The Quillen-Suslin theorem

Akhil Mathew

A classical problem (posed by Jean-Pierre Serre) was to determine whether there were any nontrivial algebraic vector bundles over affine space $\mathbb{A}^n_k$ for k an algebraically closed field. In other words, it was to determine whether a finitely generated projective module over the ring $k[x_1, \dots, x_n]$ is necessarily free. The topological analog, whether (topological) vector bundles on $\mathbb{C}^n$ are trivial is easy because $\mathbb{C}^n$ is contractible. The algebraic case is harder.

The problem was solved affirmatively by Quillen and Suslin. In this writing, we would like to describe an elementary proof, due to Vaserstein, of the Quillen-Suslin theorem.

Stable freeness

An initial step, already taken by Serre, was to show that any finitely generated projective module over a polynomial ring $k[x_1, \dots, x_n]$ (for k a field) is stably free. Recall that a finitely generated module is said to be *stably free* if it becomes free after adding a finitely generated free module.

Remark 1. Given a projective module P, there is always a free module F such that $B \oplus F$ is free. To see this, first choose *projective* module Q such that $P \oplus Q$ is free, and then take $F = Q \oplus P \oplus Q \oplus \cdots$. It is easy to see that $P \oplus F \cong F$ and that F is free (if one appropriately groups the terms); this is the *Eilenberg swindle*. So, the finiteness conditions are really necessary here.

By the Serre-Swan theorem, one should think of projective modules as vector bundles, and, in particular, if X is a compact Hausdorff space, we can actually identify (via an equivalence of categories) vector bundles on X with finitely generated projective modules over the ring of continuous functions $C(X)$. Then, it follows that:

Proposition 2. *A stably free module over $C(X)$ is the same thing as a stably trivial vector bundle on X: that is, a vector bundle that becomes trivial after adding a trivial vector bundle.*

This observation allows one to get a simple example of a stably free module which is not free. The tangent bundle to S^n is stably trivial (in fact, its one-dimensional normal bundle is trivial), but it is not trivial unless $n = 1, 3, 7$ (which is in fact a consequence of the Hopf invariant one theorem).

The first part of the proof of the Quillen-Suslin theorem is accomplished by:

Theorem 3. *Let R be a noetherian ring such that every finitely generated projective module over R is stably free. Then the same property holds true for $R[x]$.*

By induction, we see:

Corollary 4. *Every finitely generated projective module over $k[x_1, \ldots, x_n]$, for any field k, is necessarily stably free.*

This result is actually a special case of a theorem of Grothendieck. Given a ring R, we can form the group $K_0(R)$, which is defined to be the Grothendieck group of the category of finitely generated projective R-modules. Two projective modules P, P' map to the same element of $K_0(R)$ if and only if there is a finite free module F such that $P \oplus F \cong P' \oplus F$. Consequently, $K_0(R) = \mathbb{Z}$ if and only if every projective R-module is stably free. The next result of Grothendieck is thus a generalisation of the previous theorem:

Theorem 5. *For a ring R, extension of scalars $R \to R[x]$ induces an isomorphism $K_0(R) \to K_0(R[x])$.*

The same is actually true of the higher K-groups, by a theorem of Quillen. We will not describe the proof here.

Unimodular vectors

The main step is to go from "stably free" to free. Equivalently, we have to show that if we let $A = k[x_1, \ldots, x_n]$, then any split injection

$$A^r \to A^s$$

has a free cokernel. Let us start with the case $r = 1$; this will turn out to be sufficient. We are interested in a condition such that any split injection $i\colon A \to A^s$ will have a free cokernel, which is to say that i is isomorphic to the canonical imbedding $e_1\colon A \to A^s$ sending an element $x \in A$ to $(x, 0, 0, \ldots, 0)$.

We can reformulate the problem in a possibly more intuitive way. To give a split injection $i\colon A \to A^s$ is the same as giving a vector $v \in A^s$ whose components generate the unit ideal in A. To say that the injection $A \to A^s$ induced is isomorphic to the standard inclusion e_1 is to say that there is an isomorphism of A^s taking v to the vector $e_1 = (1, 0, \ldots, 0)$. Alternatively, it is to say that the element $v \in A^s$ can be completed to a basis for A^s.

Definition 6. Let A be any ring. A vector $v \in A^s$ is *unimodular* if its components generate the unit ideal in A. For two unimodular vectors v, w, we write

$$v \sim w$$

if there is a matrix $M \in \mathrm{GL}_S(A)$ such that $Mv = w$. This is clearly an equivalence relation.

So, the problem we are faced with now is to show that, for the rings of the form $A = k[x_1, \ldots, x_n]$, any two unimodular vectors are equivalent. Alternatively, we have to check when one is equivalent to the standard one $e_1 = (1, 0, \ldots, 0)$. Stated another way, we have to check whether there is an automorphism of A^s carrying v onto $(1, 0, \ldots, 0)$. If we can show this, then it will follow that any split injection $A \hookrightarrow A^s$ has a free cokernel.

