Serre's Conjecture For Projective Modules
(Seminar Report)

Javadekar Omkar Deepak
Roll No. 185090007

In this report we are going to see a proof of well known result in commutative algebra, called *Serre's conjecture*. It is also known as Quillen–Suslin theorem. The conjecture was made by J. P. Serre in 1955. In 1958 C. S. Seshadri proved the conjecture for polynomial ring in two variables. Finally, Daniel Quillen and Andrei Suslin indepenently gave first complete proofs of Serre's conjecure in 1976. Leonid Vaserstein later gave a simpler proof of this result. The statement of Serre's conjecture is very simple to understand, and it is as follows:
Every finitely generated projective module over a polynomial ring in finitely many variables over a field is a free module.

For the proof of Serre's conjecture we will follow the following four steps:
Step 1: We will show that finite projective modules over polynomial rings are stably free.
Step 2: We will define the notions like unimodular extension property, unimodular column extnsion property, and prove a crucial result called Horrocks theorem.
Step 3: We will show that polynomial rings have unimodular column extension property.
Step 4: Finally, we will conclude the proof of Serre's conjecture by showing that polynomial rings have unimodular column extension property.

1 Stably Free Modules

From now on, all rings are assumed to be commutative with multiplicative identity.

Definition 1.1. An R-module F is said to be *free* if it has a basis, i.e. if $F \cong \bigoplus_{i\in\Lambda} R$.

Definition 1.2. An R-module P is said to be *projective* if there exists a free R-module F and an R-module Q such that $F = P \oplus Q$.

Definition 1.3. An R-module E is said to be *stably free* if there exists a finitely generated free module F such that $E \oplus F$ is free of finite rank.

Theorem 1.4. Let M be a projective module. Then M is stably free if and only if M admits a finite free resolution .

[1] This is the report of the public seminar I gave on October 26, 2020 in MA792 Communication Skills-II course on Serre's conjecture for projective modules.

Proof. If M is stably free, then for some finite free module F, $M \oplus F$ is finite free. Thus, M has a finite free resolution

$$0 \to F \to M \oplus F \to M \to 0$$

Conversely let

$$0 \to E_n \to \cdots \to E_1 \to E_0 \to M \to 0$$

be a finite free resolution of M. We induct on n. For $n = 0$ the result is trivial. Let M_1 denote the kernel of $E_0 \to M$. Since M is projective, $E_0 = M \oplus M_1$. Now M_1 is projective, and has a free resolution of length $< n$. Thus, by induction hypothesis $M_1 \oplus F$ is finite free for some finite free module F. Therefore, $M \oplus (M_1 \oplus F) = E_0 \oplus F$ is finite free. □

Theorem 1.5. Let R be a commutative Noetherian ring. Let x be a variable . If every finite R-module has a finite free resolution, then every finite $R[x]$-module has a finite free resolution.

Proof. We use the following theorem in the proof.

Theorem: If any two modules from the short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

have a finite free resolution, then so does the third. (*)

Let M be a finite $R[x]$-module. Consider a filtration of M as follows:

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

such that $M_i/M_{i+1} \cong R[x]/P_i$ for some prime P_i. In view of (*), it suffices to prove the theorem for $M = R[x]/P$ where P is prime. Moreover, from the short exact sequence $0 \to P \to R[x] \to R[x]/P \to 0$, again by using (*) we note that M has a finite free resolution if and only if P has a finite free resolution.

Let $\mathfrak{p} = P \cap R$. Then $\mathfrak{p}$ is a prime ideal of R. Let if possible, there is a prime P for which $R[x]/P$ does not admit a finite free resolution. Among all such M we select one for which the intersection $\mathfrak{p}$ is maximal in the family of prime ideals obtained as above. Such a maximal element exists because $R[x]$ is Noetherian.

Consider the integral domain $R_0 = R/\mathfrak{p}$. Let $P_0 = P/\mathfrak{p}R[x]$. THen we may view M as an $R_0[x]$ module, equal to R_0/P_0. Let $f_1, \ldots, f_n$ generate P_0, and let f be a polynomial of minimal degree in P_0. Let K_0 denote the quotient field of R_0. Then by division algorithm,

$$f_i = q_i f + r_i, \quad \text{for} \quad i = 1, \ldots, n$$

where $q_i, r_i \in K_0[x]$ and $\deg(r_i) < \deg(f)$. Let d_0 be a common denominator for the coefficients of all q_i, r_i. Then $d_0 \neq 0$ and

$$d_0 f_i = q_i' f + r_i'$$

where $q_i' = d_0 q_i$ and $r_i' = d_0 r_i$ lie in $R_0[x]$. Then by the choice of f, we get $r_i' = 0$ for all i.

