ON SERRE'S PROBLEM ON PROJECTIVE MODULES¹

MOSHE ROITMAN

ABSTRACT. The main purpose of this paper is to prove the following result concerning Serre's problem: Any projective module of rank n over $k[X_1, \dots, X_n]$ (where k is an infinite field) is free. We give also simple proofs (based on Serre's theorem that $K_0(k[X_1, \dots, X_n]) = \mathbb{Z}$) to the following particular case of Bass' theorem: any projective module of rank $> n$ over $k[X_1, \dots, X_n]$ (k any field) is free, and to Seshadri's theorem: finitely generated projective modules over $k[X, Y]$ are free.

1. Introduction. In the following "ring" means a commutative ring with unit.

For any ring R and $n \geq 1$ the following statements are equivalent:

- (i) For any module P , $P \oplus R \cong R^n \Rightarrow P$ is free.
- (ii) Any row $[a_1, \dots, a_n]$ of elements of R with $(a_1, \dots, a_n) = R$ can be completed to an invertible matrix over R (see [1, §9]).

By Bass' theorem (see [3, §22, p. 58]) any projective module of rank $> n$ over $k[X_1, \dots, X_n]$ (k any field) is free (see a proof below), and so the following two statements are equivalent for any field k and any n :

- (i) Any projective module of rank n over $k[X_1, \dots, X_n]$ is free.
- (ii) Any row $[a_1, \dots, a_{n+1}]$ such that $(a_1, \dots, a_{n+1}) = k[X_1, \dots, X_n]$ can be completed to an invertible matrix.

The method of establishing our results is to perform elementary transformations on a given row to obtain the row $[1, 0, \dots, 0]$.

The main result of this paper (projective modules of rank n over $k[X_1, \dots, X_n]$, k an infinite field, are free) was greatly generalized by R. Swan, H. Bass and M. P. Murthy. As a corollary of their work they achieved the following result: projective modules of rank r over $k[X_1, \dots, X_n]$ are free if $r > (n+1)/2$ (k an infinite field). We nevertheless believe there may be some interest in the method we use to obtain our more limited result.

Received by the editors March 14, 1974.

AMS (MOS) subject classifications (1970). Primary 13C10.

¹ This is part of the author's Ph.D. thesis prepared at the Hebrew University of Jerusalem under the supervision of Professor Harry Furstenberg, to whom the author expresses his gratitude.

2. The main result.

Theorem. Any projective module of rank n over $k[X_1, \dots, X_n]$ (where k is an infinite field) is free.

By the Introduction it is enough to prove the following

Proposition. Any row $[a_1, \dots, a_{n+1}]$ such that $(a_1, \dots, a_{n+1}) = k[X_1, \dots, X_n]$ (k an infinite field) can be completed to an invertible (in fact an elementary) matrix over $k[X_1, \dots, X_n]$. (Here and in the sequel an elementary matrix in $M_k(R)$ is a matrix in $E_k(R)$.)

Lemma 1. Let R be a ring and $a_i \in R$ ($1 \leq i \leq n$) such that a proper subset of $\{a_i\}$ generates R as an ideal. Then the row $[a_1, \dots, a_n]$ can be completed to an elementary matrix.

Proof. Let us suppose e.g. that $(a_2, \dots, a_n) = R$. We add $1 - a_1$ (which is a linear combination with coefficients in R of $a_2, \dots, a_n$) to a_1 to get 1, and then we obtain by elementary transformations the row $[1, 0, \dots, 0]$.

Lemma 2. Let R be an integral domain, $a, b \in R$ such that $(a, b) = (1)$. Then $x = a + bX$ is a prime element in the polynomial ring $R[X]$.

