On seminormality

Thierry Coquand

February 6, 2006

We give an elementary and essentially self-contained proof[1] that a reduced ring R is seminormal if and only if the canonical map $\mathsf{Pic}\ R \to \mathsf{Pic}\ R[X]$ is an isomorphism, a theorem due to Swan [15], generalizing some previous results of Traverso [16]. By a simple modification of this argument, we obtain a constructive proof, and hence an algorithm [12], associated to a classical proof which is not so easy otherwise to access, since it requires a journey through [15, 16, 1] or, in the domain case, through [14, 13, 2, 6, 7].

We recall [15] that R is *seminormal* if and only if 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, as we will show in this note, the statement that the canonical map $\mathsf{Pic}\ R \to \mathsf{Pic}\ R[X]$ is an isomorphism can also be formulated in an elementary way. Swan's original definition includes that R is reduced, but, as noticed by Costa [4], reduceness 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 [9] surveys the work on commutative seminormal ring up to day.

1 General Lemmas

To any commutative ring R we can associate the group of projective modules of rank one, with tensor product as group operation. This is the *Picard group* $\mathsf{Pic}\ R$ of the ring R. If R is an integral domain then $\mathsf{Pic}\ R$ is isomorphic to the *class* group of R, group of invertible ideals in the field of fraction of R, modulo the principal ideals. So this group generalizes to an arbitrary ring the class group introduced originally by Kummer.

It is possible to give a more concrete description of this group. We can represent a finitely generated projective module over R by a $n \times n$ idempotent matrix, considering the submodule of R^n generated by the n column vectors of this matrix. If M and M' are two idempotent matrices over R, not necessarily of the same size, we write $M \simeq_R M'$ to express that M and M' represents isomorphic modules over R. If M represents a projective module of rank one, $M \simeq_R 1$ expresses that M represents a free module over R.

The first lemma gives a simple necessary and sufficient condition for a projection matrix of rank one to represent a free module.

Lemma 1.1 *Let M be a projection matrix of rank one over a ring A. We have $M \simeq_A 1$ if and only if there exist $x_i, y_j \in A$ such that $m_{ij} = x_i y_j$. If we write x the column vector (x_i) and y the row vector (y_j) this can be written as $M = xy$. Furthermore the column vector x and the row vector y are uniquely defined up to a unit by these conditions: if we have another column*

[1] The only non trivial result that we use is a basic theorem of Kronecker, proved in an elementary way in the references [3, 5, 10].

vector x' and row vector y' such that $M = x'y'$ then there exists a unit u of A such that $x = ux'$ and $y' = uy$.

Proof. Assume $M^2 = M$ and $M \simeq_A 1$. If I be the the module generated by the columns of M then I is a projective module of rank 1. Let x be a column vector in $A^{n\times 1}$ that generates the module I. There exists then a row vector y such that $xy = M$. Since $M^2 = M$ we have $(yx-1)M = 0$ and so $1 = yx$. If we have also $M = x'y'$ then similarly $y'x' = 1$. If we take $u = y'x$ and $v = yx'$ we have then $uv = 1$ and $x = ux'$, $y' = uy$. □

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. The next results are concerned with the following situation: we have a $n \times n$ matrix M over a ring $A[X]$, A reduced ring, such that $M(0) = P_n$ and we are interested in the case where $M \simeq_{A[X]} 1$.

Lemma 1.2 *If E is a reduced ring, and $f, g \in E[X]$ are such that $fg = 1$ then $f = f(0)$ and $g = g(0)$ in $E[X]$.*

Proof. We can assume $f(0) = g(0) = 1$. We write then $f = 1 + a_1X + \ldots + a_mX^m$ and $g = 1 + b_1X + \ldots + b_nX^n$. It is then direct that we have $b_n^k a_{m-k} = 0$ for $k = 0, \ldots, m$. In particular $b_n^m = 0$ and so $b_n = 0$ since E is reduced. We obtain similarly $b_{n-1} = 0, \ldots, b_1 = 0$. □

Corollary 1.3 *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 $M \simeq_{R[X]} 1$ then $f_i, g_j \in R[X]$.*

