n-1}.*

Proof. To any $(b_1, \ldots, b_n) \in Um_n(R)$ we can associate $P = P(b_1, \ldots, b_n)$, the solution space (i.e. kernel) of the R-homomorphism $R^n \xrightarrow{(b_1,\ldots,b_n)} R$. Such a P is a typical module for which $P \oplus R \cong R^n$, by (3.3). Suppose now

$$P(b_1, \ldots, b_n) \cong_\beta P(c_1, \ldots, c_n) \tag{3.12}$$

for another $(c_1, \ldots, c_n) \in Um_n(R)$ (β the isomorphism). Then, in virtue of the well-known Five Lemma (Lemma A.16), we can complete the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P(b_1,\ldots,b_n) & \longrightarrow & R^n & \xrightarrow{(b_1,\ldots,b_n)} & R & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \beta} & & \vdots{\scriptstyle \exists\alpha} & & \downarrow{\scriptstyle Id} & & \\ 0 & \longrightarrow & P(c_1,\ldots,c_n) & \longrightarrow & R^n & \xrightarrow{(c_1,\ldots,c_n)} & R & \longrightarrow & 0 \end{array} \tag{3.13}$$

with a suitable isomorphism $\alpha : R^n \to R^n$. If $M \in GL_n(R)$ denotes the matrix of this isomorphism α, applying the right square of the diagram to a basis e_i of R^n we obtain

$$(b_1, \ldots, b_n) = (c_1, \ldots, c_n) \cdot M. \tag{3.14}$$

Conversely, suppose $(b_1, \ldots, b_n) = (c_1, \ldots, c_n) \cdot M$ for some $M \in GL_n(R)$. Then, if $w \in M_{1\times n}$ is so that $(b_1, \ldots, b_n)w^T = 0$, it is clear that Mw^T satisfies $(c_1, \ldots, c_n)Mw^T = 0$. The other direction is done analogously using M^{-1} (which exists), and so the automorphism defined by M induces an isomorphism of the two kernels $P(b_1, \ldots, b_n) \cong P(c_1, \ldots, c_n)$.

The second statement of the proposition is immediate- it is clear that $P(1, 0, \ldots, 0) \cong \text{Ker}(R^n \xrightarrow{(1,0,\ldots,0)} R) \cong R^{n-1}$. □

Corollary 3.15. *Let $(b_1, \ldots, b_n) \in Um_n(R)$. Then these two statements are equivalent:*

(i) $(b_1, \ldots, b_n)$ *is completable.*

(ii) $(b_1, \ldots, b_n) \sim (1, 0, \ldots, 0)$.

Proof. $i) \implies ii)$: Suppose $(b_1, \ldots, b_n) \in Um_n(R)$ can be extended to an invertible matrix $M' \in GL_n(R)$. If $M'M = I_n$, then $e_1 = e_1M'M = (b_1, \ldots, b_n)M =$, i.e. $(b_1, \ldots, b_n) \sim e_1$.

$ii) \implies i)$: If $(b_1, \ldots, b_n) = (1, 0, \ldots, 0)M$, with $M \in GL_n(R)$, then M is a completion of $(b_1, \ldots, b_n)$ to a square invertible matrix, and so $(b_1, \ldots, b_n)$ is completable. □

This characterization of completable unimodular rows in Corollary 3.15 will be extremely important in the sequel. In Chapter 4 we will prove that every f.g. projective module over $k[x_1, \ldots, x_n]$ is stably free, and in Chapter 5 we will prove that $\forall f \in Um_n(k[x_1, \ldots, x_n])$ we have $f \sim e_1$, thus proving the Quillen-Suslin Theorem, as every f.g. stably free module will then be free by Proposition 3.11.

Chapter 4

The Hilbert-Serre Theorem

This chapter is entirely devoted to prove that projective modules over $k[x_1, \dots, x_n]$ *are* stably free, a result informally referred to as the "Hilbert-Serre Theorem", as it was proved by Serre using arguments more or less similar to those used in some sophisticated proofs of the well-known Hilbert's Syzygy Theorem. This equivalence is what will allow us to prove the Quillen-Suslin Theorem in the next chapter, using some of the properties and characterizations of stably free modules we saw in Chapter 3, when we introduced them. Quite surprisingly, the fact that finitely generated projective modules over $k[x_1, \dots, x_n]$ are stably free was known "from the beginning" historically speaking, as it was proved in 1958 by Serre himself, just three years after the initial problem was formulated. Nevertheless, it would take almost twenty years more to prove that stably free modules over $k[x_1, \dots, x_n]$ are indeed free, thus solving affirmatively the conjecture.
Our way of proving this result requires some new mathematical tools, such as various types of resolutions of modules, which will take some pages to present.

4.1 Finite free and stably free resolutions

Definition 4.1. *We say that a R-module M has a **finite free resolution** if there exists a resolution*

$$0 \to F_n \to \cdots \to F_0 \to M \to 0 \tag{4.1}$$

with each F_i finite free (that is, each $F_i \cong R^{n_i}$ for some $n_i \in \mathbb{N}$).

Free resolutions will be our key characterization for proving that a projective module M is stably free, as the following theorem shows:

Theorem 4.2. *Let M be a projective R-module. Then M is stably free $\iff$ M admits a finite free resolution*

Proof. $\Rightarrow$) Trivial, as M being stably free is equivalent to the existence of a short exact sequence like the one in formula (3.3),

$$0 \to R^m \to R^n \to M \to 0 \tag{4.2}$$

for some $m, n \in \mathbb{N}$, which is a obviously a finite free resolution.

$\Leftarrow$) Assume the existence of a finite free resolution like the one in (4.1). We'll prove that M is stably free by induction on the length n of its resolution:
If $n = 0$, then we get $0 \to F_0 \to M \to 0$, so M is already isomorphic to a finite free module and is thus stably free. Assume now that it holds for $n \leq n_0$, and we'll prove it for $n_0 + 1$. Given a finite free resolution

$$0 \to F_{n_0+1} \to \cdots \to F_0 \to M \to 0 \tag{4.3}$$

we can consider $M_1 = \mathrm{Ker}(F_0 \to M)$, and as M is projective, $F_0 \cong M \oplus M_1$ and M_1 is also projective. Hence, we obtain the two natural exact sequences

$$\begin{aligned} 0 \to M_1 \to F_0 \to M \to 0 \\ 0 \to F_{n_0+1} \to \cdots \to F_1 \to M_1 \to 0 \end{aligned} \tag{4.4}$$

as, by the exactness of the original sequence, $M_1 = \mathrm{Ker}(F_0 \to M) = \mathrm{Im}(F_1 \to F_0)$, so the natural morphism $F_1 \to M_1$ is surjective.
Then M_1 has a finite free resolution of length n_0, so by the induction hypothesis there exists a finite free module F such that $M_1 \oplus F$ is free. Since $F_0 \oplus F$ is also finite free and $F_0 \oplus F \cong (M \oplus M_1) \oplus F \cong M \oplus (M_1 \oplus F)$, we can conclude that M is stably free. □

We introduce now another kind of resolution which will be more practical in our proofs, as we will see:

Definition 4.3. *A resolution*

$$0 \to E_n \to \cdots \to E_0 \to M \to 0 \tag{4.5}$$

is called ***stably free*** *if all the modules E_i are (finite) stably free.*

The next proposition shows us how closely related these two kinds of resolutions are. Note that M need not be projective:

Proposition 4.4. *Let M be a R-module. Then M has a finite free resolution of length $n \iff M$ has a stably free resolution of length n.*

Proof. $\Rightarrow$) Trivial, since every finite free resolution is a stably free resolution.

$\Leftarrow$) Suppose we have a stably free resolution for M like the one in the definition above. As the E_i are stably free, we have that, for each $i \leq n$, there exists a F_i finite free such that $E_i \oplus F_i$ is (finite) free. Observe that, taking $F = F_i \oplus F_{i+1}$, we can form an exact sequence

$$0 \to E_n \to \cdots \to E_{i+1} \oplus F \to E_i \oplus F \to \cdots \to E_0 \to M \to 0 \tag{4.6}$$

with

$$\begin{array}{ccccccc} E_{i+2} & \xrightarrow{\partial_{i+2} \oplus 0} & E_{i+1} \oplus F & \xrightarrow{\partial_{i+1} \oplus id} & E_i \oplus F & \xrightarrow{\partial_i - 0} & E_{i-1} \\ e & \longmapsto & (\partial_{i+2}(e), 0) & & & & \\ & & (e, f) & \longmapsto & (\partial_{i+1}(e), f) & & \\ & & & & (e, f) & \longmapsto & \partial_i(e) \end{array}$$

In this way, we have changed two consecutive modules in the resolution to make them free, and this process can be done inductively starting with E_0 and E_1 ($F = F_0 \oplus F_1$), then with E_1 and E_2 (with $F = F_2$, as $E_1 \oplus F_0 \oplus F_1$ is already finite free) and so on, obtaining a finite free resolution of the module M:

$$0 \to E_n \oplus F_n \to \cdots \to E_2 \oplus F_2 \oplus F_3 \to E_1 \oplus F_0 \oplus F_1 \oplus F_2 \to E_0 \oplus F_0 \oplus F_1 \to M \to 0 \quad (4.7)$$

□

Definition 4.5. *We say that a module M is of **finite stably free dimension** if it admits a finite stably free resolution. Its stably free dimension is the minimum length of all such resolutions.*

It's not hard to guess that our main goal will be to prove that every finitely generated projective module over $k[x_1, \ldots, x_n]$ is of finite stably free dimension, which will imply it is stably free by the results presented so far. Various technical steps, one after the other, will be necessary to demonstrate that. Although, technically speaking, R need not be Noetherian to prove the results in the next section, this hypothesis will be key to simplify substantially some of the propositions we will come upon with. However, the first of them are easily demonstrable without this assumption. We begin with the Schanuel's Lemma and a useful consequence of it:

Lemma 4.6. ***(Schanuel's Lemma):*** *For a R-module M, suppose we have the two short exact sequences*

$$\begin{aligned} 0 \to K \to P \to M \to 0 \\ 0 \to K' \to P' \to M \to 0 \end{aligned} \quad (4.8)$$

where P, P' are projective. Then there is an isomorphism $K \oplus P' \cong K' \oplus P$.

Proof. Since P is projective, for $P' \to M$ there exists a homomorphism $\phi : P \to P'$ making the right square in the diagram below commute:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{i} & P & \longrightarrow & M & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle id} & & \\ 0 & \longrightarrow & K' & \xrightarrow{j} & P' & \longrightarrow & M & \longrightarrow & 0 \end{array} \quad (4.9)$$

We have that $\mathrm{Im}(i) = \mathrm{Ker}(P \to M)$ and, since the right square of (4.9) commutes, we have $\mathrm{Im}(\phi \circ i) \subseteq \mathrm{Ker}(P' \to M) = \mathrm{Im}(j) \cong K'$, so we can then define the morphism $\varphi : K \to K'$ which sends each element $k \in K$ to the element $k' \in K'$ such that $\phi(i(k)) = j(k')$, thus obtaining the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{i} & P & \xrightarrow{r} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle id} & & \\ 0 & \longrightarrow & K' & \xrightarrow{j} & P' & \xrightarrow{s} & M & \longrightarrow & 0 \end{array} \quad (4.10)$$

It is easy to prove that, with the construction above, we get an exact sequence:

$$\begin{aligned} 0 \longrightarrow K &\xrightarrow{i\oplus\varphi} P\oplus K' \xrightarrow{\phi - j} P' \longrightarrow 0 \\ k &\longmapsto (ik, \varphi k) \\ & (p,k') \mapsto \phi p - jk' \end{aligned} \tag{4.11}$$

(we have changed a bit the notation to make the diagram look clearer, with $ik = i(k)$,...)
$i \oplus \varphi$ is trivially injective from the fact that i is injective, and from the commutativity of (4.10) it is clear that the composition is 0, so $\mathrm{Im}(i\oplus\varphi) \subseteq \mathrm{Ker}(\phi - j)$.
To see $\mathrm{Im}(i\oplus\varphi) \supseteq \mathrm{Ker}(\phi - j)$, consider a (p,k') with $\phi(p) - j(k') = 0$. Then $\phi(p) = j(k')$ and $j(k') \in \mathrm{Ker}(s)$, so $\phi(p) \in \mathrm{Ker}(s)$ and $p \in \mathrm{Ker}(r)$. As $\mathrm{Ker}(r) = \mathrm{Im}(i)$, there exists a $k \in K$ with $p = i(k)$, and by definition of φ, $\varphi k = k'$, so $(p,k') = (i(k), \varphi(k))$ and $\mathrm{Im}(i\oplus\varphi) \supseteq \mathrm{Ker}(\phi - j)$.
To see that $\phi - j$ is surjective, it is enough to see that for $p' \in P'$, there must be a $p \in P$ with $r(p) = s(p')$ (as r is surjective), and clearly $s(\phi(p) - p') = r(p) - s(p') = 0$, so $\phi(p) - p' \in \mathrm{Ker}(s) = \mathrm{Im}\, j \cong K'$, so there exists a $k' \in K'$ with $p' = \phi(p) - j(k')$ and $\phi - j$ is thus surjective.