Proof. Let $uv \equiv 0 \pmod{x}$ in $R[X]$, $u = \sum_{i=0}^n u_i X^i$, $u_i \in R$. Then

$$\begin{aligned} bu &= bu_0 + bu_1 X + \dots + (bu_{n-1} - u_n a)X^{n-1} + u_n X^{n-1}(a + bX) \\ &\equiv bu_0 + \dots + (bu_{n-1} - u_n a)X^{n-1} \pmod{x}. \end{aligned}$$

In this way we get $c \in R$ such that $b^n u \equiv c(x)$, and also $d \in R$ such that for a suitable m : $b^m v \equiv d(x)$. Now, $b^{m+n} uv \equiv cd \equiv 0 \pmod{x}$ and, as R is an integral domain, we get $c = 0$ or $d = 0$. Let e.g. $c = 0$ and then $b^n u \equiv 0 \pmod{x}$. Now, suppose for some t ,

$$bt = b \left(\sum_{i=0}^k t_i X^i \right) = (a + bX) \left(\sum_{j=0}^m s_j X^j \right).$$

For all j ($0 \leq j \leq m$), $as_j \equiv 0 \pmod{b}$ in R , and therefore $s_j \equiv 0 \pmod{b}$ for all j , and so $t \equiv 0 \pmod{x}$. Applying this successively to $b^n u$ we get $u \equiv 0 \pmod{x}$ and therefore x is prime.

Proof of the proposition. Without loss of generality assume $n \geq 2$. Let us adjoin to k n indeterminates $u_1, \dots, u_n$. Let $K = k(u_1, \dots, u_n)$.

Let $[a_1, \dots, a_{n+1}]$ be a row over $k[X_1, \dots, X_n]$ such that

$(a_1, \dots, a_{n+1}) = (1)$. First we shall complete this row to an elementary matrix over $K[X_1, \dots, X_n]$. We shall perform a series of elementary transformations on the row and, by Lemma 1, we can suppose at every stage that the ideal generated by any n elements of the row in $K[X_1, \dots, X_n]$ is not (1) .

We shall prove at a later stage that it is possible to choose b_i ($1 \leq i \leq n$) such that, if $a'_i = a_i + u_i b_i$, then

- (i) $b_i \in (a'_1, \dots, a'_{i-1}, a_{i+1}, \dots, a_{n+1})$ in $k[u_1, \dots, u_{i-1}, X_1, \dots, X_n]$.
- (ii) $(a_i, b_i) = k[u_1, \dots, u_{i-1}, X_1, \dots, X_n]$.
- (iii) The ideal $m = (a'_1, \dots, a'_n)$ is maximal in $K[X_1, \dots, X_n]$ and $K[X_1, \dots, X_n]/m$ is a separable algebraic field extension of K .

At this stage suppose that we can choose b_i 's as above.

By (iii) $L = K[X_1, \dots, X_n]/m$ is a separable algebraic field extension of K ; therefore, as K is infinite, there is a linear combination of X_i over K , $Y = \sum_{i=1}^n \alpha_i X_i$, such that $L = K[\bar{Y}]$ (see [4, §40, p. 126]). Take Y as one of n indeterminates: $K[X_1, \dots, X_n] = K[Y_1, \dots, Y_n]$, $Y = Y_1$, and then $a_{n+1} - Y_2 \equiv f(Y_1) \pmod{m}$ for a suitable polynomial $f(Y_1)$ over K . By change of indeterminates we can suppose that $Z = Y_2 + f(Y_1)$ is an indeterminate over K .

We got the row $[a'_1, \dots, a'_n, Z + u]$ where $u \in (a'_1, \dots, a'_n)$. We can pass to the row $[a'_1, \dots, a'_n, Z]$. By adding to the a'_i 's suitable multiples of Z we can suppose that the indeterminate Z does not appear in the polynomials $a'_1, \dots, a'_n$. But then if $1 = \sum_{i=1}^n t_i a'_i + tZ$ we get $1 = \sum_{i=1}^n t_i (Z=0) a'_i$, and so by Lemma 1 the proof for $K[X_1, \dots, X_n]$ is finished.

Now, if $[a_{ij}]$ is a matrix over $K[X_1, \dots, X_n]$ such that $\det[a_{ij}] = 1$ with $[a_1, \dots, a_{n+1}]$ as the first row, we can specialize over k the coefficients of the a_{ij} 's (which are in K) to elements of k , because k is infinite. In this way we get an invertible matrix over $k[X_1, \dots, X_n]$ with first row $[a_1, \dots, a_{n+1}]$. Similarly, we can get an elementary matrix over $k[X_1, \dots, X_n]$ with first row $[a_1, \dots, a_{n+1}]$.

