On seminormality

Thierry Coquand

September 21, 2005

We give an elementary and essentially self-contained proof[1] that a reduced ring R is seminormal iff the canonical map $\mathsf{Pic}\ R \rightarrow \mathsf{Pic}\ R[X]$ is an isomorphism, a theorem due to Swan [12], generalising some previous results of Traverso [13]. By a simple modification of this argument, we obtain a constructive proof, and hence an algorithm [9], associated to a classical proof which is not so easy otherwise to access, since it requires a journey through [12, 13, 1] or, in the domain case, through [11, 10, 5, 6].

We recall [12] that R is *seminormal* iff if $b^2 = c^3$ then there exists $a \in R$ such that $b = a^3$ and $c = a^2$. This is a remarkably simple (and technically first-order) condition. Similarly, the statement that the canonical map $\mathsf{Pic}\ R \rightarrow \mathsf{Pic}\ R[X]$ is an isomorphism can also be formulated in an elementary way, see the statement of Theorem 2.2. Swan's original definition includes that R is reducible, but, as noticed by Costa [3], reducibility follows from seminormality: if $d^2 = 0$ then $d^2 = d^3 = 0$ and so there exists $a \in R$ such that $d = a^2 = a^3$. We have then $d = aa^2 = ad$ and so $d = a(ad) = d^2 = 0$. Section 7 of Chapter VIII of [7] surveys the work on commutative seminormal ring up to day.

1 Main theorem

Lemma 1.1 *Let M be a projection matrix of rank 1 over a ring A. The matrix M represents a free module iff there exists $x_i, y_j \in A$ such that $m_{ij} = x_i y_j$. Furthermore the column vector (x_i) and the line vector (y_j) are uniquely defined up to a unit by these conditions: if we have $x'_i, y'_j \in A$ such that $m_{ij} = x'_i y'_j$ then there exists a unit u of A such that $x_i = ux'_i$ and $y'_j = uy_j$.*

Proof. Let I be the the module generated by the columns of M. Let (x_i) be a column vector in A^n that generates the module I. There exists y_j such that $x_i y_j = m_{ij}$. If we have also $m_{ij} = x'_i y'_j$ then we have $\Sigma x'_i y'_i = 1$ and so $x'_i = \Sigma x'_j m_{ij}$. This shows that the vector (x'_i) is in the module I and so is also a generator of I. Hence there exists a unit u of A such that $x_i = ux'_i$. In the same way, there exists a unit v such that $y'_j = vy_j$. Writing $\Sigma x_i y_i = \Sigma x'_i y'_i = 1$ we see that $u = v$. $\square$

We let P_n be the $n \times n$ matrix p_{ij} with $p_{11} = 1$ and $p_{ij} = 0$ if $i, j \neq 1, 1$ and I_n the $n \times n$ identity matrix.

Corollary 1.2 *Let E be an extension of the ring R which is reduced. Let M be a $n \times n$ projection matrix over $R[X]$ such that $M(0) = P_n$. Assume that $f_i, g_j \in E[X]$ are such that $m_{ij} = f_i g_j$ and $f_1(0) = 1$. If M represents a free module over $R[X]$ then $f_i, g_j \in R[X]$.*

[1] The only non trivial result that we use is a basic theorem of Kronecker, proved in an elementary way in the references [2, 4, 8].

Proof. By Lemma 1.1 there exists $f'_i, g'_j \in R[X]$ such that $m_{ij} = f'_i g'_j$. We can assume $f'_1(0) = 1$. By Lemma 1.1 there exists a unit u of $E[X]$ such that $f_i = uf'_i$ and $g'_j = ug_j$. We have $u(0) = 1$ and since E is reduced $u = u(0) = 1$. □

Theorem 1.3 *Let A be seminormal and $M = (m_{ij})$ be a $n \times n$ projection matrix of rank 1 over $A[X]$ such that $M(0) = P_n$. We assume that C is a finite reduced integral extension of A generated by the coefficients of $f_i, g_i \in C[X]$, $1 \leq i \leq n$ satisfying $m_{ij} = f_i g_j$ and $f_1(0) = 1$. We have $f_i, g_j \in A[X]$ and hence $C = A$.*

Proof. Since A is seminormal, the conductor $I = \{r \in A \mid rC \subseteq A\}$ of C in A is an ideal radical of A *and* C and is equal to

$$I = \{r \in A \mid rf_i,\ rg_j \in A[X]\}$$

Indeed, we prove first that if $u \in C$ and $u^2 \in I$ then $u \in A$. This follows from $u^2 \in I \subseteq A$ and $u^3 = u^2 u \in A$. We have then $a \in A$ such that $a^2 = u^2$, $a^3 = u^3$ and this implies $(a-u)^3 = 0$ and since C is reduced, $a = u$ and hence $u \in A$.