Finally, with the short exact sequence of (4.11) and using the fact that P' is projective, the sequence splits, and we obtain $K \oplus P' \cong K' \oplus P$, as we wanted to prove.

□

Definition 4.7. *We say that two modules M_1, M_2 are **stably isomorphic** if there exist finite free modules F_1, F_2 such that $M_1 \oplus F_1 \cong M_2 \oplus F_2$.*

Lemma 4.8. *Let M_1 and M_2 be stably isomorphic and*

$$\begin{aligned} 0 \to N_1 \to E_1 \to M_1 \to 0 \\ 0 \to N_2 \to E_2 \to M_2 \to 0 \end{aligned} \tag{4.12}$$

be exact sequences, where E_1, E_2 are stably free. Then N_1 and N_2 are also stably isomorphic.

Proof. By definition, there is an isomorphism $M_1 \oplus F_1 \cong M_2 \oplus F_2$, so we can obtain two natural exact sequences

$$\begin{aligned} 0 \to N_1 \to E_1 \oplus F_1 \to M_1 \oplus F_1 \to 0 \\ 0 \to N_2 \to E_2 \oplus F_2 \to M_2 \oplus F_2 \to 0 \end{aligned} \tag{4.13}$$

so by Schanuel's Lemma, $N_1 \oplus E_2 \oplus F_2 \cong N_2 \oplus E_1 \oplus F_1$. Since E_1, E_2 are stably free for some $\bar{F}_1$ and $\bar{F}_2$ (so $E_1 \oplus \bar{F}_1$ and $E_2 \oplus \bar{F}_2$ are free), taking $\bar{F} = \bar{F}_1 \oplus \bar{F}_2$ we obtain $N_1 \oplus (E_2 \oplus \bar{F} \oplus F_2) \cong N_2 \oplus (E_1 \oplus \bar{F} \oplus F_1)$ and N_1, N_2 are thus stably isomorphic. □

4.2 R Notherian

From now on, R will refer to a commutative Noetherian ring. We will see that, under this hypothesis, we can prove quite easily that finite free resolutions behave well with

respect to short exacts sequences, in the sense of Theorem 4.12, the key result needed to finally demonstrate the Hilbert-Serre Theorem, in the last section. Also, to simplify the text, we will write **FR** for "finite free resolution" and **SFR** for "finite stably free resolution".

The following proposition shows us, using the previous lemma, how easily *any* "partial" stably free resolution of a module M can be completed to a SFR of M:

Proposition 4.9. *Suppose M has stably free dimension n (it admits a SFR of length n). Now let*

$$E_m \to \cdots \to E_0 \to M \to 0 \tag{4.14}$$

be an exact sequence with E_i stably free for $i = 0, \ldots, m$. Then

(i) If $m < n-1$ there exists a stably free module E_{m+1} such that the exact sequence above can be continued preserving its exactness to

$$E_{m+1} \to \cdots \to E_0 \to M \to 0 \tag{4.15}$$

(ii) If $m = n-1$ and we take $E_n = \mathrm{Ker}(E_{n-1} \to E_{n-2})$, then E_n is stably free and thus

$$0 \to E_n \to \cdots \to E_0 \to M \to 0 \tag{4.16}$$

is a stably free resolution.

Proof. (i) It follows immediately from the fact that R is Noetherian: as each E_i is finitely generated, we can pick E_{m+1} to be finite free (and thus stably free).

(ii) Taking $E_n = \mathrm{Ker}(E_{n-1} \to E_{n-2})$, we have two exact sequences

$$\begin{aligned} 0 \to E_n \to \cdots \to E_0 \to M \to 0 \\ 0 \to E'_n \to \cdots \to E'_0 \to M \to 0 \end{aligned} \tag{4.17}$$

the second one being a SFR of M. We can see that E_n is stably free using an inductive argument inserting the kernels $K_n = \mathrm{Ker}(E_n \to E_{n-1}) = \mathrm{Im}(E_{n+1} \to E_n)$ and K'_n defined similarly for the E'_i in each exact sequence:
By Lemma 4.8, K_0 and K'_0 are stably isomorphic, as we have the two exact sequences

$$0 \to K_0 \to E_0 \to M \to 0 \qquad 0 \to K'_0 \to E'_0 \to M \to 0 \tag{4.18}$$

But also $K_0 = \mathrm{Im}(E_1 \to E_0)$, $K'_0 = \mathrm{Im}(E'_1 \to E'_0)$, and as $K_1 = \mathrm{Ker}(E_1 \to E_0)$, $K'_1 = \mathrm{Ker}(E'_1 \to E'_0)$, we have the natural short exact sequences

$$0 \to K_1 \xrightarrow{i} E_1 \to K_0 \to 0 \qquad 0 \to K'_1 \xrightarrow{i} E'_1 \to K'_0 \to 0 \tag{4.19}$$

Using the same argument, K_1 and K'_1 in (4.19) are again stably isomorphic, and this can be done repeatedly so, at the end, we get that $K_{n-1} = \mathrm{Ker}(E_{n-1} \to E_{n-2})$ and $K'_{n-1} = \mathrm{Ker}(E'_{n-1} \to E_{n-2})$ are stably isomorphic. But $K_{n-1} = E_n$ as we defined it, and $K'_{n-1} \cong E'_n$ using the left-exactness of the second sequence. If $K_{n-1} \oplus F \cong K'_{n-1} \oplus F$ (for F, F' finite free), as K'_{n-1} is already stably free, $K'_{n-1} \oplus F$ is also stably free and then $K_{n-1} \oplus F$ is stably free too, which necessarily implies $K_{n-1} = E_n$ is stably free.

□

As a consequence, we get this corollary, which will have relevant consequences:

Corollary 4.10. *If, for E stably free,*

$$0 \to N \to E \to M \to 0 \tag{4.20}$$

is exact, then M is of stably free dimension $\leq n \iff N$ is of stably free dimension $\leq n-1$.

Proof.
- $\Leftarrow$) It is enough to "glue" on the left hand side a SFR of N, so we get the (easy to see) exact sequence

$$0 \to E_{n-1} \to \cdots \to E_0 \xrightarrow{\alpha} E \to M \to 0 \tag{4.21}$$

  where α is the natural composition $E_0 \to N \to E$.

- $\Rightarrow$) As M has stably free dimension n, by Proposition 4.9 we can construct a SFR

$$0 \to E_n \to \cdots \to E_1 \to E \to M \to 0 \tag{4.22}$$

  As $N \cong \mathrm{Ker}(E \to M) = \mathrm{Im}(E_1 \to E)$, the natural sequence

$$0 \to E_n \to \cdots \to E_1 \to N \to 0 \tag{4.23}$$

  is exact and thus a SFR of N with length $n-1$.

□

The previous corollary and the simple construction of the next lemma will be our final requirements for proving Theorem 4.12:

Lemma 4.11. *Given the short exact sequence of finitely generated R-modules*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \tag{4.24}$$

there exist R-modules N', N, N'' and stably free modules E', E, E'' such that the following diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E' & \longrightarrow & E & \longrightarrow & E'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array} \tag{4.25}$$

is commutative and exact along its rows and columns.

Proof. As the modules are finitely generated, it is clear that M' and M'' can each be represented as the image of a finite free module (which is stably free). Hence it is enough to prove that the following diagram is commutative and exact along its rows and columns:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Ker}(\phi_1) & \xrightarrow{\bar{i}} & \mathrm{Ker}(\varphi) & \xrightarrow{\bar{\pi}} & \mathrm{Ker}(\phi_2) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & R^m & \xrightarrow{i} & R^m \oplus R^n & \xrightarrow{\pi} & R^n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \phi_2} & & \\
0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array} \tag{4.26}$$

where φ is the morphism such that, for $(x, y) \in R^m \oplus R^n$, $\varphi(x, y) = f(\phi_1(x)) + \bar{\varphi}(y)$, and $\bar{\varphi}$ is defined over a basis e_i of R^n so that $g(\bar{\varphi}(e_i)) = \phi_2(e_i)$ (which can be done because g is surjective), and extended linearly. It is clear that φ is a morphism, and that it is surjective (applying the well-known Five Lemma (Lemma A.16), with ϕ_1, ϕ_2 epimorhisms).
Once defined φ, it is immediate to verify that the restrictions $\bar{i}$ and $\bar{\pi}$ are well defined too, and that the diagram is commutative. It's also trivial that it is exact along all its columns and rows except for the one above, which is also easy to prove:
$\bar{i}$ is injective because i is injective, and clearly $\mathrm{Im}(\bar{i}) \subseteq \mathrm{Ker}(\bar{\pi})$, as $\bar{\pi} \circ i = 0$. $\mathrm{Ker}(\bar{\pi}) \subseteq \mathrm{Im}(\bar{i})$ because, if $x \in \mathrm{Ker}(\bar{\pi})$, its second component must be zero, and thus it is the image for i of some $x' \in R^m$, which will belong to $\mathrm{Ker}(\phi_1)$ as $0 = \varphi(i(x')) = f(\phi_1(x'))$ and f is injective. Finally, $\bar{\pi}$ is surjective because for $x \in \mathrm{Ker}(\phi_2)$, there exists $x' \in R^m \oplus R^n$ with $\bar{\pi}(x') = x$, and $\phi_2(\pi(x')) = g(\varphi(x')) = 0 \Rightarrow \varphi(x') \in \mathrm{Im}(f)$. As ϕ_1 is surjective, taking $\bar{x} \in R^m$ with $f(\phi_1(\bar{x})) = \varphi(x')$, we have that $0 \neq i(\bar{x}) - x' \in \mathrm{Ker}(\varphi)$ with $\bar{\pi}(i(\bar{x}) - x') = x$.
This concludes the proof. □

Theorem 4.12. *Let*

$$0 \to M' \to M \to M'' \to 0 \tag{4.27}$$

be an exact sequence of R-modules. Then, if any two of these modules have a FR, so does the third.

