Serre's Conjecture on Projective Modules *

Debapriyo Majumdar
Chennai Mathematical Institute
e-mail: deb@cmi.ac.in

Abstract: In this text we will give a sketch of a proof of Serre's theorem on Projective modules, i.e. any finitely generated projective module M over the polynomial ring $K[x_1, \cdots, x_n]$ of a principal ideal domain K is free. By Horrocks' theorem, we have that for a local ring R, if there is a monic polynomial $f \in R[x]$ such that M_f is a free $R[x]_f$ module, then M is a free $R[x]$ module. The Quillen-Suslin theorem generalizes Horrocks theorem for any ring R, dropping the condition that R is local. Serre's conjecture is proved using this theorem.

Any ring here will mean a commutative ring with identity and usually will be denoted by R. Unless otherwise stated, M will denote an R module. $\mathrm{Max}(R)$ and $\mathrm{Spec}(R)$ will denote the sets of all maximal and prime ideals of R respectively.

1 Elementary Definitions and Results

Definition Let R be a ring. For a prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$, the *height* $h(\mathfrak{p})$ of $\mathfrak{p}$ is defined as the supremum of the lengths n of all chains of prime ideals of the form

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}.$$

It will be useful to note the following facts [AM] regarding height of a prime ideal.

Fact 1 *If K is a field, then every prime ideal in $K[x_1, x_2, \cdots, x_n]$ has height $\leq n$.*

Fact 2 *In a unique factorization domain R, the prime ideals of height 1 are precisely the principal ideals generated by prime elements.*

Definition Let M be an R module. The *presentation* of M belonging to a system of generators $\{m_\lambda\}_{\lambda \in \Lambda}$ of M is the exact sequence of R modules

$$0 \to K \to R^\Lambda \stackrel{\alpha}{\to} M \to 0$$

where α maps the canonical basis element e_λ of R^Λ to m_λ. The R module K is called the *module of relations* of the generating system $\{m_\lambda\}_{\lambda \in \Lambda}$. An element of K is called a *relation.*

*A note based on a reading course taken by the author during his visit to École Normale Supérieure (ENS), in the months of May and June 2001, as a part of an exchange programme between Chennai Mathematical Institute (CMI) and ENS. The work was carried out under the guidance of Prof. François Loeser, DMA, ENS.

Definition An R module M is called *finitely presentable* if there is an $n \in \mathbb{N}$ and an exact sequence of R modules

$$0 \to K \to R^n \to M \to 0$$

where K is finitely generated.

Definition A *projective module* is a direct summand of a free module.

Proposition 3 *Let M be an R module, P and Q be submodules of M. Then $P = Q$ iff $P_{\mathfrak{m}} = Q_{\mathfrak{m}}$ for all $\mathfrak{m} \in \mathrm{Max}(R)$.*

Proof. [Kunz]: p 93.

Theorem 4 *Let R be any ring and let $f, g \in R$ such that $D(f) \cup D(g) = \mathrm{Spec}(R)$ (For an ideal $I \subset R$, by $D(I)$ we denote the set of all prime ideals $\mathfrak{p} \in \mathrm{Spec}(R)$ which do not contain I. For an element $f \in R$, $D(f)$ is the set of all $\mathfrak{p} \in \mathrm{Spec}(R)$ such that $f \notin \mathfrak{p}$). Let M be an R module. If M_f is a finitely presentable R_f module and M_g is a finitely presentable R_g module then M is a finitely presentable R module.*

Proof. [Kunz]: p 97.

Definition For an R module N we call the $R[x]$ module $R[x] \otimes_R N$ the *extension module* of N to $R[x]$ and denote it by $N[x]$. The module $N[x]$ can be identified with the set of all polynomials $n_0 + xn_1 + \cdots + x^d n_d$ with coefficients $n_i \in N$. An $R[x]$ module M is called *extended* (from R) if there is an R module N such that $M \cong N[x]$ as $R[x]$ modules and M is called *locally extended* at a maximal ideal $\mathfrak{m} \in \mathrm{Max}(R)$ if the $R_{\mathfrak{m}}[x]$ module $M_{\mathfrak{m}}$ is extended from $R_{\mathfrak{m}}$.