Let $N_0 = P_0/\langle f \rangle$, so N_0 is a module over $R_0[x]$, and we can also view N_0 as a module over $R[x]$. When so viewed, we denote N_0 by N. Let $d \in R$ be any element reducing to d_0 mod $\mathfrak{p}$. Then $d \notin \mathfrak{p}$ since $d_0 \neq 0$. The module N_0 has a finite filtration such that each factor module of the filtration is isomorphic to some $R_0[x]/Q_0$ where Q_0 is an associated prime of N_0. Let Q be the inverse image of Q_0 in $R[x]$. These prime ideals Q are precisely the associated primes of N in $R[x]$. Since d_0 kills N_0 it follows that d kills N and therefore d lies in every associated prime of N. By the maximality property in the selection of P, it follows that every one of the factor modules in the filtration of N has a finite free resolution, and by (*) it follows that N itself has a finite free resolution.

Now we view $R_0[x]$ as an $R[x]$-module, via the canonical homomorphism

$$R[x] \to R_0[x] = R[x]/\mathfrak{p}R[x].$$

By assumption, $\mathfrak{p}$ has a finite free resolution as R-module, say

$$0 \to E_n \to \cdots \to E_o \to \mathfrak{p} \to 0.$$

We now form the modules $E_i[x]$ in the obvious sense to obtain a finite free resolution of $\mathfrak{p}[x] = \mathfrak{p}R[x]$. From the exact sequence

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

we conclude that $R_0[x]$ has a finite free resolution a $R[x]$-module.

Since R_0 is an integral domain, it follows that $\langle f \rangle$ in $R_0[x]$ is $R[x]$ isomorphic to $R_0[x]$. Therefore it has a finite free resolution as $R[x]$-module. Thus, applying (*) to the exact sequence

$$0 \to \langle f \rangle \to P \to N \to 0$$

we get that P_0 has a finite free resolution, and once again applying (*) to the exact sequence

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

we get that P has a finite free resolution. This completes the proof. □

Theorem 1.6 (Hilbert–Serre)**.** If k is a field and $x_1, \ldots, x_r$ independent variables, then every finite projective module over $k[x_1, \ldots, x_r]$ is stably free, or equivalently, admits a finite free resolution .

Proof. Follows by inductuion on r using above theorem, and the fact that if R is Noetherian then so is $R[x]$. □

2 Horrocks Theorem

Definition 2.1. Let R be a commutative ring. Let $f = (f_1, \ldots, f_n) \in R^n$ is called *unimodular* if $R = \langle f_1, \ldots, f_n \rangle$. We say that f has the *unimodular extension property* if there exists a matrix in $GL_n(R)$ with first column $(f_1, \ldots, f_n)^T$.

Definition 2.2. A ring R is said to have the *unimodular column extension property* if every unimodular vector $f \in R^n$ has the unimodular extension property, for all positive integers n.

Theorem 2.3 (Horrocks)**.** Let $(A, \mathfrak{m})$ be a local ring and let $R = A[x]$ be the polynomial ring in one variable over A. Let $f \in R^n$ be unimodular such that some component has leading coefficient 1. Then f has the unimodular extension property.

Proof. If $n = 1$, then $f = f_1$ itself is a unit, and we are done. If $n = 2$, then using $R = \langle f_1(x), f_2(x) \rangle$ we see that there exist $g_1(x), g_2(x) \in A[x]$, such that

$$1 = f_1(x)g_1(x) + f_2(x)g_2(x)$$

and hence we get a 2×2 invertible matrix

$$\begin{bmatrix} f_1(x) & -g_2(x) \\ f_2(x) & g_1(x) \end{bmatrix}.$$

So, we assume $n > 2$ and do an induction of the smallest degree d of a component of f with leading coefficient 1. Note that if $d = 0$, then the result is obvious. So, assume $d > 0$. Without loss of generality, we may assume that f_1 has leading coefficient 1, degree d, and that $\deg(f_i) < d$ for $i \neq 1$. Since f is unimodular, a relation $\sum g_i f_i = 1$ shows that not all coefficients of $f_2, \dots f_n$, lie in the maximal ideal $\mathfrak{m}$. Without loss of generality, we may assume that some coefficient of f_2 does not lie in $\mathfrak{m}$ and so is a unit since A is local. We write