Proof. By Proposition 4.4, the Theorem is equivalent to proving that if any two of these modules have a SFR, so does the third:

- Suppose M' and M verify that. Then M is finitely generated, which implies M'' is also finitely generated. We can then reason by induction on the stably free dimension of M. Using the notation of the Lemma 4.11, both N' and N have a SFR, with the stably free dimension of N being $\leq n - 1$. Thus, inductively and by Corollary 4.10, we can reduce the problem to the case in which the stably free dimension of M is 0. But then M is already stably free, so gluing a SFR of M' on the left-hand side as we

did in Corollary 4.10, one can trivially obtain a SFR of M''

$$0 \to E_m \to \cdots \to E_0 \to M \to M'' \to 0 \tag{4.28}$$

- Suppose now M' and M'' verify that. Then both are finitely generated, and by the construction in Lemma 4.11, we see that M is finitely generated too. If both M' and M'' have stably free dimensions 0, then they are projective and one has $M \cong M' \oplus M''$. Thus, M is itself stably free and has the trivial finite SFR. Now it's enough to reduce to this case by induction: suppose n to be the maximum of the stably free dimensions of M' and M''. Then, in the notation of Lemma 4.11, the maximum of the stably free dimensions of N' and N'' is $\leq n-1$. Repeating this process, one arrives finally to the case in which the stably free dimensions of both N' and N'' are zero, and gluing the intermediate stably free modules all the way down using Corollary 4.10, one can get a SFR for M.
- Finally, suppose M and M'' verify that. This implies M'' and M are finitely generated, and as they are Noetherian, M' is also finitely generated. Now the result follows by reducing, as done before, to the case in which the stably free dimension of M is 0, so it is already stably free and we can use a SFR of M'' and Corollary 4.10 to conclude that M' admits a SFR.

□

4.3 Proof of the Hilbert-Serre Theorem

With all these previous results, we can finally prove the Hilbert-Serre Theorem, which is a simple consequence of the following theorem:

Theorem 4.13. *Let R be a commutative Noetherian ring and x a variable. Then every finitely generated R-module admits a FR $\implies$ every finitely generated $R[x]$-module admits a FR.*

This is how:

Corollary 4.14. ***(Hilbert-Serre Theorem):*** *If k is a field and $x_1, \ldots, x_n$ are independent variables, then every finitely generated projective module over $k[x_1, \ldots, x_n]$ is stably free.*

Proof. It follows from the previous theorem by simple induction: it is clear that a finitely generated projective k-module is a finite-dimensional k-vector space, so it is naturally finite free and thus stably free. As a field k is Noetherian, by the Hilbert's Basis Theorem, $k[x_1, \ldots x_r]$ is Noetherian $\forall r \in \mathbb{N}$, so we can iterate this process by adding a new variable at each step until we reach n, hence obtaining that every finitely generated projective $k[x_1, \ldots, x_n]$-module admits a FR and is thus stably free by Theorem 4.2. □

To prove Theorem 4.13 we will use a tensor product argument at the end. We recall that a flat module over a ring R is an R-module M such that taking the tensor product over R with M preserves exact sequences. Also, when we use the tensor product with $R[x]$, the module obtained is naturally a $R[x]$-module by extension of scalars. We state the following lemma, which will be apparent to those familiar with flat modules:

Lemma 4.15. *$R[x]$ is a flat R-module and for any ideal $I \subset R$, $I \otimes_R R[x] \cong I[x]$.*

Proof. The first assertion is immediate for being $R[x]$ R-free. The second follows from tensoring the following short exact sequence with $\otimes_R R[x]$

$$0 \to I \to R \to R/I \to 0, \tag{4.29}$$

and having in mind that $R \otimes_R R[x] \cong R[x]$ and $R/I \otimes_R R[x] \cong R[x]/IR[x] = R[x]/I[x]$. □

The remaining pages of this chapter are devoted to the intricate proof of Theorem 4.13:

Proof. (Theorem 4.13): Let M be a finite $R[x]$-module. As we saw in Chapter 1, section 3 (Theorem 1.13), M admits a finite filtration:

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0 \tag{4.30}$$

with each M_i/M_{i+1} isomorphic to $R[x]/P_i$ for some prime P_i of $R[x]$ (M_{n-1} is already isomorphic to $R[x]/P$ for some prime P). Applying Theorem 4.12 multiple times with the short exact sequences of $R[x]$-modules

$$\begin{gathered} 0 \to M_n \to M_{n-1} \to M_{n-1}/M_n \to 0 \\ \cdots \\ 0 \to M_1 \to M_0 \to M_0/M_1 \to 0 \end{gathered} \tag{4.31}$$

we obtain recursively that $M_{n-1}, \ldots, M_0 = M$ will admit a FR if a $R[x]$-module of the form $R[x]/P_i$ for some prime P_i does. Thus, it suffices to prove it for $M \cong R[x]/P$, with P a prime ideal in $R[x]$. Now, in light of the exact sequence

$$0 \to P \to R[x] \to R[x]/P \to 0 \tag{4.32}$$

and Theorem 4.12 again, a $R[x]$-module M of this form will admit a FR if and only if P (regarded as a $R[x]$-module) does, as $R[x]$ clearly admits one (the trivial FR).
Observe that, with P prime in $R[x]$, $P \cap R$ is prime in R (if for $a, b \in R$ we have $ab \in P \cap R \implies ab \in P \implies a$ or $b \in P$ (P prime) $\implies a$ or $b \in P \cap R$).

We will reason by contradiction- a rather long one, actually:
Suppose there is some $M = R[x]/P$ which does not admit a FR, which happens iff P does not admit a FR, by formula (4.32) and Theorem 4.12. Among all of these M we can select one for which the intersection $R \cap P = \mathfrak{p}$ is maximal in R- otherwise we could obtain an infinite chain $\cdots \subsetneq \mathfrak{p}_i \subsetneq \mathfrak{p}_{i+1} \subsetneq \ldots$, in contradiction with R being Noetherian.
Define now $R_0 = R/\mathfrak{p}$ (so R_0 is an integral domain and Noetherian) and $P_0 = P/\mathfrak{p}R[x] (= P/\mathfrak{p}[x])$. By the Hilbert Basis Theorem, $R_0[x]$ is Noetherian, and P_0 is naturally a $R_0[x]$-module with $\lambda \cdot \overline{x} = \overline{\lambda \cdot x}$, also finitely generated because P is an ideal of $R[x]$, which is Noetherian. All this implies that P_0 is a Noetherian $R_0[x]$-module.

Thus, let $f_1, \ldots, f_n$ be a finite set of generators for P_0, and let f be a polynomial of minimal degree in P_0. If we take K_0 the quotient field of R_0 (recall that R_0 is an integral domain), then $K_0[x]$ is an Euclidean domain, and by the Euclidean algorithm we can write

$$f_i = q_i f + r_i \text{ for } i = 0, \ldots, n \tag{4.33}$$

with q_i, $r_i \in K_0[x]$ and $\deg(r_i) < \deg(f)$. If we take d_0 the product of the denominators of all the coefficients in $q_i, r_i \, \forall i$, then $d_0 \neq 0$ because R_0 is a domain, and

$$d_0 f_i = q_i' f + r_i' \tag{4.34}$$

where $q_i' = d_0 q_i$ and $r_i' = d_0 r_i$ all lie in $R_0[x]$. Since $\deg(f)$ is minimal in P_0 and $\deg(r_i') = \deg(r_i) < \deg(f) \; \forall i$ (d_0 is an scalar), it follows that $r_i' = 0 \, \forall i$ so, as $R_0[x]$-modules,

$$d_0 P_0 \subseteq R_0[x] f = (f) \tag{4.35}$$

Now let $N_0 = P_0/(f)$, so N_0 is a module over $R_0[x]$. N_0 may also be viewed as a module over $R[x]$ with $\lambda \cdot \overline{x} = \overline{\lambda \cdot x}$, case in which we will denote it by N.
Let $d \in R$ be any element reducing to $d_0 \mod \mathfrak{p}$. Then $d \notin \mathfrak{p}$, since $d_0 \neq 0$. As P_0 is a Noetherian $R_0[x]$-module, N_0 is also a Noetherian $R_0[x]$-module, and again by section 1.3 (Theorem 1.13), it admits a finite filtration such that each N_i'/N_{i+1}' factor module of the filtration is isomorphic to some $R_0[x]/Q$, where Q is an associated prime of N_0. Let Q_i' be the inverse images of Q_i in $R[x]$ via the natural morphism $R[x] \to R_0[x]$. Then the Q_i' are prime in $R[x]$, and it is not hard to see that they are precisely the associated primes of N in $R[x]$ (recall Corollary 1.14), and each contains $\mathfrak{p}R[x] = \mathfrak{p}[x]$, by construction of N_0. Since d_0 annihilates N_0 (that is, $d_0 N_0 = 0$), it follows that d annihilates N and therefore d lies in every associated prime of N. As we took $d \notin \mathfrak{p}$, the inclusion $Q_i' \cap R \supsetneq \mathfrak{p}$ is strict and, by the maximality property in the selection of P, it follows by the same sequence in (4.32) and Theorem 4.12 that every one of the factor modules in this filtration of N admits a FR, and by the same argument as in (4.31), it follows that N itself admits a FR as a $R[x]$-module.

Now we just have to apply Theorem 4.12 repeatedly to the following exact sequences: As $\mathfrak{p}$ is an ideal of a Noetherian ring, it is finitely generated and by hypothesis has a FR has a R-module, say

$$0 \to E_n \to \cdots \to E_0 \to \mathfrak{p} \to 0 \tag{4.36}$$

Via the tensor product with the flat R-module $R[x]$ (Lemma 4.15), we may simply form the $R[x]$-modules $E_i[x] = R[x] \otimes_R E_i$ to obtain a exact sequence of $R[x]$-modules which are actually $R[x]$-free, and thus we have a FR for $R[x] \otimes_R \mathfrak{p} \cong \mathfrak{p}[x] = \mathfrak{p}R[x]$ as a $R[x]$-module. Considering $R_0[x]$ as an $R[x]$-module, from the exact sequence

$$0 \to \mathfrak{p}R[x] \to R[x] \to R_0[x] \to 0 \tag{4.37}$$

we conclude that $R_0[x]$ also admits a FR.
Now the principal ideal (f) in $R_0[x]$, seen as a $R[x]$-module, is isomorphic to $R_0[x]$ via the $R[x]$-morphism $f \mapsto 1$ (recall (4.35)), and therefore (f) admits a FR. Theorem 4.12 applied to the short exact sequence of $R[x]$-modules

$$0 \to (f) \to P_0 \to N \to 0 \tag{4.38}$$

shows that P_0 admits a FR; and further applied to the short exact sequence

$$0 \to \mathfrak{p}R[x] \to P \to P_0 \to 0 \tag{4.39}$$

shows that P admits a FR, contradicting our assumption that P did not admit one! This proves that every $M = R[x]/P$ admits a FR, and our proof of Theorem 4.13 is done. □

Chapter 5

Proof of the Quillen-Suslin Theorem

In this chapter we will finally give a proof of the Theorem this whole work is about. Now that we know that finitely generated projective modules over $k[x_1, \ldots, x_n]$ are stably free, we will use one of their key characterizations given in Chapter 3: we will see that any unimodular row $(f_1, \ldots, f_m)$ with $f_i \in k[x_1, \ldots, x_n]$ is completable- that is, it can be extended to an invertible matrix with coefficients in $k[x_1, \ldots, x_n]$ (Proposition 3.11).
Curiously, the proof we will explain in this chapter is neither from Quillen nor Suslin- it was found by Vaserstein only three months after the conjecture was solved in 1976, inspired by the proof of Suslin and using a previous result by Horrocks. It is so considerably shorter and simpler than the demonstrations provided by the former two that it is usually referred to as the "8-line proof of the Serre's conjecture", although we will pleasingly spend some more pages to explain it in detail.
Also, we will need to prove the case in one variable before, to start the inductive argument in our final demonstration. Fortunately, this case is quite straightforward, although it will take us some time, as we will provide a constructive proof that will be relevant when we discuss some algorithm aspects of the Quillen-Suslin Theorem in Chapter 6.