The choice of the b_i 's. If $\text{char } k = 0$, then we choose b_i 's inductively such that the conditions (i) and (ii) above are fulfilled. This is possible because

$$(a'_1, \dots, a'_{i-1}, a_i, \dots, a_{n+1}) = k[u_1, \dots, u_{i-1}, X_1, \dots, X_n]$$

for any i , $1 \leq i \leq n$, inasmuch as each such row is obtained from the preceding

one by an elementary transformation. By Lemma 2 we find inductively that the ideals $(a'_1, \dots, a'_i)$ are prime in $k[u_1, \dots, u_i, X_1, \dots, X_n]$ respectively, and therefore in $k[u_1, \dots, u_n, X_1, \dots, X_n]$ and also in $K[X_1, \dots, X_n]$. By Lemma 1, we can assume that in $K[X_1, \dots, X_n]$:

$$0 \subsetneq (a'_1) \subsetneq (a'_1, a'_2) \subsetneq \dots \subsetneq (a'_1, \dots, a'_n)$$

and because $\dim_{Kr}(K[X_1, \dots, X_n]) = n$ we get that the ideal $m = (a'_1, \dots, a'_n)$ is maximal in $K[X_1, \dots, X_n]$ and so the condition (iii) is also fulfilled.

Suppose now $\text{char } k = p \neq 0$. We can assume $a_i(X_1, \dots, X_1) \neq 0$ for $1 \leq i \leq n$. Otherwise, if say $a_1(X_1, \dots, X_1) = 0$, we add to a_1 an element $u \in (a_2, \dots, a_{n+1})$ such that $(a_n, u) = k[X_1, \dots, X_n]$, and then $u(X_1, \dots, X_1) \neq 0$ because, for any polynomial $t \in k[X_1, \dots, X_n]$, the polynomial $t(X_1, \dots, X_1) = 0 \Leftrightarrow t \in (X_2 - X_1, \dots, X_n - X_1)$ and the latter ideal is not (1).

Let $c_1 \in (a_2, \dots, a_{n+1})$ in $k[X_1, \dots, X_n]$ be such that

$$(a_1, c_1) = (1); \quad b_1 = (a_1^p a_2^p \dots a_n^p X_1 + 1)c_1^p; \quad a'_1 = a_1 + u_1 b_1.$$

Define successively

$$c_i \in (a'_1, \dots, a'_{i-1}, a_{i+1}, \dots, a_{n+1})$$

in $k[u_1, \dots, u_{i-1}, X_1, \dots, X_n]$ such that

$$(a_i, c_i) = 1; \quad b_i = (a_1^p \dots a_n^p X_i + 1)c_i^p; \quad a'_i = a_i + u_i b_i.$$

Clearly $(a'_i, b_i) = 1$ in $k[u_1, \dots, u_{i-1}, X_1, \dots, X_n]$.

We can assume that the ideal $(a'_1, \dots, a'_n)$ is maximal in $K[X_1, \dots, X_n]$.

Let $\bar{X}_i$ stand for the class of X_i modulo this ideal. Let us prove that

$$|\partial a'_i / \partial X_j|(\bar{X}_1, \dots, \bar{X}_n) \neq 0.$$

We set

$$\begin{aligned} D &\stackrel{\text{def}}{=} \left| \frac{\partial a'_i}{\partial X_j} \right| = \left| \frac{\partial a_i}{\partial X_j} + u_i a_1^p \dots a_n^p c_i^p \delta_{ij} \right|, \\ T &\stackrel{\text{def}}{=} \prod_{i=1}^n (a_1^p \dots a_n^p X_i + 1) D = \left| (a_1^p \dots a_n^p X_i + 1) \frac{\partial a_i}{\partial X_j} + a_1^p \dots a_n^p u_i b_i \delta_{ij} \right| \\ &\equiv \left| (a_1^p \dots a_n^p X_i + 1) \frac{\partial a_i}{\partial X_j} - a_1^p \dots a_n^p a_i \delta_{ij} \right| \pmod{(a'_1, \dots, a'_n)}. \end{aligned}$$