Note that if $M \cong N[x]$ then $N \cong M/xM$ as R modules.

Theorem 5 (Quillen) *A finitely presentable $R[x]$ module M is extended if and only if it is locally extended at all $\mathfrak{m} \in \mathrm{Max}(R)$.*

Proof. [Kunz]: p 101.

Theorem 6 *Let R be a local ring with maximal ideal $\mathfrak{m}$ and P be a finitely presentable R module. Then P is free iff there is an exact sequence of R modules $0 \to F \overset{\alpha}{\to} M \to P \to 0$ where M is projective and the mapping $F/\mathfrak{m}F \to M/\mathfrak{m}M$ induced by α is an injection.*

Proof. [Kunz]: p 111.

Theorem 7 *A finitely generated module over any ring R is projective iff it is finitely presentable and locally free.*

Proof. [Lam]: p 15, [Kunz]: p 113.

Proposition 8 *Let M be a finitely generated projective R module and $\mathfrak{p} \in \mathrm{Spec}(R)$ such that $M_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$ module. Then there exists $f \in R \setminus \mathfrak{p}$ such that M_f is a free R_f module.*

Proof. [Kunz]: p 113.

2 The Passage from Local to Global

Theorem 9 (Horrocks: 1964) *Let R be a local ring. If M is a finitely generated projective $R[x]$ module and there exists a monic polynomial $f \in R[x]$ such that M_f is a free $R[x]_f$ module then M is a free $R[x]$ module.*

Proof. We choose a basis $\mathcal{B}$ of M_f consisting of elements of M and let F denote the submodule of M spanned by $\mathcal{B}$. Define $P = M/F$.

Claim 1 *The R module P is finitely presentable.*

Proof of Claim 1. Clearly $P_f = 0$ and hence there is a positive integer n such that $f^n P = 0$. Hence we have

$$P \cong \frac{M/F}{f^n(M/F)} \cong \frac{M/f^n M}{(F + f^n M)/f^n M}$$

Now, $M/f^n M$ is a finitely generated projective module over $S = R[x]/f^n$. Since f is monic, S is a free R module of finite rank and so is $M/f^n M$. Since $(F + f^n M)/f^n M$ is also finitely generated as an R module, $P = M/F$ is finitely presentable. □

Claim 2 *For R modules M, P and F, $M \cong P \oplus F$.*

Proof of Claim 2. Let $\mathfrak{m}$ be the maximal ideal of the local ring R and let $\overline{f}$ denote the image of f in $R/\mathfrak{m}[x]$. Then $(F/\mathfrak{m}F)_{\overline{f}} = (M/\mathfrak{m}M)_{\overline{f}}$. So the canonical mapping $F/\mathfrak{m}F \to M/\mathfrak{m}M$ is injective. Since $R[x]$ is free as an R module, M is projective as an R module too. So, applying Theorem 6 to the exact sequence $0 \to F \to M \to P \to 0$ we see that P is free as an R module and $M \cong P \oplus F$ as R modules. □

We will show that F can be enlarged and P can be made smaller so that P becomes zero and then we'll be done.

Let $p_1, \cdots, p_s \in M$ be representative for a basis of the R module P and let $\{p_{s+1}, \cdots, p_t\}$ be an $R[x]$ basis of F. If $s = 0$ we are done. So, let us assume that $s > 0$. Then, for $1 \leq k \leq s$ we have the equations:

$$-xp_k = \sum_{i=1}^{s} \alpha_{ki} p_i + \sum_{j=s+1}^{t} b_{kj} p_j \tag{1}$$

where $\alpha_{ki} \in R, b_{kj} \in R[x]$. If M is not free, by this equation 1, any relation for M the form

$$\sum_{i=1}^{s} a_i p_i + \sum_{j=s+1}^{t} b_j p_j = 0, a_i, b_j \in R[x]$$

can be reduced to a relation of the form

$$\sum_{i=1}^{s} \alpha_i p_i + \sum_{j=s+1}^{t} \tilde{b}_j p_j = 0$$

for $\alpha_i \in R, \tilde{b}_j \in R[x]$. Since $M \cong P \oplus F$, it follows that $\alpha_i = \tilde{b}_j = 0$ for $1 \leq i \leq s$ and $s+1 \leq j \leq t$. Therefore, with respect to the generating system $\{p_1, \cdots, p_t\}$ the $R[x]$ module M has a relation matrix of the form

$$(A + xI_s|B) \quad A = (\alpha_{ki}), \alpha_{ki} \in R, B = (b_{kj}), b_{kj} \in R[x] \tag{2}$$

where I_s is the $s \times s$ identity matrix.