5.1 The case of one variable $k[x]$

It is well known that $k[x]$ is a PID- moreover, it is an Euclidean domain, with the well-known Euclidean algorithm of division of polynomials in one variable. In fact, one could ignore the "completability" of a unimodular row $f \in Um_n(k[x])$ and prove directly that any finitely generated projective module over a PID must be free. This could be deduced from the following theorem, that we will not prove:

Theorem 5.1. *In a PID, any submodule of a free module is a free module.*

Observe that, if we assume this theorem, it follows immediately that any finitely gen-

erated projective module P is free. Indeed, it is clear that there exists an exact sequence

$$0 \to \text{Ker}(f) \to R^n \xrightarrow{f} P \to 0 \tag{5.1}$$

which splits, so $P \hookrightarrow R^n$ and is thus naturally isomorphic to a submodule of R^n, and hence is free.

However, we will take a different approach to the case $k[x]$, a more constructive one- we will provide an algorithm which will show how to extend to an invertible matrix $n \times n$ any unimodular row $f \in Um_n(k[x])$ using the division algorithm, thus proving affirmatively that any stably free module (and thus every f.g. projective module by Corollary 4.14) over $k[x]$ is free. It goes without saying that this process can be carried out computationally, and in fact it will appear again as a necessary algorithm in Chapter 6, so we will explain it in detail.

So, assume that $f = (f_1, \dots, f_n) \in Um_n(k[x])$. This means that there do exist $g_i \in k[x]$ such that $\sum_{i=1}^n g_i f_i = 1$, and so $(f_1, \dots, f_n) = (1)$ or, equivalently,

$$gcd(f_n, gcd(f_{n-1}, gcd(f_{n-2}, \dots gcd(f_3, gcd(f_2, f_1)) \dots))) = gcd(f_1, \dots, f_n) = 1 \tag{5.2}$$

Recall that the *gcd* of two polynomials in one variable always exists for being $k[x]$ an Euclidean domain, and is unique up to scalar multiplication. Also, recall that $gcd(f, g)$ can be computed by doing recursive divisions until we reach zero, with the *gcd* being the last non-zero element in that process. The *gcd* of more than two polynomials is obtained recursively with the formula (5.2), though the order doesn't matter at all.

Now, recall that, at the end of Chapter 3, we saw that a unimodular row $f \in Um_n(R)$ is completable $\iff$ $f \sim_{GL_n(R)} e_1$, where $e_1 = (1, 0, \dots) \in R^n$. Note that, if $fM = e_1$ with $M \in GL_n(R)$, then $f = e_1 M^{-1}$, and so f is the first row of M^{-1}, and thus finding M is equivalent to completing f to an invertible matrix if we compute M^{-1} afterwards, for example, using the adjugate formula (Remark 3.7). Thus, we will describe a way to obtain a $M \in GL_n(k[x])$ for which $fM = e_1$. To do so, we will use what we call elementary matrices:

Definition 5.2. *In our context, an **elementary matrix** is a matrix with one of these three forms:*

1) $E_{ij}(x)$, the identity matrix except for a $y \in k[x]$ element in the entry ij, $i \neq j$.

2) $D_i(\lambda)$, a diagonal matrix with all ones except for a $\lambda \in k \backslash 0$ in the entry ii.

3) P_{ij}, the identity matrix but with the rows (or columns) i and j permuted, $i \neq j$.

Example 5.3. *Here are three examples of the three kinds of matrices in the case $n = 3$:*

$$E_{12}(x^2+3x) = \begin{pmatrix} 1 & x^2+3x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad D_3(\tfrac{3}{4}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{3}{4} \end{pmatrix} \quad P_{23} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Remark 5.4. *It is immediate to verify that these three kinds of matrices belong to $GL_n(k[x])$, with inverses $E_{ij}(-x)$, $D_i(\frac{1}{\lambda})$ and P_{ij} (itself) respectively in each case.*

Remark 5.5. *In general, the concept of* elementary matrix *refers only to the first kind of matrix presented above. This is because they are the only ones which always have determinant 1. Note that, in our case, D_i is invertible because k is a field, but we could not define it over a more general ring. The matrices P_{ij} are usually omitted because they have determinant -1. Nevertheless, we will include both kinds in our definition, as they will prove to be very useful in our case.*

It is not hard to guess why these matrices are relevant- they encode the usual row operations that can be done to f. That is:

$$fE_{ij}(x) = (f_1, \dots, f_j + xf_i, \dots, f_n)$$
$$fD_i(\lambda) = (f_1, \dots, \lambda f_i, \dots, f_n)$$
$$fP_{ij} = (f_1, \dots, f_j, \dots, f_i, \dots, f_n) \text{ (with } j > i \text{, interchanged).}$$

This proves that f is completable $\iff$ any of the f' obtained using this row operations is completable, as they are done with matrices in $GL_n(k[x])$. In our case, we will see that, if $f \in Um_n(k[x])$, we can obtain e_1 directly using this elementary row operations, and so f will be completable. This approach also has a remarkable consequence: we can "store" all the multiplications by elementary matrices in the process, so at the end we will have $fM = e_1$, and to obtain the completion of f to an invertible matrix, M^{-1}, one just has to multiplicate the inverses of the stored elementary matrices (which have the simple form of Remark 5.4) in the reverse order. This being said, we present here our algorithmic proof using these row operations:

Theorem 5.6. *Any unimodular row $f \in Um_n(k[x])$ satisfies $f \sim_{GL_n(k[x])} e_1$.*

Proof. (algorithmic):

1) We will start with f_1 and f_2. First, we bring to the first position the one with maximal degree, by permuting them, if necessary (we will always do this, to clarify the explanation). If they have the same degree, no permutation is necessary.

2) If f_2 has leading coefficient $\alpha \neq 1$, we multiply f by $D_2(\frac{1}{\alpha})$, so it now has leading coefficient 1. Again, this is just in order to clarify the explanation.

3) We start now the division algorithm: if r =deg(f_1) and s =deg(f_2), we can now get $f_1 := f_1 - LT(f_1)x^{r-s}f_2$ (by multiplying f by $E_{21}(-LT(f_1)x^{r-s}f_2)$). This reduces the degree of f_1 at least by one, and we obtain a new f_1.

4) We repeat steps 1-3 until we get $f_1 = gcd(f_1, f_2)$ (which coincides with the *gcd* of the original f_1 and f_2). This will always happen, as in the third step the degree of f_1 always decreases and, independently of how many times we do the steps, one will eventually reach zero.

5) If $f_1 \neq 1$, we permute f_3 (which has not intervened so far) with f_2, and do again the steps 1-4 until we get $f_1 = gcd(f_3, gcd(f_1, f_2))$.

6) If $f_1 \neq 1$, we permute f_4 with f_2 and start the whole process again...

7) We do this with all the remaining f_i.

   By the end, we must for sure have $f_1 = 1$, as $gcd(f_1, \ldots, f_n) = 1$. This may have happened well before having to do the process for all the f_i. In either case, it is clear that, as soon as f has the form $f = (1, f_2', \ldots, f_n')$, the last step is

8) Multiply f by $E_{1i}(-f_i')$ for each i, to obtain $f = (1, 0, \ldots, 0)$.

□

Though this algorithm may not be the most efficient one, it clearly works and gives a constructive way to extend any unimodular row f to an invertible matrix, so our case in one variable is done.

Remark 5.7. *Note that the algorithm can be used with polynomial rows which are not unimodular, that is, with $gcd(f_1, \ldots, f_n) = p(x) \neq 1$, to reduce them to the form $(p(x), 0, \ldots, 0)$. In Chapter 6, section 2 we may found this situation, and we will use this algorithm exactly as it is described.*

5.2 Horrock's Theorem

Let us head now to our theorem in more than one variable. To do so, we will need first another result, the Horrock's Theorem, which proves that a unimodular row f always satisfies $f \sim_{GL_n(R)} e_1$ in the case in which R is a local ring and f has one component with leading coefficient 1 (recall from Definition 1.5 that a local ring is a ring which only has one maximal ideal). We state before two little remarks:

Remark 5.8. *In the same spirit as in the case of one variable shown before, we can permute the components of f or add a multiple gf_i to f_j ($j \neq i$), so f will be completable $\iff$ any one of its transformations by these row operations is completable, which correspond to the matrices $E_{ij}(x)$ and P_{ij} introduced in the previous section. Observe that, as we are in a more general ring, we will not use the matrices D_i (Remark 5.5). Anyway, we will not need them, as, by hypothesis, one component will have leading coefficient 1.*

Remark 5.9. *Recall from Remark 2.5 that, in a local ring $(A, \mathfrak{m})$, $x \notin \mathfrak{m} \iff x$ is a unit.*

With this in mind,

Theorem 5.10. ***(Horrock's Theorem):*** *Let $(A, \mathfrak{m})$ be a local ring and let $A[x]$ be the polynomial ring in one variable over A. Let f be a unimodular row in $A[x]^n$ such that some component has leading coefficient 1. Then f is completable.*

Proof. (Suslin): If $n = 1$ and 2 the theorem is obvious even without assuming that A is local. Assume now $n \geq 3$, and we will proceed by induction on the smallest degree d of a component of f with leading coefficient 1. First we note that, by permuting if necessary and by the Euclidean algorithm and row operations, we may assume that f_1 has leading coefficient 1, degree d and that $\text{def}(f_j) < d$ for $j \neq 1$. Since f is unimodular, there exists a

relation $\sum_{i=1}^{n} g_i f_i = 1$. This expression actually shows that not all coefficients of $f_2, \ldots, f_n$ can lie in the maximal ideal $\mathfrak{m}$ because in this case, if we read that expression $\bmod \mathfrak{m}[x]$, we would have $\overline{\sum_{i=1}^{n} g_i f_i = 1} = \overline{g_1 f_1} = \bar{1}$, but this is impossible because f_1 has leading coefficient 1, and $g_1 f_1$ can not reduce to a constant $\bmod \mathfrak{m}[x]$. Without loss of generality, we may assume, permuting if necessary, that some coefficient of f_2 does not lie in $\mathfrak{m}$ and is so a unit, since A is local (Remark 5.8). Write now

$$\begin{aligned} f_1(x) &= x^d + a_{d-1}x^{d-1} + \cdots + a_0 \qquad \text{with } a_i \in \mathfrak{o}, \\ f_2(x) &= b_s x^s + \cdots + b_0 \qquad \text{with } b_i \in \mathfrak{o},\ s \leq d-1, \end{aligned}$$

so that some b_i is a unit. Let $\mathfrak{a}$ be the ideal generated by all the leading coefficients of polynomials $g_1 f_1 + g_2 f_2$ of degree $\leq d-1$. Then $\mathfrak{a}$ contains all the coefficients b_i, $i = 0, \ldots, s$. One can see this by descending induction, starting with b_s, which is obvious $(0 \cdot f_1 + 1 \cdot f_2)$, and then using repeatedly a linear combination like

$$x^{d-s} f_2(x) - b_s f_1(x) = (b_{s-1} - b_s a_{d-1}) x^{d-1} + \ldots. \tag{5.3}$$

(and then by adding $b_s a_{d-1} x^{d-1} + \ldots$ to (5.3), which will be of the form $g_1 f_1 + g_2 f_2$ by descending induction). Therefore $\mathfrak{a}$ contains a unit and is thus the total ideal A, so there exists a polynomial $g_1 f_1 + g_2 f_2$ of degree $\leq d-1$ and leading coefficient 1. By row operations, we may now get a polynomial of degree $\leq d-1$ and leading coefficient 1 in the i-th place of f, for some $i \neq 1, 2$. We can now start the process all over again, ultimately getting $d = 0$, case in which f has 1 in some component and all the others are in A, and it is obvious that $f \sim e_1$ using elementary row operations. This concludes the proof. □

Note that, for $f \in A[x]^n$, we can write $f = f(x)$, and there is a natural "constant" vector $f(0)$, formed by the constant coefficients. Implicitly in the proof of Horrock's Theorem, we get the following corollary:

Corollary 5.11. *Let $(A, \mathfrak{m})$ be a local ring. Let f be a unimodular vector in $A[x]^n$ such that some component has leading coefficient 1. Then $f \sim f(0)$ over $A[x]$.*