Let

$$S = |(a_1^p \cdots a_n^p X_i + 1) \partial a_i / \partial X_j - a_1^p \cdots a_n^p a_i \delta_{ij}|.$$

Then $S \in k[X_1, \dots, X_n]$. The ideal $(a_1^p \cdots a_n^p X_i + 1)_{1 \leq i \leq n}$ in $k[X_1, \dots, X_n]$ is not (1): otherwise

$$1 = \sum_{i=1}^n \alpha_i (a_1^p \cdots a_n^p X_i + 1).$$

Then we get by the substitutions $X_i \rightarrow X_1$ ($i = 2, \dots, n$) that

$$X_1 a_1^p \cdots a_n^p (X_1, \dots, X_1) + 1$$

is invertible, and this is impossible because $a_1^p \cdots a_n^p (X_1, \dots, X_1) \neq 0$.

Now it is clear that $S \not\equiv 0 \pmod{(a_1^p \cdots a_n^p X_i + 1)_{1 \leq i \leq n}}$ and so $S \neq 0$.

Suppose $S \in (a'_i, \dots, a'_n)$ in $K[X_1, \dots, X_n]$. Then, as the ideal $(a'_i, \dots, a'_n)$ is prime in $k[u_1, \dots, u_n, X_1, \dots, X_n]$ we get $S \in (a'_1, \dots, a'_n)$ in $k[u_1, \dots, u_n, X_1, \dots, X_n]$:

$$S = \sum_{i=1}^n \alpha_i (a_i + u_i b_i), \quad \alpha_i \in k[u_1, \dots, u_n, X_1, \dots, X_n].$$

Over $k(u_1, \dots, u_n, X_1, \dots, X_n)$ perform successively the substitutions $u_n = -a_n/b_n, u_{n-1} = -a_{n-1}/b_{n-1}, \dots, u_1 = -a_1/b_1$ to get $S = 0$, a contradiction. (Recall: $0 \neq b_i \in k[u_1, \dots, u_{i-1}, X_1, \dots, X_n]$; by (ii) the b_i 's do not vanish by these successive substitutions.)

Finally, $D \equiv S \not\equiv 0 \pmod{(a'_1, \dots, a'_n)}$ in $K[X_1, \dots, X_n]$, and so $a'_i(\bar{X}_1, \dots, \bar{X}_n) = 0$ but

$$\left| \frac{\partial a'_i}{\partial X_j} \right| (\bar{X}_1, \dots, \bar{X}_n) \neq 0$$

Therefore $K[\bar{X}_1, \dots, \bar{X}_n]$ is a separable algebraic field extension of K [2, Corollary to Theorem 40, Chapter II, §17, p. 126].

3. A proof of Bass' theorem.

Lemma 3. *Let R be a ring, $x \in R$, α an ideal in R . If $x + \alpha$ is contained in a finite union $\bigcup_{i=1}^n \mathfrak{p}_i$ of prime ideals, then it is contained in one of them.*

Proof. We go by induction on n . Let $x + \alpha \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$ and $i \neq j \Rightarrow \mathfrak{p}_i \not\subseteq \mathfrak{p}_j$. If $x \in \bigcap_{i=1}^n \mathfrak{p}_i$, then $\alpha \subseteq \bigcup \mathfrak{p}_i$ and so there is a $\mathfrak{p}_i$: $\alpha \subseteq \mathfrak{p}_i, x + \alpha \subseteq$

$\mathfrak{p}_i$. Let $x \notin \mathfrak{p}_n$. Then $(x + (\alpha \cap \mathfrak{p}_n)) \cap \mathfrak{p}_n = \emptyset$ and therefore $x + \alpha \cap \mathfrak{p}_n \subseteq \bigcup_{i=1}^{n-1} \mathfrak{p}_i$. By the inductive assumption $x + \alpha \cap \mathfrak{p}_n \subseteq \mathfrak{p}_i$ for a suitable $\mathfrak{p}_i$, $i \leq n-1$. We get $x \in \mathfrak{p}_i$ because $0 \in \alpha \cap \mathfrak{p}_n$ and also $\alpha \cap \mathfrak{p}_n \subseteq \mathfrak{p}_i \Rightarrow \alpha \subseteq \mathfrak{p}_i$, and finally $x + \alpha \subseteq \mathfrak{p}_i$.