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, Lemma 1.2 shows $u = u(0) = 1$. □

Lemma 1.4 *Let R be a gcd domain [12] and $M = (m_{ij})$ is a projection matrix of rank one such that m_{11} is regular then $M \simeq_R 1$.*

Proof. For this, we take $f_1 \in R$ to be a gcd of the first line m_{1j}. We have then g_j such that $g_j f_1 = m_{1j}$. Since m_{11} is regular, so is f_1 and g_j is uniquely defined by this equations. Since M is of rank one we have $m_{11}m_{ij} = m_{i1}m_{1j}$ and so $g_1 m_{ij} = m_{i1}g_j$, so that g_1 divides all $m_{i1}g_j$ and so divides their gcd, which is m_{i1}. This determines uniquely f_i such that $g_1 f_i = m_{i1}$ and it follows from $m_{11}m_{ij} = m_{i1}m_{1j}$ that we have $m_{ij} = f_i g_j$. □

Corollary 1.5 *If K is a field, $R = K[X_1, \ldots, X_n]$ and M is a $n \times n$ projection matrix of rank one over R such that $M(0) = P_n$ then $M \simeq_R 1$.*

Proof. We know that R is a gcd domain [12] and we can apply Lemma 1.4. □

This result extends from the case of field to the case of reduced zero-dimensional (von Neumann regular) rings, using that such a ring is isomorphic to the ring of global sections of a sheaf of fields over a Stone space [8] (see also section 3.4.3 of [11]).

Corollary 1.6 *If C is a reduced zero-dimensional ring, $R = C[X_1, \ldots, X_n]$ and $M = (m_{ij})$ is a $n \times n$ projection matrix of rank one over R such that $M(0) = P_n$ then $M \simeq_R 1$.*

Proof. Using Corollary 1.5 we can find a system of orthogonal idempotents p_k and $f_i^k, g_j^k \in C[X_1, \ldots, X_n]$ such that $p_k m_{ij} = p_k f_i^k g_j^k$ in $C[X_1, \ldots, X_n]$ and $\Sigma p_k = 1$. We can then take $f_i = \Sigma p_k f_i^k$ and $g_j = \Sigma p_k g_j^k$, and we have $m_{ij} = f_i g_j$ in $C[X_1, \ldots, X_n]$. □

Lemma 1.7 *Let $M = (m_{ij})$ be a $n \times n$ projection matrix of rank one over $A[X]$, A reduced ring, such that $M(0) = P_n$ and such that, for all $a \in A$, if $M \simeq_{A[1/a][X]} 1$ then $a = 0$ in A. We have $1 = 0$ in A.*

Proof. If A is not trivial, let $\mathfrak{p}$ be a minimal prime of A and S its complement in A. Then A_S is a field and so, by Corollary 1.5, $M \simeq_{A_S[X]} 1$: we can find $f_i, g_j \in A_S[X]$ such that $m_{ij} = f_i g_j$ in $A_S[X]$. There is then $s \in S$ such that $f_i, g_j \in A[1/s][X]$ and $m_{ij} = f_i g_j$ in $A[1/s][X]$, so that $M \simeq_{A[1/s][X]} 1$. This implies $s = 0$ which contradicts $s \in S = A - \mathfrak{p}$. □

The formulation of the previous lemma may seem surprising. Another, classically equivalent, formulation would be: if A is nontrivial reduced ring then there exists a non zero element $a \in A$ such that M represents a free module over $A[1/a][X]$. We give a constructive proof of Lemma 1.7 in Appendix 2.

Lemma 1.8 *If A is a reduced ring then A has a reduced zero-dimensional (von Neumann regular) extension.*

Proof. There are different ways of building such extension. For instance, one may first show how to extend A by adding a quasi-inverse a^* to an element $a \in A$, for instance, by taking $A[a^*] = A[1/a] \times A/\sqrt{<a>}$. One then take the inductive limits of such extensions.

An alternative construction of $A[a^*]$ is to take $A[a^*] = A[1/a] \times A/<a>^{\perp\perp}$ where $I^\perp$ denotes the annihilator ideal of I. □

If A is an integral domain, we can take the fraction field of A. (This is indeed what we obtain with the second construction.)