Proof. As there exists $\sum_{i=1}^{n} g_i f_i = 1$, there must be at least one constant term of some f_i which does not lie in the maximal ideal $\mathfrak{m}$ and is thus a unit, so $f(0) \sim e_1$ (by elementary row operations). By the proof provided before, $f \sim e_1$ and, by transitivity, $f \sim f(0)$. □

5.3 The proof

Horrock's Theorem being proven, we are interested in getting a similar descent over non-local rings. To do so we just need the following two results, both generalizing the arguments shown above. To prove them, it is necessary to recall the notions of multiplicative subset and localization introduced in Chapter 1, section 2:

Lemma 5.12. *Let R be an integral domain, and S a multiplicative subset. Let x, y be independent variables (that is, there is no polynomial relation between them). Then, if $f(x) \sim f(0)$ over $(S^{-1}R)[x]$, then there exists $c \in S$ such that $f(x + cy) \sim f(x)$ over $R[x, y]$.*

Proof. As R is an integral domain, $S^{-1}R$ is also an integral domain and so is $(S^{-1}R)[x]$. Thus, $N \in GL_n((S^{-1}R)[x]) \Rightarrow \det(N) \in (S^{-1}R)^*$, and $\det(N(x))$ is constant regarded as a function in x. Now let $M(x) \in GL_n((S^{-1}R)[x])$ be such that $f(x) = M(x)f(0)$. Then the expression $M(x)^{-1}f(x)$ is constant as a function in x, as $M(x)^{-1}f(x) = f(0)$, and is thus invariant under translation $x \mapsto x + y$. Consider now the matrix

$$G(x, y) = M(x)M(x + y)^{-1}. \tag{5.4}$$

Then $G(x, y)f(x + y) = M(x)f(0) = f(x)$. Also, we have $G(x, 0) = Id$, whence

$$G(x, y) = Id + yH(x, y), \tag{5.5}$$

where $H(x, y)$ has its coefficients in $(S^{-1}R)[x, y]$. R being an integral domain, clearly there exists $c \in S$ such that cH has its coefficients in $R[x, y]$ (the product of all the denominators, for example). Then $G(x, cy)$ also has its coefficients in $R[x, y]$. Since $\det(M(x))$ is constant in $S^{-1}R$, it follows that $\det(M(x + cy))$ is equal to this same constant and therefore that $\det(G(x, cy)) = 1$. Hence, there exists $G(x, cy) \in GL_n(R[x, y])$ with $G(x, cy)f(x + cy) = f(x)$, which proves the lemma. □

This lemma allows us to prove the equivalent of the Corollary 5.11 of the Horrock's Theorem for a general integral domain, our last but necessary step before proving the Quillen-Suslin Theorem:

Theorem 5.13. *Let R be an entire ring, and let f be a unimodular row in $R[x]^n$, such that one component has leading coefficient 1. Then $f(x) \sim f(0)$ over $R[x]$.*

Proof. Let J be the set of elements $c \in R$ such that $f(x + cy)$ is equivalent to $f(x)$ over $R[x, y]$. Lets see that J is an ideal:

- If $c \in J$ and $a \in R$, replacing y by ay in the definition of equivalence shows that $f(x + cay)$ is equivalent to $f(x)$ over $R[x, ay]$, and thus over $R[x, y]$ (as $R[x, ay] \subseteq R[x, y]$), so $ac \in J$.
- Analogously, if $c, c' \in J$, $f(x + (c + c')y)$ is equivalent to $f(x)$ over $R[x, (c + c')y]$, and thus over $R[x, y]$ (as $R[x, (c + c')y] \subseteq R[x, y]$), so $c + c' \in J$.

Now let $\mathfrak{p}$ be a prime ideal of R. By Corollary 5.11, we know that $f(x)$ is equivalent to $f(0)$ over $R_{\mathfrak{p}}[x]$, and by Lemma 5.12, it follows that there exists some $c \in R$ and $c \notin \mathfrak{p}$ such that $f(x + cy)$ is equivalent to $f(x)$ over $R[x, y]$. Hence J is not contained in $\mathfrak{p}$. Repeating this argument $\forall \mathfrak{p} \in Spec(R)$ shows that J is not contained in any maximal ideal, and is thus the total ideal R. Hence, $f(x + y)$ is equivalent to $f(x)$ over $R[x, y]$, so there exists an invertible matrix $M(x, y)$ over $R[x, y]$ such that

$$f(x + y) = M(x, y)f(x). \tag{5.6}$$

Since the homomorphic image of an invertible matrix is invertible, we have $M(y) = M(0, y) \in GL_n(R[y])$, and we can substitute x with a 0 in (5.6) to get

$$f(y) = M(y)f(0), \tag{5.7}$$

which concludes the proof of the theorem. □

We can now see how this last result, together with the arguments used in our proof of the Noether's Normalization Theorem in Chapter 1 (section 4, Theorem 1.19, Remark 1.20), allow us to prove our desired theorem:

Theorem 5.14. ***(Quillen-Suslin Theorem):*** *Let k be a field and let f be a unimodular row in $f[x_1, \ldots, x_r]^n$. Then f is completable.*

Proof. We proceed by induction on r. If $r = 1$, then we have $k[x_1]$, just one variable, and this case was proved in the first section of this chapter, Theorem 5.6.
Take now $f \in Um_n(k[x_1, \ldots x_n])$, and assume that the theorem holds for $r-1$ variables, with $r \geq 2$. We write

$$R = k[x_1, \ldots, x_{r-1}]$$

We may view f as a vector of polynomials in the last variable x_r, that is, over $R[x_r]$, and we want to apply Theorem 5.13. Note that we will be able to do so if some component of f has leading coefficient 1 in the variable x_r. We reduce the theorem to this case as follows. The proof of the Noether's Normalization Theorem (Theorem 1.19, Remark 1.20) shows that there exists a change of variables

$$y_r = x_r \qquad y_i = x_i - x_r^{m_i} \tag{5.8}$$

with certain m_i such that the polynomial vector g obtained by substitution

$$f(x_1, \ldots, x_r) = g(y_1, \ldots, y_r) \tag{5.9}$$

has one component with y_r-leading coefficient equal to 1. Now, by Theorem 5.13, there exists a matrix $N(y_1, \ldots, y_r)$ invertible over $R[y_r]$ such that

$$g(y_1, \ldots, y_r) = N(y_1, \ldots, y_r)g(y_1, \ldots, y_{r-1}, 0). \tag{5.10}$$

As $g(y_1, \ldots, y_{r-1}, 0)$ is clearly unimodular and in $k[y_1, \ldots, y_{r-1}]^{(n)}$, it can be completed to an invertible matrix by induction hypothesis. Doing this repeatedly concludes the proof by induction and we are done.

□

So, with all the results proved previously in this work, it is clear that we can restate Theorem 5.14 in more familiar words- particularly, in the way the Quillen-Suslin Theorem is usually formulated:

Let k be a field. Then every finitely generated projective module over the polynomial ring $k[x_1, \ldots, x_r]$ is free.

Chapter 6

Algorithms for the Quillen-Suslin Theorem

We have seen that the Quillen-Suslin Theorem has the rather satisfying consequence that every unimodular row f with its components in $k[x_1, \ldots, x_n]$ can be extended to an invertible matrix. Though in Chapter 5 (section 1, Theorem 5.6) we explained in detail an algorithm for doing so in the case of one variable $k[x]$, the proof of the general case in Chapter 5 (section 3) was not constructive at all. The goal of this chapter is to provide an algorithm for the general case with $k = \mathbb{C}$, that is, given $f \in Um_m(\mathbb{C}[x_1, \ldots, x_n])$, finding a way to extend it to an invertible matrix.

6.1 The paper by Logar and Sturmfels

The content of this chapter is extracted from a famous paper by A. Logar and B. Sturmfels called *Algorithms for the Quillen-Suslin Theorem*. This paper is quite ambitious: knowing, by the Quillen-Suslin Theorem, that projective modules over polynomial rings are free, they provide algorithms for computing such a free basis for an arbitrary projective module P over $R := \mathbb{C}[x_1, \ldots, x_n]$ given in one of the following three ways:

(1) as a cokernel, i.e. we have an explicit exact sequence

$$R^m \xrightarrow{A} R^l \to P \to 0$$

(2) as a column space, i.e. we have an explicit exact sequence

$$R^m \xrightarrow{A} P \to 0$$

(3) as a kernel of a $l \times m$-matrix A, i.e. we have

$$0 \to P \to R^m \xrightarrow{A} R^l$$

Like many articles dealing with algorithmic/ computational algebra, the paper relies heavily on Gröbner basis techniques, in the sense that many of the steps of these algorithms are thought to be carried out by using them- we recommend the reader who is unfamiliar with these to read the introductory but illustrative exposition written by Sturmfels himself [12], which provides a general idea on how do they work. Nonetheless, the tone of *Algorithms for the Quillen-Suslin Theorem* is kept general on the whole, and not many details are given on how to actually implement these techniques- the authors content themselves with only specifying when a certain step of the process can be accomplished using Gröbner basis, referring the reader to other papers where these particular techniques are more explicit and detailed.

Finally, the paper remarks how polynomial projective modules and the problem of extending certain matrices to invertible matrices appear in some branches of applied mathematics, and how these algorithms have a number of interesting potential applications, being control theory, the study of modules of splines (or piecewise polynomial functions) over polyhedral cell complexes and computational geometry some of them.

6.2 Extension of unimodular rows to invertible matrices

However, the algorithms for the three cases described above are complex and studying them here exceeds the aim of this chapter. Fortunately for us, a key subroutine for each of them is an algorithmic and constructive proof of the following theorem, also present in the paper, which should sound very familiar to us by now:

Theorem 6.1. ***(Unimodular row completion):*** *Let $f = (f_1, \dots, f_m) \in Um_m(\mathbb{C}[x_1, \dots, x_n])$. Then there exists an invertible $m \times m$-matrix U over $\mathbb{C}[x_1, \dots, x_n]$ such that $f \cdot U = e_1$.*

As U^{-1} has f as its first row, this is equivalent to giving a constructive way of extending f to an invertible matrix (computing U^{-1} afterwards), so the result is quite interesting on its own. The rest of this chapter will be devoted to understanding this algorithmic proof. In general terms, it proceeds by induction on the number n of variables, and it consists of two main parts. The first one is a "local loop" which generates solutions for finitely many suitable local rings. In the crucial second phase, it passes from the local to the global by, in some way, "patching together" the previously computed local solutions. In the spirit of the paper, we will be more interested in the procedure than in its implementation, so we shall just indicate with the upper index GB the steps that can be executed using Gröbner basis, without entering in many details if not necessary.