Lemma 1 *There exists matrices $B_0 \in M(s \times (t-s); R)$ and $\tilde{B} \in M(s \times (t-s); R[x])$ such that $B = B_0 + (A + xI_s)\tilde{B}$.*

Proof. Divide B with remainder by the linear polynomial $A + xI_s$. □

By this lemma, relation (1) can be written in the form

$$(A + xI_s)\left[\begin{pmatrix} p_1 \\ \vdots \\ p_s \end{pmatrix} + \tilde{B}\begin{pmatrix} p_{s+1} \\ \vdots \\ p_t \end{pmatrix}\right] + B_0 \begin{pmatrix} p_{s+1} \\ \vdots \\ p_t \end{pmatrix} = 0.$$

Therefore by changing the $p_i (1 \leq i \leq s)$ by suitable linear combinations of the $p_j (s+1 \leq j \leq t)$ we can make sure that the matrix B in (2) also has coefficients in R only. So, let us assume that $b_{kj} \in R$.

Lemma 2 *The $s \times s$ minors of $(A + xI_s|B)$ generate the unit ideal in $R[x]$.*

Proof. ([Lang]:p 483 - 485) It is enough to show the result locally for all $\mathfrak{M} \in \text{Max}(R[x])$. By Theorem 7, $M_{\mathfrak{M}}$ is a free $R[x]_{\mathfrak{M}}$ module and from $(M_{\mathfrak{M}})_f = (F_{\mathfrak{M}})_f$ it follows that the rank of $M_{\mathfrak{M}}$ is same as that of $F_{\mathfrak{M}}$, namely $t - s$. The exact sequence

$$0 \to K \to R[x]^t_{\mathfrak{M}} \to M_{\mathfrak{M}} \to 0$$

where K is the $R[x]_{\mathfrak{M}}$ submodule of $R[x]^t_{\mathfrak{M}}$ spanned by the rows of the matrix $(A + xI_s|B)$ splits. Therefore, K is a free $R[x]_{\mathfrak{M}}$ module of rank s. Since the rows of the matrix can be extended to a basis of $R[x]^t_{\mathfrak{M}}$, at least one $s \times s$ minor is a unit in $R[x]^t_{\mathfrak{M}}$. □

Let g denote the monic polynomial $det(A + xI_s)$ and $\mathfrak{a}$ denote the ideal in R generated by the coefficients of B. Then it follows by lemma 2 that

$$R[x] \subset R[x]g + R[x]\mathfrak{a}.$$

and hence $R[x] = R[x]g + R[x]\mathfrak{a}$. Since g is monic, the ring $T = R[x]/(g)$ is free as an R module. Going modulo g we have $T = T\mathfrak{a}$ and hence it follows that $\mathfrak{a} = R$. Since R is local, at least one coefficient of B is a unit in R.

Now, by elementary column operations and then elementary row operations we can bring the matrix in 2 into a matrix of the following form:

$$\left(\begin{array}{c|c} & 0 \\ A' + xI_{s-1}|B' & \vdots \\ & 0 \\ \hline 0\ldots\ldots\ldots 0 & 1 \end{array}\right)$$

where A' and B' have coefficients in R and I_{s-1} is the $(s-1)\times(s-1)$ identity matrix. Since only elementary operations have been made, the lemma 2 holds for this matrix also. Hence we can apply the same argument to $(A' + xI_{s-1}|B')$ and ultimately bring it to the form

$$(0|I_s),$$

where I_s is the $s \times s$ identity matrix. But this implies that M is a free $R[x]$ module of rank $(t-s)$, hence the Theorem. ■

Theorem 10 (Quillen-Suslin:1976) *Let R be any ring. If M is a finitely generated projective $R[x]$ module and there exists a monic polynomial $f \in R[x]$ such that M_f is a free $R[x]_f$ module then M is a free $R[x]$ module.*

Proof. Let $\mathfrak{m} \in \text{Max}(R)$. Then $M_\mathfrak{m}$ is a finitely generated projective $R_\mathfrak{m}[x]$ module for which $(M_\mathfrak{m})_f$ is a free $(R_\mathfrak{m}[x])_f$ module. By Theorem 9 (Horrocks' Theorem), $M_\mathfrak{m}$ is a free $R_\mathfrak{m}[x]$ module and hence extended.