We now prove that $u \in I$ which will prove that I is a radical ideal. For this, let c be an element of C. We know $u^2c^2 \in A$ and $u^3c^3 = u^2uc^3 \in A$ since $u^2 \in I$. Hence as previously, we conclude $uc \in A$. This shows $u \in I$.

Since C is generated by the coefficients of f_i and g_j and they are all integral over A we conclude from the fact that I is radical that we have also

$$I = \{r \in A \mid rf_i,\ rg_j \in A[X]\}$$

Indeed, if $ru \in A$ for all coefficients u of f_i and g_j then we have $r^N u \in A$ for all $u \in C$ for a big enough N. Hence $r^N \in I$ and so $r \in I$.

To prove $C = A$, it is enough to show $1 \in I$. Otherwise, let $\mathfrak{p}$ be a minimal prime of A containing I, and let S be the complement of $\mathfrak{p}$ in A. Then I_S is the maximal ideal of A_S. Let R be the quotient field A_S/I_S. Since $R[X]$ is principal, the matrix M represents a free module over $R[X]$. Also $E = C_S/I_S$ is a reduced extension of R. By Corollary 1.2 we have $f_i, g_j \in R[X]$. So there is a $s \in S$ such that $sf_i, sg_j \in A[X]$, which contradicts $s \notin I$. □

We notice that we don't need to state that the coefficients of f_i and g_j are integral over A, since this is implied by the other conditions. Indeed, if u is a coefficient of f_i, it follows from $f_i g_j \in A[X]$ that $ug_j(0)$ is integral over A for all j. This is a consequence of Kronecker's theorem [2, 4, 8] that states that if $P_1 P_2 = Q$ in $A[X]$ then any product $u_1 u_2$, where u_i is a coefficient of P_i, is integral over the coefficients of Q. Since $g_1(0) = 1$ this implies that u is integral over A.

In Appendix 2, we show how to explain constructively the use of minimal prime ideals in this argument.

2 Picard groups in the domain case

As an application, we can prove the following result, which expresses concretely the fact that the canonical map $\mathsf{Pic}\ A \to \mathsf{Pic}\ A[X]$ is an isomorphism, in the case where A is a seminormal domain.

Lemma 2.1 *Let R be a gcd domain and $M = (m_{ij})$ is a projection matrix of rank 1 such that m_{11} is regular then M represents a free module over R: there exists $f_i, g_j \in R$ such that $m_{ij} = f_i g_j$.*

Proof. For this, we take $f_1 \in R$ to be a gcd of the first line m_{1j}. This determines uniquely all the g_j and then all the other f_i. More precisely, once we have f_1 the equality $g_j f_1 = m_{1j}$ determines g_j. Since M is of rank 1 we have $m_{11}m_{ij} = m_{i1}m_{1j}$ and so $h_1 m_{ij} = m_{i1}g_j$, so that h_1 divides all $m_{i1}g_j$ and so divides their gcd, which is m_{i1}. This determines uniquely f_i such that $h_1 f_i = m_{i1}$ and it follows from $m_{11}m_{ij} = m_{i1}m_{1j}$ that we have $m_{ij} = f_i g_j$. □

Theorem 2.2 *If A is a seminormal domain, and $M = (m_{ij})$ is a $n \times n$ projection matrix of rank 1 of $A[X]$ such that $M(0) = P_n$ then there exists $f_i, g_j \in A[X]$ such that $m_{ij} = f_i g_j$ and $f_1(0) = 0$.*