$$\begin{aligned} f_1(x) &= x^d + a_{d-1}x^{d-1} + \cdots + a_0 \\ f_2(x) &= \qquad\qquad b_s x^s + \cdots + b_0 \end{aligned}$$

with $a_i \in A$, $b_i \in A, s < d$, such that some b_i is a unit. Let $\mathfrak{a}$ be the ideal generated by all leading coefficients of polynomials $h_1 f_1 + h_2 f_2$ of degree $< d$. We claim that $\mathfrak{a}$ contains all the coefficients $b_i, i = 0, ..., s$. Note that $b_s \in \mathfrak{a}$ is obvious $(0 \cdot f_1(x) + 1 \cdot f_2(x))$. And by repeated use of a linear combination like

$$x^{d-s} f_2(s) - b_s f_1(x) = (b_{s-1} - b_s a_{d-1})x^{d-1} + \cdots$$

(and then by adding $b_s a_{d-1} x^{d-1} + \cdots$) it follows that all b_i's are in $\mathfrak{a}$. Therefore $\mathfrak{a}$ is the unit ideal, and there exists a polynomial $h_1 f_1 + h_2 f_2$ of degree $< d$ with leading coefficient 1. By row operations, we now get a polynomial of degree $< d$ and leading coefficient 1 as some component in the i-th place, for some $i \neq 1, 2$. Therefore, the proof is complete by induction. □

Definition 2.4. The column vectors $f, g \in R^n$ are said to be *equivalent* over R if $f = Mg$ for some $M \in GL_n(R)$, and we write $f \sim g$ in such a case.

Corollary 2.5. Let A be a local ring, $R = A[x]$, and $f \in R^n$ be a unimodular vector with one component having leading coefficient 1. Then $f \sim (1, 0, \dots, 0)$.

Proof. By Horocks theorem, there exists $M \in GL_n(R)$ with first column equal to f. Then $M^{-1} f = (1, 0, \dots, 0)^T$. □

Corollary 2.6. Let A be a local ring, $R = A[x]$. Let f be a unimodular vector in R^n such that some component has leading coefficient 1. Then $f \sim f(0)$ over R.

Proof. By previous corollary, $f \sim (1, 0, \ldots, 0)$. Since f is unimodular, and A is local, there is a component of f having constant term which is a unit in A. Therefore there exists $M \in GL_n(A) \subseteq GL_n(R)$ such that $f(0)$ is its first column, and hence $f(0) \sim (1, 0, \ldots, 0)$. □

3 Polynomial Rings and Unimodular Column Extension Property

Lemma 3.1. Let R be an integral domain, and let S be a multiplicative subset. Let x, y be independent variables. 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. Let $M \in GL_n(S^{-1}R[x])$ be such that $f(x) = M(x)f(0)$. Then $M(x)^{-1}f(x) = f(0)$ is constant, and thus invariant under translation $x \mapsto x + y$. Let

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

Then $G(x, y)f(x + y) = f(x)$. We have $G(x, 0) = I$, and hence

$$G(x, y) = I + yH(x, y)$$

with $H(x, y) \in S^{-1}R[x, y]$. There exists $c \in S$ such that cH has coefficients in $R[x, y]$. Thus, we have $G(x, cy)f(x + cy) = f(x)$ and $G(x, cy)$ has all entries in $R[x, y]$. We also have $G(x, cy) = M(x)M(x + cy)^{-1}$. Since $M(x)$ is invertible, $\det M(x)$ is constant in $S^{-1}R$, and thus it follows that $\det M(x + cy)$ is equal to the same constant. Therefore, $\det G(x, cy) = 1$. This proves the lemma. □