Now, consider the polynomial ring $R[x^{-1}]$ with indeterminate x^{-1}. The rings of fractions $R[x]_x$ and $R[x^{-1}]_{x^{-1}}$ are isomorphic, given by the map $x \mapsto x^{-1}$. So, henceforth we write $R[x, x^{-1}]$ for this ring.

Let $f = x^n + a_1x^{n-1} + \cdots + a_n$ and $g = 1 + a_1x^{-1} + \cdots + a_nx^{-n}$ where $a_i \in R$. Note that $g = x^{-n}f$ and since x^{-n} is a unit in $R[x, x^{-1}]$, we have $R[x, x^{-1}]_f \cong R[x, x^{-1}]_g$. Since M_f is a free $R[x]_f$ module, $(M_x)_f \cong (M_x)_g$ is a free $R[x, x^{-1}]_g$ module.

Since the elements x^{-1} and g generate the unit ideal in $R[x^{-1}]$ we have $\text{Spec}(R[x^{-1}]) = D(x^{-1}) \cup D(g)$. It follows that there is an $R[x^{-1}]$ module M' such that M'_g is a free $R[x^{-1}]_g$ module and the rank of M'_g as an $R[x^{-1}]_g$ module is same as the rank of $(M_x)_g$ as an $R[x, x^{-1}]_g$ module. Also, $M'_{x^{-1}} \cong M_x$ as $R[x, x^{-1}]$ modules . So, M' is finitely presentable by Theorem 4.

Now we can prove that M is free. For a maximal ideal $\mathfrak{m} \in \text{Max}(R)$, we have $(M'_\mathfrak{m})_{x^{-1}} \cong (M_\mathfrak{m})_x$ and this module is free over $R_\mathfrak{m}[x, x^{-1}]$. Since x^{-1} is a monic polynomial in $R[x^{-1}]$, by Theorem 9 (Horrocks' Theorem) $M'_\mathfrak{m}$ is a free $R_\mathfrak{m}[x^{-1}]$ module. M' is finitely presentable and locally extended, so by Theorem 5 (Quillen's Theorem) it is globally extended. Hence $M' \cong N'[x^{-1}]$ for some R module N' where $N' \cong M'/x^{-1}M' \cong M'/(x^{-1} - 1)M'$.

Since M'_g is a free $R[x^{-1}]_g$ module and $g \equiv 1 (\text{mod } x^{-1})$, $M'_g/x^{-1}M'_g \cong M'/x^{-1}M'$ is a free R module. Therefore $M'/(x^{-1} - 1)M'$ is also a free R module. But

$$\frac{M'}{(x^{-1}-1)M'} \cong \frac{M'_{x^{-1}}}{(x^{-1}-1)M'_{x^{-1}}} \cong \frac{M_x}{(x-1)M_x} \cong \frac{M}{(x-1)M}$$

so $M/(x-1)M$ is a free R module. Hence $M/(x-1)M \cong M/xM \cong N$ is free and thus M is free. ■

3 Serre's Conjecture

Theorem 11 (Serre's Conjecture) *If K is a principal ideal domain then all finitely generated projective modules over the polynomial ring $K[x_1, \cdots, x_n]$ are free.*

Proof. If $n = 0$ then we are done since submodules of a free module of finite rank over a principal ideal domain are free. A finitely generated projective module is a submodule of a free module of finite rank.

Let $n > 0$ and assume the result for $n-1$ variables by induction. Let M be a finitely generated projective module over $K[x_1, \cdots, x_n]$. Denote by S the set of monic polynomials in $K[x_1]$. Note that S is multiplicatively closed. Then M_S is a finitely generated projective module over $K[x_1, x_2, \cdots, x_n]_S$ and this ring is same as $K[x_1]_S[x_2, \cdots, x_n]$.