Proposition. *Let R be a noetherian ring, $\dim_{K_r} R = n$. If P is an R -module such that $P \oplus R \cong R^m$, $m \geq n+2$, then P is free.*

Proof. By the Introduction it is enough to prove the following statement.

Any row $[a_1, \dots, a_m]$, $m \geq n+2$, over R can be completed to an invertible (in fact an elementary) matrix.

Suppose the contrary. By Lemma 3 we will be able to add to a_1 a linear combination b_1 of $a_2, \dots, a_m$ such that $a'_1 = a_1 + b_1$ does not belong to any prime ideal associated with the zero ideal in R ; by Lemmas 3 and 1 we can add successively to a_i an element b_i of $(a_{i+1}, \dots, a_m)$ such that $a'_i = a_i + b_i$ does not belong to any prime ideal associated with $(a'_1, \dots, a'_{i-1})$ ($i = 1, \dots, m-1$). In this way we get a prime sequence $\langle a'_1, \dots, a'_{m-1} \rangle$, $m-1 > n$, but this contradicts $\dim_{K_r} R = n$.

Corollary. *Any projective module of rank $> n$ over $k[X_1, \dots, X_n]$ (k any field) is free. (This is a particular case of Bass' theorem.)*

Proof. The corollary is immediate from the preceding proposition and Serre's theorem that $K_0(K[X_1, \dots, X_n]) = \mathbb{Z}$, i.e. for any finitely generated projective P there is a finitely generated free module F such that $P \oplus F$ is free. [1, Theorem 6.6, p. 101].

4. A proof of Seshadri's theorem.

Theorem (Seshadri). *Any finitely generated projective module over $k[X, Y]$ (k any field) is free.*

It is enough to prove the following

Proposition. *Let R be a principal ideal domain. Then the ring $R[X]$ is a Hermite ring (i.e. any unimodular row can be completed to an invertible matrix).*

Proof. Let $[a_1, \dots, a_n]$ be a unimodular row over $R[X]$. Let K be the field of quotients of R . Then the given row can be completed to an invertible matrix over $K[X]$, and so to a matrix over $R[X]$ with determinant $r \neq 0$ in R .

If r is not invertible, let p be a prime factor of r . As $R/(p)$ is a field, $R/(p)[X]$ is a euclidean domain and therefore, by elementary transformations over $R[X]$, we can bring the row $[a_1, \dots, a_n]$ to the form $[a'_1, \dots, a'_n]$, where $a'_1 \equiv 1$, $a'_2 \equiv 0, \dots, a'_n \equiv 0 \pmod{pR[X]}$. We get a matrix $[a_{ij}]_{1 \leq i, j \leq n}$ such that $a_{1i} = a'_i$ ($1 \leq i \leq n$), $\det[a_{ij}]_{1 \leq i, j \leq n} = r$ and so $\det[a_{ij}]_{2 \leq i, j \leq n} \equiv 0 \pmod{pR[X]}$. By elementary transformations over $R[X]$ on the matrix $[a_{ij}]_{2 \leq i, j \leq n}$ we obtain a matrix with first row of zeros mod $pR[X]$, and furthermore we get a matrix of size $n \times n$ with determinant r , whose first row $[a''_1, \dots, a''_n]$ is obtained from $[a'_1, \dots, a'_n]$ by elementary transformations on $[a'_2, \dots, a'_n]$ and whose first and second row are, mod $pR[X]$, $[1, 0, \dots, 0]$ and $[0, 0, \dots, 0]$ respectively. We divide all the members of the second row by p to get a matrix with first row $[a''_i]$ and determinant r/p . Continuing in this way we finally obtain an invertible matrix over $R[X]$ whose first row is obtained from $[a_1, \dots, a_n]$ by elementary transformations, and so the proof is finished.