Here is an easy first step:

Proposition 7. *Over a PID R, any two unimodular vectors are equivalent.*

Proof. In fact, unimodular vectors $v \in R^m$ correspond to imbeddings $R \to R^m$ which are split injections. But if we have a split injection in this way, the cokernel is free (as we are over a PID), and consequently there is a basis for R^m one of whose elements is v. This implies that v is conjugate to e_1. □

In a similar manner, if we use the fact that a finitely generated projective module over a *local* ring is free, then we obtain:

Corollary 8. *Over a local ring R, any two unimodular vectors are equivalent.*

Polynomial rings over a local ring

The proof of the Quillen-Suslin theorem is essentially to induct on the number of variables. To do this, we will need an auxiliary result which states that, under mild hypotheses, a unimodular vector in a polynomial ring is equivalent to a unimodular vector in the *base* ring. This will be proved locally – one prime at a time. So, we start with:

Theorem 9 (Horrocks)**.** *Let $A = R[x]$ for $R, (\mathfrak{m})$ a local ring. Then any unimodular vector in A^s one of whose elements has leading coefficient one is equivalent to e_1.*

Proof. Let $v(x) = (v_1(x), \ldots, v_s(x))$ be a unimodular vector. Suppose without loss of generality that the leading coefficient of $v_1(x)$ is one, so that $v_1(x) = x^d + a_1 x^{d-1} + \ldots$. If $d = 0$, then v_1 is a unit and there is nothing to prove. We proceed by induction on d.

Then, by making elementary row operations (which do not change the equivalence class of $v(x)$), we can assume that $v_2(x), \cdots, v_s(x)$ all have degree $\leq d-1$. Consider the coefficients of these elements. At least one of them must be a unit. In fact, if we reduce $\bmod \mathfrak{m}$, then not all the $v_i, i \geq 2$ can go to zero or the $v_i(x)$ would not generate the unit ideal $\bmod \mathfrak{m}$. So let us assume that $v_2(x)$ contains a unit among its coefficients.

The claim is now that we can make elementary row operations so as to find another unimodular vector, in the same equivalence class, one of whose elements is monic of degree $\leq d - 1$. If we can show this, then induction on d will easily complete the proof.

Lemma 10. *If we have two polynomials $a(x), b(x) \in R[x]$, with $\deg a = d$ and a monic, and b of degree $\leq d-1$ containing at least one coefficient which is a unit, there is a polynomial $a(x)e(x) + b(x)f(x) \in (a(x), b(x))$ of degree $\leq d-1$ whose leading coefficient is one.*

Proof. This is easy to see with a bit of explicit manipulation. □

This means that there are $e(x), f(x)$, such that $e(x)v_1(x) + f(x)v_2(x)$ has degree $\leq d-1$ and leading coefficient a unit. If we keep this fact in mind, we can, using row and column operations, modify the vector $v(x)$ such that it contains a monic element of degree $\leq d-1$. We just add appropriate multiples of v_1, v_2 to v_3 to make the leading coefficient a unit. This works if $s \geq 3$. If $s = 1$ or $s = 2$, the lemma can be checked directly. □

Consider the ring $R[x]$, and let $v(x) \in R[x]^s$ be a unimodular vector. We want a condition to conclude that $v(x) \sim v(0)$, where $v(0) \in R^s \subset R[x]^s$ is the vector obtained by pointwise substitution. This will be the inductive argument we need for the Quillen-Suslin theorem. We already have a good criterion for when this is true in the case R local.

Corollary 11. *If R is local and $v(x) \in R[x]^s$ is a unimodular vector one of whose elements is monic, then $v(x) \sim v(0)$.*

Proof. $v(0)$ is a unimodular vector in R, hence equivalent to e_1. We have also seen that $v(x)$ is equivalent to e_1. □

The goal of the next step is to generalize this to the case where R is not assumed local.

Localisation

Lemma 12. *Let R be a domain. We start by observing that if $v(x) \sim v(0)$ in $R[x]^s$, then $v(x+y) \sim v(x)$ over $R[x, y]$.*

Proof. By hypothesis there is a matrix $M(x) \in \mathrm{GL}_S(R[x])$ such that

$$M(x)v(x) = v(0),$$

which means that

$$M(x+y)v(x+y) = v(0).$$

We just have to then observe that

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

so we can take $M(x)^{-1}M(x+y) \in \mathrm{GL}_S(R[x, y])$ as the relevant matrix taking $v(x+y)$ into $v(x)$. □

The next lemma will be the required step to reduce to the case of R local.

