# THE PROOF OF THE QUILLEN-SUSLIN THEOREM

## 1. Unimodular Vectors

**Definition 1.** *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.*

**Proposition 2.** *Over a principal ideal domain $R$, 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 $e_1 = (1, 0, \dots, 0)$. □

**Theorem 3** (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 $v(x) = (v_1(x), \dots, v_s(x))$ be a unimodular vector. Suppose without loss of generality that the leading coefficient of $v_1(x)$ is one, so that $v_1(x) = x^d + a_1 x^{d-1} + \dots$. If $d = 0$, then $v_1$ is a unit and there is nothing to prove. We will induct on $d$.

Then, by making elementary row operations (which don't change the equivalence class of $v(x)$), we can assume that $v_2(x), \dots, v_s(x)$ 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 mod $\mathfrak{m}$, then not all the $v_i, i \geq 2$ can go to zero or the $v_i(x)$ would not generate the unit ideal mod $\mathfrak{m}$. 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.

Now, here is a lemma: 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. 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. □

**Corollary 4.** *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.* In fact, $v(0)$ is a unimodular vector in $R$, hence equivalent to $e_1$. We have also seen [in Theorem 3] that $v(x)$ is equivalent to $e_1$. □

**Lemma 5.** *Suppose $v(x) \sim v(0)$ over the localization $R_S[x]$. 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 $N(x,cy) \in R[x,y]$. □

**Corollary 6.** *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 homomorphism $x \mapsto 0, R[x,y] \to R[y]$, we will get that $v(y) \sim v(0)$ in $R[y]$.

We start by observing that $I$ is an ideal. In fact, 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 [Corollary 4], we have that

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

By Lemma 5, this means that there is a $q \in R - \mathfrak{m}$ 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. □

Let $R$ be a commutative ring. For any ideal $\mathfrak{A}$ in $R[t]$, let $\ell(\mathfrak{A})$ be the set in $R$ consisting of zero and all the leading coefficients of polynomials in $\mathfrak{A}$. This is clearly an ideal in $R$ (containing $\mathfrak{A} \cap R$). We shall need the following lemma which relates the height of $\ell(\mathfrak{A})$ to the height of $\mathfrak{A}$. (By definition, $\mathrm{ht} I = \min\{\mathrm{ht}\mathfrak{p}\}$ where $\mathfrak{p}$ ranges over all prime ideals $\supseteq I$. The height of the unit ideal is taken to be $\infty$.)

**Lemma 7.** *Let $R$ be a commutative noetherian ring, and $\mathfrak{A}$ be an ideal in $R[t]$. Then $\mathrm{ht}\ell(\mathfrak{A}) \geqslant \mathrm{ht}\mathfrak{A}$.*

*Proof.* First assume $\mathfrak{A}$ is a prime ideal, $\mathfrak{P}$; let $\mathfrak{p} = \mathfrak{P} \cap R$. If $\mathfrak{P} = \mathfrak{p}[t]$, clearly $\ell(\mathfrak{P}) = \mathfrak{p}$, so $\mathrm{ht}\ell(\mathfrak{P}) = \mathrm{ht}\mathfrak{p} = \mathrm{ht}\mathfrak{p}[t] = \mathrm{ht}\mathfrak{P}$ by (II.7.7). If $\mathfrak{P} \supsetneq \mathfrak{p}[t]$, clearly $\ell(\mathfrak{P}) \supsetneq \mathfrak{p}$, so, again by (II.7.7), $\mathrm{ht}\ell(\mathfrak{P}) > \mathrm{ht}\mathfrak{p} = \mathrm{ht}\mathfrak{P} - 1$, i.e., $\mathrm{ht}\ell(\mathfrak{P}) \geqslant \mathrm{ht}\mathfrak{P}$. For the general case, let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ be the prime ideals of $R[t]$ that are minimal over $\mathfrak{A}$. (We know that $r < \infty$ by (II.7.6), since $R[t]$ is noetherian by Hilbert's Basis Theorem. Also, we may assume $r \geqslant 1$, for if $\mathfrak{A}$ is the unit ideal, we have $\mathrm{ht}\,\ell(\mathfrak{A}) = \infty = \mathrm{ht}\,\mathfrak{A}$.) From

$$\prod \mathfrak{P}_i \subseteq \bigcap \mathfrak{P}_i = \mathrm{rad}\,\mathfrak{A},$$