It is enough to show that $K[x_1]_S$ is a principal ideal domain, for then M_S will be a free $K[x_1, \cdots, x_n]$ module by induction hyphthesis. Then by proposition 8 there is an $f \in S$ for which M_f is a free $K[x_1, \cdots, x_n]_f$ module. Since this f is monic, using Quillen-Suslin Theorem, M is a free $K[x_1, \cdots, x_n]$ module.

Claim *The ring $R = K[x_1]_S$ is a principal ideal domain.*

Proof of Claim. Since K is a principal ideal domain, so $K[x_1]$ is an unique factorization domain and hence $K[x_1]_S$, being the ring of fractions, is also an unique factorization domain. Let $\mathfrak{p} \in \mathrm{Spec}(R)$. If $\mathfrak{p} \cap K = 0$ then $R_{\mathfrak{p}}$ is a ring of fractions of $Q(K)[x_1]$ (By $Q(K)$ we mean the fraction field of K). Therefore $h(\mathfrak{p}) \leq 1$ by fact 1 and $\mathfrak{p}$ is a principal ideal by fact 2. Otherwise if $\mathfrak{p} \cap K = (p)$ with some prime $p \in K$, then $R/(p) = K/(p)(x_1)$ is a field, so $\mathfrak{p} = (p)$. So, any $\mathfrak{p}(\neq 0) \in \mathrm{Spec}(R)$ is generated by a prime element $\pi \in R$.

Now, let a_1, a_2 be non zero elements in R and let c be their greatest common divisor. If $\mathfrak{p} = (\pi) \in \mathrm{Spec}(R)$ and if $\pi^{\nu_i} | a_i$ for $i = 1, 2$ then $\pi^{\mathrm{Min}\{\nu_1, \nu_2\}} | c$. It follows that $(a_1, a_2)R_{\mathfrak{p}} = cR_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$ and hence the ideal $(a_1, a_2) = (c)$ by proposition 3. Hence $R = K[x_1]_S$ is a principal ideal domain. □

This concludes the proof of Serre's conjecture. ■

A Brief History[Lam]: In 1955, on p.243 of his famous article "Faisceaux algébriques cohérents" (FAC), Serre wrote: "On ignore s'il existe des A-modules projectifs de type fini qui ne soient pas libres." Soon, the freeness of finitely generated projective modules over $K[x_1, \cdots, x_n]$ (K a field) became famous as Serre's Conjecture. Serre might have objected that what he posed as an open problem became his "conjecture" by world acclamation, but the fine distinction between "Serre's problem" and "Serre's conjecture" can be safely forgotten now. Culminating almost twenty years of effort by Algebraists, Quillen and Suslin proved (independently) in 1976, that finitely generated projective modules over $R = K[x_1, \cdots, x_n]$ are, indeed free. A very brief history of this development can be given as follows:

If M has rank 1, a Theorem of Gauss implies that M is free using that $K[x_1, \cdots, x_n]$ is an UFD. For $n = 1$, it is a standard result. This is even true for non commutative case, so K can be assumed to be a just a division ring here.

In 1958, Seshadri proved Serre's Conjecture for 2 variables. In 1957/58, Serre himself showed that $M \cong R^r \oplus Q$ where Q has rank $\leq n$, reducing the conjecture to the case that $\mathrm{rank}(M) \leq n$.

In 1963/64, Bass showed that M is free for rank $> n$ or if M is non-finitely generated. Horrocks' Theorem, as proved in this article, was also proved in 1964.

In 1971, Ojanguren and Sridharan showed that for $n \geq 2$, the problem has a negative answer in the non commutative case.

In 1974, Roitman proved the result for algebraically closed field K and $\text{rank}(M) = n$. In January, 1976, Quillen and Suslin (independently) proved Serre's Conjecture.

Acknowledgment: I thank Prof. François Loeser for his guidance and the senior students in ENS for their help during my work here.

References

[AM] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, 1969.

[Kunz] Ernst Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, 1981.

[Lam] T. Y. Lam, *Serre's Conjecture*, Springer-Verlag, Lecture Notes in Mathematics (vol: 635), 1978.

[Lang] Serge Lang, *Algebra* 2nd Edition, Addison-Wesley Publishing Company, 1984.