Lemma 1.9 *Let M be a $n \times n$ projection matrix of rank one over $A[X]$, A reduced ring, such that $M(0) = P_n$. There exists a reduced extension C of A such that $M \simeq_{C[X]} 1$.*

Proof. This follows from Lemma 1.8 and Corollary 1.6. □

2 Picard groups for seminormal rings

Lemma 2.1 *Let A be seminormal and C be a reduced extension of A. The conductor*

$$I \;=\; \{r \in A \mid rC \subseteq A\}$$

of C in A is an ideal radical of A and C

Proof. 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 $u^2 c^2 \in A$ and $u^3 c^3 = u^2 u c^3 \in A$ since $u^2 \in I$. Hence as previously, we conclude $uc \in A$. This shows $u \in I$. □

Lemma 2.2 *(key lemma) Let A be seminormal and $M = (m_{ij})$ be a $n \times n$ projection matrix of rank one 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 $f_i, g_i \in C[X]$, $1 \le i \le n$ 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 by Lemma 2.1.

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 $1 \in I$. For this we show that $1 = 0$ in the ring A/I. This follows from Lemma 1.7. Indeed if M represents a free module over $(A/I)[1/a][X]$ then, since $(C/I)[1/a]$ is a reduced extension of $(A/I)[1/a]$, we can apply Corollary 1.3 and conclude that $f_i, g_j \in (A/I)[1/a][X]$ so that $a = 0$ in A/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 [3, 5, 10] 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.

Lemma 2.3 *If A is seminormal, and M is a $n \times n$ projection matrix of rank one of $A[X]$ such that $M(0) = P_n$ then $M \simeq_{A[X]} 1$.*

Proof. This follows from Lemmas 1.9 and 2.2. □

Theorem 2.4 *If A is seminormal 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 one over $A[X]$ such that $M(0) \simeq_A 1$, then $M \simeq_{A[X]} 1$. By Lemma 1.1 we have a column vector x in $A^{n\times 1}$ and a row vector y in $A^{1\times n}$ such that $xy = M(0)$ 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

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

In this way we reduce further the problem to the case where $M(0) = P_{n+1}$, and we can then apply Lemma 2.3. □

We notice also that the previous reasoning applies directly for $A[X_1, \dots, X_n]$. Indeed, Kronecker's theorem holds for polynomials in several variables as well: if $P_1 P_2 = Q \in A[X_1, \dots, X_n]$ then, any product $u_1 u_2$ where u_i is a coefficient of P_i, is integral over the coefficients of Q [5].

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

Theorem 2.5 *If A is seminormal then the canonical map* $\mathsf{Pic}\ A \rightarrow \mathsf{Pic}\ A[X_1, \ldots, X_n]$ *is an isomorphism.*

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

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 $a_1, \ldots, a_n \in C$ such that $a_{i+1}^2, a_{i+1}^3 \in A[a_1, \ldots, a_i]$ and $C = A[a_1, \ldots, a_n]$. 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 Lemma 2.2 to conclude that $B = C$. Since our argument is constructive, it can be seen as an algorithm which computes such $a_1, \ldots, a_n \in C$ 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 $\mathsf{Pic}\ A \rightarrow \mathsf{Pic}\ A[X]$ 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 one in $A[X]$ such that $M(0) = P_2$.

If the canonical map $\mathsf{Pic}\ A \rightarrow \mathsf{Pic}\ A[X]$ is an isomorphism, this matrix should present a free module over $A[X]$. By Corollary 1.3 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 Theorem 2.5. □

Appendix 2: A constructive proof of Lemma 1.7

Using Corollary 1.8 that we can find a reduced zero-dimensional extension C of A. By Corollary 1.6 we have $M \simeq_{C[X]} 1$. We can assume that $C = A[a_1^*, \ldots, a_n^*]$ is generated by finitely many quasi-inverse $a_1^*, \ldots, a_n^*$ of elements $a_1, \ldots, a_n$ of A. We write $e_i = a_i a_i^*$ so that e_i is idempotent and $a_i e_i = a_i,\ a_i^* e_i = a_i^*$. To simplify we take $n = 2$ from now on, but our argument is general. We can decompose C in 2^n rings

$$C = e_1 e_2 C + e_1(1 - e_2)C + (1 - e_1)e_2 C + (1 - e_1)(1 - e_2)C$$

with

$$e_1 e_2 C = e_1 e_2 A[a_1^*, a_2^*] \simeq A[1/a_1, 1/a_2] \simeq A[1/a_1 a_2]$$