First, we remark that it is computationally "cheap" to test whether a given polynomial row is unimodular or not: as in this case the f_i generate the total ring, $(f_1, \dots, f_m)$ is unimodular iff the reduced Gröbner basis of the ideal $(f_1, \dots, f_m)$ is $\{1\}$. Also, the case $n = 1$ was solved in Chapter 5, section 1 (Theorem 5.6), and the case $m = 2$ is easy as well- we just have to compute^{GB} $h_1, h_2 \in \mathbb{C}[x_1, \dots, x_n]$ such that $h_1 f_1 + h_2 f_2 = 1$ and take $U = \begin{pmatrix} h_1 & -f_2 \\ h_2 & f_1 \end{pmatrix}$. For our proof with $n \geq 2$ and $m \geq 3$ we have to introduce two new tools,

being the first one a simple consequence of the Nullstellensatz, though we provide a much more straightforward proof:

Lemma 6.2. *If the ideal $(g_1, \ldots, g_r)$ generates the whole ring, the ideal $(g_1^n, \ldots, g_r^n)$ also generates the whole ring $\forall n \in \mathbb{N}$.*

Proof. As we have an expression like $\sum_{i=1}^r h_i g_i = 1$, also $(\sum_{i=1}^r h_i g_i)^{rn} = 1^{rn} = 1$, and expanding the sum in the left hand side all its terms contain at least one power g_i^n, so it can be rewritten in the form $\sum_{i=1}^r h_i' g_i^n = 1$ and our claim follows. □

Secondly, we state some properties of the **resultant** of two polynomials in several variables. For $f, g \in \mathbb{C}[x_1, \ldots, x_{n-1}][t]$, their resultant with respect to t is defined as the determinant of their Sylvester matrix (with respect to t). It is a polynomial in $k[x_1, \ldots, x_{n-1}]$, and it can be expressed as a linear combination of f and g. It satisfies $Res(f, g, t) = 0$ iff f, g have a common factor in $k[x_1, \ldots, x_{n-1}, t]$ which has positive degree in t.
In general, one has to be cautious with substituting $c \in \mathbb{C}[x_1, \ldots, x_{n-1}]$ before or after computing the determinant, as it can give different results. However, if c does not vanish the first coefficient of f, one has, for $h = Res(f, g, t) \in \mathbb{C}[x_1, \ldots, x_{n-1}]$:

$$h(c) = 0 \iff Res(f(c,t), g(c,t), t) = 0 \tag{6.1}$$

The observant reader will notice that the demonstration of the general case below is greatly inspired by the arguments presented in section 5.3, when we gave our non-constructive proof of the Quillen-Suslin Theorem and its necessary previous results:

Proof. (Theorem 6.1, algorithmic):
We will proceed by induction on the number n of variables. Assume that $n \geq 2$ and $m \geq 3$ and that we know how to find such a matrix for $n-1$ variables. Using Noether's Normalization Theorem^{GB} (Theorem 1.19, Remark 1.20), we can change variables and permute the f_i's in order to have $f_1(x_1, \ldots, x_{n-1}, t)$ monic in $t = x_n$. Now we abbreviate $R := \mathbb{C}[x]$, where $x = (x_1, \ldots, x_{n-1})$, and let $k := 0$.

At this point we enter the local loop. Let us discuss the first loop through it:
Set $k := k + 1 = 1$, take any $a_1 \in \mathbb{C}^{n-1}$ and let $M_1 := \{g \in R | \, g(a_1) = 0\}$. Note that M_1 is a maximal ideal of R. Now define $\bar{f}_i(t) := f_i(a_1, t)$ for $i = 1, \ldots, m$. Since $f(a_1, t) = (\bar{f}_1, \bar{f}_2, \ldots, \bar{f}_m)$ is clearly a unimodular row over $\mathbb{C}[t]$, we have

$$(p) + (\bar{f}_1) = \mathbb{C}[t], \tag{6.2}$$

where p generates the principal ideal $(\bar{f}_2, \ldots, \bar{f}_m)$ in $\mathbb{C}[t]$. Note that, as $p = gcd(\bar{f}_2, \ldots, \bar{f}_m)$, we can use the Euclidean algorithm (section 5.1, Theorem 5.6, Remark 5.7) to find it and also store the $(m-1) \times (m-1)$-matrix $E(t)$ over $\mathbb{C}[t]$ such that

$$(\bar{f}_2(t), \ldots, \bar{f}_m(t)) \cdot E(t) = (p(t), 0, \ldots, 0). \tag{6.3}$$

It follows from the definition of the $\bar{f}_i$ that $f_i(x,t) - \bar{f}_i(t) \in M_1[t]$. This and (6.3) imply

$$f(x,t) \cdot \begin{pmatrix} 1 & 0 \\ 0 & E(t) \end{pmatrix} = (f_1(x,t), p(t) + q_2(x,t), q_3(x,t), \ldots, q_m(x,t)) \tag{6.4}$$

with $q_2, \dots, q_m$ elements of $M_1[t]$ and $q_2(a_1, t) = 0$.

We next compute^{GB} the resultant $r_1(x)$ of the two polynomials f_1 and $p + q_2$ with respect to the variable t, and find^{GB} $v, w \in R[t]$ such that

$$v(x,t)f_1(x,t) + w(x,t)(p(t) + q_2(x,t)) = r_1(x) \tag{6.5}$$

As f_1 is monic in t, by (6.1) the resultant has the property that $r_1(x_0) = 0$ if and only if there exists $t_0 \in \mathbb{C}$ with $f_1(x_0, t_0) = p(t_0) + q_2(x_0, t_0) = 0$. In view of this observe that, if $r_1(a_1) = 0$, we would have $f_1(a_1, \bar{t}) = \bar{f}_1(\bar{t}) = 0 = p(\bar{t})$ for some $\bar{t} \in \mathbb{C}$, and any linear combination of p and $\bar{f}_1$ would be a multiple of $(t - \bar{t})$, in contradiction with (6.2), where we saw they generate $\mathbb{C}[t]$. This implies $r_1(a_1) \neq 0$, hence r_1 is a unit in the corresponding local ring $R_{M_1} = \{\frac{f}{g} | \, f, g \in R, g(a_1) \neq 0\}$ and we set $r_1^{-1} = \frac{1}{r_1}$. Now, note that the $m \times m$-matrix

$$U_1(x,t) := \begin{pmatrix} 1 & 0 \\ 0 & E(t) \end{pmatrix} \begin{pmatrix} vr_1^{-1} & -(p+q_2) & 0 & \dots & 0 \\ wr_1^{-1} & f_1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -q_3 & \dots & -q_m \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \tag{6.6}$$

is clearly invertible over $R_{M_k}[t]$ (the two matrices on the right have determinant 1, while the first one is invertible by construction) and, by (6.4), (6.5) and (6.6), we have

$$f(x,t) \cdot U_1(x,t) = (1, 0, \dots, 0) \tag{6.7}$$

Finally, if $r_1 \in \mathbb{C}$, we exit the local loop; if not, we return to its beginning.

How does the procedure change for the following iterations of the main loop? We could want to find (and store) more matrices $U_i(x,t)$, but certifying some extra conditions. Fortunately for us, the process is almost identical: the only changes are, if assume we have already gone through it k times and we set now $k := k + 1$,

1) At the beginning we must find^{GB} a common zero $a_k \in \mathbb{C}^{n-1}$ of the polynomials $r_1, r_2, \dots, r_{k-1}$ (remember that in the first iteration we took $a_1 \in \mathbb{C}$ arbitrary), and take $M_k := \{g \in R | \, g(a_k) = 0\}$, obviously maximal too.

2) At the end of the case $k = 1$, we exited the loop if $r_1 \in \mathbb{C}$. Now we have to check^{GB} whether the ideal $(r_1, \dots, r_k)$ is equal to the whole ring R. If yes, then we exit the local loop; if not, we return to its beginning and start the procedure all over again.

Observe that in each loop, also the first one, we test whether the $\{r_1, \dots, r_k\}$ generate the whole ring R. This is because, for the second part of our algorithm, we are really interested in obtaining an expression like (6.8). As $r_i(a_k) = 0 \quad \forall i < k$ and $r_k(a_k) \neq 0$, this guarantees $r_k \notin (r_1, \dots, r_{k-1})$ in each step, and the termination criterion "$(r_1, \dots, r_k) = R$" will be satisfied after a finite number of iterations by Hilbert's basis theorem. Then, for our

m = number of elements in the unimodular row, the powers $\{r_1^m, \ldots, r_k^m\}$ also generate the unit ideal in R by Lemma 6.2, and we can find^{GB} elements $g_1, \ldots, g_k \in R$ such that

$$g_1 r_1^m + g_2 r_2^m + \cdots + g_k r_k^m = 1 \text{ in } R. \tag{6.8}$$

We arrive now to the second part of the algorithm. In the following we abbreviate $U_i(t) := U_i(x,t)$. We introduce now two new variables s and z, and define the matrices

$$\Delta_i(s,z) := U_i(s) \cdot U_i^{-1}(s+z) \text{ for } i = 1, \ldots, k. \tag{6.9}$$

The matrix $\Delta_i(s,z)$ has entries in $R_{M_k}[s,z]$ and is clearly still invertible over this ring. Remember that the coefficients of the matrices $U_i(t)$ are fractions (they belong to $R_{M_k}[t]$) and, by construction, $r_i \in R$ is a common denominator for $U_i(s)$ and $U_i(s+z)$, as r_i is independent of the variable. The inverse of $U_i(s+z)$ equals its adjugate up to scalar, and thus simple computation shows that r_i^{m-1} is a common denominator for $U_i(s+z)$ and, in consequence, r_i^m is a common denominator for $\Delta_i(s,z)$.
Now expand $\Delta_i(s,z)$ as a polynomial in z with matrix coefficients over $R_{M_k}[s]$:

$$\Delta_i(s,z) = \Delta_{i0}(s) + \Delta_{i1}(s)z + \Delta_{i2}(s)z^2 + \cdots + \Delta_{id_i}(s)z^{d_i}. \tag{6.10}$$

It follows directly from (6.9) and (6.10) that $\Delta_{i0}(s) = \Delta_i(s,0)$ equals the identity matrix I_m. Replacing z by zr_i^m we get

$$\Delta_i(s, zr_i^m) = I_m + r_i^m \Delta_{i1}(s)z + r_i^{2m}\Delta_{i2}(s)z^2 + \cdots + r_i^{d_i m}\Delta_{id_1}(s)z^{d_i}. \tag{6.11}$$

Since r_i^m is a common denominator for $\Delta_i(s,z)$, it is a common denominator for all the summands in the expansion (6.10). Hence all summands on the right hand side of (6.11) are denominator-free, and $\Delta_i(s, zr_i^m)$ is an invertible matrix over the *polynomial* ring $R[s,z]$. Observe furthermore that, having in mind (6.7) and (6.9), we have

$$f(s) \cdot \Delta_i(s, zr_i^m) = f(s + zr_i^m) \text{ in } R[s,z]. \tag{6.12}$$

Finally, define

$$U(t) := \Delta_1(t, -tg_1 r_1^m) \cdot \Delta_2(t - tg_1 r_1^m, -tg_2 r_2^m) \cdot \Delta_3(t - tg_1 r_1^m - tg_2 r_2^m, -tg_3 r_3^m) \cdot \\ \ldots \cdot \Delta_k(t - \sum_{i=1}^{k-1} tg_i r_i^m, -tg_k r_k^m), \tag{6.13}$$

where the g_i are the polynomials of the expression (6.8). These matrices in (6.13) are obtained from $\Delta_i(s, zr_i^m)$ by polynomial specializations $R[s,z] \to R[t]$, so they are all invertible over $R[t]$ and, consequently, $U(t)$ is invertible over $R[t]$. By repeated application of (6.12) and in light of the expression (6.8), we get

$$f(t) \cdot U(t) = f(t - \textstyle\sum_{i=1}^{k} tg_i r_i^m) = f(0).$$

Now, the row $f(0) \in R^m = \mathbb{C}[x_1, \ldots, x_{n-1}]^m$ is unimodular in $n-1$ variables. By induction on the number of variables, the algorithm can be carried out reducing all the variables and our constructive proof of Theorem 6.1 is done. □

Appendix A

Basic concepts and definitions

The following notions are fundamental in modern algebra and will appear constantly throughout the whole text. The results will be stated without proof:

A.1 Modules

Modules are 'vector spaces over rings', i.e., the concept of a module generalizes that of a vector space, replacing the underlying field by a general ring:

Definition A.1. *Let R be a (non necessarily commutative) ring. A **left** R**-module** M is an abelian group (always written additively) together with a map $R \times M \to M$, $(a, x) \mapsto ax$ (the scalar multiplication) satisfying:*

1. $a(x + y) = ax + ay$, $\forall a \in R, \forall x, y \in M$
2. $(a + b)x = ax + ay$, $\forall a, b \in R, \forall x \in M$
3. $(ab)x = a(bx)$, $\forall a, b \in R, \forall x \in M$
4. $1_R x = x$, $\forall x \in M$, *where* 1_R *is the multiplicative identity in* R

Remark A.2. *A **right** R-module is defined nearly the same way, but with 'scalars' operating on the right side, so we write xa instead of ax, where $a \in R$ and $x \in M$, in the conditions above. The only remarkable change is in* 3), *where we would obtain* 3′) $(ab)x = b(ax)$, $\forall a, b \in R, \forall x \in M$ *(with the right side notation, $x(ab) = (xa)b$, the usual associative law).*

Remark A.3. *The distinction between left and right modules is necessary if we don't assume R to be commutative. However, over commutative rings, there is no difference between both definitions, and we simply call them R-modules (our case).*

From now on R will denote a commutative unitary ring.
In the same spirit as for vector spaces, we can define for any module M the natural concepts of a **submodule**, **generating set** and **linear independence**.