we see that $(\prod \mathfrak{P}_i)^N \subseteq \mathfrak{A}$ for some $N$. Applying "$\ell$" to this, and using the fact that $\ell(I) \cdot \ell(J) \subseteq \ell(I \cdot J)$, we get $\prod \ell(\mathfrak{P}_i)^N \subseteq \ell(\mathfrak{A})$. Let $\mathfrak{p}$ be a prime over $\ell(\mathfrak{A})$ with $\mathrm{ht}\,\ell(\mathfrak{A}) = \mathrm{ht}\,\mathfrak{p}$. Then $\ell(\mathfrak{P}_i) \subseteq \mathfrak{p}$ for some $i$, from which we get

$$\mathrm{ht}\,\mathfrak{A} \leqslant \mathrm{ht}\,\mathfrak{P}_i \leqslant \mathrm{ht}\,\ell(\mathfrak{P}_i) \leqslant \mathrm{ht}\,\mathfrak{p} = \mathrm{ht}\,\ell(\mathfrak{A}). \qquad \square$$

**Theorem 8** (Suslin's Monic Polynomial Theorem)**.** *Let $R$ be a commutative noetherian ring of Krull dimension $d < \infty$. Let $\mathfrak{A}$ be an ideal in $A = R[t_1, \ldots, t_m]$, with $\mathrm{ht}\,\mathfrak{A} > d$. Then there exist new "variables" $s_1, \ldots, s_m \in A$ with $A = R[s_1, \ldots, s_m]$ such that $\mathfrak{A}$ contains a polynomial that is monic as a polynomial in $s_1$.*

*Proof.* We induct on $m$. If $m = 0$, $\mathrm{ht}\,\mathfrak{A} > d$ means $\mathfrak{A} = R$ so the result is trivial. For $m \geqslant 1$, write $B = R[t_1, \ldots, t_{m-1}]$; we view $\mathfrak{A}$ as an ideal in $B[t_m] = A$, and get $\ell(\mathfrak{A}) \subseteq B$. By (3.2), $\mathrm{ht}\,\ell(\mathfrak{A}) \geqslant \mathrm{ht}\,\mathfrak{A} > d$, so, by the inductive hypothesis, we can write $B = R[s_1, \ldots, s_{m-1}]$ such that there exists $g \in \ell(\mathfrak{A})$ that is monic in $s_1$, say,

$$g = s_1^T + g_{T-1}s_1^{T-1} + \cdots + g_0 \quad (g_i \in R[s_2, \ldots, s_{m-1}]).$$

By definition of $\ell(\mathfrak{A})$, $\mathfrak{A}$ contains a polynomial

$$f = g \cdot t_m^N + b_{N-1}t_m^{N-1} + \cdots + b_0, \quad b_i \in B.$$

Let $M$ be the highest power of $s_1$ occurring in $b_0, \ldots, b_{N-1}$. Set $t_m = s_m + s_1^K$, so $A = B[t_m] = R[s_1, \ldots, s_m]$. In $b_{N-1}t_m^{N-1} + \cdots + b_0$, $s_1$ occurs with exponent $\leqslant M + K(N-1)$. On the other hand,

$$g \cdot t_m^N = (s_1^T + g_{T-1}s_1^{T-1} + \cdots + g_0)(s_m + s_1^K)^N$$

is monic of degree $T + KN$ in $s_1$. For $K$ sufficiently large, we have $T + K \cdot N > M + K(N-1)$, so $f$ is monic as a polynomial in $s_1$. $\square$

**Lemma 9.** *Let $R$ be a commutative noetherian ring, and $(a_1, \dots, a_n) \in \mathrm{Um}_n(R)$. Then $(a_1, \dots, a_n) \sim_{\mathrm{E}_n(R)} (a'_1, \dots, a'_n)$ where, for any $r \leqslant n$, $\mathrm{ht}((a'_1, \dots, a'_r)) \geqslant r$.*