Remarks. We found that if k is an infinite field, then any projective module of rank $\geq n$ over $k[X_1, \dots, X_n]$ is free. This result includes Seshadri's theorem for $k[X, Y]$ in the case k is infinite.

It is easy to prove for any ring R and any $n > 1$ that the following two statements are equivalent:

- (i) $P \oplus R \cong R^n \Rightarrow P$ contains R as a direct summand.
- (ii) For any $x_1, \dots, x_n \in R$ such that $(x_1, \dots, x_n) = R$ there are a_i : $(a_1, \dots, a_n) = R$, $\sum_{i=1}^n a_i x_i = 1$.

From this we get at once that $P \oplus R \cong R^{2n} \Rightarrow P$ contains R as a direct summand, and so we can limit Serre's problem to projective modules of even rank (Serre's problem is: if k is a field, are all the finitely generated projective modules over $k[X_1, \dots, X_n]$ free?). We get for example that for $n = 3, 4$ any finitely generated projective module over $k[X_1, \dots, X_n]$ is free iff any projective module of rank 2 is free (for $n = 4$, k is supposed to be infinite). For further developments in Serre's problem, especially for the results of A. Suslin and L. N. Vašerštein, see H. Bass, *Libération des modules projectives sur certains anneaux de polynômes* (Séminaire Bourbaki, no. 448, June 1974).

REFERENCES

1. Aron Simis, *When are projective modules free?* Queen's Papers in Pure and Appl. Math., no. 21, Queen's University, Kingston, Ont., 1969. MR 41 #260.

2. O. Zariski and P. Samuel, *Commutative algebra*. Vol. 1, University Series in Higher Math., Van Nostrand, Princeton, N. J., 1958. MR 19, 833.

3. H. Bass, *K-theory and stable algebra*, Inst. Hautes Études Sci. Publ. Math. No. 22 (1964), 5–60. MR 30 #4805.

4. B. L. van der Waerden, *Modern algebra*. Vol. I, Springer, Berlin, 1930; English transl., Ungar, New York, 1949. MR 10, 587.

INSTITUTE OF MATHEMATICS, HEBREW UNIVERSITY OF JERUSALEM, JERUSALEM, ISRAEL

PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 50, July 1975

HOMOLOGICAL ALGEBRA IN TOPOI

D. H. VAN OSDOL

ABSTRACT. Let $\mathbf{A}$ be the category of sheaves of universal algebras of some fixed type on a Grothendieck topology. There is defined a cohomology theory H^* such that if A is an object in $\mathbf{A}$ and M is an $\mathbf{A}$ -module then $H^1(A, M)$ is in one-to-one correspondence with the equivalence classes of singular extensions of A by M . When $\mathbf{A}$ is the category of sheaves of R -modules for some sheaf of rings R , then $H^n(A, M) \cong \text{Ext}^n(A, M)$ for all $n \geq 0$.

The purpose of this note is to extend the results of [4] and [5] to general topoi, i.e. to sheaves on a Grothendieck topology. The extension has been made possible by the following theorem: Let $\mathbf{E}$ be a topos. Then there exists a complete Boolean algebra B and a left exact cotriple G on $\tilde{\mathbf{B}}$ (= sheaves on B for the canonical topology) such that $\mathbf{E}$ and $\tilde{\mathbf{B}}_G$ (= the category of G -coalgebras) are equivalent categories.

Barr's proof of this theorem can be found in [1]. Lawvere, who conjectured the theorem, paraphrases it by saying that any topos has enough Boolean-valued points. The value of the theorem is that in $\tilde{\mathbf{B}}$ subobjects have complements and epimorphisms split, i.e. $\tilde{\mathbf{B}}$ is very "set-like". One

Received by the editors March 1, 1974 and, in revised form, April 3, 1974.
AMS (MOS) subject classifications (1970). Primary 18C15, 18F10; Secondary 18G15.

Key words and phrases. Cotriple, topos, principal object, extension.

Copyright © 1975, American Mathematical Society