Proof. We let K be the field of fractions of A. Since $K[X]$ is a gcd domain, we can apply Lemma 2.1 and find $f_i, g_j \in K[X]$ such that $f_i g_j = m_{ij}$ and $f_1(0) = 1$. By the previous theorem we have $f_i, g_j \in A[X]$. □

Corollary 2.3 *If A is a seminormal domain then the canonical map* $\mathsf{Pic}\ A \to \mathsf{Pic}\ A[X]$ *is an isomorphism.*

Proof. We have to prove that if M is a projection matrix of rank 1 over $A[X]$ such that $M(0)$ represents a free module over A, then M represents a free module over $A[X]$. By Lemma 1.1 we have $x_i, y_j \in A$ such that $x_i y_j = m_{ij}(0)$ so that, if x is the column vector (x_i) and y the line vector (y_j) we have $M(0) = xy$ and $1 = yx$. By adding a line and a column of 0 to the matrix M, we can assume that $M(0)$ is similar to a matrix P_{n+1}: indeed we have[2]

$$\begin{pmatrix} 0 & 0 \\ 0 & xy \end{pmatrix} = \begin{pmatrix} 0 & y \\ -x & I_n - xy \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & -y \\ x & I_n - xy \end{pmatrix}$$

and

$$I_{n+1} = \begin{pmatrix} 1 & 0 \\ 0 & I_n \end{pmatrix} = \begin{pmatrix} 0 & y \\ -x & I_n - xy \end{pmatrix} \begin{pmatrix} 0 & -y \\ x & I_n - xy \end{pmatrix} = \begin{pmatrix} 0 & -y \\ x & I_n - xy \end{pmatrix} \begin{pmatrix} 0 & y \\ -x & I_n - xy \end{pmatrix}$$

In this way we reduce further the problem to the case where $M(0) = P_{n+1}$, and we can then apply Theorem 2.2. □

We notice also that the previous reasoning applies directly for $A[X_1, \dots, X_n]$. Indeed, if K is a field then $K[X_1, \dots, X_n]$ is a gcd domain [9], and Kronecker's theorem holds for polynomials in several variables as well: $P_1 P_2 = Q \in A[X_1, \dots, X_n]$ then, any product $u_1 u_2$ where u_i is a coefficient of P_i, is integral over the coefficients of Q [4].

Corollary 2.4 *If A is a seminormal domain then the canonical map* $\mathsf{Pic}\ A \to \mathsf{Pic}\ A[X_1, \dots, X_n]$ *is an isomorphism.*

As a very special case, we get a direct proof of Quillen-Suslin's theorem for projective modules of rank 1.

[2] These identities are due to Claude Quitté and allow for a self-contained argument.

3 General case

The hypothesis that A is a domain was only used to build a reduced extension L of A for which we can find $f_k, g_l \in L[X]$ such that $f_k g_l = m_{kl}$ and $f_1(0) = 1$.

Indeed when we have such an extension, we can consider the subalgebra C generated by the coefficients of f_i and g_j. This is a finite integral extension of A and Theorem 1.3 applies.

Thus, the problem reduces to show the existence of a reduced extension L of A for which we can find $f_k, g_l \in L[X]$ such that $f_k g_l = m_{kl}$ and $f_1(0) = 1$. The proof of Theorem 2.2 shows how to find $f_k, g_l \in K[X]$ satisfying $f_1(0) = 1$ and $\phi(m_{kl}) = f_k g_l$ whenever we have a map $\phi : A \to K$, where K is a field (and f_k, g_l are even uniquely determined by these conditions). It is thus enough to find enough such maps $\phi_\alpha : A \to K_\alpha$ so that $A \to \Pi K_\alpha$ is injective. We can for instance take all maps $A \to A/\mathfrak{p} \to K_\mathfrak{p}$ where $K_\mathfrak{p}$ is the field of fraction of $A/\mathfrak{p}$. Since A is reduced, L is an extension of A.