Definition A.4. *If U is a submodule of an R-module M, then the factor group M/U is also an R-module, namely the **factor module** M **module** U. If $x \in M$ and $\bar{z}$ denotes the residue class of any $z \in M$, then $a\bar{x} = \bar{ax}$, which is well defined.*

Also:

Definition A.5. *We say that an R-module M is finitely generated if there exist $m_1, \ldots, m_n \in M$ such that for any $x \in M$, there exist $a_1, \ldots, a_n \in R$ with $x = a_1 m_1 + \cdots + a_n m_n$.*

However, in contrast with vector spaces, modules do not necessarily have a **basis**, that is, a linearly independent set of generators. This motivates the notion of a free module:

Definition A.6. *We say that an R-module F is **free** if it admits a basis. In this case, if E is a basis of F, then every element $f \in F$ can be written uniquely as*

$$\sum_{e \in E} a_e e,\ a_e \in R,\ a_e = 0 \text{ for almost all } a_e \text{ (i.e. all except a finite number of them)},$$

*and F is isomorphic (*Definition A.10*) to $R^{(E)}$ (direct sum of $|E|$ copies of R).*

Finally:

Definition A.7. *Let $(M_i)_{i \in I}$ be a family of modules, not necessarily finite.*

- *Their **direct sum**, written*
$$\bigoplus_{i \in I} M_i$$
is defined to be those families $(x_i)_{i \in I}$ where $x_i = 0$ for all but finitely many $i \in I$.
- *Their **direct product**, written*
$$\prod_{i \in I} M_i$$
*is defined to be **all** families $(x_i)_{i \in I}$.*
- *Let I be some set and M a module. Then*
$$M^{(I)} := \bigoplus_{i \in I} M_i \quad \text{and} \quad M^I := \prod_{i \in I} M_i, \quad \text{where } M_i = M \quad \forall i \in I$$

Remark A.8. *Both the direct sum and the direct product of R-modules have an obvious structure of R-module. Also, for I finite, the two definitions coincide.*

A.2 Module homomorphisms

Homomorphisms of modules, i.e. linear maps, are defined as for vector spaces:

Definition A.9. *Let M and N be R-modules. A map $f : M \to N$ is called an R-**module homomorphism** or R-**linear** if:*

$$f(x+y) = f(x) + f(y), \quad f(ax) = af(x),$$

where $x, y \in M$ and $a \in R$.

The concepts of **mono/ epi/ iso /endo /automorphism** between modules are defined in the obvious way. In this sense:

Definition A.10. *M and N are isomorphic ($M \cong N$) if there is an isomorphism $f : M \to N$. In this case, there exists an isomorphism $f^{-1} : N \to M$ such that $f^{-1} \circ f = id_M$, $f \circ f^{-1} = id_N$.*

It's easy to see that:

Proposition A.11. *Given a R-module homomorphism $f : M \to N$, $\mathrm{Ker}(f)$ and $\mathrm{Im}(f)$ (naturally defined) are submodules of M and N, respectively.*

The usual Homomorphism Theorem and Isomorphism Theorems hold. We state the first one, commonly used in our text:

Theorem A.12. ***(Homomorphism Theorem):*** *Let $f : M \to N$ be a module homomorphism and $U \subset \mathrm{Ker}(f)$ a submodule. Then f factorizes through the canonical map $\pi : M \to M/U$, i.e. f is the composition of linear maps*

$$M \xrightarrow{\pi} M/U \xrightarrow{f'} N$$

*where f' is (well-)defined by $f'(\bar{x}) = f(x)$ (we say f' is **induced** by f). Especially, f induces an isomorphism $M/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$.*

At this stage:

Proposition A.13. *Let M, N be R-modules. The set of all R-module homomorphisms from M to N, denoted by $\mathrm{Hom}_R(M, N)$, is an abelian group, addition defined by $(f+g)(x) := f(x) + g(x)$.*

Moreover, if R is commutative, $\mathrm{Hom}_R(M, N)$ has the structure of an R-module: $(af)(x) := af(x)$. (Caution: in the case R is not commutative, the earlier map is not always R-linear).

Remark A.14. *$\mathrm{Hom}_R(R^m, R^n)$ can be identified with the additive group of all $m \times n$-matrices with entries in R, addition defined componentwise.*

Finally, "chains" and commutative diagrams of modules and homomorphisms will appear a lot. We state now some definitions involving them and a very famous result:

Definition A.15. *Let $(M_i)_{i \in I}$ be a (not necessarily finite) family of modules.*

- *A sequence of linear maps between the M_i*

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

  *such that $\mathrm{Im}(f_{n+1}) \subset \mathrm{Ker}(f_n)\ \forall n$ is called a **complex of modules**.*

- *When we have the equality $\mathrm{Im}(f_{n+1}) = \mathrm{Ker}(f_n)\ \forall n$, we call the complex an **exact sequence**.*

- *An exact sequence of the form $0 \to M \xrightarrow{f} N \xrightarrow{g} L \to 0$ is called a **short exact sequence**. Here exactness means: f is injective, g is surjective and $\mathrm{Im}(f) = \mathrm{Ker}(g)$.*

Lemma A.16. ***(The Five Lemma):*** *Suppose we have the following commutative diagram of modules and homomorphisms, where the rows are exact*

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \downarrow{\scriptstyle \varphi_4} & & \downarrow{\scriptstyle \varphi_5} \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5 \end{array}$$

Then:
1. *If φ_2, φ_4 are injective and φ_1 surjective $\implies$ φ_3 is injective.*
2. *If φ_2, φ_4 are surjective and φ_5 injective $\implies$ φ_3 is surjective.*
3. *If φ_2, φ_4 are isomorphisms, φ_1 is surjective and φ_5 is injective $\implies$ φ_3 is an isomorphism.*

A.3 Noetherianity

Noetherian rings and modules play a huge role in commutative algebra and in this work, as polynomial rings with a finite number of variables are Noetherian:

Definition A.17. *We say that a ring R is Noetherian if it satisfies the ascending chain condition. That is, every chain of ideals $\{I_i\}_{i\in\mathbb{N}}$ with $I_i \subseteq I_{i+1}$ eventually stabilizes ($\exists I_n$ tq $I_i = I_n \forall i \geq n$).*

Remark A.18. *It is not hard to show that this is equivalent to the fact that every ideal of R is finitely generated.*

Remark A.19. *One can see easily that any field k is Noetherian, as it only has two ideals, the zero ideal and the total ideal.*

This is probably the most famous result involving them:

Theorem A.20. ***(Hilbert's Basis Theorem):*** *If R is a Noetherian ring and x a variable, then $R[x]$ is a Noetherian ring.*

Corollary A.21. *If k is a field, then $k[x_1, \ldots, x_n]$ is a Noetherian ring.*

The concept of Noetherianity can be generalized in a natural way to modules:

Definition A.22. *For a commutative ring R, we say that a R-module M is Noetherian if it satisfies that every chain of submodules $\{M_i\}_{i\in\mathbb{N}}$ with $M_i \subseteq M$ and $M_i \subseteq M_{i+1}$ eventually stabilizes.*

Remark A.23. *Again, this is equivalent to the fact that every R-submodule of M, M itself included, is finitely generated.*

Remark A.24. *It follows that if $f : M \to N$ is an homomorphism between Noetherian modules, $\mathrm{Ker}(f)$ and $\mathrm{Im}(f)$ are again Noetherian modules and thus finitely generated.*

Finally, this proposition and its consequence will be used extensively in our work:

Proposition A.25. *If R is a Noetherian commutative ring and M a finitely generated R-module, then M is Noetherian.*

Remark A.26. *The proposition above shows that every finitely generated projective or stably free $k[x_1, \ldots, x_n]$-module is Noetherian.*

Appendix B

Proof of Proposition 2.14

This appendix has the purpose of providing a comprehensive proof of the interesting Proposition 2.14, stated in the second section of Chapter 2. The demonstration exposed here is mainly extracted from the famous book *Algèbre Commutative* by Bourbaki.

In its full generality, the Proposition says:

Proposition B.1. *Suppose a finitely generated R-module P satisfies:*

(i) $P_{\mathfrak{p}}$ *is* $R_{\mathfrak{p}}$*-free* $\forall \mathfrak{p} \in Spec(R)$.

(ii) With $r_{\mathfrak{p}} := rank_{R_{\mathfrak{p}}}(P_{\mathfrak{p}})$*, the function* $\mathfrak{p} \mapsto r_{\mathfrak{p}}$ *is locally constant in the topological space* $Spec(R)$ *(every point of* $Spec(R)$ *admits a neighbourhood in which this function is constant).*

Then P is a finitely generated projective R-module.

As it was anticipated in Chapter 2, its proof is difficult, but delightful. Although we will expose many of the previous notions and results necessary to fully understand it, the most elementary/ standard ones will be left out and just stated below due to lack of space. Thus, we will assume that the reader is at least familiar with these well-known facts:

- An R-module M is projective iff $\mathrm{Hom}_R(M, -)$ is exact (section 2.1).
- For any R-module M, the functor $\mathrm{Hom}_R(M, -)$ is left-exact if and only if the original sequence is exact.
- The functor of localization commutes with finite direct sums (Lemma 2.11)
- A complex being exact is a local property- that is, $N' \to N \to N''$ is exact if and only if $N'_{\mathfrak{p}} \to N_{\mathfrak{p}} \to N''_{\mathfrak{p}}$ is exact $\forall \mathfrak{p} \in Spec(R)$.
- An R-morphism being injective/ surjective/ bijective is also a local property- that is, $u : M \to N$ is a mono/epi/isomorphism iff $u_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_p$ is $\forall \mathfrak{p} \in Spec(R)$.
- For M an R-module, $S^{-1}M = 0 \iff S \cap Ann_R(M) \neq \emptyset$
- With M and N R-free modules and $u : M \to N$ an homomorphism, u is an isomorphism $\Leftrightarrow$ M and N have the same rank and u is surjective ($\sim$ Proposition 3.5).
- The basic properties of the Zariski topology in $Spec(R)$.

We start with what it means for a R-module to be finitely presented:

Definition B.2. *We say that an R-module M is **finitely presented** if there exists an exact sequence $R^m \to R^n \to M \to 0$, for suitable natural numbers m and n.*

Intuitively, a finitely presented module is a finitely generated module with a finite number of relations on some generating set. It is immediate that a projective R-module P is finitely generated iff it is finitely presented. One direction is trivial, while the other can be deduced from the the split R-morphism $R^n \twoheadrightarrow \mathrm{Ker}(\varphi)$, where $\varphi : R^n \twoheadrightarrow P$.

Now, Lemma B.4 shows us that, in some way, Hom and localization commute with each other in the case M is finitely presented, but first:

Remark B.3. *For a R-module M, any R-linear morphism $\varphi : R \to M$ is completely determined by $\varphi(1)$, thus* $\mathrm{Hom}(R, M) \cong M$.