*Proof.* Suppose we have already $\mathrm{ht}((a_1, \dots, a_r)) \geqslant r$, for some $r$. Consider $(\bar{a}_{r+1}, \dots, \bar{a}_n) \in \mathrm{Um}_{n-r}(\overline{R})$, where $\overline{R} = R/(a_1, \dots, a_r)$. Note that we can find an element $a'_{r+1} = a_{r+1} + b_{r+2}a_{r+2} + \cdots + b_n a_n$ such that $\bar{a}'_{r+1}$ avoids all the minimal primes of $\overline{R}$. Then

$$(a_1, \dots, a_r, a_{r+1}, \dots) \sim_{\mathrm{E}_n(R)} (a_1, \dots, a_r, a'_{r+1}, \dots).$$

Let $\mathfrak{p}$ be any prime containing $(a_1, \dots, a_r, a'_{r+1})$. Since $\bar{\mathfrak{p}}$ cannot be minimal in $\overline{R}$, there exists another prime, $\mathfrak{p}'$, such that $(a_1, \dots, a_r) \subseteq \mathfrak{p}' \subsetneq \mathfrak{p}$. Thus,

$$\mathrm{ht}\,\mathfrak{p} > \mathrm{ht}\,\mathfrak{p}' \geqslant \mathrm{ht}(a_1, \dots, a_r) \geqslant r,$$

i.e., $\mathrm{ht}\,\mathfrak{p} \geqslant r+1$. It follows that $\mathrm{ht}(a_1, \dots, a_r, a'_{r+1}) \geqslant r+1$, so the proof proceeds by induction. □

**Lemma 10.** *Let $R$ be a commutative noetherian ring, of Krull dimension $d < \infty$, and let $A = R[t_1, \dots, t_m]$. If $f = (f_1, \dots, f_n) \in \mathrm{Um}_n(A)$, $n \geqslant d+2$, then $f \sim_G (1, 0, \dots, 0)$.*

*Proof.* We induct on $m$; the case $m = 0$ is trival. To deal with the general case, find $f \sim_{\mathrm{E}_n(A)} (f'_1, \dots, f'_n)$ such that $\mathrm{ht}((f'_1, \dots, f'_r)) \geqslant r$ for every $r \leqslant n$. In particular, $\mathfrak{A} = (f'_1, \dots, f'_{n-1})$ has height $\geqslant n-1 > d$. By Suslin's Monic Polynomial Theorem, there exist new variables $s_1, \dots, s_m$ such that $A = R[s_1, \dots, s_m]$, and such that $\mathfrak{A}$ contains $f'_1 g_1 + \cdots + f'_{n-1} g_{n-1}$ that is monic as a polynomial in $s_1$. Using elementary transformations, we may replace $f'_n$ by

$$f'_n + s_1^N (f'_1 g_1 + \cdots + f'_{n-1} g_{n-1}),$$

so we may assume that $f'_n$ is already monic as a polynomial in $s_1$. By (1.7),

$$\begin{aligned}(f'_1, \dots, f'_n) &\sim_G (f'_1(0, s_2, \dots, s_m), \dots, f'_n(0, s_2, \dots, s_m)) \\ &\in \mathrm{Um}_n(R[s_2, \dots, s_m]).\end{aligned}$$

By the inductive hypothesis, the latter is $\sim_G (1, 0, \dots, 0)$. □

**Theorem 11.** *Let $R = k[x_1, \dots, x_n]$ be a polynomial ring over a principal ideal domain $k$, and let $v \in R^n$ be a unimodular vector. Then $v \sim e_1$.*

*Proof.* We can now prove this by induction on $n$. When $n = 0$, it is immediate (by Proposition 2).

Suppose $n \geq 1$. Then we can treat $R$ as $k[x_1, \dots, x_{n-1}, X]$, 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 $k[x_1, \dots, x_{n-1}]$.

If $v(X)$ has a term with leading coefficient one, then the previous results [Corollary 6] enable us to conclude that $v(X) \sim v(0)$, and as $v(0)$ lies in $k[x_1, \dots, x_{n-1}]$ we can use induction to work downwards. By Lemma 10, possibly after a change of variables $x_1, \dots, x_n$, 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 $v$ monic. 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. □

## 2. Stably Freeness

**Definition 12.** *A finitely generated module $P$ over a commutative ring $R$ is said to be stably free if there exists a finitely generated free module $F$ such that the direct sum $P \oplus F$ is a free module.*

**Proposition 13.** *Let $M$ be a projective module. Then $M$ is stably free if and only if $M$ admits a finite free resolution.*