Constructively, even if A is not a domain, the reasoning of Theorem 2.2 gives a finite covering $D(b_i) \cap V(\vec{a_i})$ of spec A (for the constructible topology), and for each i a family $f^i_k, h^i_l \in A_i[X]$, with $A_i = A_{b_i}/\sqrt{<\vec{a_i}>}$, such that $f^i_1(0) = 1$ and $f^i_k h^i_l = m_{kl} \in A_i[X]$. Notice that each A_i is reduced. Also, if $a \in A$ and $a = 0$ in A_i then $D(a) \cap D(b) \cap V(\vec{a_i}) = 0$. Hence $a \in A$ becomes 0 in each A_i iff a is nilpotent. Thus, if A is reduced, we have built in this way a reduced extension $L = \Pi A_i$ of A for which we can find $f_k, g_l \in L[X]$ such that $f_k g_l = m_{kl}$ and $f_k(0) = 1$.

Conclusion

In general, if A is reduced and C is the integral extension of A generated by the coefficients of f_i and g_j we can still conclude that there are finitely many constants $a_1, \dots, a_n \in C$ such that $a^2_{i+1}, a^3_{i+1} \in A[a_1, \dots, a_i]$ and $C = A[a_1, \dots, a_n]$. Indeed, we consider the intermediary extension $B \subseteq C$ of elements that belong to such a chain of seminormal extensions, and we can apply the reasoning of Theorem 1.3 to conclude that $B = C$. Since our argument is constructive, it can be seen as an algorithm which computes such $a_1, \dots, a_n \in C$ from the coefficients of the matrix M.

Appendix 1: Schanuel's example

Conversely, one can show that if A is reduced and the canonical map $\mathsf{Pic}\ A \to \mathsf{Pic}\ A[X]$ is an isomorphism, then A is seminormal. The construction is elementary and due to Schanuel. Take $b, c \in A$, assume $b^3 = c^2$ and let B be a reduced extension of A with $a \in B$ such that $b = a^2, c = a^3$. We consider the polynomials in $B[X]$

$$f_1 = 1 + aX,\ f_2 = bX^2,\ g_1 = (1 - aX)(1 + bX^2),\ g_2 = bX^2$$

The matrix $M = (f_i g_j)$ is a projection matrix of rank 1 in $A[X]$ such that $M(0) = P_2$.

If the canonical map $\mathsf{Pic}\ A \to \mathsf{Pic}\ A[X]$ is an isomorphism, this matrix should present a free module over $A[X]$. By Corollary 1.2 this implies $f_i, g_j \in A[X]$ and so we have $a \in A$.

Corollary A.1 *If A is seminormal so is $A[X]$.*

Proof. This follows from Schanuel's example and Corollary 2.4. □

Appendix 2: A constructive proof of Theorem 1.3

If M is a rectangular matrix over a ring, we write $\Delta_k(M)$ the ideal generated by all minors of M of order k. If $m = a_0 + \ldots + a_k X^k$ in $R[X]$ we call a_k the (formal) leading coefficient of m (this coefficient may be 0) and k the (formal) degree of m. If $M = (m_{ij})$ is a matrix over $R[X]$, we write $C(M)$ the set of constants $r \in R$ that can be written of the form $\Sigma u_i v_j m_{ij}$ with $u_i, v_j \in R[X]$.

Lemma A.2 *Let R be a reduced ring. If M is a matrix over $R[X]$ such that $\Delta_1(M) = 1$ then the annihilator of $C(M)$ is 0.*

Proof. Let a be an element such that $aC(M) = 0$, by working in the localisation R_a, we reduce the statement to: if $C(M) = 0$ then $1 = 0$ in R.

Notice that each localisation $R_u,\ u \in R$ is reduced, and that $1 = 0$ in R_u iff $u = 0$ in R. Notice also that an elementary transformation on M does not change neither $C(M)$ nor $\Delta_1(M)$.

We first prove that statement in the case where at least one m_{ij} has a a leading coefficient u which is invertible, by induction on the degree n of such m_{ij}. If $n = 0$ the statement is clear, since then $u \in C(M)$. Also, if we have a leading coefficient v of one m_{kl} of degree $< n$, then by induction we have $1 = 0$ in R_v and hence $v = 0$ in R, so any m_{kl} of formal degre $< n$ is equal to 0. This shows that m_{ij} divides all m_{kl}, since by elementary transformations, we can make first all $m_{il},\ l \neq j$ of formal degree $< n$, and so 0, and then all $m_{kj},\ k \neq i$ and finally all remaining m_{kl} to be 0 as well. So $\Delta_1(M) = <m_{ij}> = 1$ and so $1 = 0$ in R.