Lemma 13. *Suppose $v(x) \sim v(0)$ over the localisation $R_S[x]$. Then there exists a $c \in S$ such that $v(x) \sim v(x + cy)$ over $R[x, y]$.*

Proof. As before, we can choose a matrix $M(x) \in \mathrm{GL}_S(R_S[x])$ such that $M(x)v(x) = v(0)$, and then the matrix $N(x, y) := M(x)^{-1}M(x + y)$ has the property that

$$N(x, y)v(x + y) = v(x).$$

It follows that if we substitute cy for y, then we have

$$N(x, cy)v(x + cy) = v(x).$$

The claim is that we can choose $c \in S$ such that $N(x, cy)$ actually has R-coefficients. In fact, this is because $N(x, 0) = I$, which implies that $N(x, y) = I + yW$ for some matrix W with values in $R_S[x, y]$. If we replace y with cy for c an element of S, then we can clear the denominators in W and arrange it so that $N(x, cy) \in R[x, y]$. □

Here, now, is the promised result which will be the crucial inductive step:

Corollary 14. *Suppose R is any ring, and $v(x) \in R[x]^s$ is a unimodular vector one of whose leading coefficients is one. Then $v(x) \sim v(0)$.*

Proof. Let us consider the set I of $q \in R$ such that $v(x + qy) \sim v(x)$ in $R[x, y]$. If we can show that $1 \in I$, then we will be done, because after applying the morphism $x \mapsto 0, R[x, y] \to R[y]$, we will get that $v(y) \sim v(0)$ in $R[y]$.

We start by observing that I is an ideal. Suppose $v(x + qy) \sim v(x)$ and $v(x + q'y) \sim v(x)$. Then, substituting $x \mapsto x + q'y$ in the first leads to

$$v(x + q'y + qy) \sim v(x + q'y) \in R[x, y]$$

and since $v(x + q'y) \sim v(x)$, we get easily by transitivity that $q + q' \in I$. Similarly, we have to observe that if $q \in I$ and $r \in R$, then $v(x + qry) \sim v(x)$. But this is true because one can substitute $y \mapsto ry$.

Since I is an ideal, to show that $1 \in I$ we just need to show that I is contained in no maximal ideal. Let $\mathfrak{m} \subset R$ be a maximal ideal. We then note that, by what we have already done for local rings, we have that

$$v(x) \sim v(0) \quad \text{in} \quad R_{\mathfrak{m}}[x].$$

By the lemma, this means that there is a $q \in R \setminus \mathfrak{m}$ such that $v(x + qy) \sim v(0)$; this means that $q \in I$. So I cannot be contained in $\mathfrak{m}$. Since this applies to any maximal ideal $\mathfrak{m}$, it follows that I must be the unit ideal. □

The Quillen-Suslin theorem

With all these preliminaries, it will be relatively straightforward to establish the main result; the first step is to show that unimodular vectors over a polynomial ring are all equivalent.

Theorem 15. *Let $R = k[x_1, \ldots, x_n]$ be a polynomial ring over a PID k, and let $v \in R^n$ be a unimodular vector. Then $v \sim e_1$.*

Proof. We prove this by induction on n. When $n = 0$, it is immediate.

Suppose $n \geq 1$. Then we can treat R as $k[x_1, \ldots, x_{n-1}, X]$ where we replace x_n by X to make it stand out. We can think of $v = v(X)$ as a vector of polynomials in X with coefficients in the smaller ring $k[x_1, \ldots, x_{n-1}]$.

If $v(X)$ has a term with leading coefficient one, then the previous results enable us to conclude that $v(X) \sim v(0)$, and as $v(0)$ lies in $k[x_1, \ldots, x_{n-1}]$ we can use induction to work downwards. The claim is that, possibly after a change of variables $x_1, \ldots, x_n$, we can always arrange it so that the leading coefficient in $X = x_n$ is one. The relevant change of variables leaves $X = x_n$ constant and

$$x_i \mapsto x_i - X^{M^i}, \quad M \gg 0 \quad (1 \leq i < n).$$

If M is chosen very large, one makes by this substitution the leading term of each of the elements of v a unit. So, without loss of generality we can assume that this is already the case. Thus, we can apply the inductive hypothesis on n to complete the proof. □

Theorem 16 (Quillen-Suslin)**.** *Let k be a PID. Then any finitely generated projective module over $k[x_1, \ldots, x_n]$ is free.*

Proof. We have to show that a stably free module over $R = k[x_1, \ldots, x_n]$ is free. That is, if P is such a finitely generated module such that $P \oplus R^m \simeq R^{m'}$, then P is free. By induction on m, one reduces to the case $m = 1$. In this case we have an exact sequence

$$0 \to R \to R^{m'} \to P \to 0$$

and we have to conclude that the coker P is free.

But the injection $R \to R^{m'}$ corresponds to a unimodular vector, and we have seen that this is isomorphic to the standard embedding $e_1 \colon R \to R^{m'}$, whose cokernel is obviously free. Thus P is free. □