Theorem 3.2. Let R be an integral domain, and let f be a unimodular vector 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 $f(x + cy) \sim f(x)$ over $R[x, y]$. Then J is an ideal. This is because $0 \in J$, and if $c \in J$ and $a \in R$ then replacing y by ay in the equivalence above shows that

$$f(x + cay) \sim f(x)$$

over $R[x, ay]$, so over $R[x, y]$. Similarly, we have that if $c, c' \in J$, then $c + c' \in J$. Now let $\mathfrak{p}$ be a prime ideal of R. Since $R_{\mathfrak{p}}$ is local, by Horrocks theorem we get that

$$f(x) \sim f(0) \text{ over } R_{\mathfrak{p}}[x].$$

Now, by the previous lemma it follows that there exists $c \in R$ and $c \notin \mathfrak{p}$ such that $f(x + cy) \sim f(x)$ over $R[x, y]$. Hence J is not contained in $\mathfrak{p}$, and so J is unit ideal in R. Thus, there exists an invertible matrix $M(x, y)$ over $R[x, y]$ such that

$$f(x + y) = M(x, y)f(x).$$

Putting 0 for x in above equation gives $f(y) \sim f(0)$. □

Theorem 3.3. Let k be a field and $R = k[x_1, \ldots, x_r]$. If f is a unimodular vector in R^n, then f has the unimodular extension property.

Proof. If $r = 1$ then $k[x_1]$, and the result is easy to prove. Assume the theorem for $r-1$ variables with $r > 1$, and put $A = k[x_1, \ldots, x_{r-1}]$. If we let $y_r = x_r$ and $y_i = x_i - x_r^{m_i}$ (for suitable $m_i \in \mathbb{N}$), then the polynomial vector

$$f(x_1, \ldots, x_r) = g(y_1, \ldots, y_r)$$

has one component with y_r-leading coefficient equal to a nonzero element of k. Without loss of generality, we may assume that it is equal to 1. By previous theorem, there exists a matrix

$$N(y_1, \ldots, y_r) = M(x_1, \ldots, x_n)$$

invertible over $A[x_r] = A[y_r]$ such that

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

and $g(y_1, \ldots, y_{r-1}, 0)$ is unimodular in $k[y_1, \ldots, y_{r-1}]^n$. Thus, the proof can be concluded by induction. □

Theorem 3.4. If R has unimodular column extension property, then every stably free R-module is free.

Proof. Let E be stably free. We induct on the rank of the free modules F such that $E \oplus F$ is free. By induction, it suffices to prove that if $E \oplus R$ is free then E is free. So, let $E \oplus R = R^n$ and let p: $R^n \to R$ denote the projection map. Suppose $\{u_1\}$ is a basis of R over itself. Viewing R as a direct summand in $E \oplus R = R^n$ we write

$$u_1 = (a_{11}, \ldots, a_{n1})^T, \qquad \text{with } \ a_{i1} \in R$$

Then u_1 is unimodular, and by the assumption u_1 is the first column of a matrix $M = (a_{ij})$ whose determinant is a unit in R. Let

$$u_j = M e_j \quad \text{ for } j = 1, \ldots, n \ ,$$

where e_j is the j-th unit column vector of R^n. Note that u_1 is the first column of M. By elementary column operations, we may change M so that $u_j \in E$ for $j = 2, \ldots, n$. Indeed, if $\mathrm{p}(e_j) = cu_1$ for $j > 1$ we replace e_j by $e_j - ce_1$. So, without loss of generality we assume that $u_2, \ldots, u_n$ lie in E. Since $M \in GL_n(R)$, M induces an automorphism of R^n as R-module with itself by $X \mapsto MX$. From the construction and the fact that $R^n = E \oplus R$ we get that M maps the free module with basis $\{e_2, \ldots, e_n\}$ onto E. This concludes the proof. □

The proof of Serre's conjecture now follows just by combining above two theorems with Theorem 1.6.

References

[1] S. S. Abhyankar, *Lectures on Algebra, Volume I*, World Scientific Publishing Co. Pte. Ltd. (2006).

[2] S. Lang, *Algebra*, Springer-Verlag New York, Graduate Texts in Mathematics, (2002).

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

[4] N. Mohan Kumar, *On a theorem of Seshadri*, https://www.math.wustl.edu/ kumar/papers/seshadri.pdf

[5] Nil Garces de Marcilla Escubedo, *The Quillen-Suslin Theorem*, http://diposit.ub.edu/dspace/bitstream/2445/125803/2/memoria.pdf

[6] https://en.wikipedia.org/wiki/Quillen–Suslin_theorem.