Indeed, since $x e_i = 0$ if and only if $x a_i = 0$, we have for $u \in A[1/a_1 a_2]$, $u e_1 e_2 = 0$ if and only if $u = 0$ in $A[1/a_1 a_2]$, and so, $e_1 e_2 C$ is isomorphic to $A[1/a_1 a_2]$.

Since M represents a free module over $C[X]$ it represents also a free module over $e_1e_2C[X]$ and so over $A[1/a_1a_2][X]$. We deduce $a_1a_2 = 0$ in A. It follows that we have $e_1e_2 = 0$ and we can simplify the decomposition of C:

$$C = e_1C + e_2C + (1 - e_1)(1 - e_2)C$$

Since e_1C is isomorphic to $A[1/a_1]$, we have $M \simeq_{A[1/a_1][X]} 1$. This implies $a_1 = 0$ in A. Similarly we have $a_2 = 0$ in A. It follows that $C = A$ and M represents a free module over $A[1/1][X]$ so that $1 = 0$ in A.

Appendix 3: Gilmer and Heitmann's counter-example

In the reference [6] the authors present an example of a reduced ring R which is equal to its own total quotient ring, but such that $\mathsf{Pic}\ R$ is *not* canonically isomorphic to $\mathsf{Pic}\ R[X]$. This example is the following. Let K be a field and let A be the K-algebra generated by $x^2, x^3, y_1, y_2, \ldots$ with the relations $x^2y_n = 0$ and $y_ny_m = 0$ for $n \neq m$. Each element in A can be written in a unique way $u = a + p(x) + t_1(y_1) + \ldots + t_n(y_n)$ with $a \in K$, and $p(0) = p'(0) = t_1(0) = \ldots = t_n(0) = 0$. If $v = b + q + s_1 + \ldots + s_n$ we have $uv = ab + bp + aq + pq + bt_1 + as_1 + t_1s_1 + \ldots + bt_n + as_n + t_ns_n$ in A. In particular $u^2 = a^2 + 2ap + p^2 + 2at_1 + t_1^2 + \ldots + 2at_n + t_n^2$ and so $u^2 = 0$ implies $u = 0$. This shows that A is reduced. If $a = 0$ we have $uy_m = 0$ for m big enough and so u is not regular. On the other hand if $a \neq 0$ then u is regular. We let S be the monoid of regular elements u, i.e. elements such that $a \neq 0$, and $R = A_S$. The ring R is reduced since A is. By construction, R is equal to its own total quotient ring. On the other hand, we cannot have $u^2 = x^2v^2, u^3 = x^3v^3$ in A with $v \in S$ so the equations $r^2 = x^2, r^3 = x^3$ have no solution $r \in R$, though $(x^2)^3 = (x^3)^2$, and so R is not seminormal.

We think that this example shows that what should be used instead of the total quotient ring is a von Neumann regular extension of the ring, as in Lemma 1.8.

Acknowledgement

Henri Lombardi suggested the problem of finding an elementary proof of Swan's theorem. Thanks also to him, to Tsit-Yuen Lam and to Peter Schuster for discussions on this topic and to Claude Quitté for many improvements, in particular the identities used in Theorem 2.4, 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] J.W. Brewer and D.L. Costa. Seminormality and projective modules over polynomial rings. *J. Algebra 58*, (1979), no. 1, 208–216.

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

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

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

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

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

[8] P. Johnstone. *Stone Spaces.* Cambridge studies in advanced mathematics 3, 1982.

[9] T-Y. Lam. *Serre's Problem on Projective Module.* to appear, 2006

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

[11] H. Lombardi and C. Quitté. *Algèbre Commutative. Modules projectifs de type fini.* to appear, 2005

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

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

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

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

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