*Proof.* If $M$ is stably free then it is trivial that $M$ has a finite free resolution. Conversely assume the existence of the resolution with the above notation. We prove that $M$ is stably free by induction on $n$. The assertion is obvious if $n = 0$. Assume $n \geqq 1$. Insert the kernels and cokernels at each step, in the manner of dimension shifting. Say

$$M_1 = \operatorname{Ker}(E_0 \to P),$$

giving rise to the exact sequence

$$0 \to M_1 \to E_0 \to M \to 0.$$

Since $M$ is projective, this sequence splits, and $E_0 \cong M \oplus M_1$. But $M_1$ has a finite free resolution of length smaller than the resolution of $M$, so there exists a finite free module $F$ such that $M_1 \oplus F$ is free. Since $E_0 \oplus F$ is also free, this concludes the proof of the theorem. □

**Lemma 14.** *Let $R$ be a ring. Let $0 \to P' \to P \to P'' \to 0$ be a short exact sequence of finite $R$-modules. If 2 out of 3 of these modules has a finite free resolution, then so is the third.*

**Proposition 15.** *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.* Let $M$ be a finite $R[x]$-module. $M$ has a finite filtration

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

such that each factor $M_i/M_{i+1}$ is isomorphic to $R[x]/P_i$ for some prime $P_i$. In light of Lemma 14, it suffices to prove the theorem in case $M = R[x]/P$ where $P$ is prime, which we now assume. In light of the exact sequence

$$0 \to P \to R[x] \to R[x]/P \to 0$$

and Lemma 14, we note that $M$ has a finite free resolution if and only if $P$ does.

Let $\mathfrak{p} = P \cap R$. Then $\mathfrak{p}$ is prime in $R$. Suppose there is some $M = R[x]/P$ which 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. This is possible in light of one of the basic properties characterizing Noetherian rings.

Let $R_0 = R/\mathfrak{p}$ so $R_0$ is entire. 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 $f_1, \ldots, f_n$ be a finite set of generators for $P_0$, and let $f$ be a polynomial of minimal degree in $P_0$. Let $K_0$ be the quotient field of $R_0$. By the euclidean algorithm, we can write

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

with $q_i, r_i \in K_0[x]$ 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 $R_0[x]$. Since $\deg f$ is minimal in $P_0$ it follows that $r_i' = 0$ for all $i$, so

$$d_0 P_0 \subset R_0[x] f = (f).$$

Let $N_0 = P_0/(f)$, 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 $d_0 \pmod{\mathfrak{p}}$. 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 $R_0[x]/\bar{Q}_0$ where $\bar{Q}_0$ is an associated prime of $N_0$. Let $Q$ be the inverse image of $\bar{Q}_0$ 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 Lemma 14 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

$$0 \to E_n \to \cdots \to E_0 \to \mathfrak{p} \to 0.$$

Then we may simply 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 as $R[x]$-module.

Since $R_0$ is entire, it follows that the principal ideal $(f)$ in $R_0[x]$ is $R[x]$-isomorphic to $R_0[x]$, and therefore has a finite free resolution as $R[x]$-module. Lemma 14 applied to the exact sequence of $R[x]$-modules

$$0 \to (f) \to P_0 \to N \to 0$$

shows that $P_0$ has a finite free resolution; and further applied to the exact sequence

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

shows that $P$ has a finite free resolution, thereby concluding the proof. □

Then we have

**Theorem 16.** *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 17.** *Every finitely generated projective module over $k[x_1, \ldots, x_n]$, for any principal ideal domain $k$, is necessarily stably free.*

## 3. Quillen-Suslin theorem

**Theorem 18** (Quillen-Suslin)**.** *Any finitely generated projective module over $k[x_1, \ldots, x_n]$ for $k$ a principal ideal domain is free.*

*Proof.* By Corollary 17, we only need 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 cokernel $P$ is free.

But the injection $R \to R^{m'}$ corresponds to a unimodular vector, and we have seen (by Theorem 11) that this is isomorphic to the standard embedding $e_1 : R \to R^{m'}$, whose cokernel is obviously free. Thus $P$ is free. □

## References

[1] https://amathew.wordpress.com/2012/01/16/the-quillen-suslin-theorem.

[2] Serge Lang, *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer, 2002.

[3] Tsit Yuen Lam, *Serre's problem on projective modules*. Springer, 2006.