From this, we conclude that if u is a leading coefficient of one m_{ij} we have $1 = 0$ in R_u and so $u = 0$ in R. Thus $M = 0$ and $1 = 0$ in R. □

Classically, one would prove the statement as follows: let $\mathfrak{p}$ be a minimal prime of R. Then $R_{\mathfrak{p}}$ is a field. The statement is clear if R is a field because, by writing M in Smith normal form, we find u_i, v_j in $R[X]$ such that $1 = \Sigma u_i v_j m_{ij}$. Thus the annihilator of $C(M)$ is included in all minimal primes $\mathfrak{p}$.

We can use this lemma to end the proof of Theorem 1.3 in a constructive way as follows. We have to prove that $1 \in I$. By Lemma A.2 applied to the matrix $M = (f_i g_j)$ modulo I it is enough to show that if $u_i, v_j \in A[X]$ and $\Sigma u_i v_j f_i g_j$ is a constant $s \in A$ modulo I then s is in I.

Since $\Sigma u_i v_j f_i g_j = (\Sigma u_i f_i)(\Sigma v_j g_j) = s$ modulo I and since I is a radical ideal, we conclude that both $s^m(\Sigma u_i f_i)$ and $s^m(\Sigma v_j g_j)$ are constants in A modulo I for some m. Indeed, we reason in $L[X]$ where $L = (C/I)_s$ which is reduced; in the ring $L[X]$ we have that $(\Sigma u_i f_i)(\Sigma v_j g_j)$ is an invertible constant, and hence both $s^m(\Sigma u_i f_i)$ and $s^m(\Sigma v_j g_j)$ are constant in C modulo I for some m. Since $f_i(0), g_j(0) \in A$, we conclude that these constants are in A.

Also

$$s^{m+1} f_i = (\Sigma v_j g_j f_i) s^m (\Sigma u_i f_i)$$

and

$$s^{m+1} g_j = (\Sigma u_i f_i g_j) s^m (\Sigma v_j g_j)$$

are in $A[X]$, and hence $s^{m+1} \in I$ and $s \in I$ as desired, since I is a radical ideal.

Acknowledgement

Henri Lombardi suggested the problem of finding an elementary proof of Swan's theorem. Thanks also to Peter Schuster for discussions on this topic and to Claude Quitté for many improvements in the presentation of this note.

References

[1] H. Bass and M. Pavaman Murthy. Grothendieck groups and Picard groups of abelian group rings. *Ann. of Math.* 86 (1967), 16-23.

[2] Th. Coquand and H. Persson. Valuations and Dedekind Prague theorem. *J. Pure Appl. Algebra*, 155 (2001), 121-129

[3] D.L. Costa. Seminormality and projective module. Séminaire d'algèbre Dubreil et Marie-Paule Malliavin, 34ème année, Vol. **924**, (1982)

[4] H. Edwards. *Divisor Theory.* Boston, MA: Birkhäuser, 1989

[5] R. Gilmer and R. Heitmann. On Pic $R[X]$ for R seminormal. *J. Pure Appl. Algebra* 16 (1980), 251-257

[6] F. Ischebeck. Zwei Bemerkungen über Seminormale Ringe. *Math. Z.* 152 (1977), 101-106

[7] T-Y. Lam. *Serre's Problem on Projective Module.* to appear, 2005

[8] H. Lombardi. Hidden constructions in abstract algebra (1) Integral dependence relations. *J. Pure Appl. Algebra* 167 (2002), 259-267

[9] R. Mines, F. Richman and W. Ruitenburg. *A course in constructive algebra.* Springer-Verlag, 1988

[10] J. Querré. Sur le groupe de classes de diviseurs. *C. R. Acad. Sci. Paris*, 284 (1977), 397-399

[11] D.E. Rush. Seminormality. *Journal of Algebra*, 67, 377-384 (1980)

[12] R. Swan. On Seminormality. *Journal of Algebra*, 67, 210-229 (1980)

[13] C. Traverso. Seminormality and the Picard group. *Ann. Scuola Norm. Sup. Pisa*, 24 (1970), 585-595.