Lemma B.4. *Let M be a finitely presented R-module and N a R-module. Then, for a multiplicatively closed subset S of R we have*

$$S^{-1}\,\mathrm{Hom}_R(M, N) \cong \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) \tag{B.1}$$

Proof. Take a presentation $R^m \to R^n \to M \to 0$. This yields an exact sequence $0 \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(R^n, N) \to \mathrm{Hom}_R(R^m, N)$ and, using Remark B.3 and Lemma 2.11, we have $\mathrm{Hom}_R(R^n, N) \cong \oplus_{i=0}^n N$, so we obtain the exact sequence

$$0 \to \mathrm{Hom}_R(M, N) \to \oplus_{i=0}^n N \to \oplus_{i=0}^m N \tag{B.2}$$

and applying the exact functor of localization, we obtain

$$\begin{aligned} 0 \to S^{-1}\,\mathrm{Hom}_R(M, N) \to S^{-1}(\oplus_{i=0}^n N) \to S^{-1}(\oplus_{i=0}^m N) \\ = 0 \to S^{-1}\,\mathrm{Hom}_R(M, N) \to \oplus_{i=0}^n S^{-1}N \to \oplus_{i=0}^m S^{-1}N \end{aligned} \tag{B.3}$$

In parallel, applying first S^{-1} to the finite presentation and then Hom, we obtain

$$0 \to \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) \to \oplus_{i=0}^n S^{-1}N \to \oplus_{i=0}^m S^{-1}N \tag{B.4}$$

and, as the last $S^{-1}R$-morphism in both exact sequences (B.3) and (B.4) is the same, by exactness the first $S^{-1}R$-module of both sequences is its kernel and we have that $S^{-1}\,\mathrm{Hom}_R(M, N)$ and $\mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$ are isomorphic as $S^{-1}R$-modules. □

In section 1.2 we only explained localization at a prime $\mathfrak{p}$, as it is the only one we use in the main exposition, but there obviously exist plenty of other multiplicatively closed subsets not of the form $R\backslash\mathfrak{p}$. For example, one could consider what is called the **localization at** f, constructed by taking $S_f = \{f^n, n \in \mathbb{N}\}$, which is obviously multiplicatively closed, with $f^0 = 1$. This kind of localization will be crucial in the following.

Recall that the Zarisky topology is defined on $Spec(R)$ as the one for which its closed sets are given by $V(I) = \{\mathfrak{p} \in Spec(R) | \mathfrak{p} \supseteq I, I \subseteq R \text{ ideal}\}$. Thus, a basis of open sets is given by the sets

$$D(f) = \{p \in Spec(R) | f \notin \mathfrak{p}, f \in R\}, \tag{B.5}$$

Remark B.5. *Note that the Zariski topology on $Spec(R)$ is always quasi-compact- that is, every open covering of $Spec(R)$ contains a finite open subcovering of it: if one takes a family of basic open sets $D(f_\alpha)$ covering $Spec(R)$, the family f_α must then generate the unit ideal, and so a finite number of these generate R.*

Proposition B.6. *Suppose we have $f_1, \dots, f_n \in Spec(R)$ such that $Spec(R) = \cup_{i=1}^n D(f_i)$ and $0 \to N' \to N \to N'' \to 0$ a complex of R-modules. Then, if $0 \to N'_{f_i} \to N'_{f_i} \to N'_{f_i} \to 0$ is exact for all f_i, $0 \to N' \to N \to N'' \to 0$ is exact.*

Proof. Note that the hypothesis $Spec(R) = \cup_{i=1}^n D(f_i)$ implies that every $\mathfrak{p} \in Spec(R)$ is contained in some $D(f_i)$, so $f_i \notin \mathfrak{p}$ and $S_{f_i} \subseteq R \backslash \mathfrak{p}$. As localization is an exact functor, the complex being exact at each S_{f_i} implies that, localizing further, the induced sequence $0 \to N'_\mathfrak{p} \to N_\mathfrak{p} \to N''_\mathfrak{p} \to 0$ is exact for all $\mathfrak{p} \in Spec(R)$ and, as being exact is a local property, the claim follows. □

Our final previous result is Lemma B.7, quite straightforward:

Lemma B.7. *Let M and N be R-modules such that N is finitely generated. Let $u : M \to N$ be an R-morphism and $\mathfrak{p} \in Spec(R)$. Then, if $u_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ is surjective, there exists $f \in R \backslash \mathfrak{p}$ such that $u_f : M_f \to N_f$ is surjective.*

Proof. Take Q the cokernel of u. As localization is exact, for any $g \in R$ the cokernel of u_g (resp. $u_\mathfrak{p}$) is Q_g (resp. $Q_\mathfrak{p}$), so by hypothesis $Q_\mathfrak{p} = 0$. As N is finitely generated, Q is finitely generated, which implies that there exists some $f \in R \backslash \mathfrak{p}$ such that $fQ = 0$ and so $Q_f = 0$, proving that u_f is surjective. □

All this being said, we can finally prove Proposition B.1. We will divide its complex proof in two steps, Propositions B.8 and B.9. In the first one, more technical, we kind of "reduce" the problem to a finite family of $f_i \in R$ whose associated open sets in the Zarisky topology cover all $Spec(R)$. In the second one, we make use of this powerful setting to finally prove our assertion.

Proposition B.8. *Under the hypotheses of Proposition B.1, there exists a finite family $f_1, \dots, f_n \in R$ generating the unit ideal such that P_{f_i} is R_{f_i}-free of finite rank $\forall i$.*

Proof. Let $\mathfrak{m}$ be a maximal ideal of R; write $r_\mathfrak{m} = n$ and let $\{x_i\}_{1 \leq i \leq n}$ be a $R_\mathfrak{m}$-basis of $P_\mathfrak{m}$. Multiplying them by invertible elements of $R_\mathfrak{m}$ if necessary, we can assume the x_i are canonical images of elements $p_i \in P$, the p_i forming thus a finite generating set for P. Now let $\{e_i\}_{1 \leq i \leq n}$ be the canonical basis of R^n and $u : R^n \to P$ the homomorphism such that $u(e_i) = p_i$ for $1 \leq i \leq n$. As u_m is clearly surjective and P is finitely generated, it follows from Lemma B.7 that there exists $f \in R \backslash \mathfrak{m}$ such that $u_f : R^n_f \to P_f$ is surjective. Now, it is clear that $u_{fg} = (u_f)_{\frac{g}{1}}$ is also surjective for all $g \in R \backslash \mathfrak{m}$ and, as the rank is locally constant, there exists $g \in R \backslash \mathfrak{m}$ satisfying $r_\mathfrak{p} = n$ for $\mathfrak{p} \in D(g)$. Thus, replacing f by fg, $f := fg$, we may assume that $r_\mathfrak{p} = n \ \forall \mathfrak{p} \in D(f)$.
In this context, $u_p : R^n_p \to P_\mathfrak{p}$ is a surjective $R_\mathfrak{p}$-morphism and $P_\mathfrak{p}$ and $R_\mathfrak{p}$ are both free R_p-modules of the same rank, which implies $u_\mathfrak{p}$ is bijective for all $\mathfrak{p} \in D(f)$. Now let $\mathfrak{p}'$ be any prime ideal of R_f and let $\mathfrak{p}$ be its inverse image in R under the canonical mapping $R \to R_f$; this way, $(R^n_f)_{\mathfrak{p}'}$ and $(P_f)_\mathfrak{p}$ may be identified with $R^n_\mathfrak{p}$ and $P_\mathfrak{p}$ localizing further (under the

canonical isomorphisms), and so $(u_f)_{\mathfrak{p}'}$ is identified with u_p and is consequently bijective. As this is valid for all prime ideals in R_f and being bijective is a local property, u_f is thus bijective and P_f is a free R_f-module of finite rank.

The whole argument above holds for any maximal ideal in R, so we have that $\forall \mathfrak{m} \in Max(R)$, there exists $f \in R \backslash \mathfrak{m}$ such that P_f is a free R_f-module of finite rank.
If we consider now $E = \{f \in R |\, P_f$ is a finitely generated free R_f-module$\}$, the previous argument shows that E is not contained in any maximal ideal of R, hence E generates the whole ring R so, by Remark B.5, there exists a finite family $\{f_i\}_{1 \leq i \leq n}$ of elements of E and $a_i \in R$ such that $\sum_{i=1}^{n} a_i f_i = 1$, which concludes the proposition.

□

Finally,

Proposition B.9. *If $f_1, \ldots, f_n \in R$ is a family like the one in Proposition B.8, then P is a finitely generated projective module.*

We just have to show that $\mathrm{Hom}_R(P, -)$ is exact. Let $0 \to N' \to N \to N'' \to 0$ be any short exact sequence of R-modules. By hypothesis, there exist $f_1, \ldots, f_n$ such that $Spec(R) = \cup_{i=1}^{n} D(f_i)$ and P_{f_i} is R_{f_i}-free of finite rank. Now, as localization is exact, we have

$$0 \to N'_{f_i} \to N_{f_i} \to N''_{f_i} \to 0 \tag{B.6}$$

exact $\forall f_i$, and as P_{f_i} is R_{f_i}-free and thus projective for all f_i, we obtain a short exact sequence

$$0 \to \mathrm{Hom}_{R_{f_i}}(P_{f_i}, N'_{f_i}) \to \mathrm{Hom}_{R_{f_i}}(P_{f_i}, N_{f_i}) \to \mathrm{Hom}_{R_{f_i}}(P_{f_i}, N''_{f_i}) \to 0 \tag{B.7}$$

$\forall f_i$. By Lemma B.4, the exact sequence of (B.7) is equivalent to an exact sequence

$$0 \to \mathrm{Hom}_R(P, N')_{f_i} \to \mathrm{Hom}_R(P, N)_{f_i} \to \mathrm{Hom}_R(P, N'')_{f_i} \to 0 \tag{B.8}$$

$\forall f_i$. Finally, applying Proposition B.6, we obtain that

$$0 \to \mathrm{Hom}_R(P, N') \to \mathrm{Hom}_R(P, N) \to \mathrm{Hom}_R(P, N'') \to 0 \tag{B.9}$$

is exact and thus P is projective, which concludes the proof of Proposition B.9 and Proposition B.1 at once.

Bibliography

[1] A. Altman and S. Kleiman, *A term of Commutative Algebra*, Preprint September 2012.

[2] M. F. Atiyah and I.G. Macdonald, *Introducción al álgebra conmutativa*, Editorial Reverté S.A., (1973), chapters 1–7.

[3] N. Bourbaki, *Commutative Algebra*, Addison-Wesley, (1972), 109–111.

[4] D. Cox, J. Little and D. O'Shea, *Ideals, varieties and algorithms*, Springer-Verlag New York Heidelberg, Undergraduate Texts in Mathematics, (2007), 150–164.

[5] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag New York Heidelberg, Graduate Texts in Mathematics **52**, (1977), chapter 2.

[6] F. Ischebeck and R. Rao, *Ideals and Reality*, Springer-Verlag Berlin Heidelberg, Springer Monographs in Mathematics, (2005), chapters 1–5.

[7] T.Y. Lam, *Serre's Problem on Projective Modules*, Springer-Verlag Berlin Heidelberg, Springer Monographs in Mathematics, (2006), chapters 1–3.

[8] S. Lang, *Algebra*, Springer-Verlag New York, Graduate Texts in Mathematics, (2002), 357, 839–850.

[9] A. Logar and B. Sturmfels, *Algorithms for the Quillen-Suslin Theorem*, Journal of Algebra **145** (1992), 231–239.

[10] J. Rotman, *An Introduction to Homological Algebra*, Springer-Verlag New York, Graduate Texts in Mathematics, (2009), chapters 2–4.

[11] J.P. Serre, *Faisceaux algèbriques cohérents*, Annals of Mathematics **61** (1955), 197–278.

[12] B. Sturmfels, *What Is... a Gröbner Basis?*, Notices of the AMS, Vol. **52** (2005), Num. 10.